



Manager Guide

 **MSactivator**



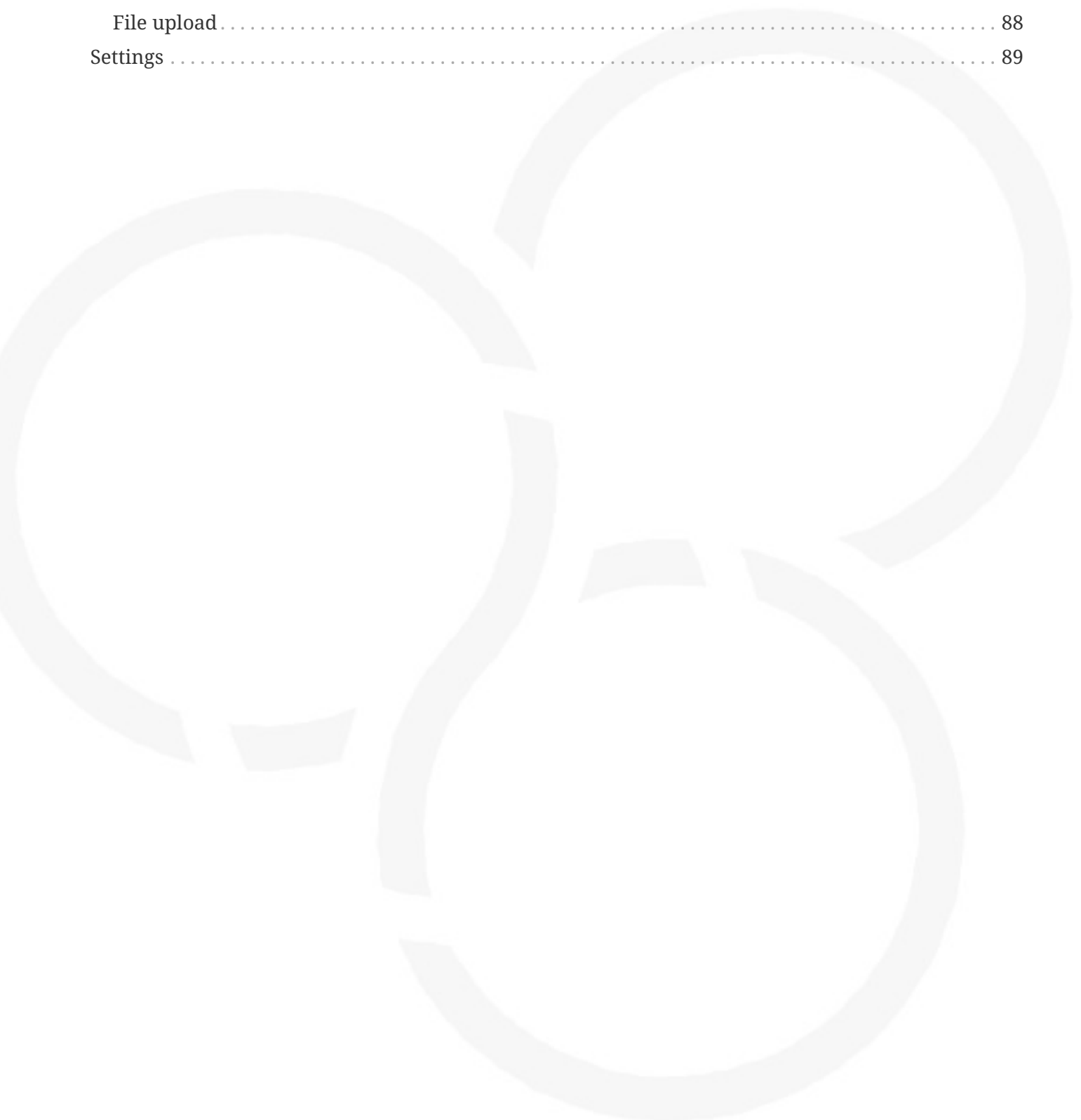
Table of Contents

Key Concepts	2
Overview	2
Understanding the Different Personas	2
Manager	2
Developer	3
A multi-layered architecture	4
Roles and Tenants	5
Infrastructure	6
Managed entities	6
Microservices	6
Deployment settings	6
Monitoring profiles	6
Automation	6
Workflow	7
BPM	7
The UI	7
Terminology	7
Manager and Developer Portal	9
Overview	9
Manager dashboard	9
Status graphs	10
Filters, sorts and search	11
Navigation	11
Customization	13
Infrastructure	14
Managed entities	14
Microservice	15
Deployment settings	15
Automation	15
Workflows	15
BPM	17
Developer Dashboard	17
Workflow library	18
Microservices library	18
Adapters library	18
Integration with Git	18
Tenants and Users	19
Overview	19

Initial connection	19
Overview	19
Tenancy management	20
Tenant	20
Subtenant	21
User management	21
Privileged administrator (ncroot)	22
Administrator	22
Privileged manager and manager	22
Roles and rights management : permission profiles	22
Audit record	23
Managed Entities	25
Overview	25
Create, update and activate a managed entity	26
Managed entity fields	27
Managed entity activation	28
Overview screen	29
Asset information	29
Monitoring information	29
Logs	31
Configuration variables	31
Configuration	33
Synchronization with the managed entity	33
Configuration of the managed entity	33
History	34
Assurance	36
Monitoring profiles	36
Overview	36
Create or edit a monitoring profile	36
SNMP trap monitoring	41
SNMP v2/v3	41
SNMP trap translation	44
Log analytics	50
Overview	50
Search logs	51
Dashboard	52
Deploy an existing dashboard for a subtenant	52
Alarm	53
Overview	53
Manage alarm rules	54
Create or edit an alarm	54

Alarm acknowledgement	55
Testing	55
Email alerting: SMTP configuration	56
Alarm severity tuning	57
Microservices	59
Overview	59
Select microservices	60
Microservice console	61
Calling the Microservice functions	61
Bulk Operations	62
Microservice design	65
Deployment Settings	66
How to use deployment	66
Create, update, delete	66
Access Control	67
Topology	68
Topology view	68
Managed Entity categories	68
Workflow and BPM launcher	69
Topology types	69
SNMP	69
VLAN	71
How it works	72
Create you custom topology	73
Step 1: prepare your development environment	73
Step 2: add a new topology type to the workflow	74
Step 3: add a new PHP script to implement the new topology	75
Step 4: implementation and tests	76
Workflows	78
Overview	78
Workflow selection	78
Workflow use	79
Create a workflow instance and run processes	79
Get information about workflow instance status	82
Access rights	83
Workflow design	83
Workflows: utilities	84
Managed entities configuration variables	84
BPM	85
Overview	85
Execution management	85

Tracking	85
Pause and resume	85
Terminating	86
Scheduling	86
Repository	88
File upload	88
Settings	89



The Installation and Configuration Guide will show you how to install, configure and activate the MSactivator™.

If you want to get started quickly, you can check the [quickstart](#) guide.

Key Concepts

Overview

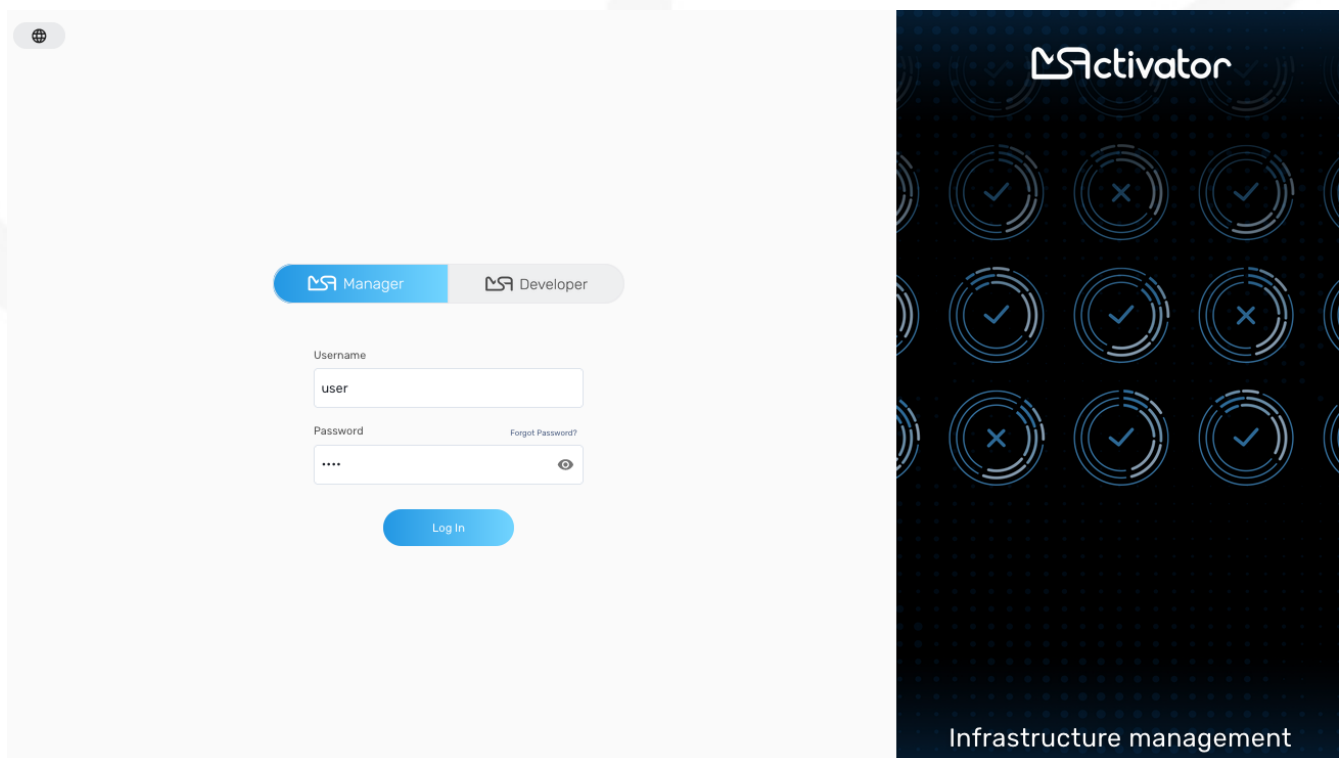
MSactivator™ is the leading Integrated Automation Platform (IAP) engineered by UBiqube for the continuous design of any IT infrastructure automation process. It is composed of Infrastructure and Automation Modules.

The Integration Module is used by infrastructure engineers to onboard / integrate the wide spectrum of related vendors and systems involved in any given IT solution, i.e. cloud technologies (public/private, containers, etc.), networks systems (virtual and physical, optical, 5G, etc.), security systems, IoT systems and devices, etc..

The Automation Module provides the IT automation developer with a unified development environment for process design without concern for the underlying infrastructure technologies / vendors used, enabling an evergreen design.

Understanding the Different Personas

On the MSactivator™ login screen, there are two different types of logins selectable via a toggle switch Manager/Developer



Manager

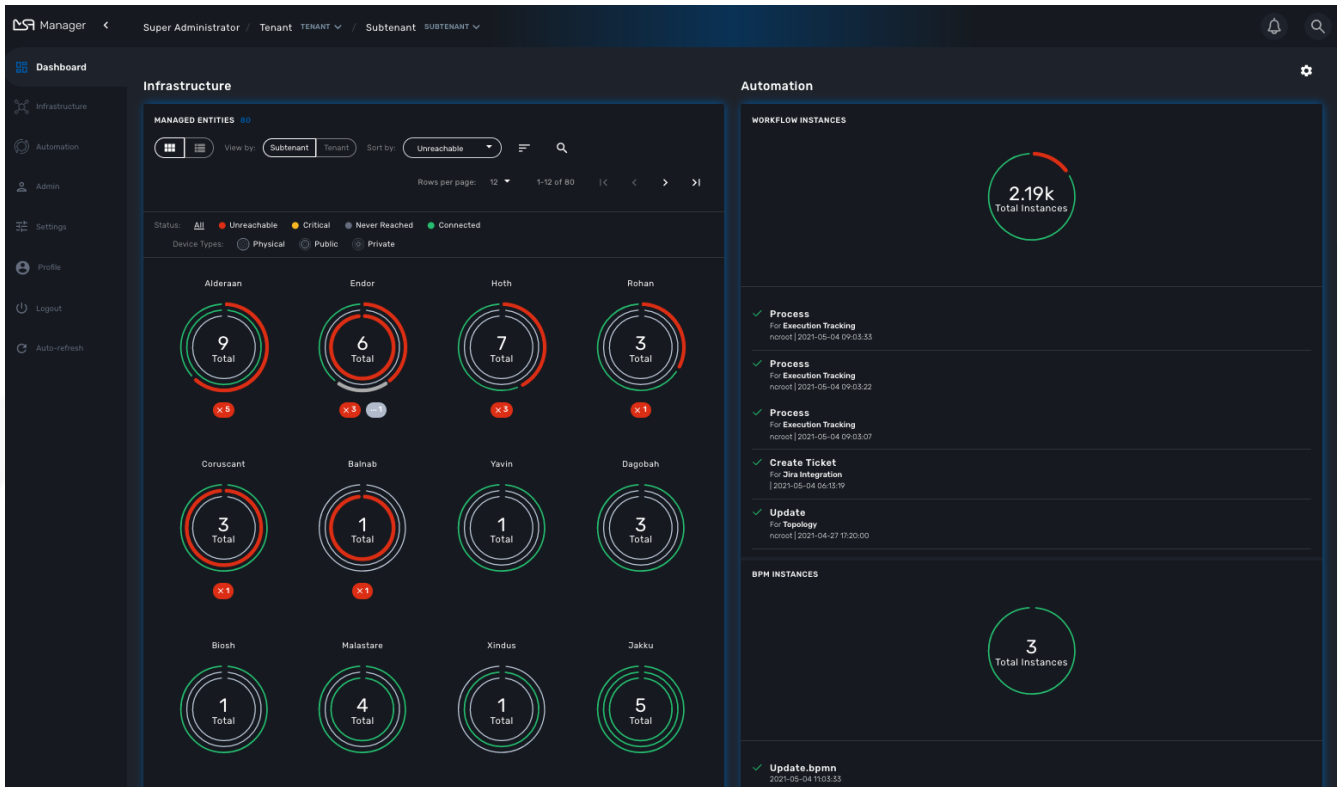
This will give you access to the manager dashboard, that allows you to monitor and manage the entities configured in your MSactivator™ installation.

This dashboard represents the "Ops" part of the "DevOps" approach, see the GUI Overview for more

details.

Login as an manager, you can directly start monitoring and managing your system.

Manager dashboard and the status of the infrastructure



Developer

Access to the developer dashboard, to design business processes, write workflows, or use visual workflows and develop microservices in the MSactivator™.

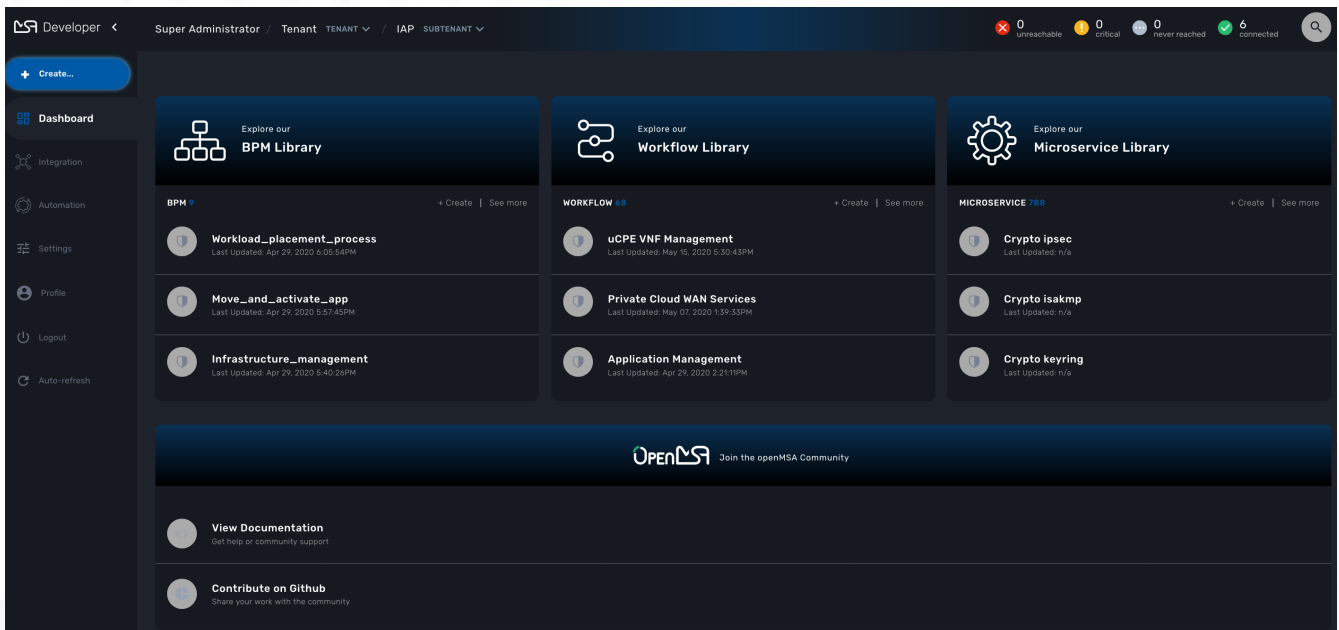
Configure your remote Git repositories to do code versioning management, share you code with your team, publish your code and contribute to the community.

This dashboard represents the "Dev" part of the "DevOps" approach, see the GUI Overview for more details.

Login as a developer, you can easily access and work on the design of your automation processes.

The swimlanes are matching the 3 layers of integration and automation: BPM, Workflows and Microservices

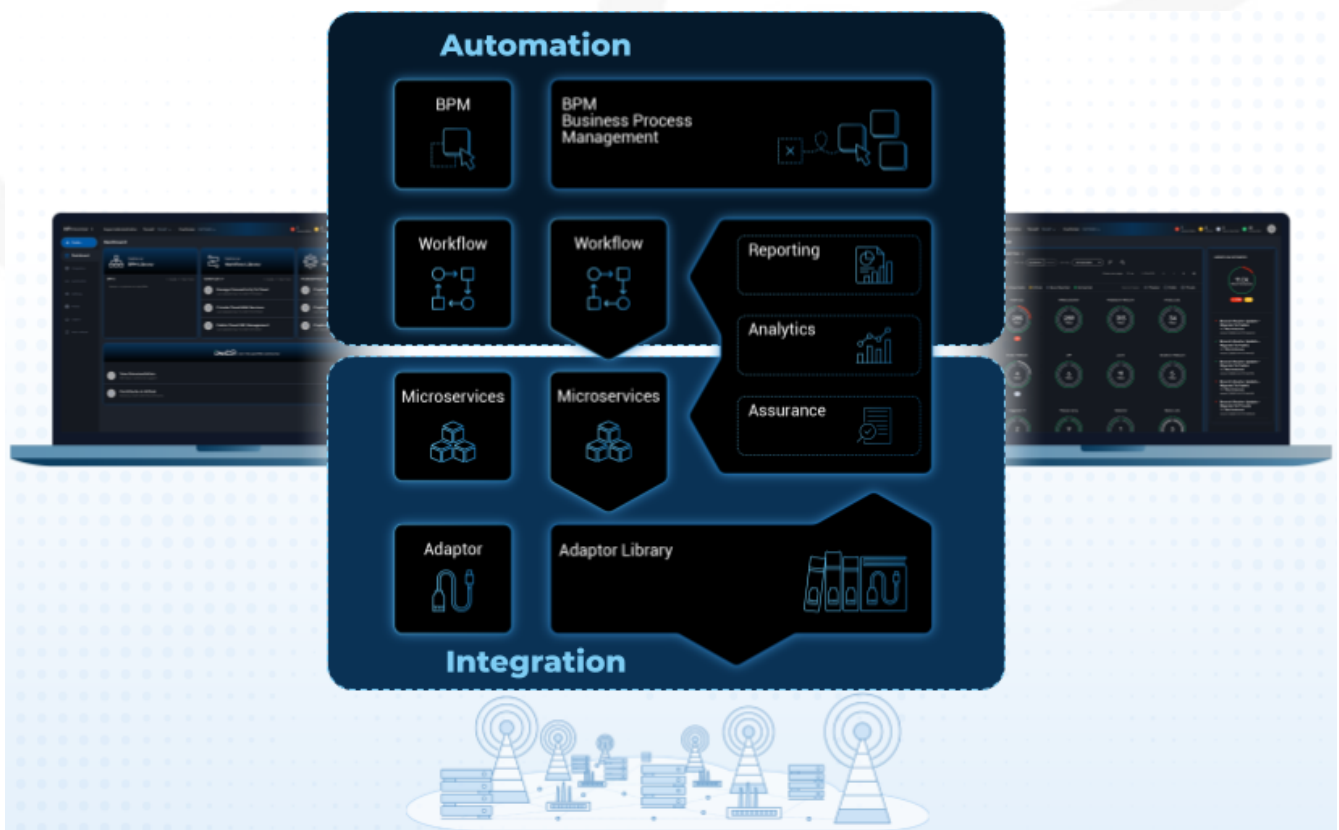
Developer dashboard and the swimlanes



The username and password you use to access either dashboard is the same, the selection on the login screen simply determines which dashboard you can see after logging in.

A multi-layered architecture

MSactivator™ architecture overview



The MSactivator™ architecture is composed of 2 main layers, the Automation layer and the Integration layer.

Each layer is composed of 2 sub-layers:

- The BPM and Workflows
- The Microservices and Adapters

Each of the layers are themselves split into 2 functional blocks: the Development and the Management.

For instance, the microservices layer is composed of an extendable library of microservices, ready to use and the development environment to update the microservices in order to extend the library.

The Reporting, Analytics and Assurance layers span vertically across the Automation and Integration layer as they are fully integrated with them.

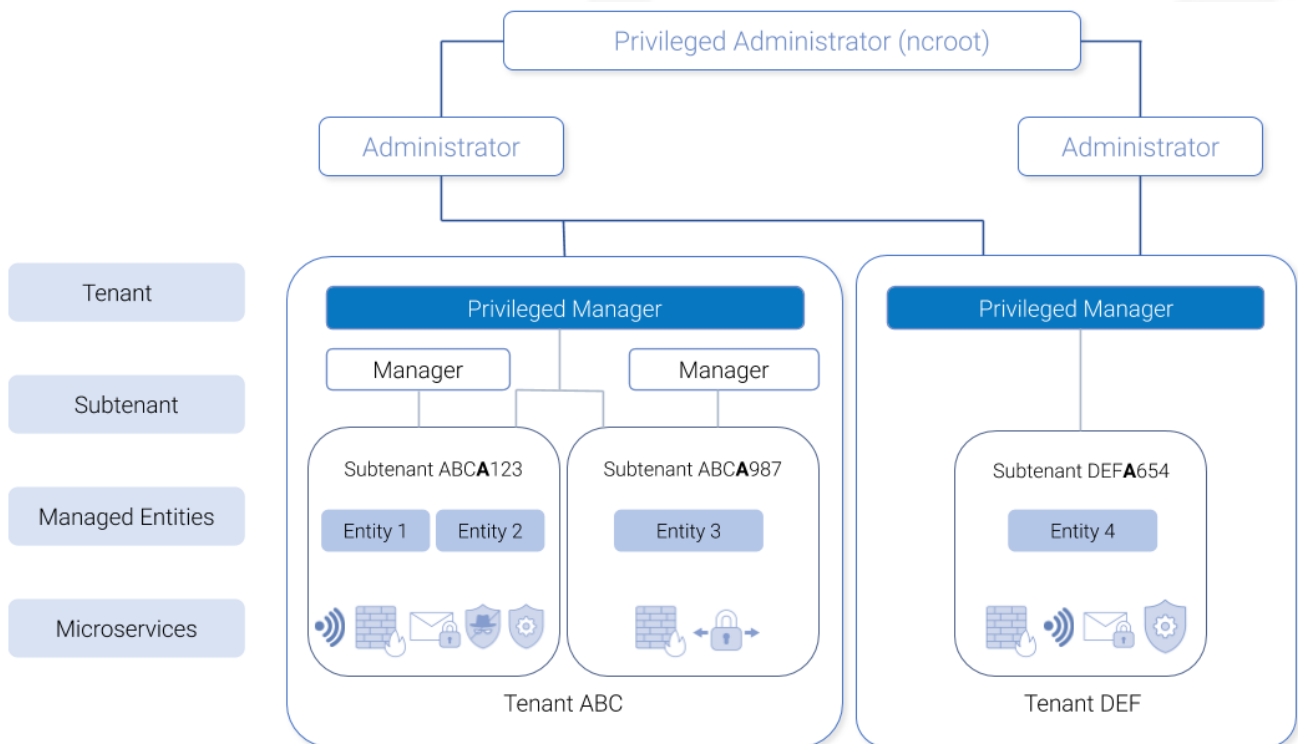
Roles and Tenants

The MSactivator™ has 2 levels of tenancy: tenant and subtenant.

These 2 levels will let you organize your managed entities based on your need will ensuring that access restriction based on the user role is fully respected.

4 user roles are available to make sure that you can assign the access and managing roles to your users based on their actual roles in your company.

Tenancy and user roles



Tenants

A tenant contains a set of subtenants. The subtenants contain the managed entities and the deployment settings.

Roles

- ncroot, the privileged admin has a global read/write access to the system.

- an admin as read/write access to a set of selected tenant.
- a privileged manager has read/write access to a tenant and his scope cannot go out of his tenant.
- a manager has a read-only access to a set of subtenants.

Infrastructure

The term "Infrastructure" relates to managed entities, microservices and deployment settings.

Managed entities

The term "Managed Entity" encompasses manageable entities such as network elements (routers, switches, load balancer, etc.), security elements such as firewalls, UTM, etc. but also virtual infrastructure and cloud management layers such as Openstack, AWS, VMWare or even container management platforms such as Rancher, K8,...

Microservices

Microservices can be used to manage a wide variety of services on numerous types of entities, such as network equipment, virtualization infrastructure managers, or even Linux servers.

Microservices is the abstraction layer between the specificities of the managed entities and the genericity required for a true multi-vendor management system.

Microservices will let you define your managed services in a fine-grained and modular manner and provide all the required functions to create, read, update, delete and import these services in a production environment.

The MSactivator™ configuration engine runs on PHP Smarty and allows some scripting to add logic to the generation of the configuration.

Deployment settings

Deployment settings are the logical entities that will bind together the configurations and the managed entities.

Monitoring profiles

Monitoring profiles are the logical entities that will let you define your KPI to monitor and bind these to the monitored entities.

Automation

MSactivator™ features two automation layers designed for different degrees of abstraction that ensure maximum flexibility.

Workflow

The workflow layer addresses domain-specific scenarios which can be highly technically scripted, appealing to DevOps and SecOps engineers.

BPM

The BPM layer offers a visual workflow editor to make MSactivator™ a strong SOAR contender for business process design which appeals to realities and is not enshrined in vendor-specific boundaries. Maximum security remediation policies can be applied as engineers creatively imagine a process applied to all domains involved (security, routing, switching, cloud hosting, etc.).

The UI

Vision: MSactivator™ is to enable a ‘DevOps-ready’ Integrated Automation Platform to enable the design of multi-vendor, multi-cloud solutions across the entire tech ecosystem (data center to WAN, edge computing and IoT: all wrapped with security).

Target users: SI engineers developing (DevOps) end-to-end solutions for their business customers, or end-users managing the lifecycle of their infrastructure or the services they are deploying (Telco, Cloud, MSSP, etc.).

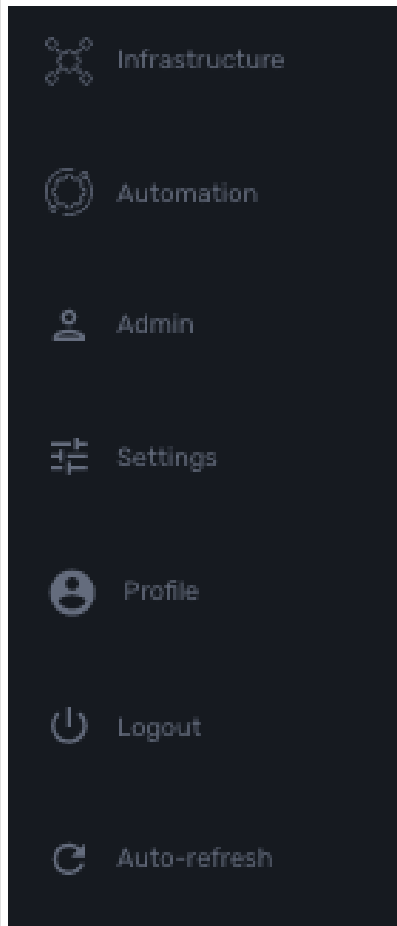
A UX reflecting the above wide variety of technical scenarios and user experiences was required and it became obvious that **this redesign was becoming a critical enabler of this strategy.**

1. The MSactivator™ UI provides two navigation environments to address both types of user:
 - **A developer-centric environment.**
 - **An end-user-centric environment.**
2. A UX structure in line with our modular MSactivator™ architecture (microservices, workflows, etc.) for consistency and greater concept adoption.
3. A universal taxonomy (naming and tagging) that would appeal to the entire ecosystem no matter the domain or the use case (data center, services, security, networking, wireless, wireline, IoT, etc.).
4. A modern UX where navigation user experience matters more than feature list.
5. A UX that connects to our community for greater intel and information-sharing among all of the MSactivator™ users and developers.
6. A UX that becomes an evergreen platform, which we continue to improve over time, making our ‘agility by design’ claim a tangible reality for our customers and partners.
7. A UX that becomes a strategic module of the MSactivator™ strategy as we head towards 5G, edge computing and IoT.

Terminology

The 10 terms that define the tree of the MSactivator™ navigation:

- 1. Infrastructure
 - 1. Managed Entities
 - 2. Microservices
 - 3. Deployment Settings
 - 4. Monitoring Profiles
- 2. Automation
 - 1. BPM
 - 2. Workflow
- 3. Alarms
 - 1. Logs
 - 2. Alarms



Manager and Developer Portal

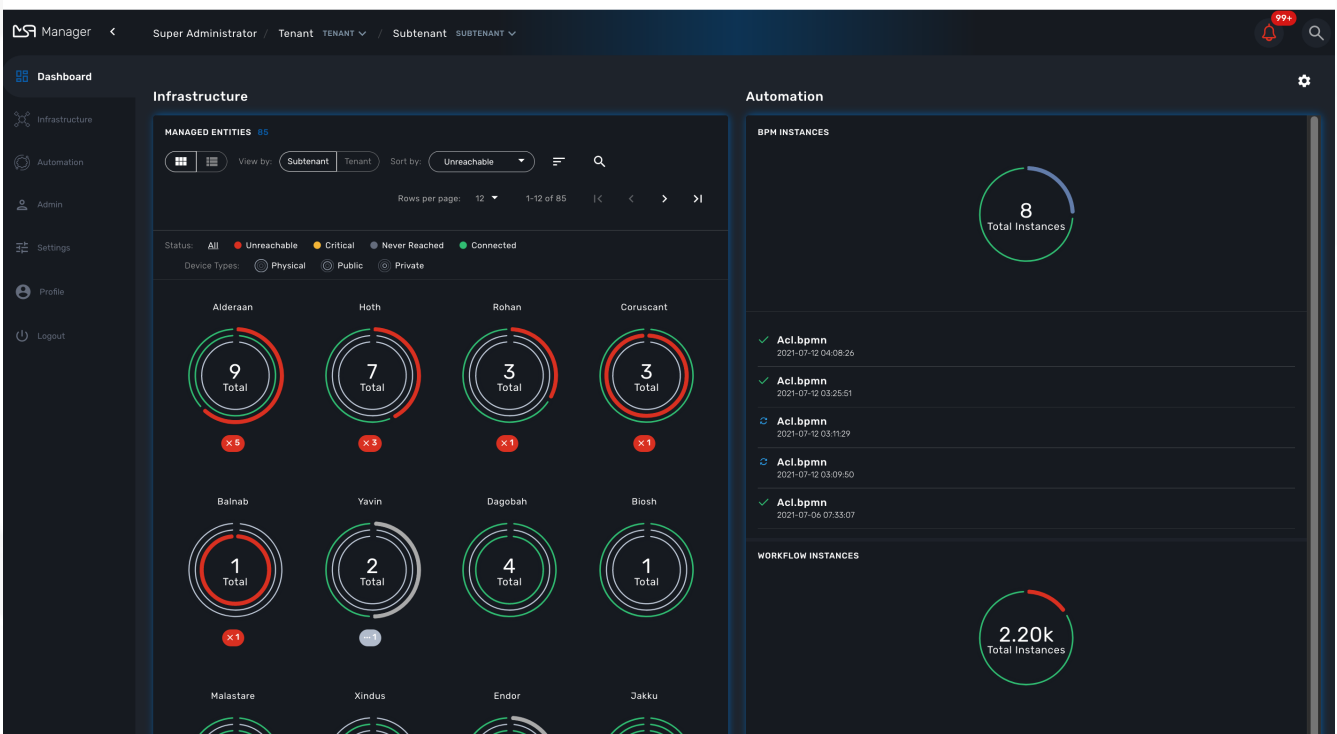
The MSactivator™ provides a web based UI split into 2 distinct spaces: a manager space and a developer space.

Overview

Each space is designed to match the specific requirements of manager and developer and at the same time provide a consistent user experience.

Manager dashboard

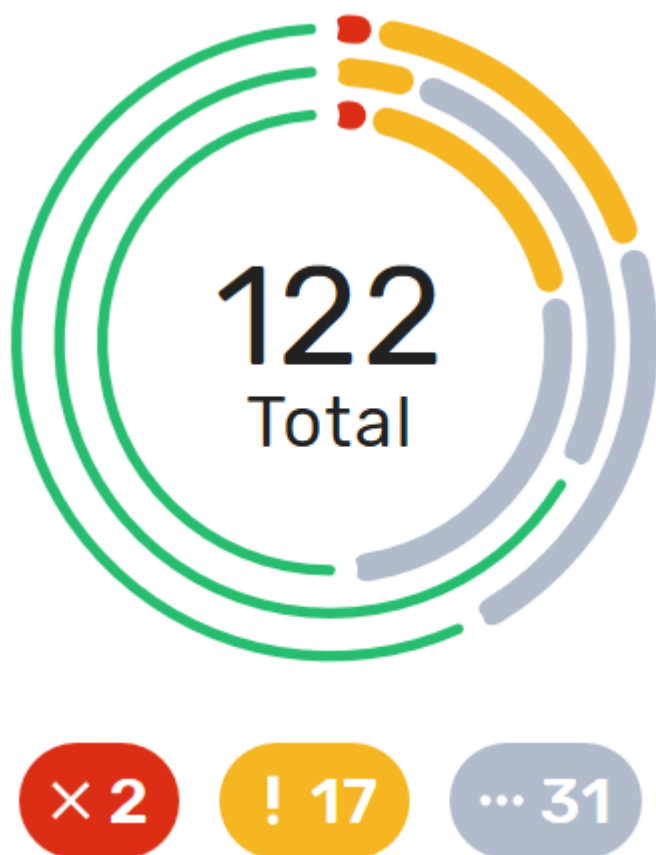
When you login as an administrator or a manager, the following dashboard is displayed



Dashboard	Display graphs to show the overall status of customer managed entities and workflow instance. Each of the graphs represents the status of the managed entities for the named customer.
Infrastructure	Shows the managed entities, microservices and deployment settings.
Automation	Shows the workflows and BPM that are in use and available for use in the system.
Alarms	For showing and searching the event and managing the alarms
Admin	Manage tenants and users.

Settings	For license activation and product version
Auto-refresh	Set an overall refresh period in seconds.

Status graphs



This graph is very convenient, as it represents a lot of data in a small area. Firstly, it is made up of three concentric circles: - The outer circle represents physical entities. - The middle circle represents public entities. - The inner circle represents private entities.

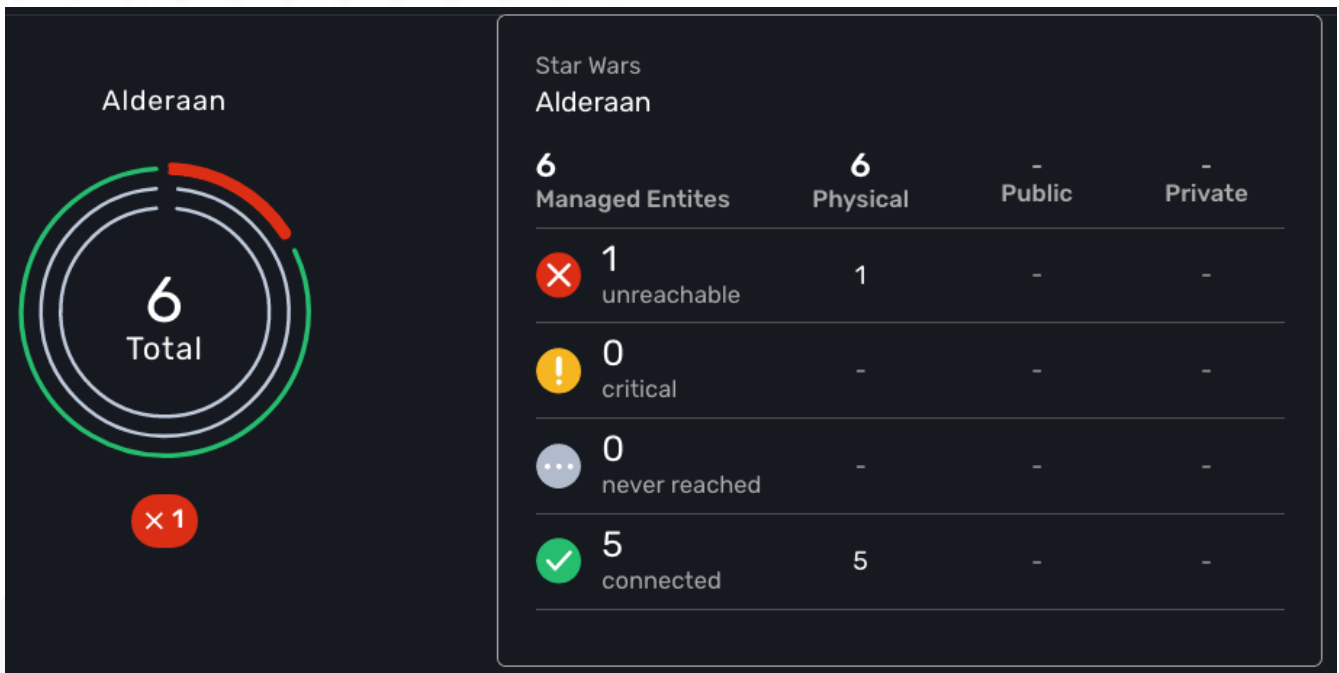
To further illustrate this, a legend is provided on the dashboard to explain each circle purpose:

Physical
 Public
 Private



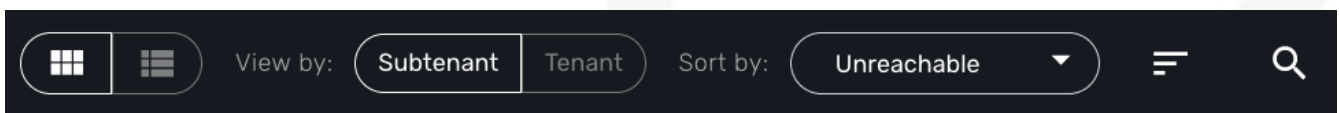
It is up to the MSactivator™ to decide the type of each entity when they are configuring that entity entry.

Finally, the number in the center of the circles is the total number of managed entities associated with that customer. If you click on any of those status graphs, you then see a pop-up table containing the same details but in a matrix like so:



Filters, sorts and search

On the administrator dashboard, there are a number of filter, sort, and search options available to help you organize and view your data.

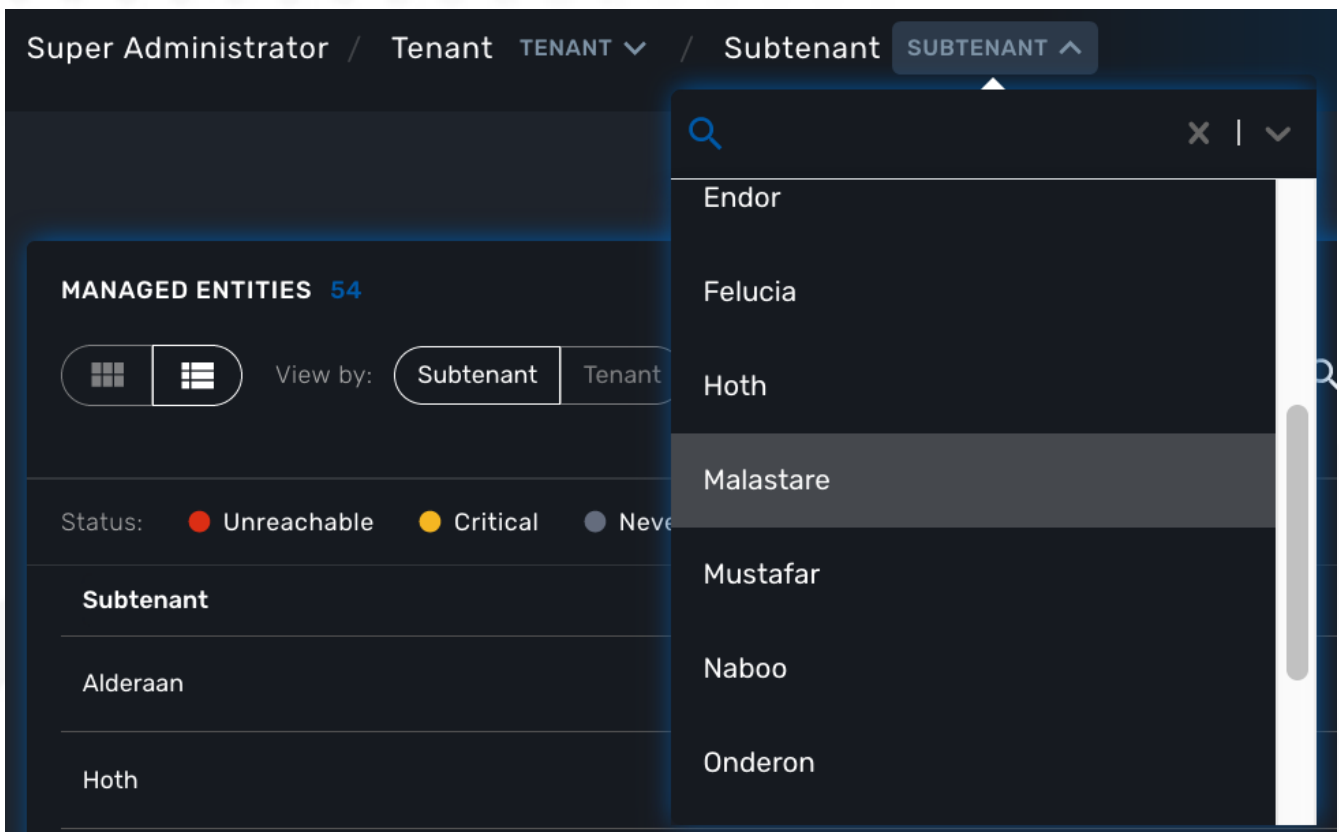


- The first icon allows you to switch between the status graphs and the compact list view of the customer entity status.
- The second icon enables you to switch between a tenant view and a customer view. When clicked, the status graphs will display the tenant-level status data, which aggregates all of the customers in each tenancy into a single graph per tenancy. We will discuss customer and tenancy navigation further in the Navigating via tenant and customer filters section.
- The third icon enables you to sort the status graph lists using the following options.
- Finally, the last icon is a magnifying glass that can be used to search for a specific tenant or customer within the list being displayed.

Navigation

How to select tenants and Subtenants

A central part of the navigation in MSactivator™ is understanding the tenant and customer that are selected. You can use the drop-downs on the top of the navigation to choose which tenant and customer you want to filter the lists of managed entities, microservices, and workflows by.



Note that the Role-Based Access Controls (RBAC) will affect what tenants and customers will be available to you. For example, if your account only has access to one tenant, you won't even have the option to select a different tenant.

Filters persistence

One very important topic to note is that your tenant and filter selection are persistent between screens.

Searching for subtenants and tenants

One useful feature in the tenant and customer selection drop-downs is the ability to search for an item by name. Auto-completion type ahead is also supported.

Clearing filters

To clear your selected tenant or customer filters, you simply click on the X button in the drop-down beside the name.

Searching for managed entities

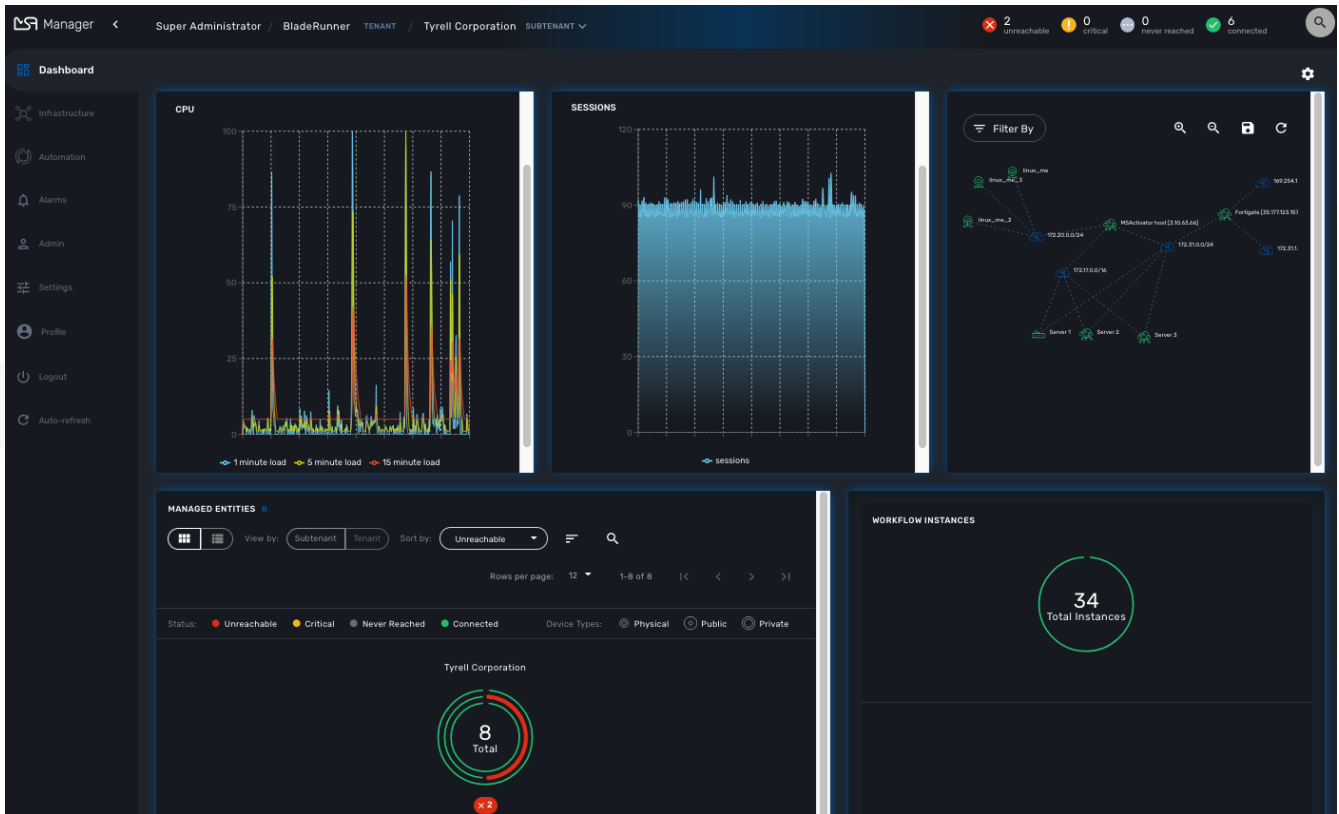
To perform a system-wide search for a managed entity by name, you should firstly click on the search icon in the top-right corner of the screen. Auto-completion type ahead is also supported.



One important point to remember about performing a managed entity search is that when you search for an entity, you are implicitly selecting the tenant that entity belongs to in the main filter drop-downs.

Customization

By default the manager dashboard displays the status of the managed entities and the workflow instance but this view can be customized to let you decide the important data that you want to display.



To customize your dashboard, click on the cog icon on the top right of the dashboard. This will open a screen where you can control the settings of your dashboard.

Use the opacity slider to see the result of your changes through the setting screen.

You can add as many component as you need, each component will be added one after the other, on the same line if there is enough space or on the line below.

The custom layout will be persisted and available for the user on any device he uses to connect (browser, tablet, phone,...).

Setting items

For each component of your custom dashboard there are a few settings available

Opacity

You can adjust the opacity to preview how your current settings look like.

Style

You can set two styles: Dashboard Panel and Drawer Button

- Dashboard Panel: provides the normal behavior as you can see the default settings.

- **Drawer Button:** name the button as you like, save, the button will appear next to the cog icon on the top-right corner of the dashboard.

Width and height

Use the sliders to control the size of the component

Component

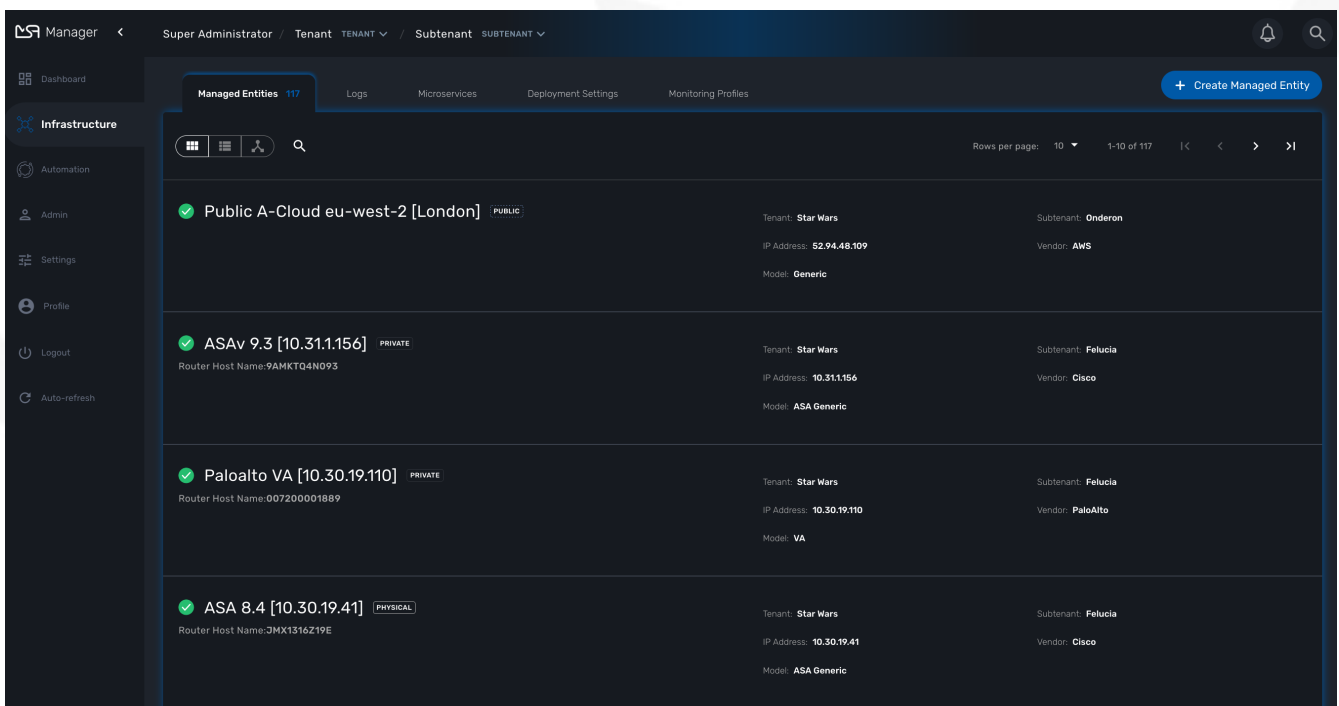
You can choose the components you want to show on the dashboard: topology view, monitoring graphs, workflow instance variables,...

The options may vary depending on the component. For instance the topology will only show if a subtenant is selected.

Infrastructure

Managed entities

To see the list of managed entities, click on the "Integration" link in the left menu



The screenshot shows the 'Managed Entities' page in the Manager interface. The page displays a list of managed entities with the following details:

Entity Name	Status	Tenant	Subtenant	IP Address	Vendor	Model
Public A-Cloud eu-west-2 [London]	PUBLIC	Star Wars	Onderon	52.94.48.109	AWS	Generic
ASAv 9.3 [10.31.1.156]	PRIVATE	Star Wars	Felucia	10.31.1.156	Cisco	ASA Generic
Paloalto VA [10.30.19.110]	PRIVATE	Star Wars	Felucia	10.30.19.110	PaloAlto	VA
ASA 8.4 [10.30.19.41]	PHYSICAL	Star Wars	Felucia	10.30.19.41	Cisco	ASA Generic

On that screen, you can use the list view toggle button to switch to a compacted view of the managed entities list. You can also adjust the amount of entities displayed on each page

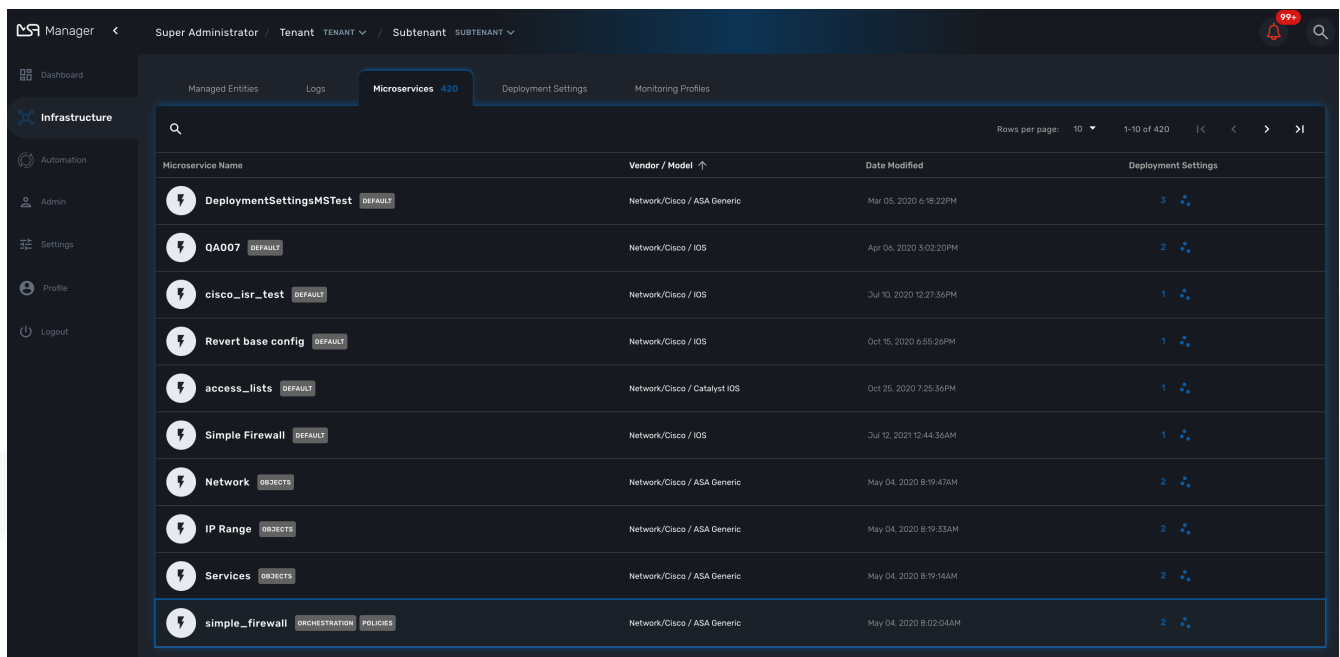
Finally, on this screen you can also perform a simple search of the managed entity you are looking for by its name.



See also - [this documentation](#) for a detailed documentation on managed entities

Microservice

To see the list of microservices, click on the link "Infrastructure" in the left menu.



The screenshot shows the NS Manager interface with the 'Microservices' tab selected. The table lists various microservices with their names, vendor/model, date modified, and deployment settings.

Microservice Name	Vendor / Model	Date Modified	Deployment Settings
DeploymentSettingsMSTest DEFAULT	Network/Cisco / ASA Generic	Mar 05, 2020 6:18:22PM	3
QA007 DEFAULT	Network/Cisco / IOS	Apr 06, 2020 3:02:20PM	2
cisco_isr_test DEFAULT	Network/Cisco / IOS	Jul 10, 2020 12:27:36PM	1
Revert base config DEFAULT	Network/Cisco / IOS	Oct 15, 2020 6:55:26PM	1
access_lists DEFAULT	Network/Cisco / Catalyst IOS	Oct 25, 2020 7:25:36PM	1
Simple Firewall DEFAULT	Network/Cisco / IOS	Jul 12, 2021 12:44:36AM	1
Network OBJECTS	Network/Cisco / ASA Generic	May 04, 2020 8:19:47AM	2
IP Range OBJECTS	Network/Cisco / ASA Generic	May 04, 2020 8:19:33AM	2
Services OBJECTS	Network/Cisco / ASA Generic	May 04, 2020 8:19:14AM	2
simple_firewall ORCHESTRATION POLICIES	Network/Cisco / ASA Generic	May 04, 2020 8:02:04AM	2

Deployment settings

You can view the list of deployment settings by clicking on the tab "Deployment Settings".

This screen will let you build your deployment settings by selecting microservice .

You will also be able to select the Managed Entities you wish to apply you configuration service on.

Automation

Workflows

To see the list of workflows select the "Automation" link in the left menu.

By default, if you are connected as a manager or an administrator you will see the list of Workflows that are associated to the subtenant you are managing

List of all the workflows available

Workflow Name	Version	Date Modified	Added to
Simple Firewall Manager	1 RELEASED	nrcroot, Jul 27, 2021 11:32:13AM	2 Subtenants
Execution Tracking	1 RELEASED	nrcroot, Jul 21, 2021 14:43:35PM	2 Subtenants
MSA Template Management	1 RELEASED	nrcroot, Jul 13, 2021 2:04:06PM	none
Multi-Firewall	1 RELEASED	nrcroot, Jul 13, 2021 2:04:06PM	none
Public Cloud VM Management	1 RELEASED	nrcroot, Jul 12, 2021 2:06:23AM	1 Subtenants
CreateME	1 RELEASED	nrcroot, Jun 30, 2021 7:29:21PM	2 Subtenants
General network service automation	1 RELEASED	nrcroot, Jun 15, 2021 9:57:59AM	1 Subtenants
Manage Device Variables	1 RELEASED	nrcroot, Jun 09, 2021 6:43:01AM	3 Subtenants
Use Microservice Reference To Select Interface	1 RELEASED	nrcroot, Jun 07, 2021 4:00:49PM	1 Subtenants

If you select a subtenant, the list will be filtered by the selected subtenant's workflows and you will see the process execution status of the workflow instances.

List of all the workflows available for a subtenant

Workflow Name	Date Modified	Instances
Manage Device Variables	Jun 09, 2021 6:43:01AM	1 Instances
Jira Integration	May 10, 2021 8:13:32PM	13 Instances
Ansible integration	Aug 13, 2020 9:47:04AM	1 Instances

To see the workflow instance for a subtenant, you can click on the Workflow name

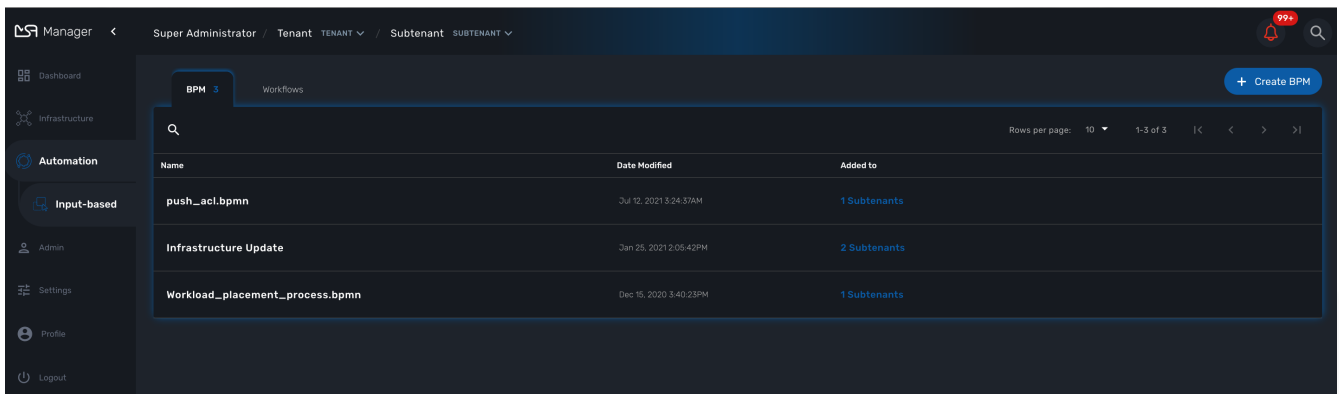
List of the workflows instances available for a subtenant

Instance ID	Device	Variable Name	Variable Value	Instance ID
ME: 1224	1224	variable_name	variable_value	Instance: 2415 / ME: UBH1224

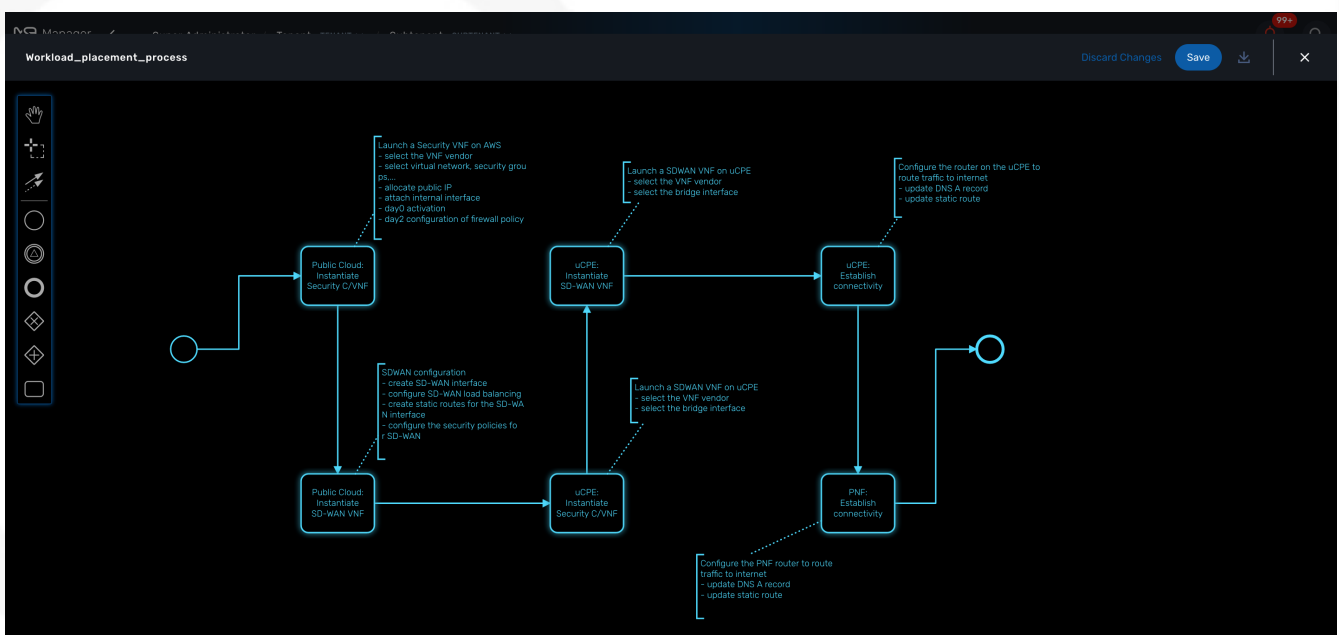
From this screen you can start using the existing instances or create a new instance for the current Workflow.

BPM

To see the list of Business Processes select the "Automation" link in the left menu

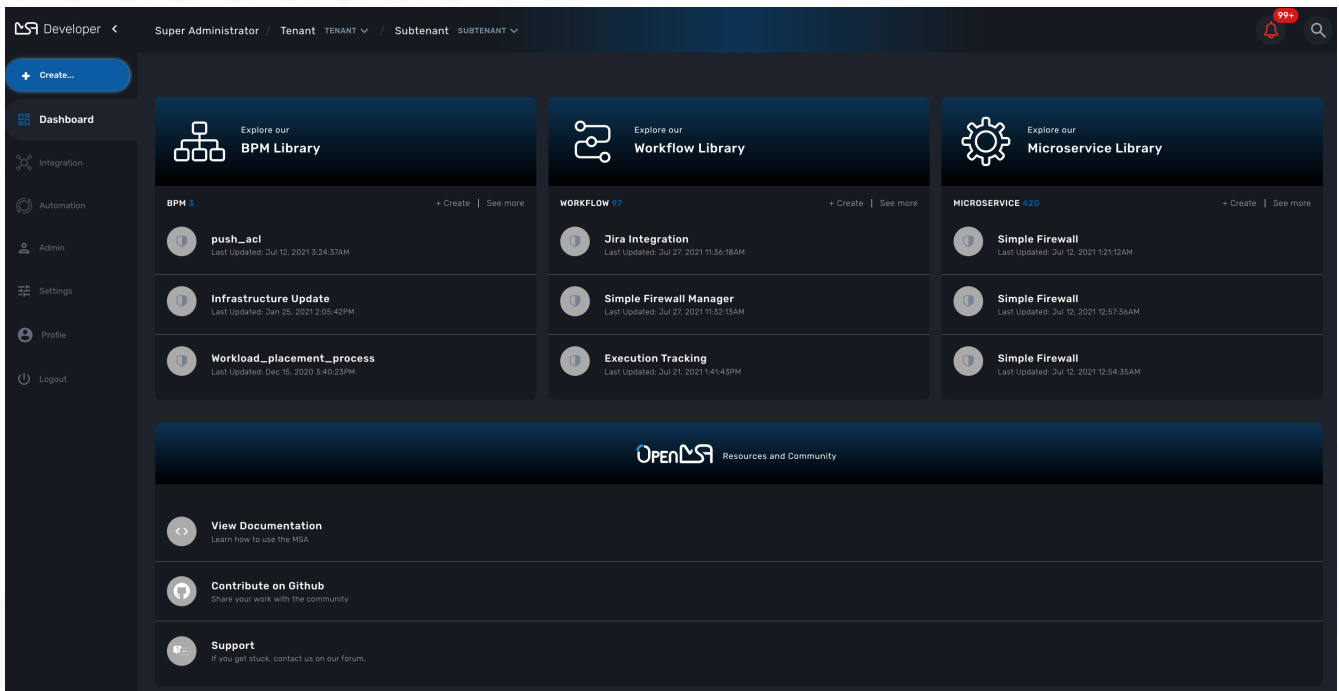


You can select a BPM by clicking on a name in the list and start working on your BPM.



Developer Dashboard

The developer dashboard in MSactivator™ is available when you chose to login as a developer. On this dashboard, one of the first things you will notice is the three vertical swimlanes:



The three swimlanes match the three main layers of the MSActivator™ framework.

Workflow library

This is where you can develop new workflows for your application. In MSActivator™, workflows can be written in either PHP or Python. A workflow is a series of tasks that you can develop to carry out any set of complex tasks that you wish to automate via our orchestration engine.

Microservices library

This is where you can develop new microservices for your application. In MSActivator™, a microservice is a way to wrap commands (Create/Read/Update/Delete/Import) into a service, that can be invoked with a workflow or even from outside MSActivator™ via our REST API.

The microservices are typically used for managing the configuration of managed entities in an abstracted, vendor-neutral way.

Adapters library

This is where you can develop new adaptors for your application, or import existing ones. The adaptors are used to connect to managed entities from MSActivator™, regardless of the network protocols supported by the entity in question. If an adaptor is not already available for your entity vendor in the library, a new one can be developed.

Integration with Git

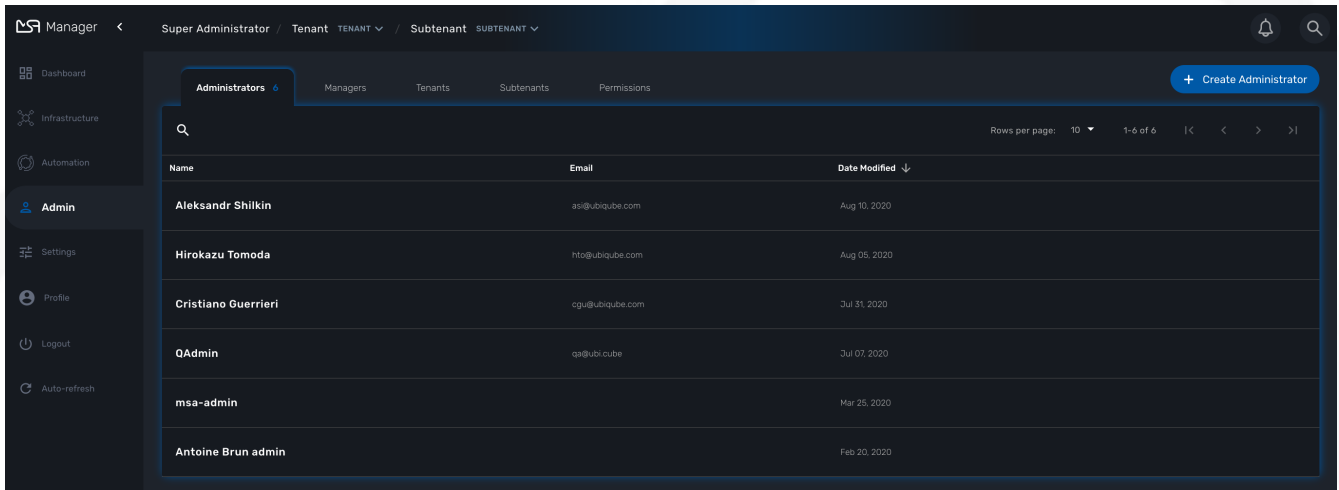
On the developer Dashboard, in the "Settings" menu, you can configure your remote repository where your library code is versioned.

Tenants and Users

The MSactivator™ platform provides a multi-roles and multi-tenancy hierarchy that should accommodate all your specific requirements.

Overview

Tenant and user management screens are available in the "Admin" section of the MSactivator™ UI.



Initial connection

The MSactivator™ comes with one pre-created super admin user: nroot (the equivalent of the root user on Linux systems). The default password for this user is "ubiquibe".

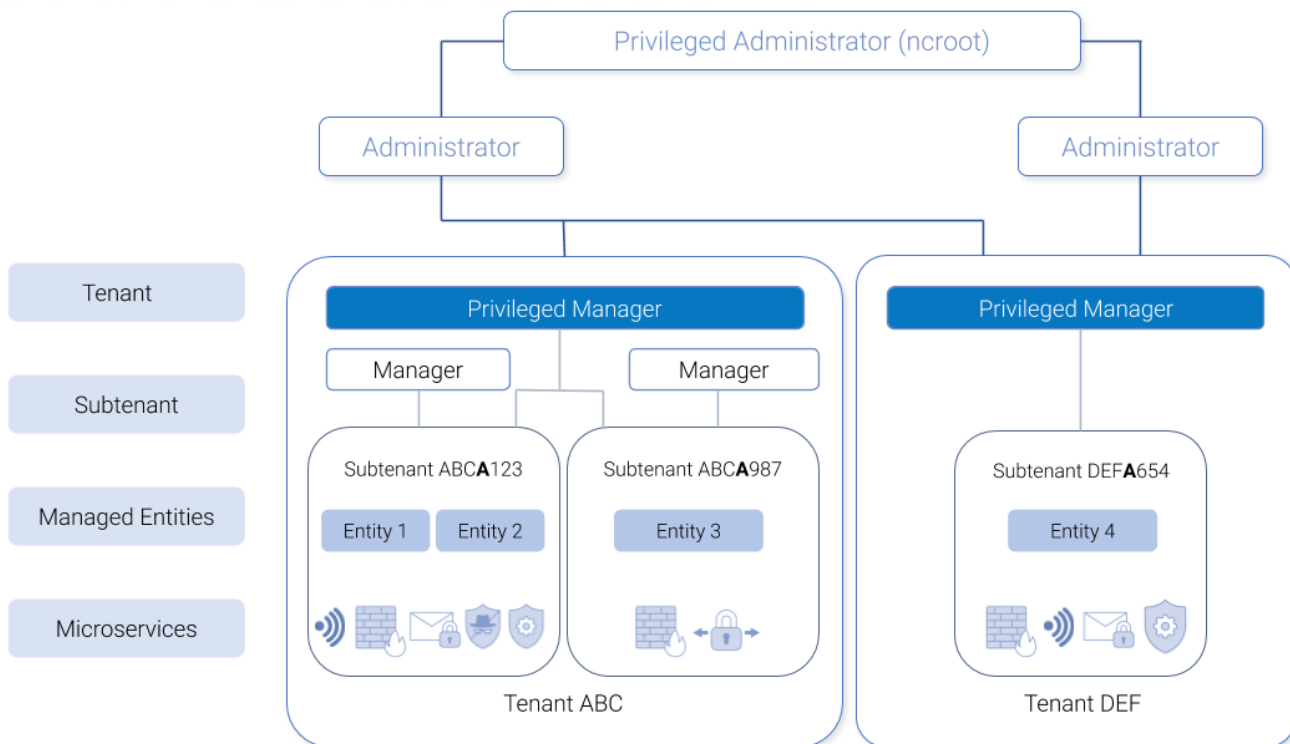
This default password should be changed, especially if the MSactivator™ is meant to be used in a production environment.

Overview

The MSactivator™ has 2 levels of tenancy: tenant and subtenant.

These 2 levels will let you organize your managed entities based on your need while ensuring that access restriction based on the user role is fully respected.

4 user roles are available to make sure that you can assign the access and managing roles to your users based on their actual roles in your company.



Tenancy management

The MSactivator™ is designed to provide multi-tenancy. A tenant is a virtual private space that can be managed as an isolated environment.

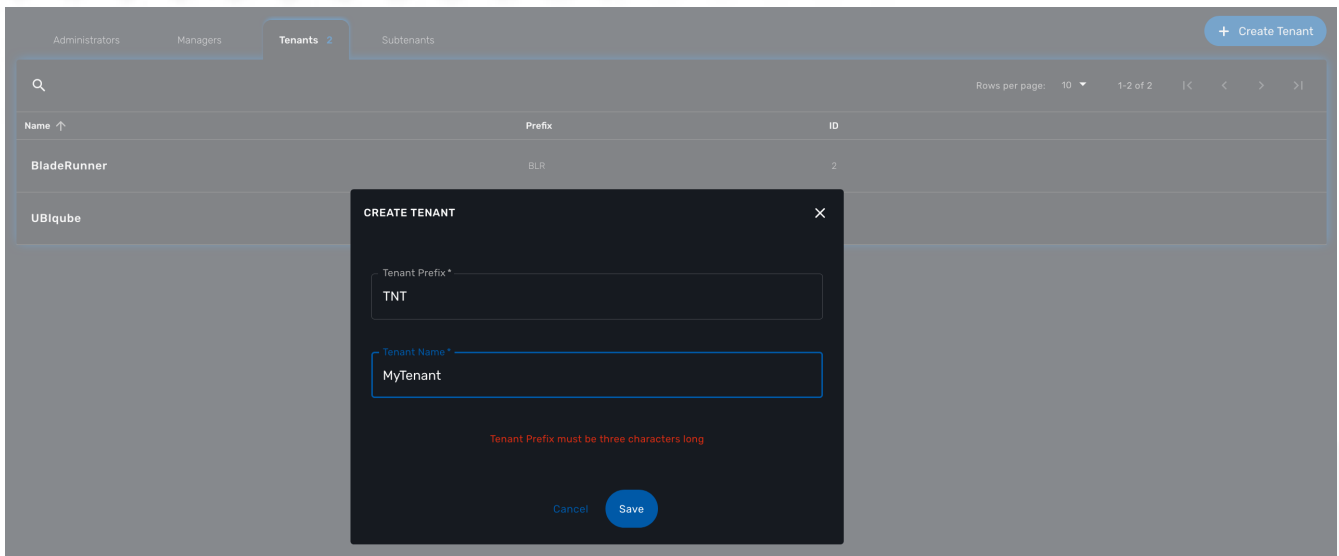
There are two levels of tenancy, tenant and subtenant, the latter being nested in the first one.

Tenancy management is provided on the UI in the "Admin" section on the left menu.

Tenant

Select the "Tenants" section in the "Admin" menu and click on the "+ Create Tenant" button to create a new tenant.

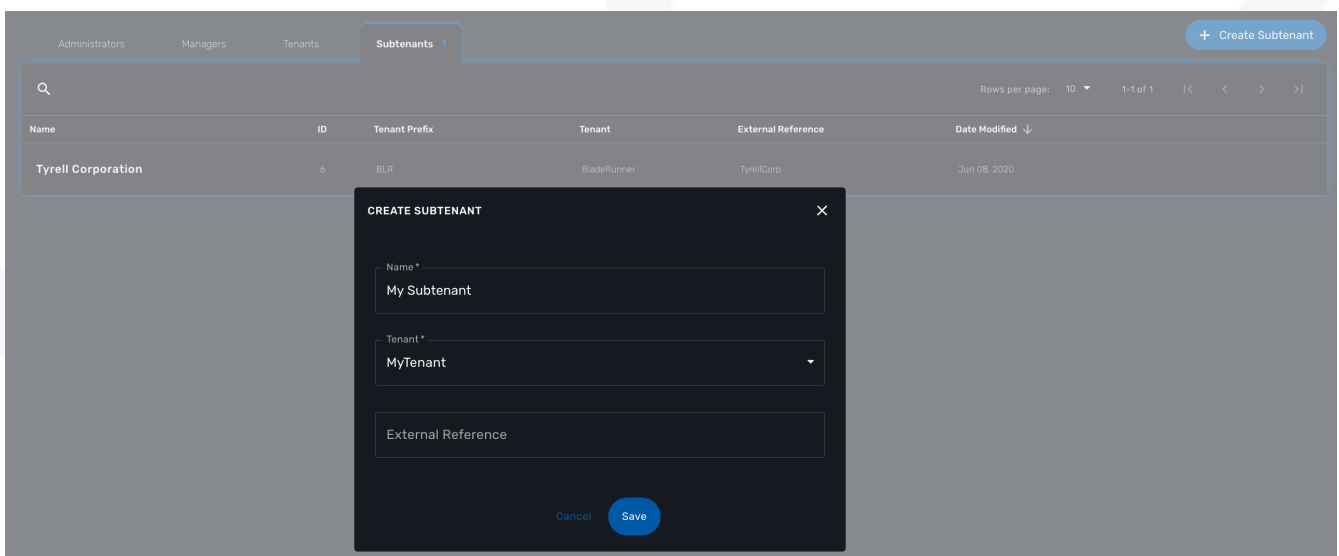
The "Tenant Prefix" is a three letters, unique identifier for the tenant. It will be combined with the subtenant or the managed database identifier to build a short, comprehensive, unique identifier that you can use to filter application logs when troubleshooting or when you need to communicate with the support team.



Subtenant

Select the "Subtenants" section in the "Admin" menu and click on the "+ Create Subtenant" button to create a new subtenant.

Carefully select the tenant where the subtenant will be created as moving a subtenant to another tenant is not possible without database update.



Save the customer form and navigate to the new subtenant tenant (click on the subtenant name in the customer list).

User management

Four types of users are available:

- nroot, the privileged administrator
- the administrator users
- the privileged manager users
- the manager users

Privileged administrator (ncroot)

ncroot is the only predefined user within the MSactivator™. It's the user with the highest level of privilege.

In addition to the action available to the other users with lower privileges, ncroot can create the tenants, upload and activate the MSactivator™ product licenses, create administrator users.

Administrator

Administrator users can only be managed by ncroot.

Administrators are associated with one or more tenants and have full access rights over these tenants.

A typical administrator job is to create the managers and privileged manager as well as the subtenant within its tenants.

Privileged manager and manager

Privileged managers are restricted to a single tenant.

Within their tenant, privileged managers have full access rights and can perform tasks such as subtenant management, device management, user and rights management.

Managers are restricted to a single tenant and, within this tenant, to a subset of subtenants.

By default, the managers have restricted, read-only access to the subtenant.

A manager may be used to provide self-care access to the MSactivator™ portal.

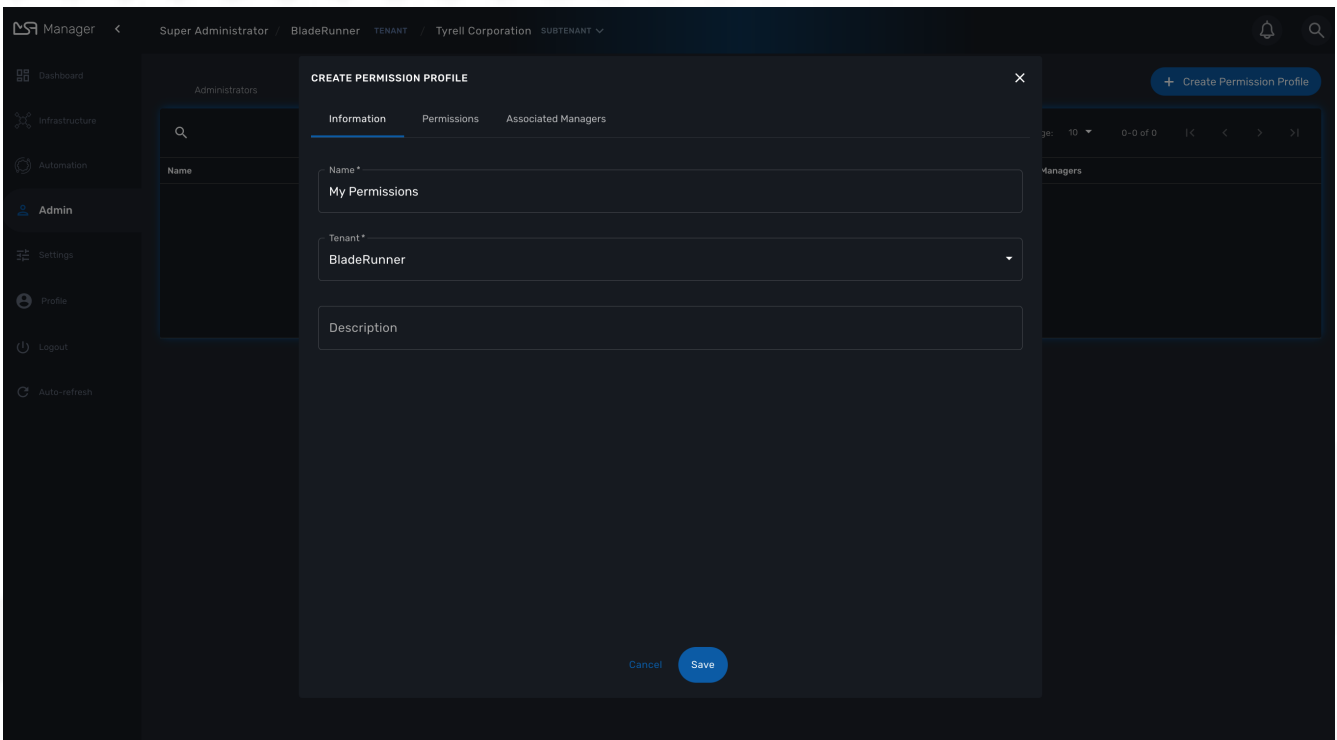
Roles and rights management : permission profiles

The MSactivator™ provides a simple authorization mechanism based on 4 user roles, the privileged administrator, the administrator, the privileged manager, and the manager.

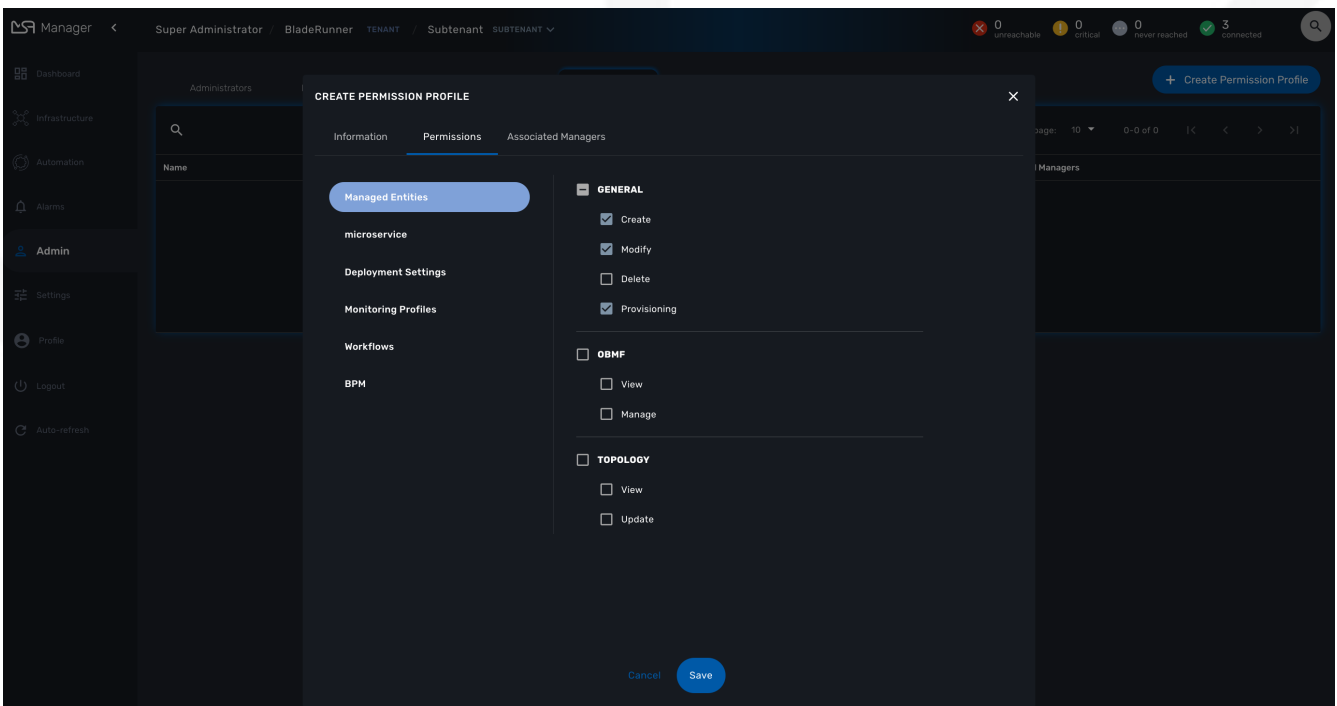
By default, managers have a very restricted access to the data. They can only view the information of the subtenant and managed entities they are entitled to. In order to grant more rights to a manager, it is possible to use a permission profile.

A permission profile is an aggregation of rights such as "create a device", "activate a device", "configure a device",... that are turned on or off depending on your user management policy. This profile is applied to a set of one or more users.

You can create a permission profile as ncroot from the "Admin" section. Permission profiles are created in the scope of a tenant therefore you need to select a tenant to manage them.



On the tab "Permissions" select the specific permission that you want to give to your managers
Permissions are organized by categories that reflect the MSactivator™ functional architecture.



Assign the permissions to managers on the tab "Associated Managers"

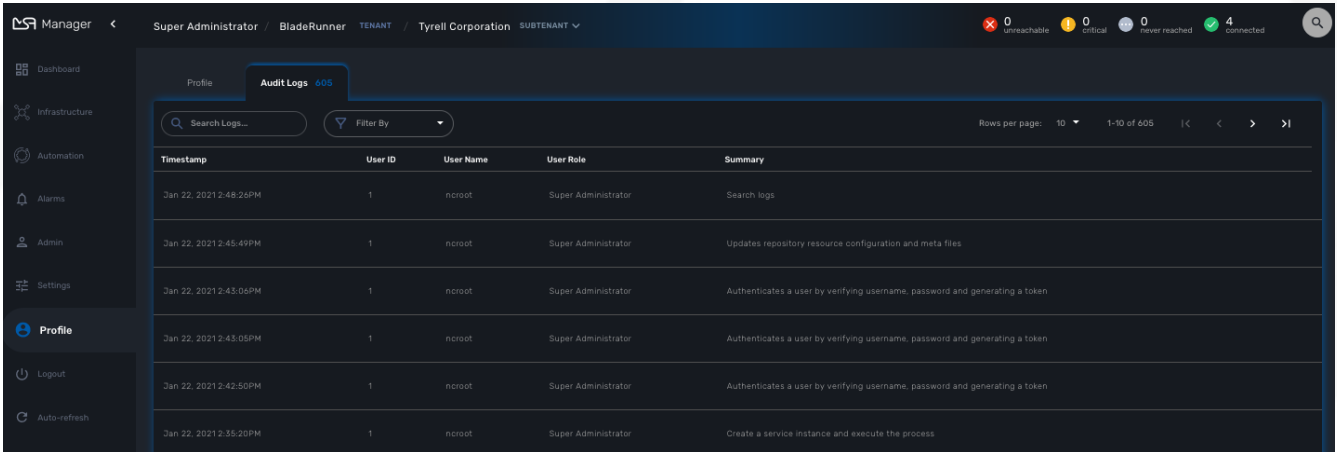
Audit record

The audit logs record every call to the MSactivator™ API, this includes user action on the UI and direct call to the REST API

Example

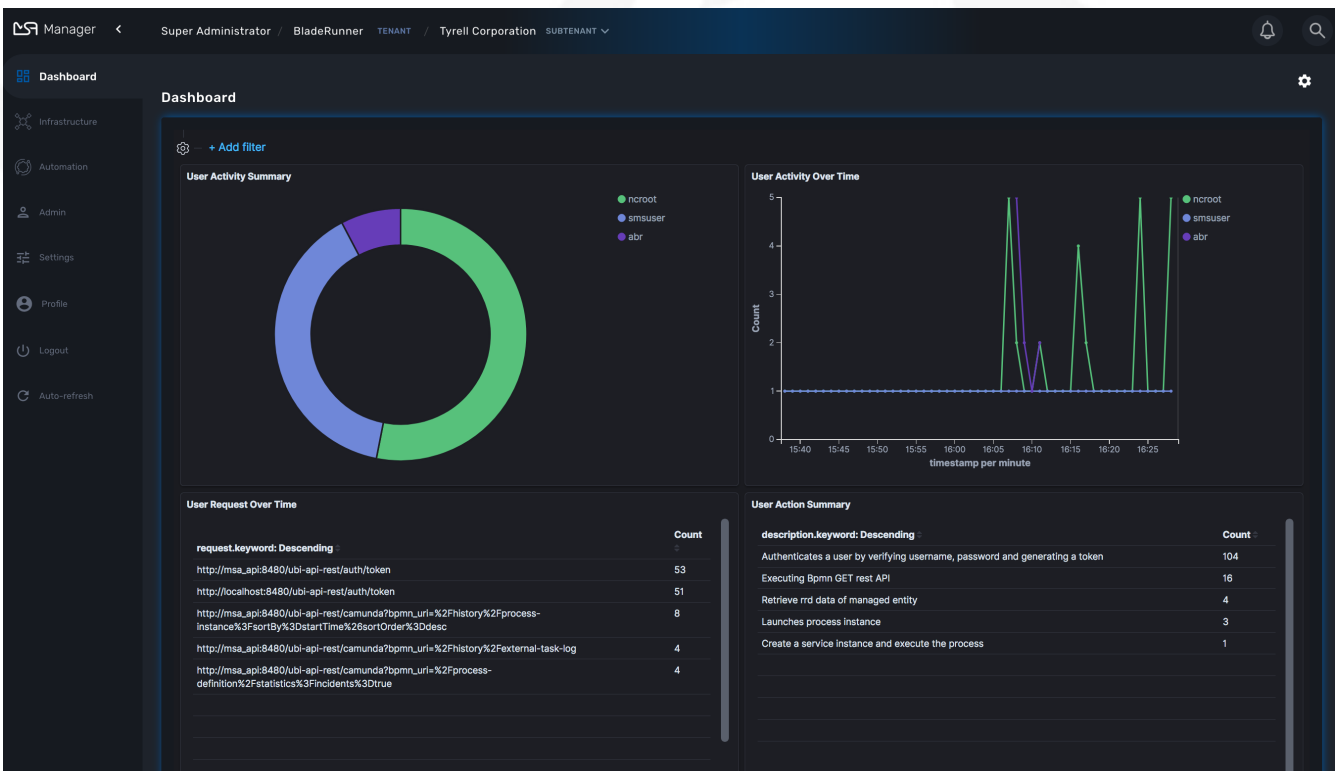
John logged in.
John opened the Management dashboard.
John applied sub-tenant filter "Hoth".
John listed the workflows attached the to sub-tenant "Hoth".
John executed the workflow "Create ME" on the sub-tenant "Hoth".
....
John logged out.

The audit logs are available for each user in the "Profile" menu, under "Audit Logs".

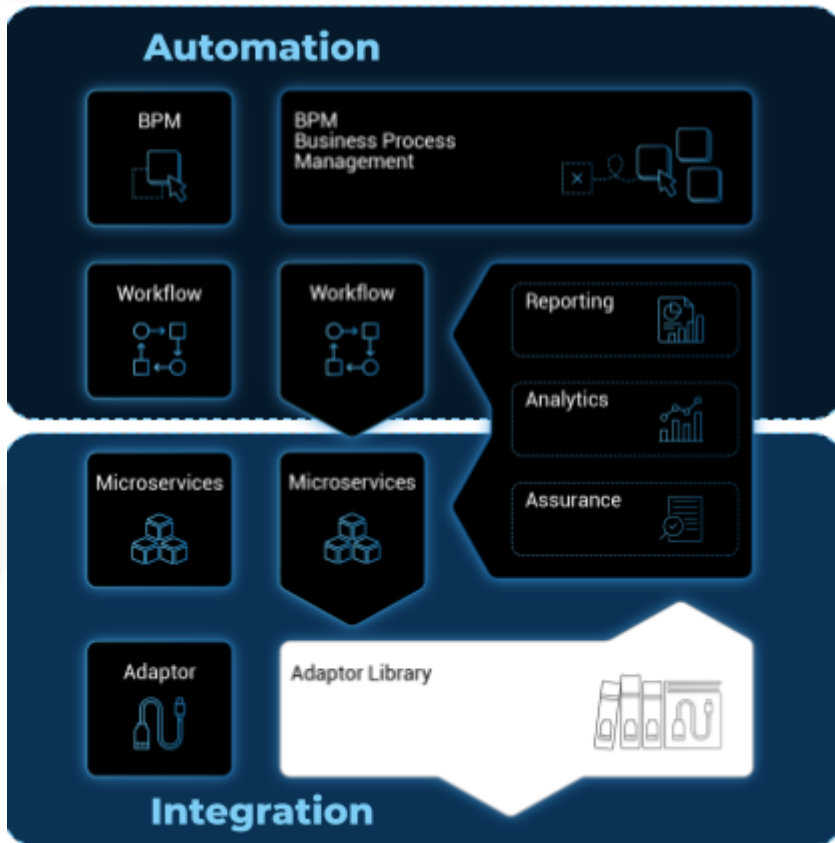


Timestamp	User ID	User Name	User Role	Summary
Jan 22, 2021 2:48:26PM	1	ncroot	Super Administrator	Search logs
Jan 22, 2021 2:45:49PM	1	ncroot	Super Administrator	Updates repository resource configuration and meta files
Jan 22, 2021 2:43:06PM	1	ncroot	Super Administrator	Authenticates a user by verifying username, password and generating a token
Jan 22, 2021 2:43:05PM	1	ncroot	Super Administrator	Authenticates a user by verifying username, password and generating a token
Jan 22, 2021 2:42:50PM	1	ncroot	Super Administrator	Authenticates a user by verifying username, password and generating a token
Jan 22, 2021 2:35:20PM	1	ncroot	Super Administrator	Create a service instance and execute the process

Since audit record are stored in Elasticsearch, you can use Kibana to design a simple user activity dashboard and display it in your super admin dashboard



Managed Entities



Managed Entities are the logical representation of any element of an infrastructure such as network devices, security devices, VNF, VIM,...

Overview

In order to become a manageable entity, an entity such as a router, a firewall or any other network function or element, physical or virtual, has to be created and activated in the MSactivator™.

These entities are managed in the "Infrastructure" section of the MSactivator™.

You can create a new managed entity or browse to an existing one and manage it.

This screen provides 3 types of view and you can switch between the detailed view, the compact view or the topology view.

Detailed list of managed entities

Status	Name	Type	Tenant	Subtenant	Vendor	Model
✓	Public A-Cloud eu-west-2 [London]	PUBLIC	Star Wars	Onderon	AWS	Generic
✓	ASAv 9.3 [10.31.1.156]	PRIVATE	Star Wars	Felucia	Cisco	ASA Generic
✓	Paloalto VA [10.30.19.110]	PRIVATE	Star Wars	Felucia	PaloAlto	VA
✓	ASA 8.4 [10.30.19.41]	PHYSICAL	Star Wars	Felucia	Cisco	ASA Generic

Create, update and activate a managed entity

To create a managed entity, click the "+ Create Managed Entity" button on the managed entity screen.

This will bring you to the form to create a managed entity.

The fields marked with a * are mandatory to create a managed entity. If a tenant or customer is selected on the global filter, then they will be pre-populated in the form. Otherwise a tenant and customer must be selected.

The selections in the "Vendor" and "Model" fields will determine the fields displayed in the "Management Information" and "Advanced Information" sections. Different managed entity types have different associated variables that are used in their provisioning and operation.



The selection of the vendor and model will determine the Adapter that will be used by the CoreEngine for configuration and assurance. It's important to select an adapter that is compatible with the managed entity model. Once a managed entity is created, it is not possible to change the model, the managed entity will have to be recreated.

The managed entity creation form can be closed by pressing the "X" button in the top bar. Any data entered into the fields will be preserved for when the user returns to the form. Clicking the "Discard Changes" button will display a confirmation prompt. If the user accepts the form state will be reset.

The update form can be accessed by clicking the pencil icon on the managed entity Listing page or on the managed entity Detail page.

Managed entity fields

These are the fields available when creating a managed entity. Some are mandatory and this is made explicit by the * on the web form.



All of these values are stored in the database and available to use by the Microservices, the Workflow, the API and the Adapters.

Tenant and subtenant

Select the tenant and subtenant the managed entity will belong to.

Only available when creating a managed entity, you can't change this value once the managed entity is created. If you selected the wrong tenant or subtenant you will have to recreate the managed entity.

Basic information

Select the category, the vendor and model for the managed entity.

This will select the adapter the MSactivator™ CoreEngine will use for configuring and monitoring the managed entity

Select the nature of the managed entity

The nature of the managed entity is an additional information that will help you organize your infrastructure into physical devices and virtual (private or public) ones

Administrative information

Set a name for the managed entity

The name is a free text field that you can use to identify your managed entity.



Although the value uniqueness is not enforced by the MSactivator™ data model, it is very common to use a hostname for the name field.

Management information

Management IP address

This is the IP address the MSactivator™ will use to manage and monitor the entity.



hostname or FQDN (Fully Qualified Domain Name) is not supported.

Management interface name

You can optionally set the management interface name here. When set, the CoreEngine will attempt to use to poll the management interface traffic with SNMP.

Hostname

The hostname of the managed entity.

The hostname is an optional field, it is used when syslog analytic is enabled for the managed entity

in order to match the incoming syslog with a managed entity. It can also be used, if needed, in the adapter for various management reasons.

Example: get the hostname value in the adapter PHP code

```
$network = get_network_profile();      ①  
$sd = &$network->SD;  
  
$hostname = $sd->SD_HOSTNAME;        ②
```

① read the managed entity data from the database

② get the value of the hostname

Management port

The management port is set to 22 by default and is used as is by most CLI command based adapters but for REST API adapters you'll have to set it to the correct value.

Advanced information

SNMP monitoring

Set the SNMP community configured on the actual managed entity.

Optionally set the monitoring port if it is not the default one (161)

Log analytics

Check to collect syslogs and optionally analyse the syslogs. The syslogs will be parsed and stored in the Elastisearch cluster.



log analytics must be enabled for SNMP trap monitoring.

Credentials

Provide the credential to authenticate to the managed entity.

The authentication is done at the adapter layer whenever it is required.

Managed entity activation

A managed entity can be activated by selecting "Activate" from the list of "Actions" at the top right of the managed entity screen.

This will show a form that takes the variables such as management IP, username and password that will be used in the activation. These fields may be pre-populated by the values given in the create form. If the variables are updated they will be used for that particular activation but will not be persistent.

When the activation is started the dialog shows the progress of the managed entity activation. This will update as the activation progresses and will show whether the activation succeeds or fails.



the activation of the managed entity is executed by the adapter for this managed entity model.

Overview screen

The overview screen is the main screen you will see when browsing to a managed entity

Overview screen



The managed entity overview screen is used to display the details of the selected entity.

You can reach this screen either by searching for a managed entity with the search field at the top right of the screen, or by selecting an entity from the managed entities list.

Asset information

The information such as the serial number, firmware, memory ... are retrieved dynamically by the adapter once the entity is activated.

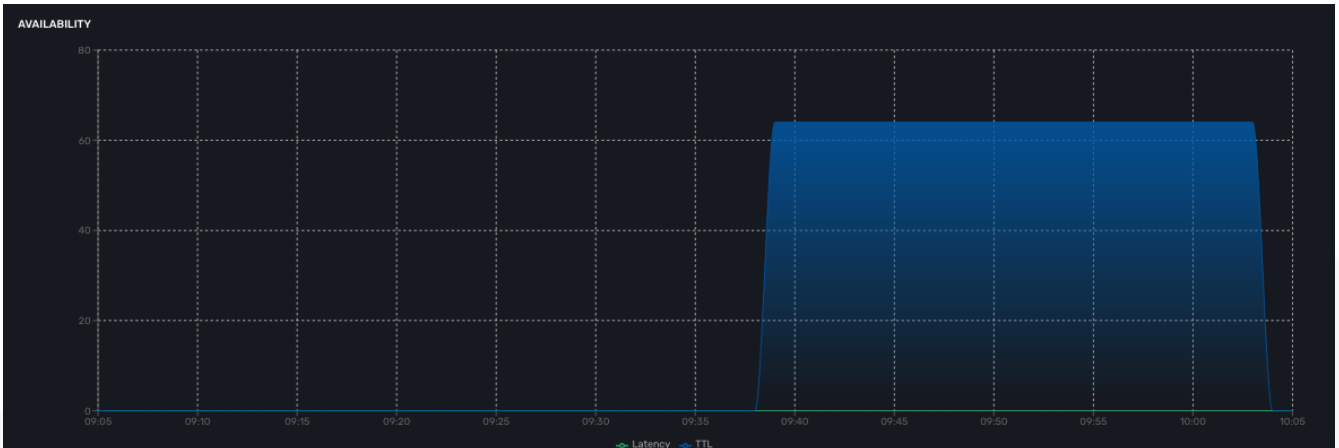
Monitoring information

By default there are 3 graphs that are displayed in the monitoring section of the overview screen:

- the availability of the managed entity
- the sysuptime of the managed entity
- the network traffic of the management interface

Availability

A graph, based on ICMP requests (1/min) issued by the CoreEngine container `msa_sms` to the management interface of the managed entity, shows the latency and TTL information.



When the connectivity fails, a event `VNOC-1-IPDOWN` is generated by the CoreEngine and indexed in Elasticsearch log index. An alarm can be configured based on this event.

When the connectivity is restored, a event `VNOC-1-IPUP` is generated and can also be used to generate an alarm.

Sysuptime

The sysuptime (System Uptime) is collected by the CoreEngine with SNMP. You need to allow SNMP requests on the managed entity and configure the SNMP community for the managed entity.



Traffic

The ingress and egress traffic of the management interface may be automatically collected provided that you have configured the management interface name in the managed entity configuration form.



Logs

Logs, internal events and threshold crossing events are listed in the tab "Logs"

In order to view and search for the syslogs, you need to activate syslogs collecting and log analytics in the managed entity configuration form. You also need to make sure that the actual managed entity is properly configured to send it's logs to the MSactivator™

Timestamp	Message	Severity	Device ID	Customer Ref	Type	Subtype
May 10, 2021 11:51:24AM GMT+02:00	<189>date=2021-05-10 time=09:51:24 devname='FGTAWSRZLD06V2D5' devid='FGTAWSRZLD06V2D5' eventtime=162064028352107023 tz='+0000' logid='0001000014' type='traffic' subtype='local' level='notice' vid='root' srcip=3.10.63.66 srcport=57004 srcintf='port1' srcintrole='undefined' dstip=172.31.0.129 dstport=161 dstintf='root' dstintrole='undefined' srccountry='United Kingdom' dstcountry='Reserved' sessionid=1106 proto=6 action='accept' policyid=0 policytype='local-in-policy' service='SNMP' transdisp='noop' app='SNMP' duration=0 sentbyte=74 rcvbyte=74 sentpkt=1 rcvpkt=1 appcat='unscanned'	NOTICE	BLR127	TyrellCorp	traffic	local
May 10, 2021 11:51:19AM GMT+02:00	<189>date=2021-05-10 time=09:51:19 devname='FGTAWSRZLD06V2D5' devid='FGTAWSRZLD06V2D5' eventtime=1620640280115014640 tz='+0000' logid='0001000014' type='traffic' subtype='local' level='notice' vid='root' srcip=89.197.210.107 srcport=48568 srcintf='port1' srcintrole='undefined' dstip=172.31.0.129 dstport=443 dstintf='root' dstintrole='undefined' srccountry='Mexico' dstcountry='Reserved' sessionid=1130 proto=6 action='deny' policyid=0 policytype='local-in-policy' service='MS-SQL' transdisp='noop' app='MS-SQL' duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 rcvpkt=0 appcat='unscanned' crscore=10 craction=262144 crlevel='medium'	NOTICE	BLR127	TyrellCorp	traffic	local
May 10, 2021 11:51:05AM GMT+02:00	<189>date=2021-05-10 time=09:51:05 devname='FGTAWSRZLD06V2D5' devid='FGTAWSRZLD06V2D5' eventtime=1620640284580284651 tz='+0000' logid='0001000014' type='traffic' subtype='local' level='notice' vid='root' srcip=162.142.125.144 srcport=59959 srcintf='port1' srcintrole='undefined' dstip=172.31.0.129 dstport=8027 dstintf='root' dstintrole='undefined' srccountry='United States' dstcountry='Reserved' sessionid=1129 proto=6 action='deny' policyid=0 policytype='local-in-policy' service='tcp/8027' transdisp='noop' app='tcp/8027' duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 rcvpkt=0 appcat='unscanned' crscore=10 craction=262144 crlevel='medium'	NOTICE	BLR127	TyrellCorp	traffic	local
May 10, 2021 11:50:53AM GMT+02:00	<189>date=2021-05-10 time=09:50:53 devname='FGTAWSRZLD06V2D5' devid='FGTAWSRZLD06V2D5' eventtime=1620640282411099289 tz='+0000' logid='0001000014' type='traffic' subtype='local' level='notice' vid='root' srcip=213.16.190.158 srcport=61631 srcintf='port1' srcintrole='undefined' dstip=172.31.0.129 dstport=80 dstintf='root' dstintrole='undefined' srccountry='Greece' dstcountry='Reserved' sessionid=1127 proto=6 action='client-rst' policyid=0 policytype='local-in-policy' service='HTTP' transdisp='noop' app='web Management' duration=5 sentbyte=80 rcvbyte=44 sentpkt=2 rcvpkt=2 appcat='unscanned'	NOTICE	BLR127	TyrellCorp	traffic	local
May 10, 2021 11:50:49AM GMT+02:00	<189>date=2021-05-10 time=09:50:49 devname='FGTAWSRZLD06V2D5' devid='FGTAWSRZLD06V2D5' eventtime=16206402818651108714 tz='+0000' logid='0001000014' type='traffic' subtype='local' level='notice' vid='root' srcip=213.16.190.158 srcport=58920 srcintf='port1' srcintrole='undefined' dstip=172.31.0.129 dstport=80 dstintf='root' dstintrole='undefined' srccountry='Greece' dstcountry='Reserved' sessionid=1188 proto=6 action='block' policyid=0 policytype='local-in-policy' service='HTTP' transdisp='noop' app='web Management' duration=1 sentbyte=508 rcvbyte=551 sentpkt=6 rcvpkt=4 appcat='unscanned'	NOTICE	BLR127	TyrellCorp	traffic	local
May 10, 2021 11:50:48AM GMT+02:00	<189>date=2021-05-10 time=09:50:48 devname='FGTAWSRZLD06V2D5' devid='FGTAWSRZLD06V2D5' eventtime=1620640281356988033 tz='+0000' logid='0720019632' type='utm' subtype='anomaly' eventtype='anomaly' level='alert' vid='root' severity='critical' srcip=213.16.190.158 srccountry='Greece' dstip=172.31.0.129 srcintf='port1' srcintrole='undefined' sessionid=0 action='detected' proto=6 service='HTTP' count=2 attack='ip_src_session' srcport=58920 dstport=80 attackid=16777322 policyid=1 policytype='db5-policy' ref='http://www.fortinet.com/ids/VID16777322' msg='anomaly: ip_src_session 2 > threshold 1, repeats 2 times since last log' crscore=50 craction=4096 crlevel='critical'	ALERT	BLR127	TyrellCorp	utm	anomaly

Configuration variables

In addition to the UI fields, it is also possible to create custom additional configuration variable to a managed entity. Configuration variables offer a convenient way to extend the data model of the managed entity without any core product customization.

A configuration variables is a key/value couple stored in the database, associated to a managed entity.

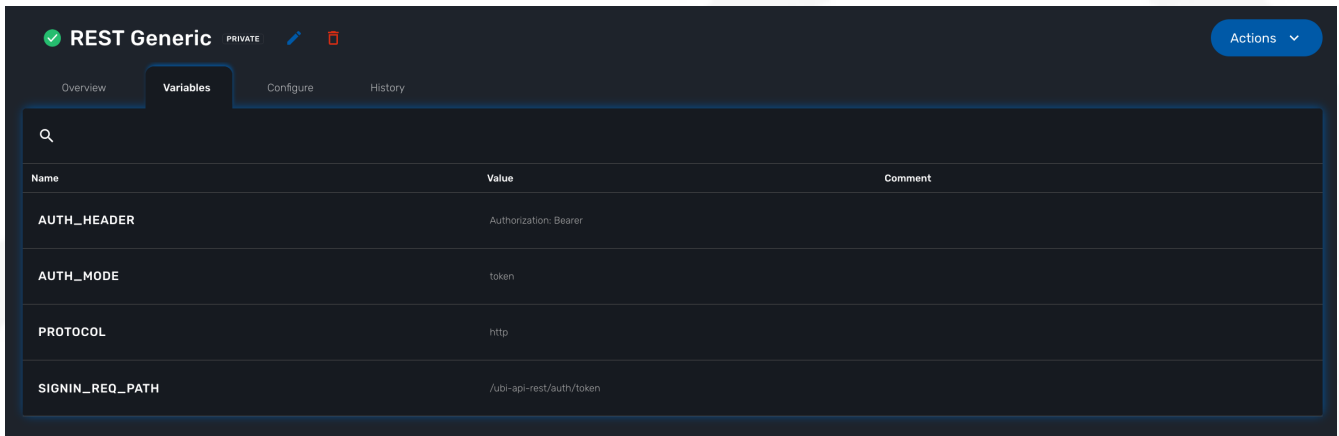
Once a configuration variable is set on a managed entity, it is available to the microservices and the device adapter but it can also simply be used to add additional administrative information to a

managed entity.

To create a configuration variable, click on the "Actions" menu on the top right of the managed entity screen and select "Create Variable".

Example 1: the REST generic adapter

The [REST generic adapter](#) uses configuration variables to customize its behavior and adapt itself to the various type of REST API (BASIC auth vs. Token auth, HTTP vs. HTTPS,...)



The screenshot shows the 'Variables' tab of the REST Generic configuration. It contains a table with the following data:

Name	Value	Comment
AUTH_HEADER	Authorization: Bearer	
AUTH_MODE	token	
PROTOCOL	http	
SIGNIN_REQ_PATH	/ubi-api-rest/auth/token	

Example of reading a configuration variable in the REST generic adapter code.

```
$network = get_network_profile(); ①  
$sd = &$network->SD;  
  
if (isset($sd->SD_CONFIGVAR_list['PROTOCOL'])) {  
    $protocol = $sd->SD_CONFIGVAR_list['PROTOCOL']->VAR_VALUE; ②  
}
```

- ① read the managed entity data from the database
- ② get the value of the configuration variable **PROTOCOL**

Example 2: in a microservice

In a microservice, you can reference any configuration variable with the syntax `{${CONFIG_VAR_NAME}}`.

In a Import function, you can use a configuration variable to make the command to run on the device more flexible.

```
sho access-lists ACL-CUST{${CUSTOMER_REF}} ①
```

- ① make the name of the ACL depend on a configuration variable **CUSTOMER_REF**

To read or set these configuration variables, you can use the REST API `GET /variables/{deviceId}/{name}` and `PUT /variables/{deviceId}/{name}`. This is useful for all your integration use cases or you can use the [workflow from the library](#).

Configuration

Managed entities can be configured with [microservices](#). To access the microservice console, click on the tab "Configure" on the managed entity screen.

In order to be able to use one or several microservices to configure a managed entity, the microservices must be associated to the managed entity via [deployment settings](#).

Once associated to the managed entity, you can navigate to the managed entity tab "Configure" to access the [microservice configuration console](#).

On the left menu of the console, you can see the list of the microservices that are associated to the current managed entity with the deployment setting.

Synchronization with the managed entity

In order to import the configuration from the actual managed entity into the MSactivator™ configuration database, you need to click on the link "Synchronize with Managed Entity".

This will call the CoreEngine and run the Import of each of the microservice.

The Import function may not always be implemented (this depends on the design of the microservice), therefore, the CoreEngine will simply skip these microservices.

Once the synchronization is done, the console will display the microservice instance, one by line, for each microservice.

In order to ensure that the configuration stored in the database is exactly reflecting the actual configuration of the managed entity, the microservice instances, specific to the current managed entity, are deleted from the database before the actual import can start.

Configuration of the managed entity

You can create a new microservice instance by selecting a microservice on the left menu and clicking "+ Add Row" and providing the input parameters to configure.

The input parameters are defined in the microservice "Variable" section.



"+ Add Row" is only available when the Create function of the selected microservice is implemented.

To update or delete a microservice instance, you need to select the row and click on "Edit" or "Remove".



"Edit" or "Remove" actions are only available if the Update or the Delete functions of the microservice are implemented.

Once you have updated your microservice, you can either click on "Discard Changes" or "Apply Changes".

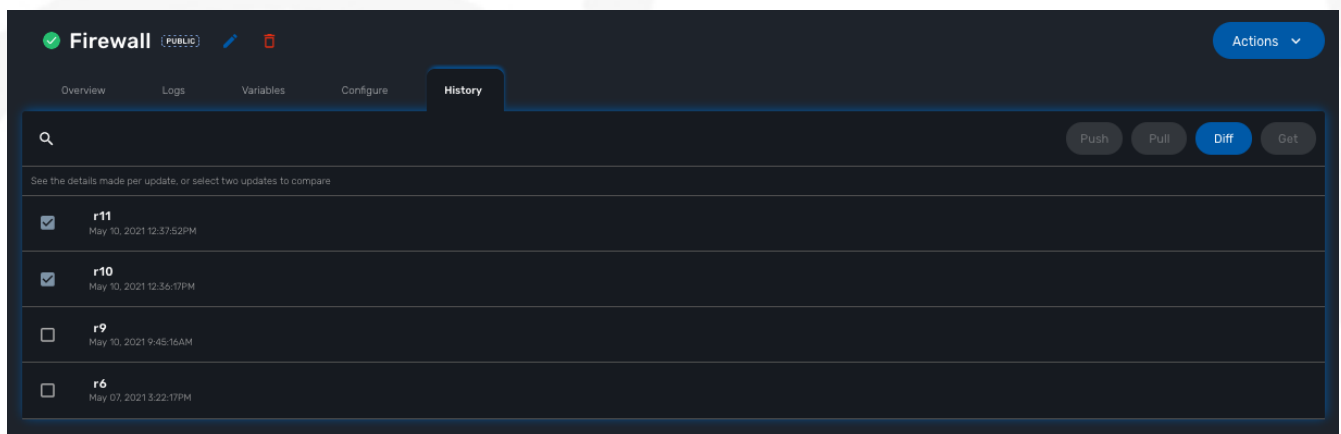
"Discard Changes" will remove all the orders that were stacked and stored in memory.

"Apply Changes" will unstack all the orders and pass all the orders that were stacked to the CoreEngine configuration daemon. The configuration daemon will process the order, build the configuration and apply it to the managed entity.

History

The MSactivator™ maintains a configuration history database that allows you to track the configuration changes that occurred on a managed entity and execute some backup/restore actions.

In the "History" tab of the managed entity, you will see the list of all configuration versions (revisions) available in the configuration database.



On this screen, you have the possibility to execute some action like restore a configuration (select a revision and use the Push button), backup a running configuration (use the Pull button) or display the differences between 2 selected revisions.

```
DIFF ONLY SHOW DIFFERENCES X
7297 end
7298 config webfilter ftgd-local-cat
7299 edit "custom1"
7300 set id 140
7301 next
7302 edit "custom2"
7303 set id 141
7304 next
7305 end
7306 config ips sensor
7307 edit "default"
7308 - set password ENC Cc0YnS T cUYF40x/B K M XTZ66k01a102tKc23a9qne Q Ps 9 LTVN P TVvrys2/B v u nBmW P
7309 + set password ENC vVxSa+R8UmW T K 6ZyTZ M 1 Q 4 9 P v 8I4jk0 u L6f0 P G EL W Crv L2CI dH
7310 - pa/HooBdupSW6HLWF E1 E W /uyJP 1 fuHs cM Qwh5Bg G u N Cf x MtIA0w 2 vu 5 j i Aoc w g b m D tZ I L y tE p 0W10 C 0G t
7311 + Kk/2YZf/3J0r71wRHp N 6 yis N ayLe x dd 2 5 R3C0DZkAqKJke i UPKaYMPeAhKhM v 1h80 b 2e3k/+ D g0wdVn649M I
7312 - M mn 8 6JNGmenZEZU H qS/Va n 263 v GhL2H Z VC 9 5q H TXI 4 f+4fB1 g ==
7313 + VYDp4pCy KQ2+ixX1Szq p C 4hV1pZ t XaM KL 8 q H 3Td n t0FPx v Iv Z ED 9 H 4 E g V0UrRA ==
7314 Expand 1748 lines ...
7315 set password ENC AAAGlRqhFSU0F8pCv8/qmN6pa2Z0GIneEPAYDGTaFP+q0Sj/cRBeFvr91J0d
7316 /wUyPkWqahf1kpcIe037FPZ6e49000e2gq7VVWIGI3botDjHshxdt9zVqJ9Uy7U04up
7317 /LhKu0NPMaRapjbydsE+9h5z0xj6aI6ThqTJZ0kLNxNecCT+R5eHhId80n1qk9A==
7318 set source built-in
7319 next
7320 end
7321 config firewall ssh setting
7322 set caname "Fortinet_SSH_CA"
7323 set untrusted-caname "Fortinet_SSH_CA_Untrusted"
7324 - set dst 1 9 2 . 169 . 1 . 0 255.255.255.0
7325 + set dst 1 2 3 . 34 . 4 . 0 255.255.255.0
7326 - set gateway 1 9 2 . 169 . 1.128
7327 + set gateway 1 . 2 . 3 . 4
7328 Expand 942 lines ...
7329 end
7330 config redistribute "bgp"
7331 end
7332 config redistribute "isis"
7333 end
7334 end
7335 config router ospf6
7336 config redistribute "connected"
7337 end
```

Close

Assurance

The MSactivator™ provides an assurance module for collecting network events and managing alarms

All the events sent by the managed or monitored entities are collected, indexed and analyzed centrally.

Monitoring profiles

Overview

You can configure and monitor your KPI with the **monitoring profiles**.

A monitoring profiles is a way to configure a set of SNMP based KPI, to configure threshold crossing based alarms and build graphs to display the KPI.

A monitoring profile has to be associated to one or more managed entity(ies) and a managed entity can also be associated to several monitoring profile(s).

Select a graphical rendering for a managed entity



Create or edit a monitoring profile

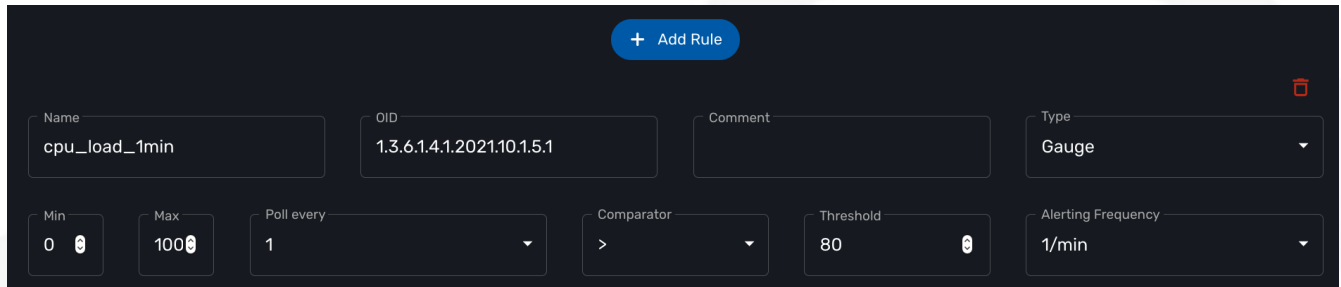
You can create a monitoring profile by browsing to the "Infrastructure" menu and selecting the tab "Monitoring Profiles" and clicking "+ Create Monitoring profile".

A monitoring profile is made out of 2 parts: the SNMP polling and the graphical rendering. Although SNMP polling is mandatory to have the MSactivator™ poll for the KPI, the graphical rendering is optional.

SNMP polling

Click "+ Add Rule" to add a new KPI.

create a new KPI



Name

The name will be used internally to identify the KPI in the KPI database and in the UI to build the graphical rendering.

OID

The MIB OID to read to get the value of the KPI.

Type

Select Gauge or Counter (see below for detail on this field).

Min/Max

For gauge, the max value will be used to trim any KPI value to the value set as max.

Poll every

Default is to poll for the KPI every minute but it possible to set a lower frequency for KPI that are less critical for instance.

Comparator, threshold and alert frequency

Configure an alarm based on threshold crossing (for instance if the CPU goes over 80%). See below for more details

Gauge or Counter

The rrd graph rendering will be different for counter or for gauge.

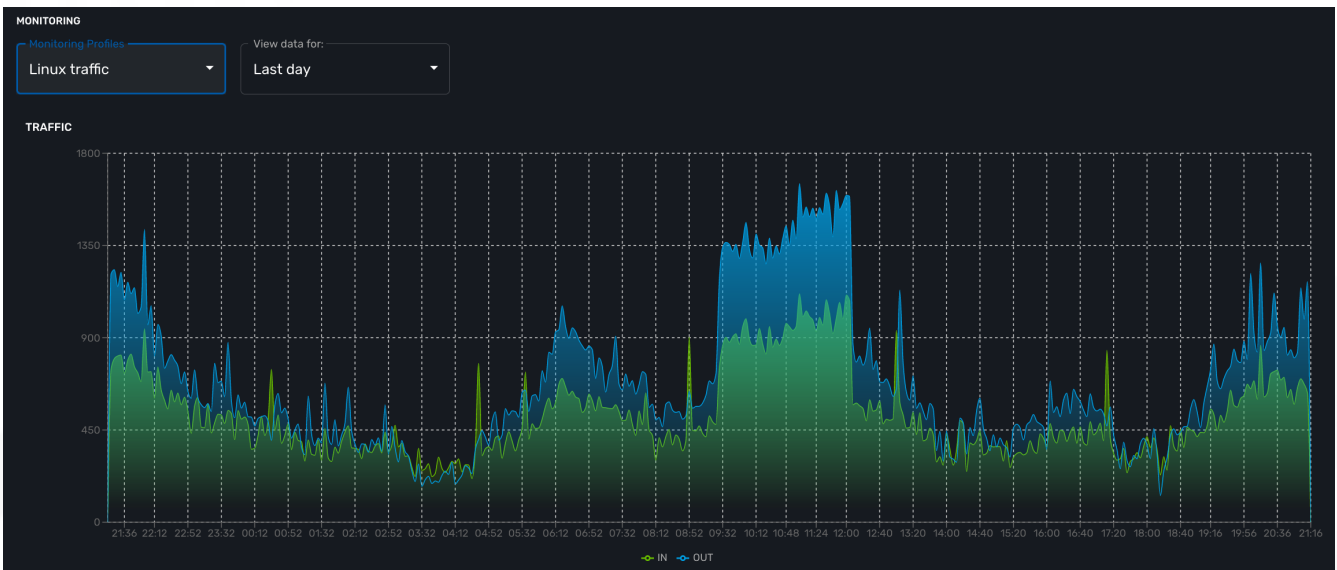
For a gauge the value of the record is the value on the graph.

For a counter a value in the graph is calculated with the difference between two consecutive records divided by the period of time. In other words a rrd counter will convert the input into a rate.

For example, if you monitor network traffic on an interface you need to use counter because the

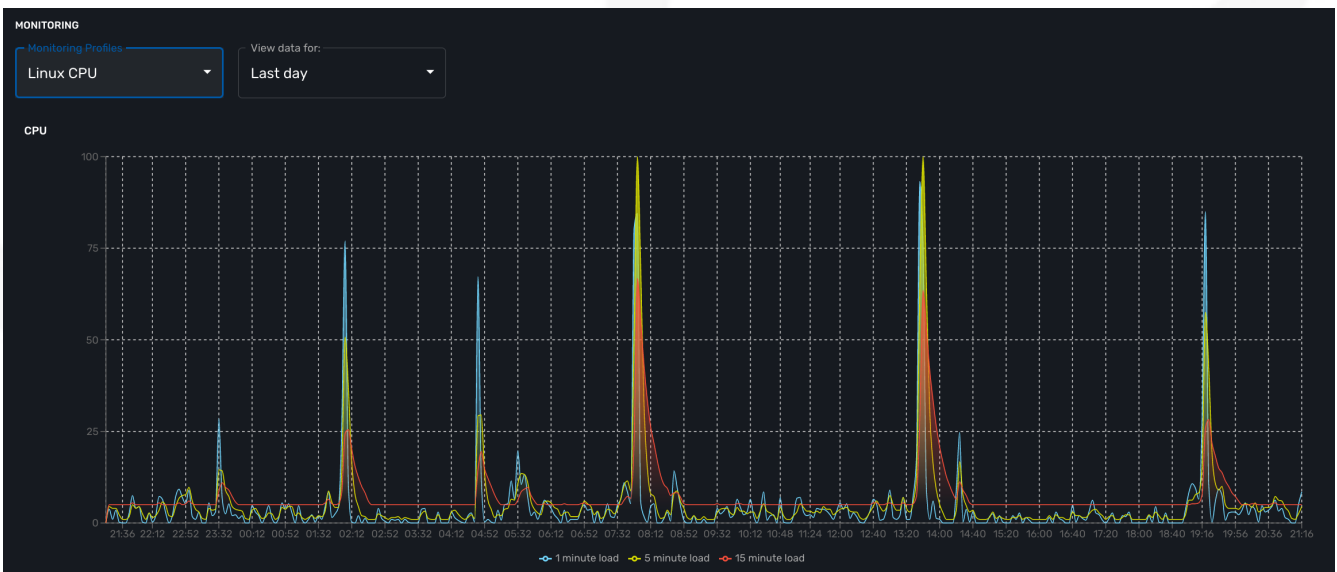
MIB stores the total traffic that went through the interface and what you want to see in the graph is actually the traffic rate and see how it evolves in time

Traffic monitoring

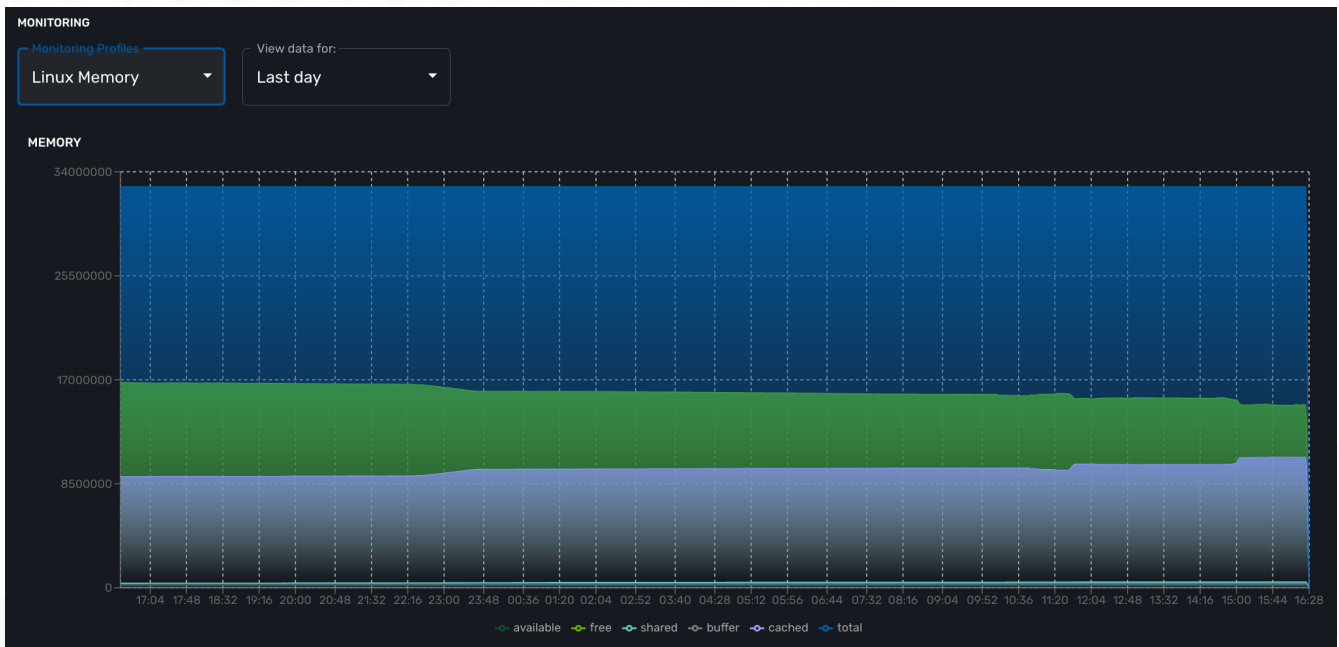


If you monitor the CPU usage, or the memory usage, you need to select a gauge because the MIB stores the actual value of the KPI.

CPU usage on a linux server



Memory usage on a linux server



MIB OID for monitoring CPU on Linux

```
cpu_load_1min : 1.3.6.1.4.1.2021.10.1.5.1 (Gauge)
cpu_load_5min : 1.3.6.1.4.1.2021.10.1.5.2 (Gauge)
cpu_load_15min : 1.3.6.1.4.1.2021.10.1.5.3 (Gauge)
```

MIB OID for monitoring the memory on Linux

```
memAvailReal : .1.3.6.1.4.1.2021.4.6.0 (Gauge)
memTotalFree : .1.3.6.1.4.1.2021.4.11.0 (Gauge)
memShared : .1.3.6.1.4.1.2021.4.13.0 (Gauge)
memBuffer : .1.3.6.1.4.1.2021.4.14.0 (Gauge)
memCached : .1.3.6.1.4.1.2021.4.15.0 (Gauge)
memTotalReal : .1.3.6.1.4.1.2021.4.5.0 (Gauge)
```

MIB OID for monitoring the traffic on eth0 on Linux

```
traffic_in : 1.3.6.1.2.1.2.2.1.10.2 (Counter)
traffic_out : 1.3.6.1.2.1.2.2.1.16.2 (Counter)
```

Threshold based VNOc events

Is possible to configure VNOc events based on KPI threshold crossing.

This is useful to monitor resources such as CPU or memory consumption. When a KPI crosses a threshold and event is generated and visible in the assurance "Logs" section.

Alert log for threshold crossing

Super Administrator / Tenant TENANT / Subtenant SUBTENANT

Alarms 6,783 Manage Alarms

SNMPthld Filter By Columns Create Alarm

Rows per page: 50 1-50 of 6,783

Timestamp	Message	Severity	Managed Entity ID	Subtenant Ref	Type	Subtype
Feb 08, 2023 5:02:41PM	%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_idle_CPU_time raised value 96 (> 70)	ALERT	BLR149	TyrellCorp	VNOc	SNMPthld-29-percentages_of_idle_CPU_time
tenant_id: BLR man_id: 14020601 _timestamp_epoch_: 1675872161174 _timestamp_: 2023-02-08T16:02:41.174314943Z mod_id: 14020601 customer_id: 6		device_mgmt_ip: 3.10.63.66 rawlog: %VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_idle_CPU_time raised value 96 (> 70) source_ip: hostname: ip-172-31-0-146 name: MSA Host - linux generic 3.10.63.66 timestamp: 1675872161142				
Feb 08, 2023 5:01:41PM	%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_idle_CPU_time raised value 95 (> 70)	ALERT	BLR149	TyrellCorp	VNOc	SNMPthld-29-percentages_of_idle_CPU_time
tenant_id: BLR man_id: 14020601 _timestamp_epoch_: 1675872101170 _timestamp_: 2023-02-08T16:01:41.170786992Z mod_id: 14020601 customer_id: 6		device_mgmt_ip: 3.10.63.66 rawlog: %VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_idle_CPU_time raised value 95 (> 70) source_ip: hostname: ip-172-31-0-146 name: MSA Host - linux generic 3.10.63.66 timestamp: 1675872101131				

When a monitoring threshold is crossed the log message will be similar to "%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_system_CPU_time raised value 1 (< 20) " where you can see that the threshold 10 has been crossed by a greater value 69.

This configuration is done at the SNMP polling rule in the monitoring profile by setting a comparator '>' or '<' and a threshold.

VNOc threshold crossing events can be used to configure alarms in order to be notified by email or SNMP trap or simply by the alarm bell icon on the top right of the screen.

Super Administrator / Tenant TENANT / Tyrell Corporation SUBTENANT

Alarms 43 Logs Manage Alarms

Alarm Acknowledgement Search Logs... Filter By Columns

Rows per page: 50 1-43 of 43

ACK: FALSE

<input type="checkbox"/>	Alarm Name	Created Time	Message	Severity	Managed Entity Name
<input type="checkbox"/>	VNOc-1-SNMPthld	Apr 05, 2023 3:32:35PM	%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_system_CPU_time raised value 1 (< 20) - MSA Host - linux generic 3.10.63.66 (3.10.63.66)	NOTICE	MSA Host - linux generic 3.10.63.66
<input type="checkbox"/>	VNOc-1-SNMPthld	Apr 05, 2023 3:31:35PM	%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_system_CPU_time raised value 1 (< 20) - MSA Host - linux generic 3.10.63.66 (3.10.63.66)	NOTICE	MSA Host - linux generic 3.10.63.66
<input type="checkbox"/>	VNOc-1-SNMPthld	Apr 05, 2023 3:30:35PM	%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_system_CPU_time raised value 1 (< 20) - MSA Host - linux generic 3.10.63.66 (3.10.63.66)	NOTICE	MSA Host - linux generic 3.10.63.66
<input type="checkbox"/>	VNOc-1-SNMPthld	Apr 05, 2023 3:29:35PM	%VNOc-1-SNMPthld: supervision - Site BLR149 snmp threshold 29-percentages_of_system_CPU_time raised value 1 (< 20) - MSA Host - linux generic 3.10.63.66 (3.10.63.66)	NOTICE	MSA Host - linux generic 3.10.63.66

Graphical rendering

For each monitoring profile you can also create a graph to aggregate and display 1 or more KPI defined in the SNMP polling section.

Since the KPI are going to be displayed in the same graph, you need to ensure that the data is consistent. Displaying CPU load and network traffic in the same graph is allowed but will not make any sense. In this case you need to have 2 monitoring profiles for each set of KPI.

Configure the graphical rendering for a set of KPI

[+ Add Graph](#)

Graph Name: CPU Units: percent

+ Data Name * X Axis Color

- cpu_load_1min 1 minute load ■ Color
- cpu_load_5min 5 minute load ■ Color
- cpu_load_15min 15 minute load ■ Color

SNMP trap monitoring

The MSactivator™ can collect and index SNMP trap out of the box.

To monitor a managed entity with SNMP trap you need to configure the managed entity with **Collect Syslog** and **Analyze Syslog** enabled.

When the MSactivator™ collects a trap, it relies on the trap source IP address to identify the managed entity by it's management IP address.

Once a management entity is identified, the trap will be processed the same way as a syslog and will be indexed in Elasticsearch. It will then be listed in the logs screen in the "Alarms" section.

Manager < Super Administrator / Tenant TENANT / Subtenant SUBTENANT

Alarms **Logs 9** Manage Alarms

TRAPSNMP Filter By Columns Create Alarm

Rows per page: 50 1-9 of 9

Timestamp	Message	Severity	Managed Entity ID	Subtenant Ref	Type	Subtype
Feb 08, 2023 4:58:09PM	<4>%VNDC-4-TrapSnmp(10): V=3 sysUpTimeInstance=42 snmpTrapOID=1.3.6.1.3.1.15.1.0	4-WARNING	BLR158	TyrellCorp		Hide
	tenant_id: BLR man_id: 14020601 rawlog: <4>%VNDC-4-TrapSnmp(10): V=3 sysUpTimeInstance=42 snmpTrapOID=1.3.6.1.3.1.15.1.0 source_ip: hostname: ip-172-31-0-161 orig: BLR158 customer_id: 6		device_mgmt_ip: 3.9.62.182 sec_node: 3f4d477c8009 _timestamp_epoch_: 1675871890226 _timestamp_: 2023-02-08T15:58:10.226082823Z mod_id: 14020601			
Feb 08, 2023 4:57:57PM	<4>%VNDC-4-TrapSnmp(10): V=3 sysUpTimeInstance=42 snmpTrapOID=1.3.6.1.3.1.15.1.0	4-WARNING	BLR158	TyrellCorp		Hide
	tenant_id: BLR man_id: 14020601 rawlog: <4>%VNDC-4-TrapSnmp(10): V=3 sysUpTimeInstance=42 snmpTrapOID=1.3.6.1.3.1.15.1.0 source_ip: hostname: ip-172-31-0-161 orig: BLR158 customer_id: 6		device_mgmt_ip: 3.9.62.182 sec_node: 3f4d477c8009 _timestamp_epoch_: 1675871878205 _timestamp_: 2023-02-08T15:57:58.205752616Z mod_id: 14020601			

SNMP v2/v3

By default the MSactivator™ will be using SNMP v2.

Starting with MSactivator™ v2.8.3 SNMPv3 is also supported.

In order to use SNMPv3 to monitor a managed entity you need to configure its variables with the SNMPv3 parameters.

- snmpv3_securityName
- snmpv3_securityLevel: possible values are noAuthNoPriv, authNoPriv, and authPriv
- snmpv3_authKey
- snmpv3_authProtocol: possible values are MD5 or SHA
- snmpv3_privKey
- snmpv3_privProtocol: possible values are DES or AES
- snmpv3_securityEngineID

Notes

For the polling, the mandatory variables are snmpv3_securityName, snmpv3_securityLevel, the others depends of snmpv3_securityLevel value, see below.

For receiving SNMP trap, the mandatory variables are snmpv3_securityName, snmpv3_securityLevel, snmpv3_securityEngineID, the others depends of snmpv3_securityLevel value, see below.

- if snmpv3_securityLevel is set to authPriv, the additional mandatory variables are snmpv3_authKey, snmpv3_authProtocol, snmpv3_privKey, snmpv3_privProtocol
- if snmpv3_securityLevel is set to authNoPriv, the additional mandatory variables are snmpv3_authKey, snmpv3_authProtocol
- if snmpv3_securityLevel is set to noAuthNoPriv, no other additional variables are mandatory

Overview		Logs		Variables		Configure		History	
<input type="text" value=""/>									
Name					Value				
snmpv3_authKey					the_authKey				
snmpv3_authProtocol					SHA				
snmpv3_privKey					the_privKey				
snmpv3_privProtocol					AES				
snmpv3_securityEngineID					30313233343536373839414243444546				
snmpv3_securityLevel					AuthPriv				
snmpv3_securityName					the_user_name				

You also need to enable "SNMP Monitoring", use the SNMPv3 user for the community field.

The parameter values should match the SNMPv3 configuration that was set in your actual device.

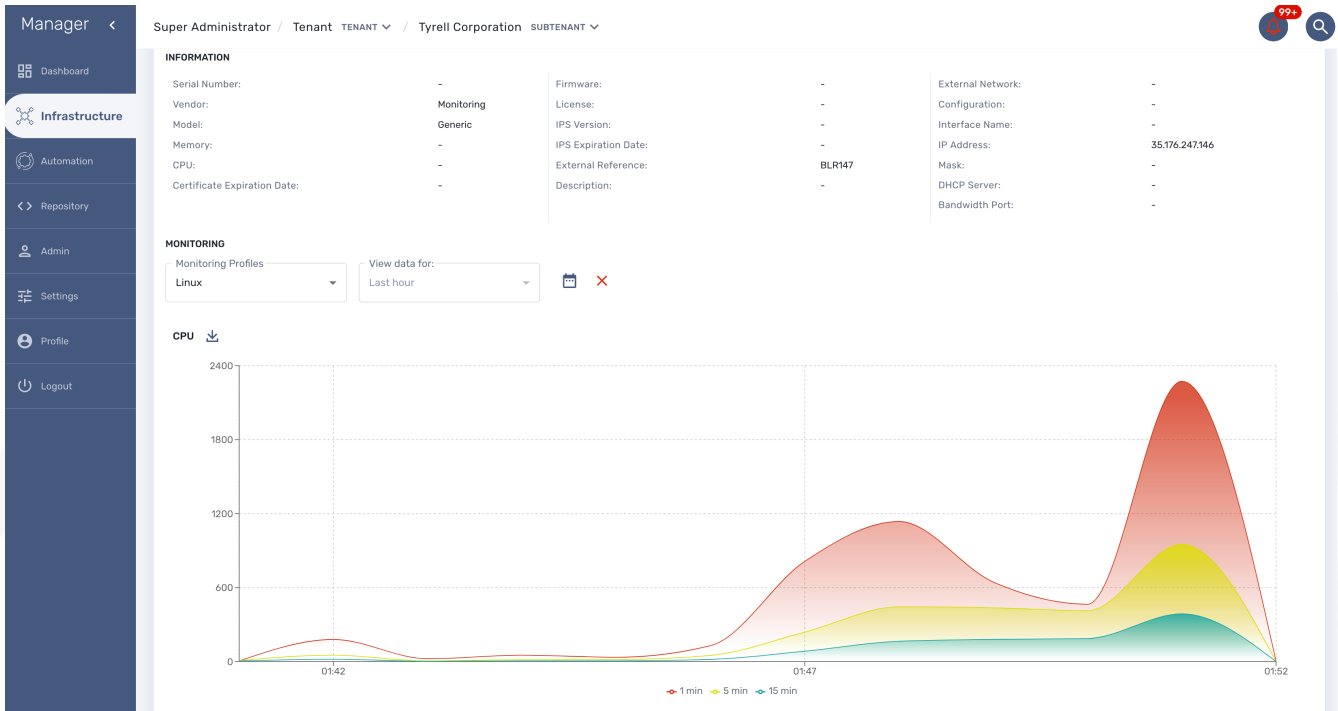
For instance on a Linux Centos7:

```
[centos@ip-172-31-0-52 ~]$ snmpwalk -v3 -u ubiquete -l authNoPriv -a MD5 -A Ubiquete2021 localhost
SNMPv2-MIB::sysDescr.0 = STRING: Linux ip-172-31-0-52.eu-west-2.compute.internal
3.10.0-957.12.2.el7.x86_64 #1 SMP Tue May 14 21:24:32 UTC 2019 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (116126) 0:19:21.26
SNMPv2-MIB::sysContact.0 = STRING: root@localhost
SNMPv2-MIB::sysName.0 = STRING: ip-172-31-0-52.eu-west-2.compute.internal
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (8) 0:00:00.08
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
```

To verify that SNMP v3 monitoring is working properly you can check that the sysuptime graph is

plotting data.

You can also monitor specific KPI based on the OID of your vendor.



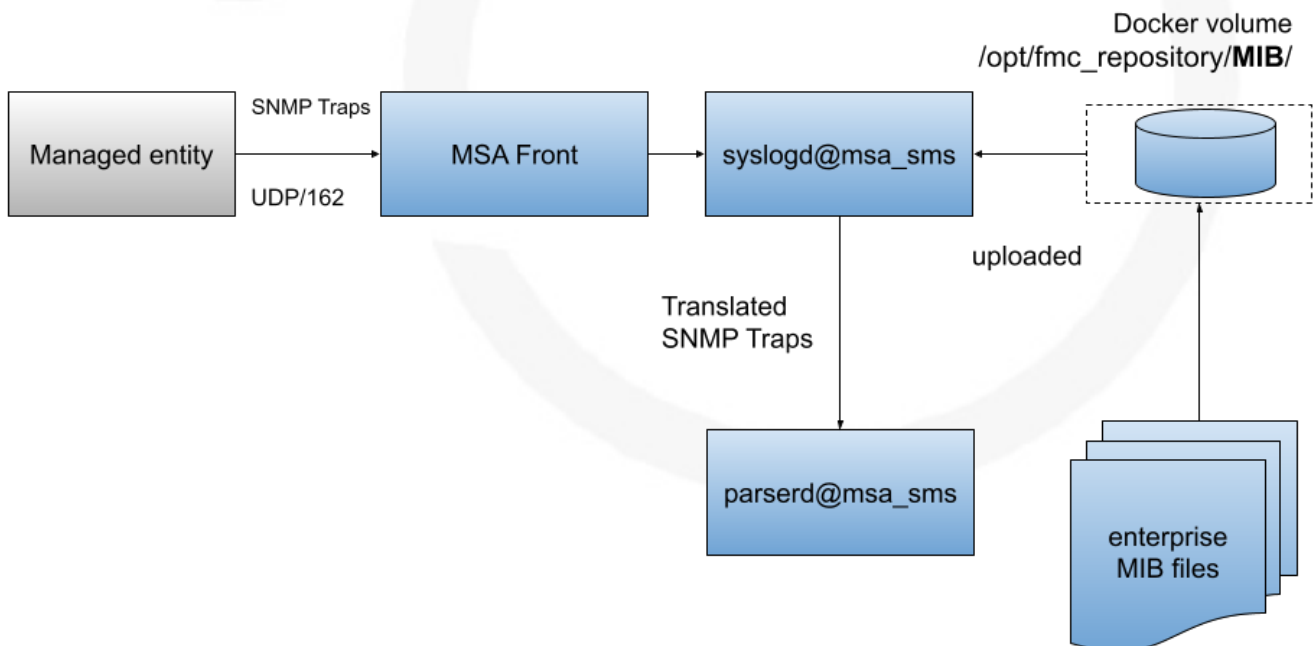
Collecting SNMPv3 trap

For SNMPv3 traps, the managed entity should be configured as explained above and the variable `snmpv3_securityEngineID` is mandatory for decoding the SNMP traps.

SNMP trap translation

Architecture overview

Dynamic SNMP trap translation based on MIB definition files



The `/opt/sms/conf/sms_syslogd.conf` contains the following configuration variables:

1. `additional-conf-path /opt/sms/conf.d`
2. `oid-translation-file oid_translated.conf`
3. `mibs-translation-path /opt/fmc_repository/Datafiles/MIBs_translation`

The `syslogd` daemon gets the new MIB configuration files from `mibs-translation-path` (polling there) and then converts them to its own usable format and store them in `additional-conf-path` (updating `oid-translation-file` too).

The MIB Translation WF will get the MIB definition files in `/opt/fmc_repository/Datafiles/MIBs/` (default value for variable `import_mibs_path` in the WF). It is manually launched and will convert them into an intermediate format and store them in `/opt/fmc_repository/Datafiles/MIBs_translation/`.



NET-SNMP lib function `read_objid` is used to perform the snmp trap translation on the fly in `sms_syslogd` daemon side NOTE: in the container `msa_sms` location where `syslogd` gets the standard MIB configuration is `/usr/share/snmp/mibs/`.

Install the MIB translation workflow

The goal of this workflow is to implement translation rules of an OID into a string from Management Information Base (MIB).

The workflow installation or update has to be done in the `msa-dev` container. For that the following command can help:

```
docker exec -it $(docker ps -q -f name=msa-dev) bash
```

The installation commands:

```
cd /opt/fmc_repository/  
git clone https://github.com/openmsa/workflow-mib-translation.git  
chown -R ncuser. workflow-mib-translation  
cd Process  
ln -s ../workflow-mib-translation/ .  
chown -R ncuser. workflow-mib-translation
```

The `workflow-mib-translation` can then be updated in an usual way like any git repository.

Once done, MIB Translation is available in the list of workflows in the MSactivator™ UI it can be attached to a subtenant.



MIB translation workflow will configure the MSactivator™ for all the managed entities. Therefore it is recommended to use a dedicated "Admin" subtenant in order to ease the use.

Workflow Name	Date Modified	Instances
MIB Translation	Feb 16, 2023 5:34:53PM	0 Instances

Execute the MIB translation workflow

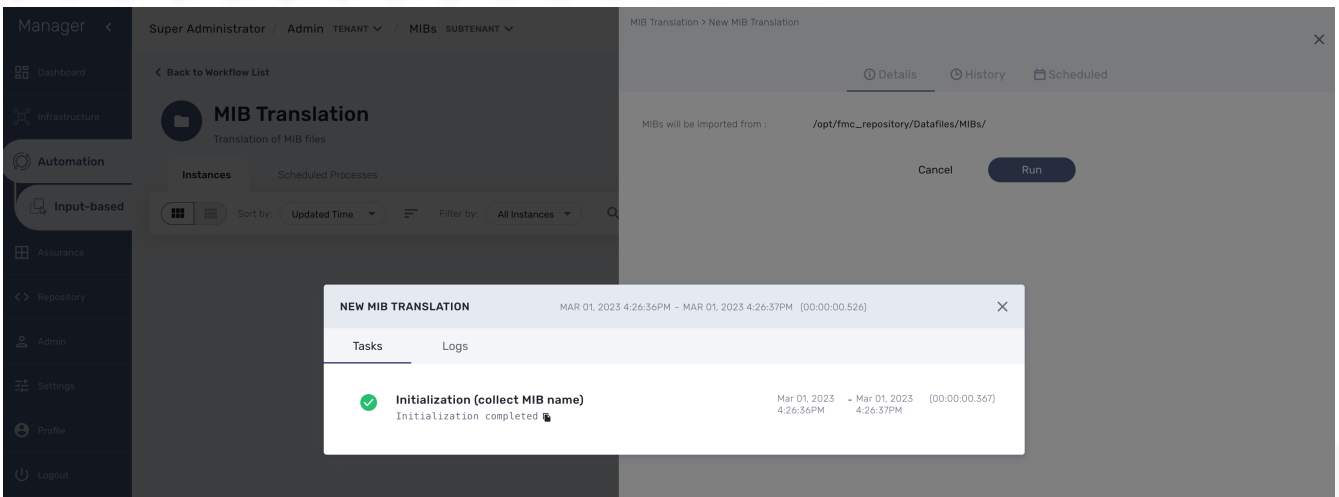
First put the MIB definition files into the repository under a folder "MIBs".

The MIB Translation WF working in 3 steps/processes

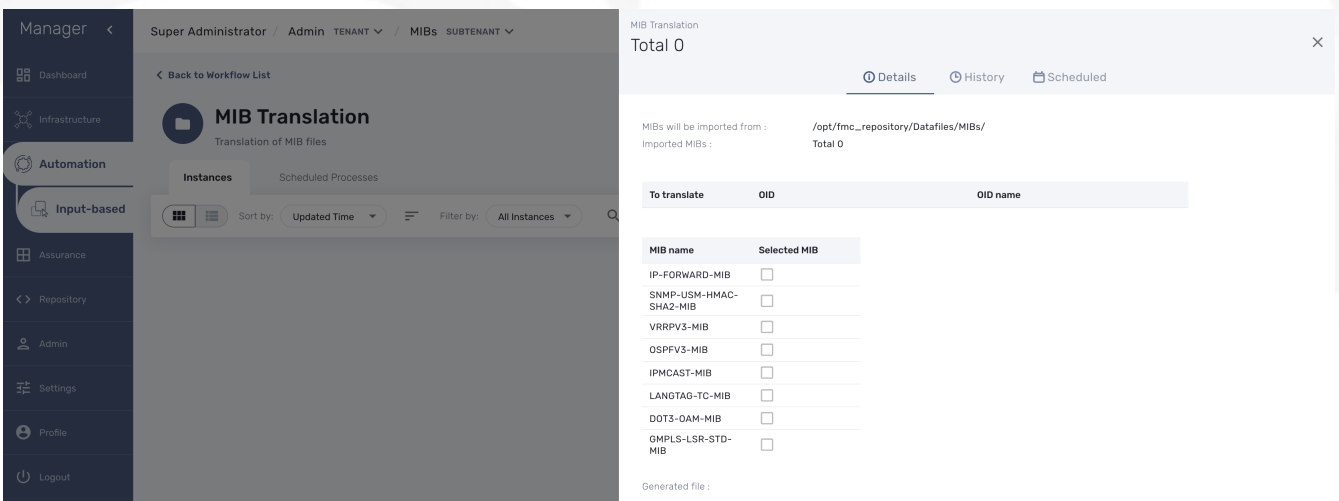
Workflow overview

Initialize import

This process is reading the text (*.txt) files in /opt/fmc_repository/Datafiles/MIBs/ in order to get the list of the available MIBs (recursive reading is supported)



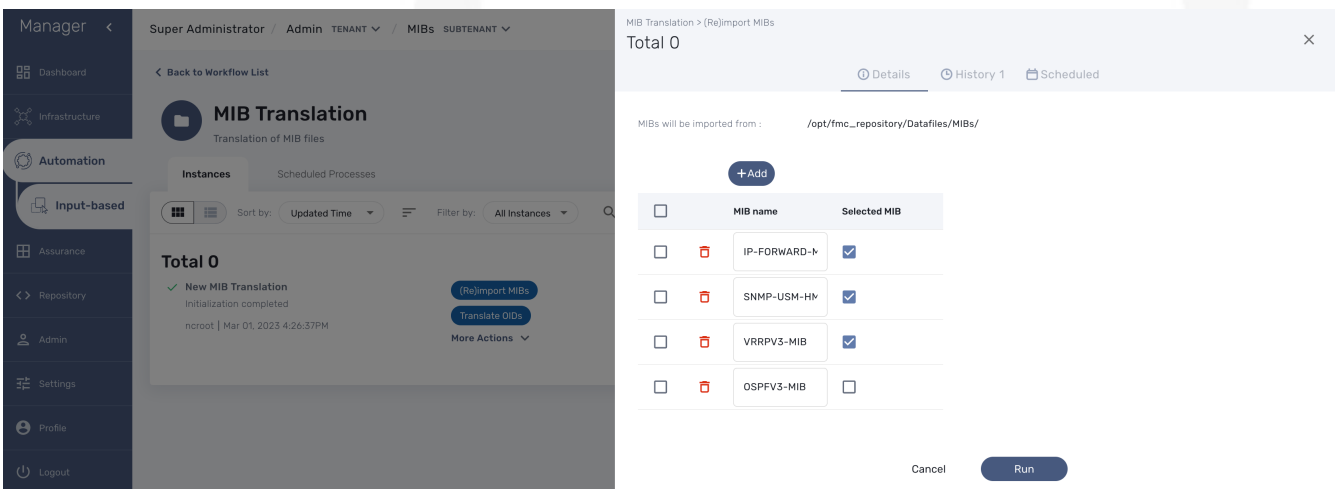
Result of the initialization



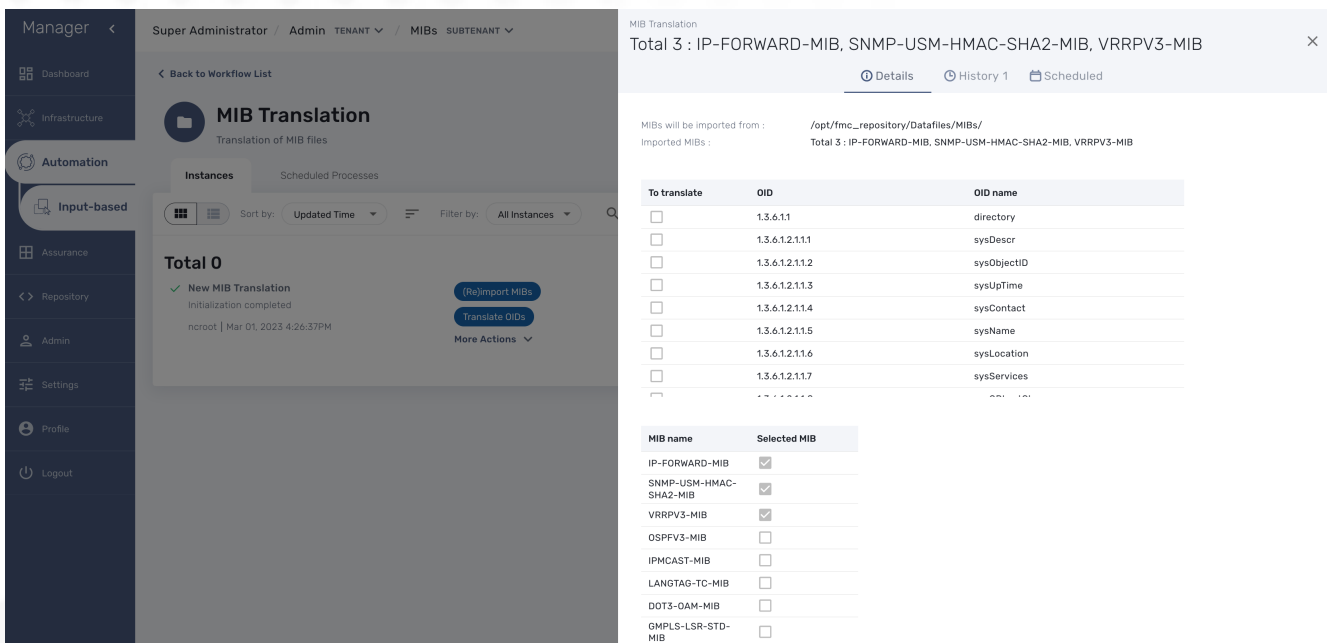
(Re)import MIBs

This process allows the user to select which MIB(s) he wants to import according to the MIB(s) list built on the first step.

Execute the process "(Re)Import MIB" and select the MIBs to process.



The result is the list of OIDs that are available for the translation.

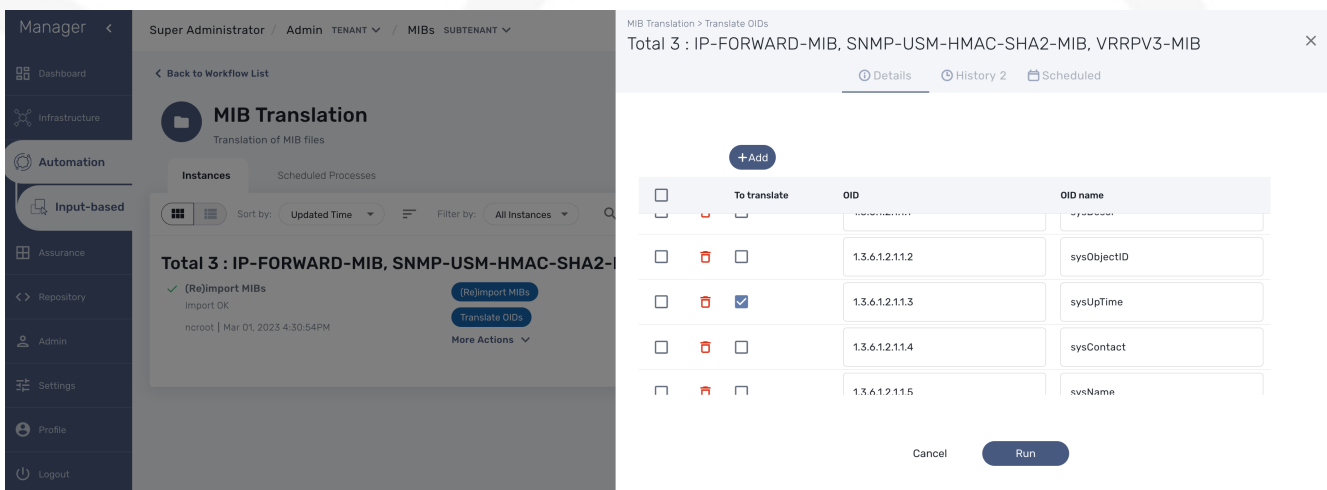


Translate OIDs

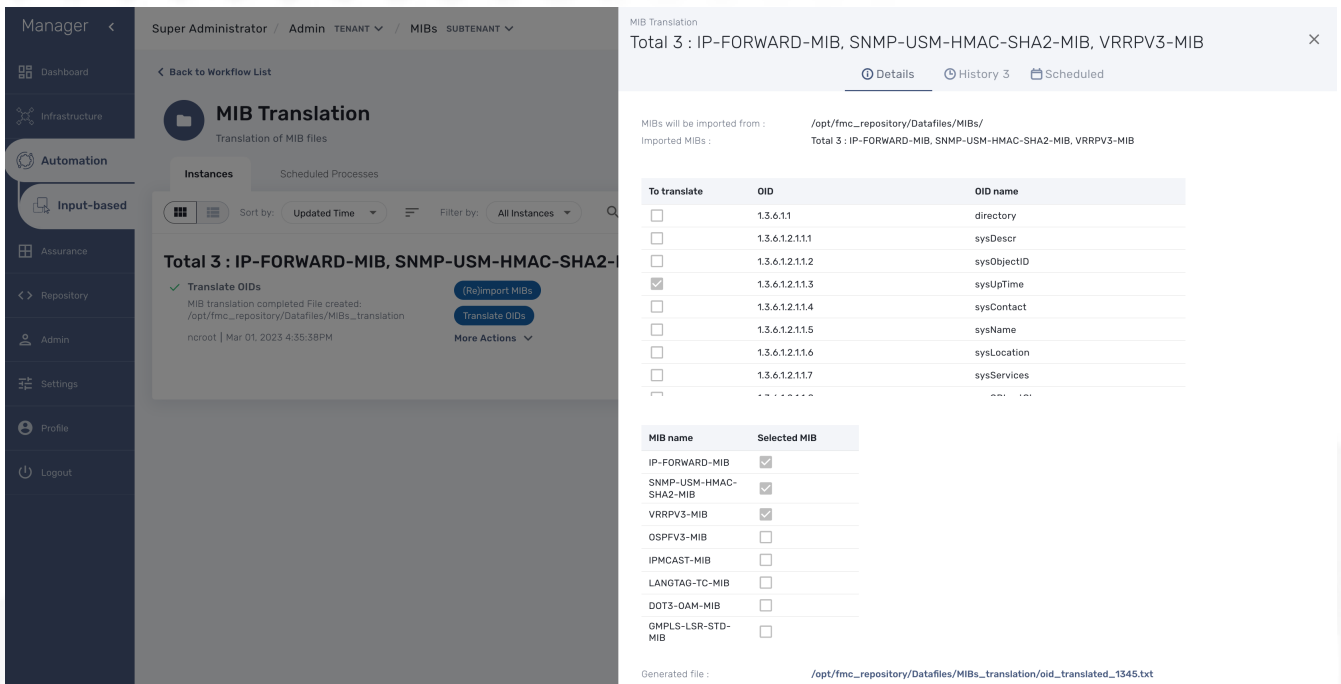
This process allows the user to select which OIDs from the MIB(s) from step 2 he wants to push as translation rules. User can not only select the tuple OIDs/Names coming from the MIB file(s), but he can overwrite the name or the OID or/and add manual entry.

Once the process runs, an export file will be created in `/opt/fmc_repository/Datafiles/MIBs_translation/` folder, that will be used in a next step by the `sms_syslogd` daemon to implement the request

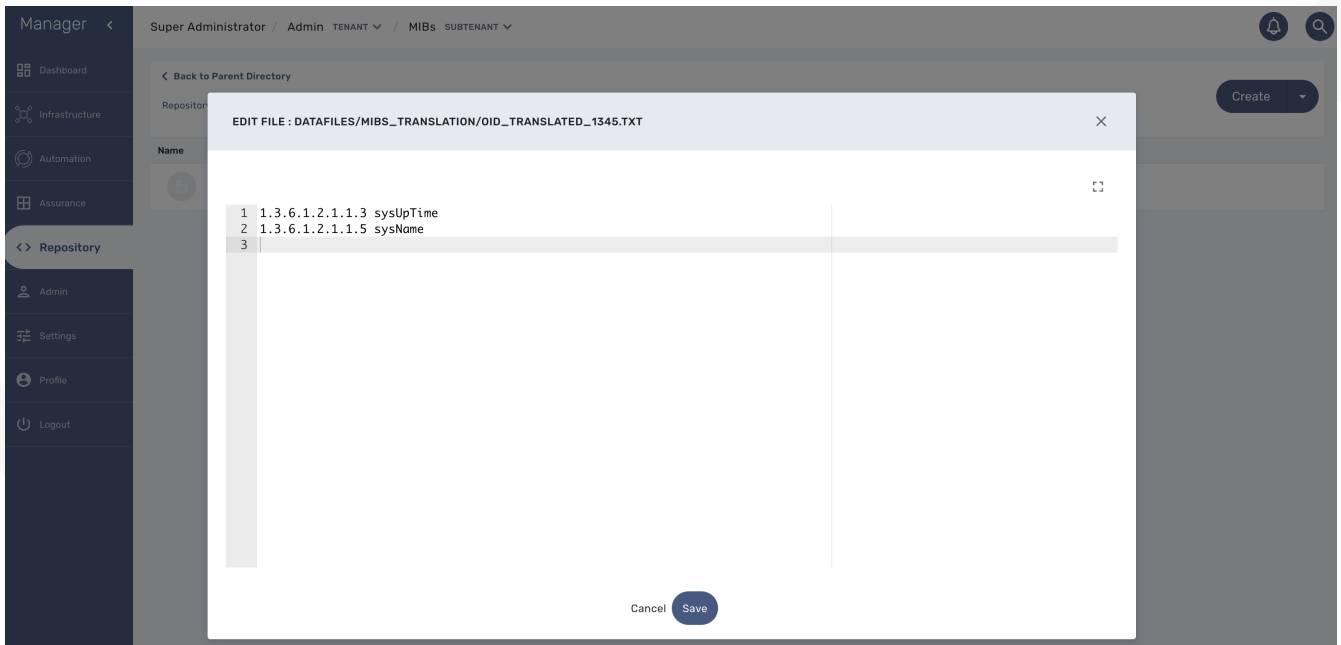
The 2 first steps will allow the end-user to manage separately a set of MIB(s) in different workflow instances. This avoids, in the case of a large set of MIBs, to manage a huge list of OIDs in the translation process by splitting the OIDs/MIBs across separate Workflow and exported files.



The result is the list of OIDs that were selected for the translation.



The generated file is visible in the repository.



Testing

We can now launch a snmp trap command with OID 1.3.6.1.2.1.1.6

```
snmptrap -v2c -c ubiquete 3.10.63.66 "" 1.3.6.1.2.1.1.6 1.3.6.1.2.1.1.6.0 s "Just here ABC"
```

Without the translation, the UI shows

Mar 02, 2023 5:24:17PM	<4>%VNOC-4-TrapSnmp(10): V=1 C=ubiquite sysUpTimeInstance=1887005 snmpTrapOID=1.3.6.1.2.1.1.6.0="Just here ABC"	4: WARNING	BLR161	Linux Centos VM - 35.177.97.79	TyrellCorp	Hide
tenant_id: BLR	device_mgmt_ip: 35.177.97.79					
man_id: 14020601	sec_node: 2104a3d63a51					
rawlog: <4>%VNOC-4-TrapSnmp(10): V=1 C=ubiquite sysUpTimeInstance=1887005 snmpTrapOID=1.3.6.1.2.1.1.6.0="Just here ABC"	_timestamp_epoch_: 167774259027					
source_ip:	_timestamp_: 2023-03-02T16:24:19.027245505Z					
hostname: ip-172-31-0-50	mod_id: 14020601					
orig: BLR161	customer_id: 6					
timestamp: 167774257757						

With the translation of 1.3.6.1.2.1.1.6 to sysLocation

Mar 02, 2023 5:29:10PM	<4>%VNOC-4-TrapSnmp(10): V=1 C=ubiquite sysUpTimeInstance=1916290 snmpTrapOID=sysLocation.1.3.6.1.2.1.1.6.0="Just here ABC"	4: WARNING	BLR161	Linux Centos VM - 35.177.97.79	TyrellCorp	Hide
tenant_id: BLR	device_mgmt_ip: 35.177.97.79					
man_id: 14020601	sec_node: 2104a3d63a51					
rawlog: <4>%VNOC-4-TrapSnmp(10): V=1 C=ubiquite sysUpTimeInstance=1916290 snmpTrapOID=sysLocation.1.3.6.1.2.1.1.6.0="Just here ABC"	_timestamp_epoch_: 167774551868					
source_ip:	_timestamp_: 2023-03-02T16:29:11.868410428Z					
hostname: ip-172-31-0-50	mod_id: 14020601					
orig: BLR161	customer_id: 6					
timestamp: 167774550810						

With a custom translation of 1.3.6.1.2.1.1.6 to MyCustomSysLocation

Mar 02, 2023 5:32:26PM	<4>%VNOC-4-TrapSnmp(10): V=1 C=ubiquite sysUpTimeInstance=1936135 snmpTrapOID=MyCustomSysLocation.1.3.6.1.2.1.1.6.0="Just here ABC"	4: WARNING	BLR161	Linux Centos VM - 35.177.97.79	TyrellCorp	Hide
tenant_id: BLR	device_mgmt_ip: 35.177.97.79					
man_id: 14020601	sec_node: 2104a3d63a51					
rawlog: <4>%VNOC-4-TrapSnmp(10): V=1 C=ubiquite sysUpTimeInstance=1936135 snmpTrapOID=MyCustomSysLocation.1.3.6.1.2.1.1.6.0="Just here ABC"	_timestamp_epoch_: 167774749900					
source_ip:	_timestamp_: 2023-03-02T16:32:29.900203910Z					
hostname: ip-172-31-0-50	mod_id: 14020601					
orig: BLR161	customer_id: 6					
timestamp: 167774748857						

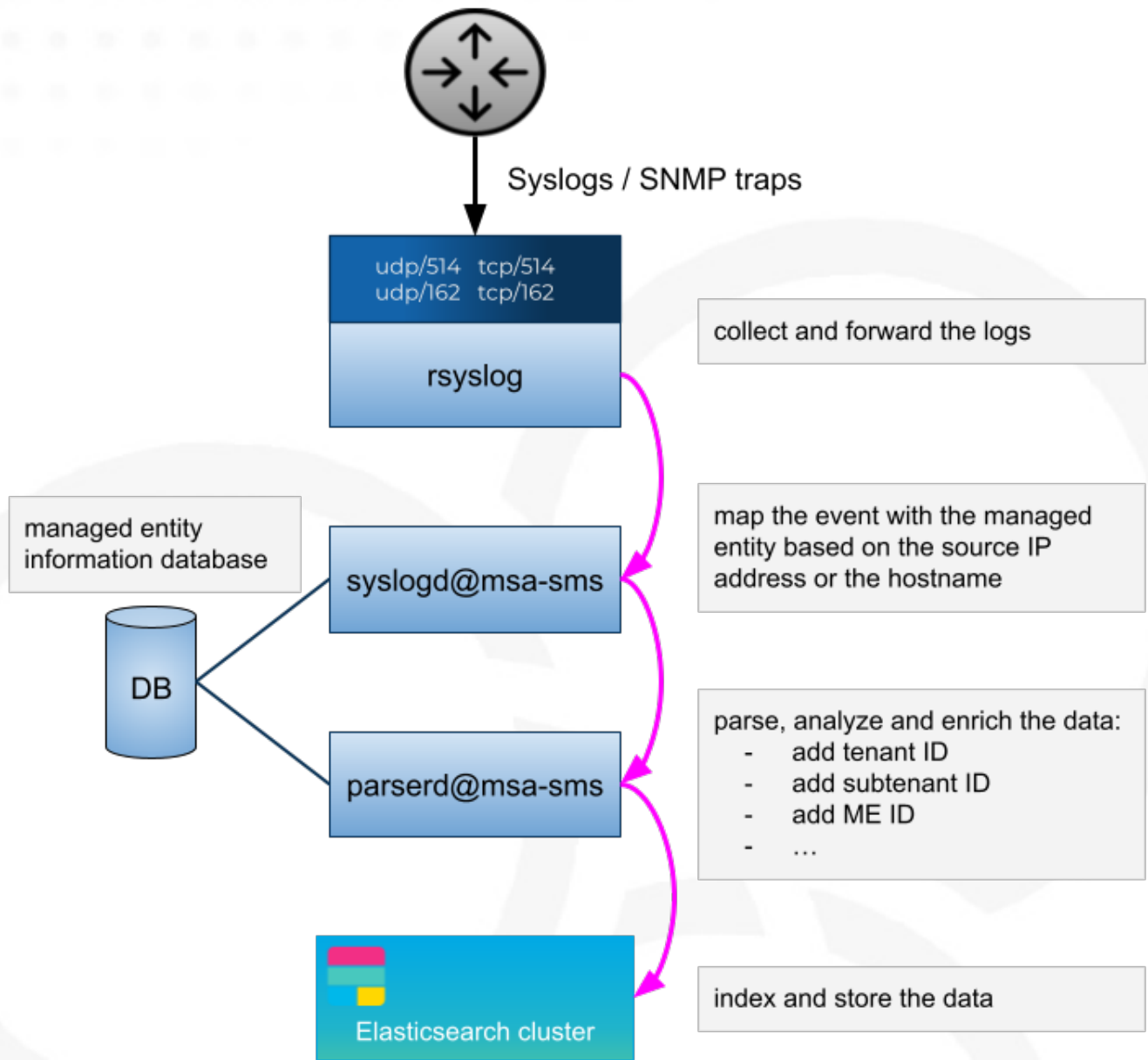
Log analytics

Overview

The MSactivator™ can collect, index and store events received from the managed entities. Once indexed, the logs are fully searchable from the user interface.

The diagram below shows the syslog processing steps from the device to Elasticsearch.

Syslog event flow



Search logs

To view and search the logs you can either access the global log and alarm view by clicking on the bell icon at the screen top right or by browsing to a specific managed entity and selecting the tab "Logs"

Log analytics screen

Timestamp	Message	Severity	Device ID	Customer Ref	Type	Subtype
May 07, 2021 3:23.08PM GMT+02:00	<189>date=2021-05-07 time=13:23:08 devname="FGTAWSRZL.D06V2D5" devid="FGTAWSRZL.D06V2D5" eventtime=162039378663787215 tz="+0000" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=185.156.74.17 srcport=49222 srcintf="port1" srcintfrole="undefined" dstip=172.31.0.129 dstport=3389 dstintf="root" dstintfrole="undefined" srccountry="Russian Federation" dstcountry="Reserved" sessionid=25788 proto=6 action="deny" policyid=0 policypolicy="local-in-policy" service="RDP" transid="nop" app="RDP" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=10 craction=262144 crlevel="medium"	S NOTICE	BLR127	TyrellCorp	traffic	local
May 07, 2021 3:23.07PM GMT+02:00	<189>date=2021-05-07 time=13:23:07 devname="FGTAWSRZL.D06V2D5" devid="FGTAWSRZL.D06V2D5" eventtime=1620393785703396369 tz="+0000" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=3.89.28.119 srcport=35202 srcintf="port1" srcintfrole="undefined" dstip=172.31.0.129 dstport=7946 dstintf="root" dstintfrole="undefined" srccountry="United States" dstcountry="Reserved" sessionid=25782 proto=6 action="deny" policyid=0 policypolicy="local-in-policy" service="tcp/7946" transid="nop" app="tcp/7946" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=10 craction=262144 crlevel="medium"	S NOTICE	BLR127	TyrellCorp	traffic	local
May 07, 2021 3:23.05PM GMT+02:00	<189>date=2021-05-07 time=13:23:04 devname="FGTAWSRZL.D06V2D5" devid="FGTAWSRZL.D06V2D5" eventtime=1620393784205622424 tz="+0000" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=89.248.165.203 srcport=58520 srcintf="port1" srcintfrole="undefined" dstip=172.31.0.129 dstport=13927 dstintf="root" dstintfrole="undefined" srccountry="Netherlands" dstcountry="Reserved" sessionid=25779 proto=6 action="deny" policyid=0 policypolicy="local-in-policy" service="tcp/13927" transid="nop" app="tcp/13927" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=10 craction=262144 crlevel="medium"	S NOTICE	BLR127	TyrellCorp	traffic	local
May 07, 2021 3:23.05PM GMT+02:00	<189>date=2021-05-07 time=13:23:03 devname="FGTAWSRZL.D06V2D5" devid="FGTAWSRZL.D06V2D5" eventtime=16203937840694849 tz="+0000" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=185.156.74.26 srcport=48440 srcintf="port1" srcintfrole="undefined" dstip=172.31.0.129 dstport=3389 dstintf="root" dstintfrole="undefined" srccountry="Russian Federation" dstcountry="Reserved" sessionid=25776 proto=6 action="deny" policyid=0 policypolicy="local-in-policy" service="RDP" transid="nop" app="RDP" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=10 craction=262144 crlevel="medium"	S NOTICE	BLR127	TyrellCorp	traffic	local
May 07, 2021 3:22.59PM GMT+02:00	<189>date=2021-05-07 time=13:22:59 devname="FGTAWSRZL.D06V2D5" devid="FGTAWSRZL.D06V2D5" eventtime=162039377967493454 tz="+0000" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=185.156.74.22 srcport=45504 srcintf="port1" srcintfrole="undefined" dstip=172.31.0.129 dstport=3389 dstintf="root" dstintfrole="undefined" srccountry="Russian Federation" dstcountry="Reserved" sessionid=25773 proto=6 action="deny" policyid=0 policypolicy="local-in-policy" service="RDP" transid="nop" app="RDP" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=10 craction=262144 crlevel="medium"	S NOTICE	BLR127	TyrellCorp	traffic	local
May 07, 2021 3:22.58PM GMT+02:00	<189>date=2021-05-07 time=13:22:58 devname="FGTAWSRZL.D06V2D5" devid="FGTAWSRZL.D06V2D5" eventtime=1620393778742147022 tz="+0000" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=185.156.74.26 srcport=3696 srcintf="port1" srcintfrole="undefined" dstip=172.31.0.129 dstport=3389 dstintf="root" dstintfrole="undefined" srccountry="Russian Federation" dstcountry="Reserved" sessionid=25772 proto=6 action="deny" policyid=0 policypolicy="local-in-policy" service="RDP" transid="nop" app="RDP" duration=0 sentbyte=0 rcvbyte=0 sentpkt=0 appcat="unscanned" crscore=10 craction=262144 crlevel="medium"	S NOTICE	BLR127	TyrellCorp	traffic	local

Dashboard

Dashboard will allow you to visualize the data store in Elasticsearch

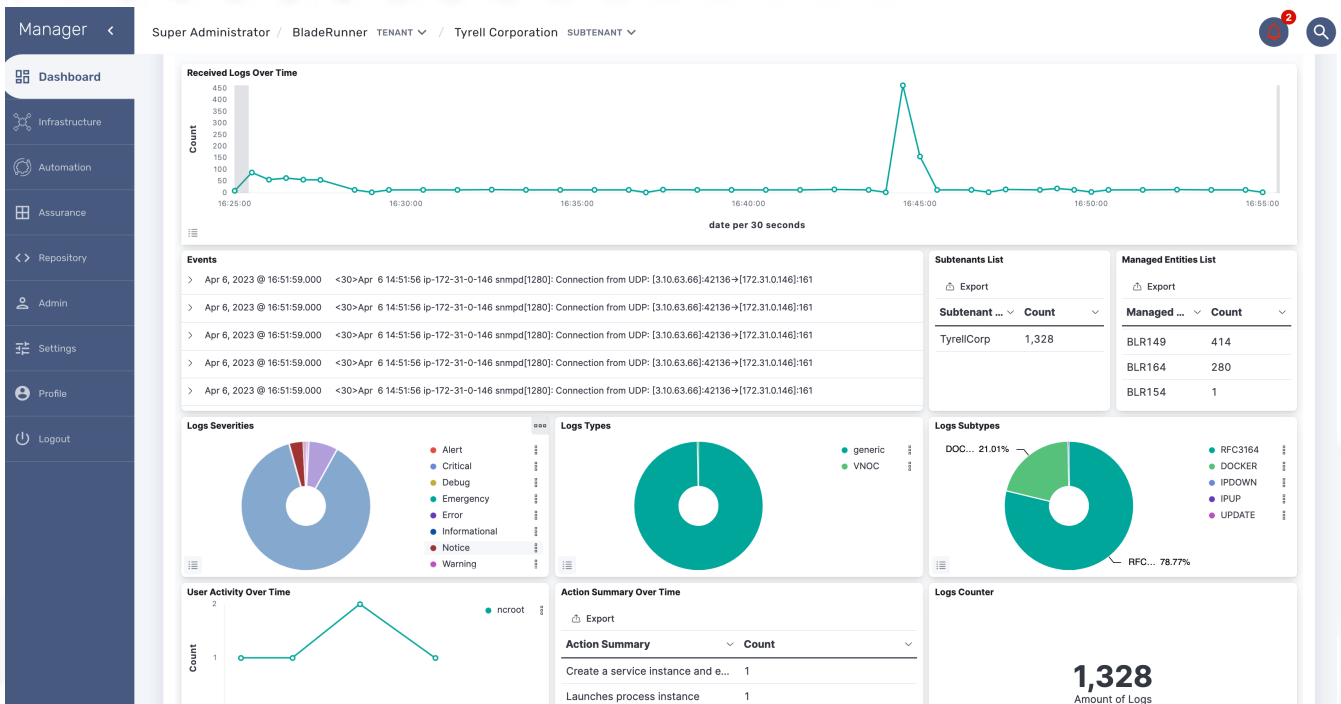
You can access Kibana on port 5601 (<https://localhost:5601/kibana>) and use Kibana to:

- discover the data indexed and stored in Elasticsearch
- create your own dashboard templates
- reuse or edit the dashboard included in the MSactivator™

Deploy an existing dashboard for a subtenant

You can use the workflow "Deploy Dashboard" to deploy the dashboards packaged in the MSactivator™.

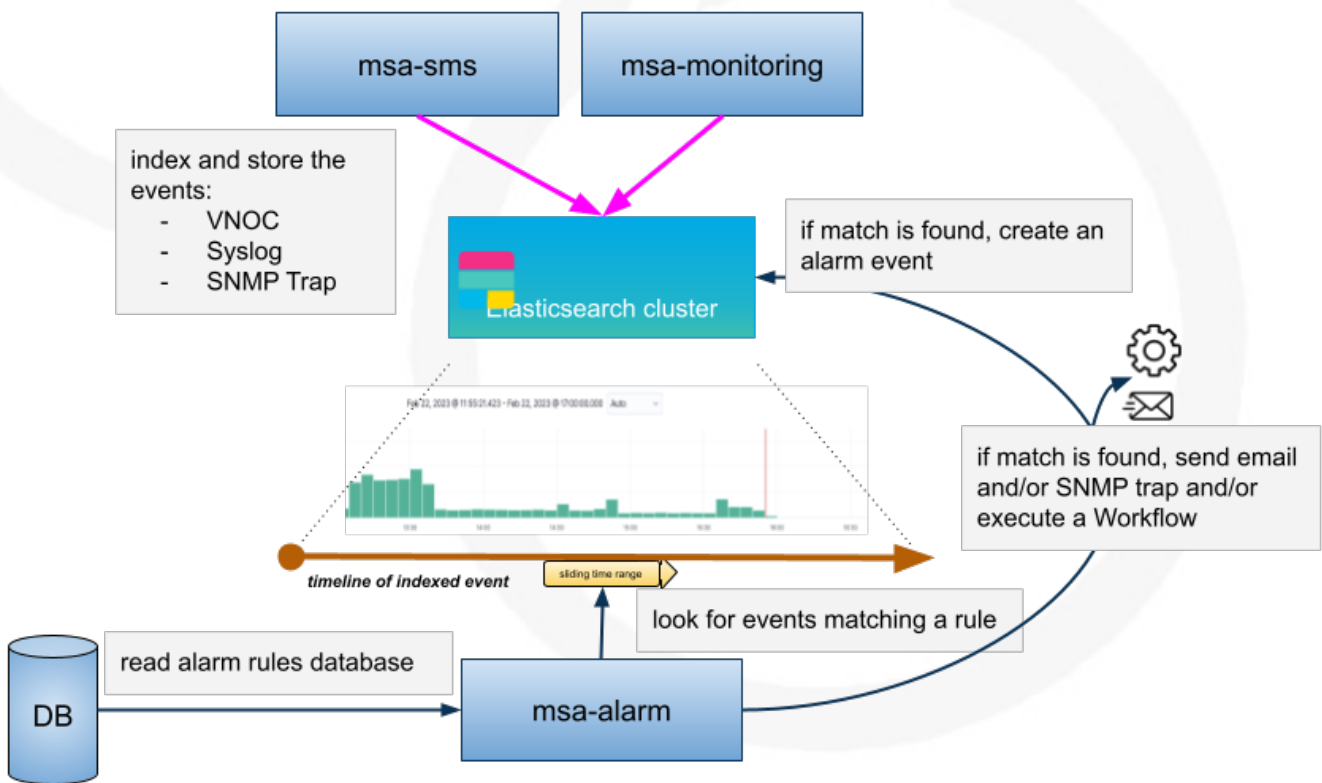
Use the Kibana URL from the workflow instance to browse to the Kibana dashboard



Alarm

Overview

The alarm management module is based on the detection of events which internal (VNOC), SNMP thresholds, or syslog sent by the managed devices and collected by the MSactivator™. Alarm management is designed to provide email notifications to customers or managers or administrator



The detection of events relies on rules configured at the super administrator level.

Rule management is available for the super administrator (ncroot). The rules are defined globally and can be modified by the operation team.

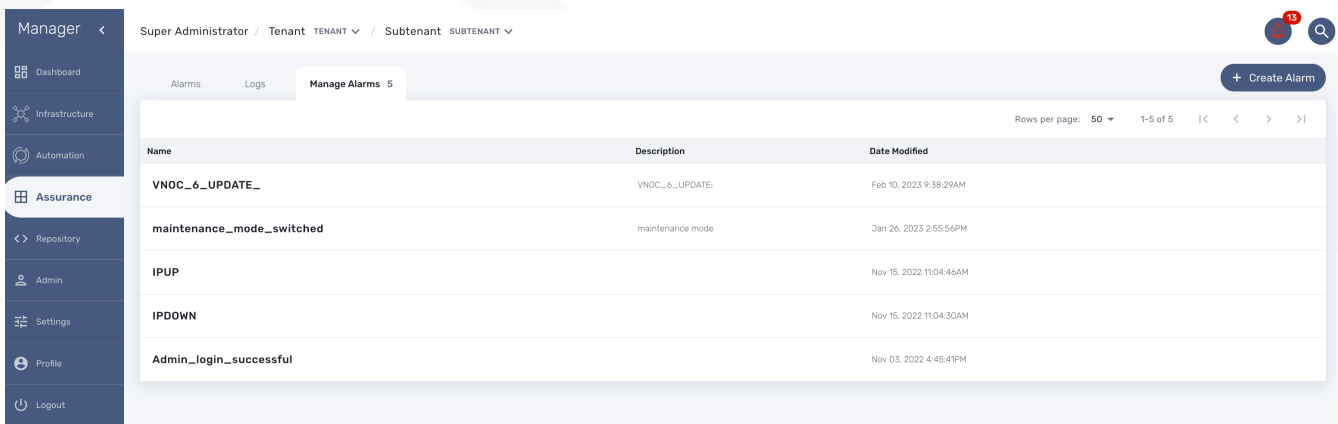
The infrastructure management team can modify the setting of the notifications on a per-event and/or per-subtenant basis. The rules are executed on a periodic basis (the period frequency can be configured) and alarms are generated whenever a rule matches.

Manage alarm rules

The Alarm management screen is available by clicking on the bell icon on the top right of the screen.

Alarm Rule can be created from the Manage Alarms tab, as show in the below screen shot. Alarm Name should be Unique across the MSactivator™ and it should not contain space.

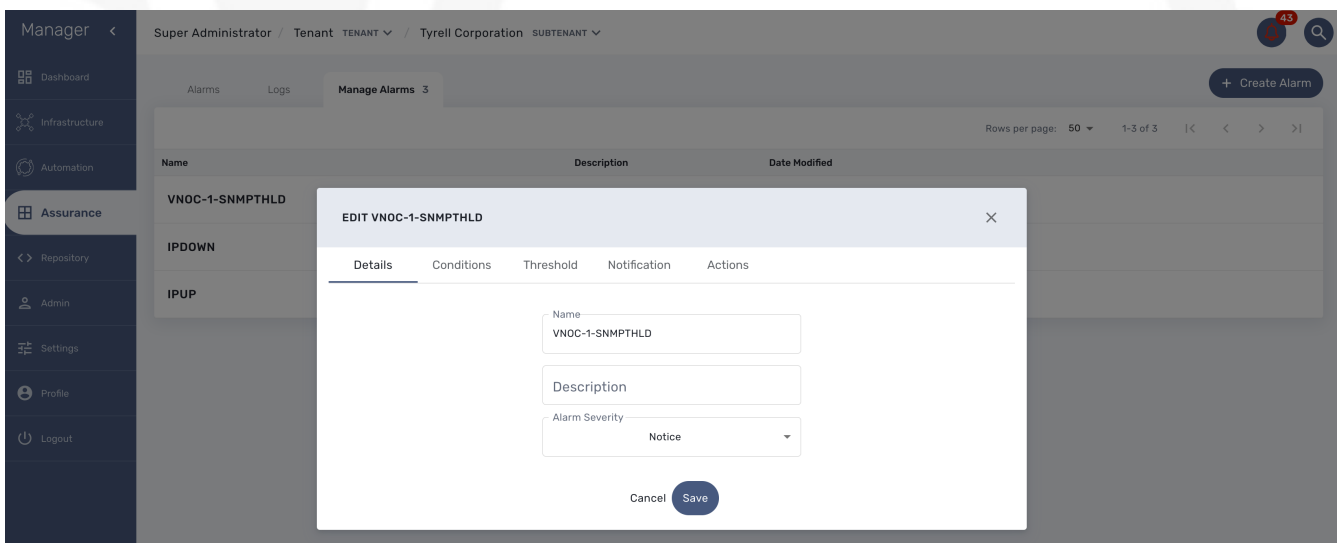
Alarm rule management screen



Create or edit an alarm

Alarm creation contains Four sections below

Create or edit an alarm



Detail

Provide a name for the alarm and the alarm severity.

Alarm severity selection will allow you to decide what will be the severity of the alarm.

Conditions

This is where we define the matching rules for the alarm.

Conditions string

A text that will be used to search in the incoming logs to generate an alarm.

Subtenant

If selected, the logs search for the alarm triggering will be considered only for the Manage Entity that belongs to that subtenant.

Manage entity

If selected, the logs search for the alarm triggering will be considered only for that Manage Entity.

Severity levels

If selected, an alarm will be triggered for the logs with only those Severities.

Threshold

Define the number of events and the time period to consider for triggering one workflow.

With the default value 0 log within 0 minute, no workflow process execution will be triggered so you need to set it at least as 1 log within 1 minute.

Notification

Select the user roles that will be notified by email when an alarm is raised.



make sure that you have set an email to your user

Actions

Choose the workflow and the process to execute when an alarm is triggered.

Alarm acknowledgement

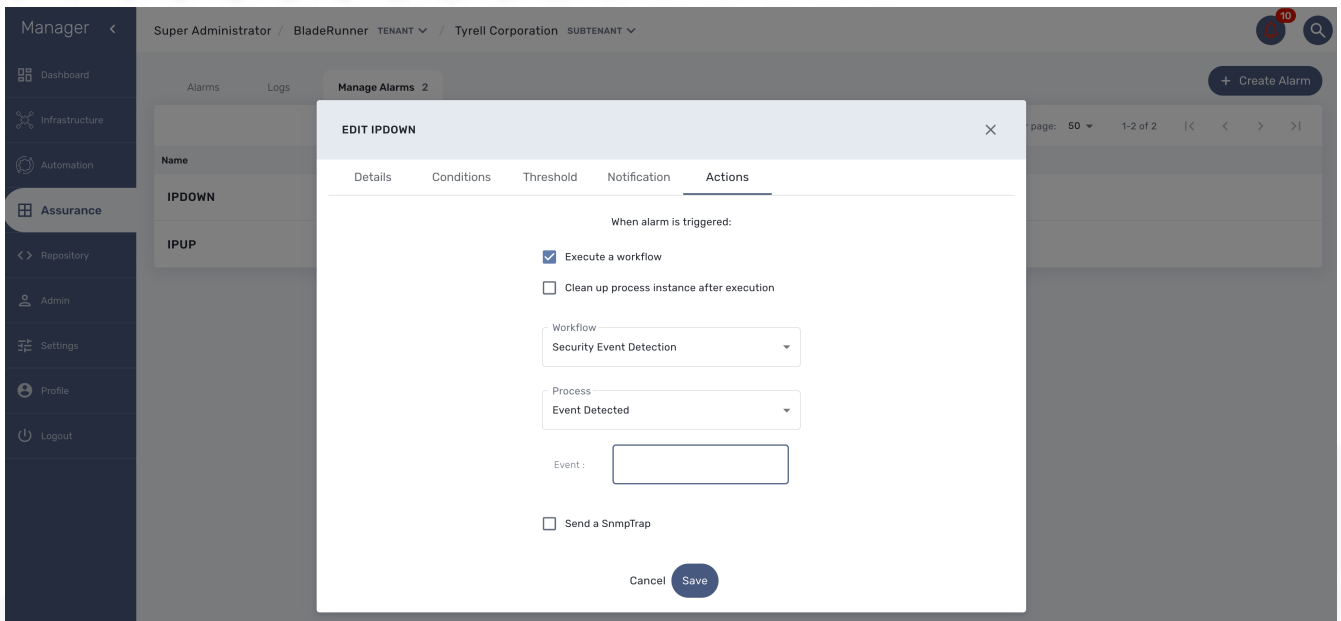
As soon as an event is detected to be an alarm, a notification badge will appear at the top right of the screen showing the number of new alarms that require a user action (acknowledgement).

You have the possibility to edit an alarm, add a comment and acknowledge the alarm.

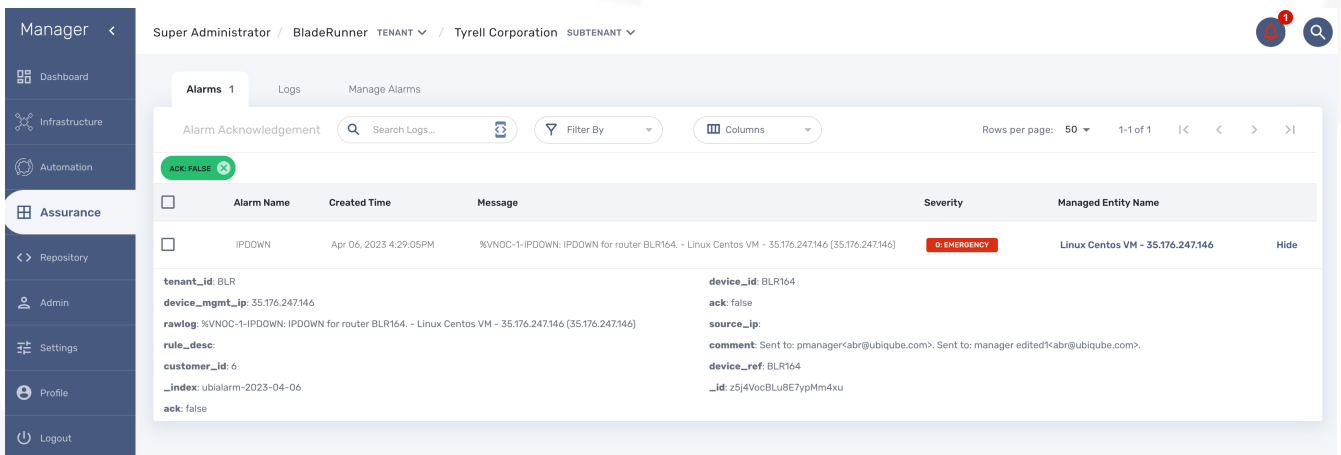
Testing

You can test the triggering of a process execution with the simple workflow "Security Event Detection" included in the mini-lab.

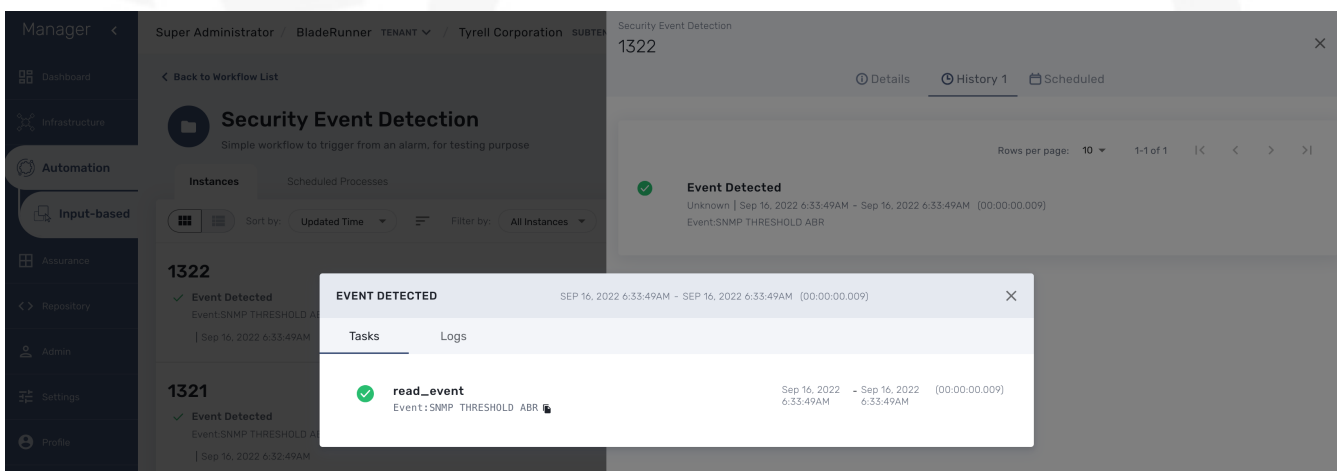
This workflow will execute a process to display the raw log that caused the alarm.



To trigger an event you can, for instance, stop one of the Linux container which will raise a IPDOWN event.



A new instance of the workflow should be created



Email alerting: SMTP configuration

For alarms to be notified as email, we need the Docker host to be properly configured as a SMTP server or relay.

Sample email

Alerts from BLR129 (linux_me_2) 172.20.0.102 ▷ Inbox x

msa@ubiquite.com

3:40 PM (0 minutes ago)

to abr ▾

Alerts generated by Linux Generic device BLR129 (linux_me_2) 172.20.0.102

Date: 2023-02-22T14:39:59+0000

Level: 1

Alert: %VNOG-1-IPDOWN: IPDOWN for router BLR129.

Reference: VNOG:IPDOWN

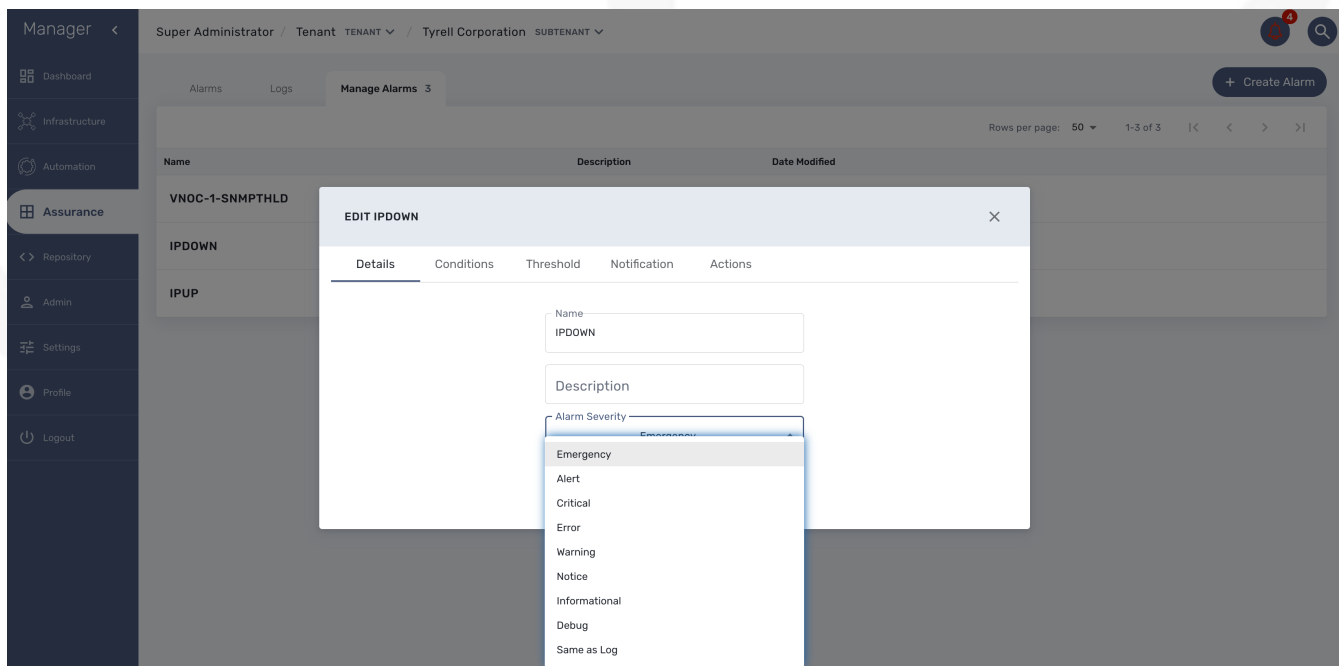
Event received:

%VNOG-1-IPDOWN: IPDOWN for router BLR129.

If you have any questions or inquiries, please reply in this mail with this case number [0yGReYYB4sT0y999II54].

Alarm severity tuning

An alarm severity can be tuned by choosing the severity of the alarm when editing the alarm rule.



By default the alarm severity is the same as the severity of the source event but by selecting the severity, you can decide that an event with a high severity level should raise an alarm with a low severity level (or the other way around).

Example: it is possible to have an alarm rule to detect the VNOG event IPDOWN and configure the rule to have the highest level (Emergency) and an other alarm rule to detect the event IPUP with a lower severity (Informational)

This is very useful if SNMP traps are configured to be sent as you may not want to have all the SNMP traps detected with the same severity level.

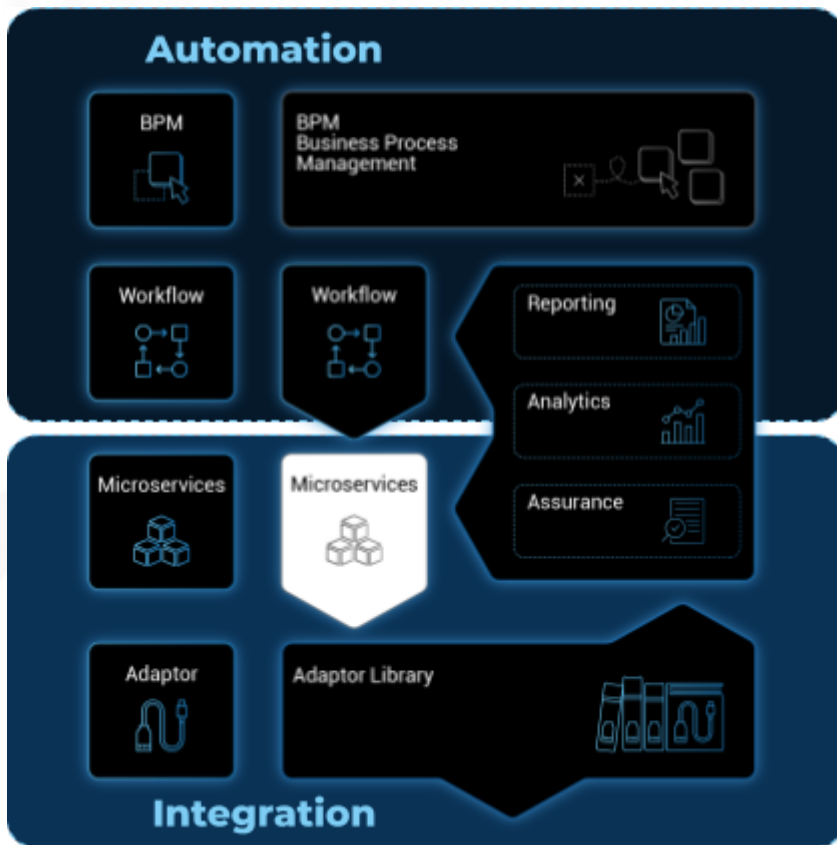
Alarms 4 Logs Manage Alarms

Alarm Acknowledgement Search Logs... Filter By Columns Rows per page: 50 1-4 of 4

ACK: FALSE

<input type="checkbox"/>	Alarm Name	Created Time	Message	Severity	Managed Entity Name	
<input type="checkbox"/>	IPDOWN	Apr 05, 2023 1:34:10PM	%VNOC-1-IPDOWN: IPDOWN for router BLR164. - Linux Centos VM - 35.176.247.146 [35.176.247.146]	EMERGENCY	Linux Centos VM - 35.176.247.146	Details
<input type="checkbox"/>	IPDOWN	Apr 05, 2023 1:30:15PM	%VNOC-1-IPDOWN: IPDOWN for router BLR159. - JUNOS_VSRX_5 (3.10.129.201)	EMERGENCY	JUNOS_VSRX_5	Details
<input type="checkbox"/>	IPUP	Apr 05, 2023 1:24:23PM	%VNOC-1-IPUP: IPUP for static router BLR159. The address is 3.10.129.201 - JUNOS_VSRX_5 (3.10.129.201)	NOTICE	JUNOS_VSRX_5	Details
<input type="checkbox"/>	IPUP	Apr 05, 2023 1:22:01PM	%VNOC-1-IPUP: IPUP for static router BLR164. The address is 35.176.247.146 - Linux Centos VM - 35.176.247.146 [35.176.247.146]	NOTICE	Linux Centos VM - 35.176.247.146	Details

Microservices



Microservices can be used to manage a wide variety of services on numerous types of devices, such as network equipment, virtualization infrastructure managers, or even Linux servers.

Overview

Any feature of any device can be managed with one or more microservices.

The MSactivator™ microservices engine is designed as an automation object-based programming language. Microservice designers define the variables and implement the Create | Read | Update | Delete method.

Such an open and agile approach is required to provide the abstraction layer on top of any device from the core to the edge.

The implementation of the functions allows us to create, update, or delete sub-parts of the configuration on our managed devices. A function can also be implemented to import the device configuration into the MSactivator™ configuration database.

Microservices can be used to manage a wide variety of services on numerous types of devices, such as network equipment, virtualization infrastructure managers, or even Linux servers.

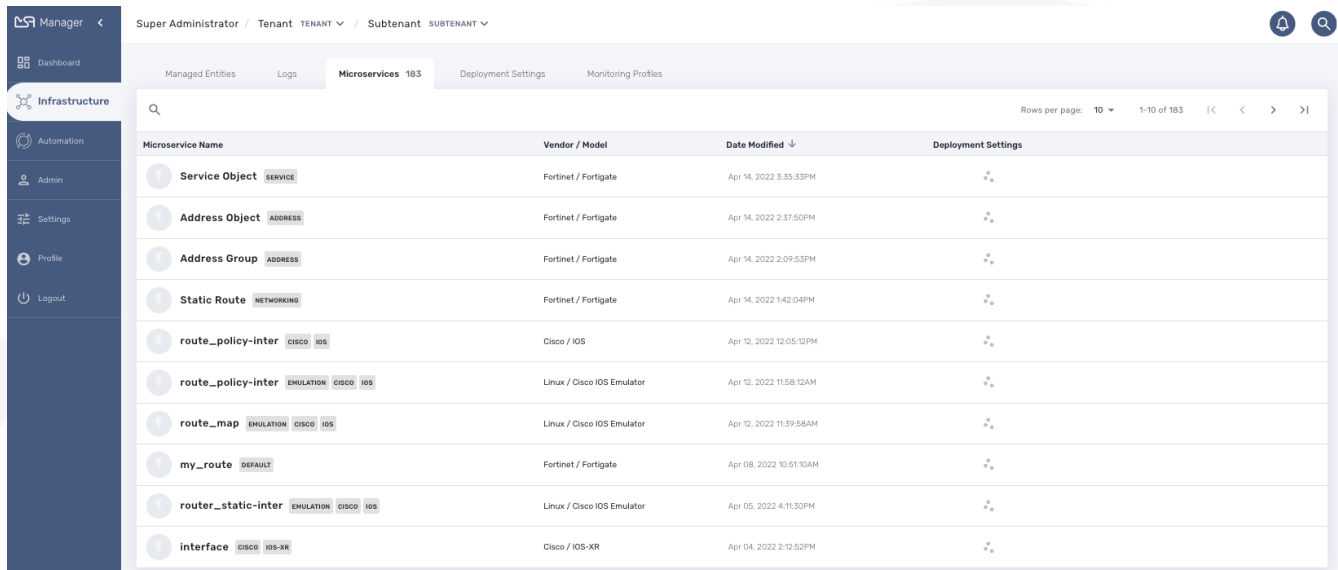
Microservices can be designed graphically in the MSactivator™ developer portal.

Scripting is not mandatory but simple programming functions, such as conditional statements, loops, and variable assignments, is available to incorporate advanced function behaviors.

Select microservices

The list microservices available can be viewed by clicking on the "Infrastructure" link from the left menu.

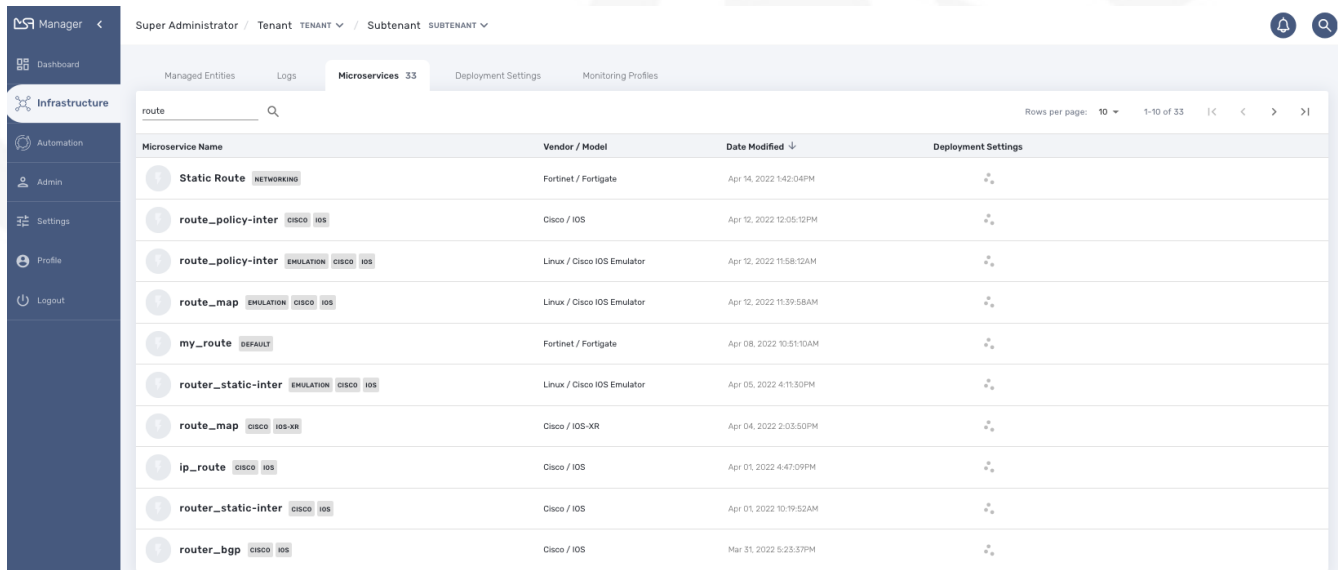
list the microservices available



Microservice Name	Vendor / Model	Date Modified ↓	Deployment Settings
Service Object <small>SERVICE</small>	Fortinet / Fortigate	Apr 14, 2022 3:35:33PM	
Address Object <small>ADDRESS</small>	Fortinet / Fortigate	Apr 14, 2022 2:37:50PM	
Address Group <small>ADDRESS</small>	Fortinet / Fortigate	Apr 14, 2022 2:09:53PM	
Static Route <small>NETWORKING</small>	Fortinet / Fortigate	Apr 14, 2022 1:42:04PM	
route_policy-inter <small>CISCO IOS</small>	Cisco / IOS	Apr 12, 2022 12:05:12PM	
route_policy-inter <small>EMULATION CISCO IOS</small>	Linux / Cisco IOS Emulator	Apr 12, 2022 11:58:12AM	
route_map <small>EMULATION CISCO IOS</small>	Linux / Cisco IOS Emulator	Apr 12, 2022 11:39:58AM	
my_route <small>DEFAULT</small>	Fortinet / Fortigate	Apr 08, 2022 10:51:10AM	
router_static-inter <small>EMULATION CISCO IOS</small>	Linux / Cisco IOS Emulator	Apr 05, 2022 4:11:30PM	
interface <small>CISCO IOS-XR</small>	Cisco / IOS-XR	Apr 04, 2022 2:12:52PM	

From this page you can search for a named microservice by using the search field with the magnifier icon.

search for microservices in the library



Microservice Name	Vendor / Model	Date Modified ↓	Deployment Settings
Static Route <small>NETWORKING</small>	Fortinet / Fortigate	Apr 14, 2022 1:42:04PM	
route_policy-inter <small>CISCO IOS</small>	Cisco / IOS	Apr 12, 2022 12:05:12PM	
route_policy-inter <small>EMULATION CISCO IOS</small>	Linux / Cisco IOS Emulator	Apr 12, 2022 11:58:12AM	
route_map <small>EMULATION CISCO IOS</small>	Linux / Cisco IOS Emulator	Apr 12, 2022 11:39:58AM	
my_route <small>DEFAULT</small>	Fortinet / Fortigate	Apr 08, 2022 10:51:10AM	
router_static-inter <small>EMULATION CISCO IOS</small>	Linux / Cisco IOS Emulator	Apr 05, 2022 4:11:30PM	
route_map <small>CISCO IOS-XR</small>	Cisco / IOS-XR	Apr 04, 2022 2:05:50PM	
ip_route <small>CISCO IOS</small>	Cisco / IOS	Apr 01, 2022 4:47:09PM	
router_static-inter <small>CISCO IOS</small>	Cisco / IOS	Apr 01, 2022 10:19:52AM	
router_bgp <small>CISCO IOS</small>	Cisco / IOS	Mar 31, 2022 5:23:37PM	

From this page you can create or edit microservices - which is part of microservice design (cf. section below).

The list of microservice can be sorted by name, vendor/model, last update date and number of deployment settings.

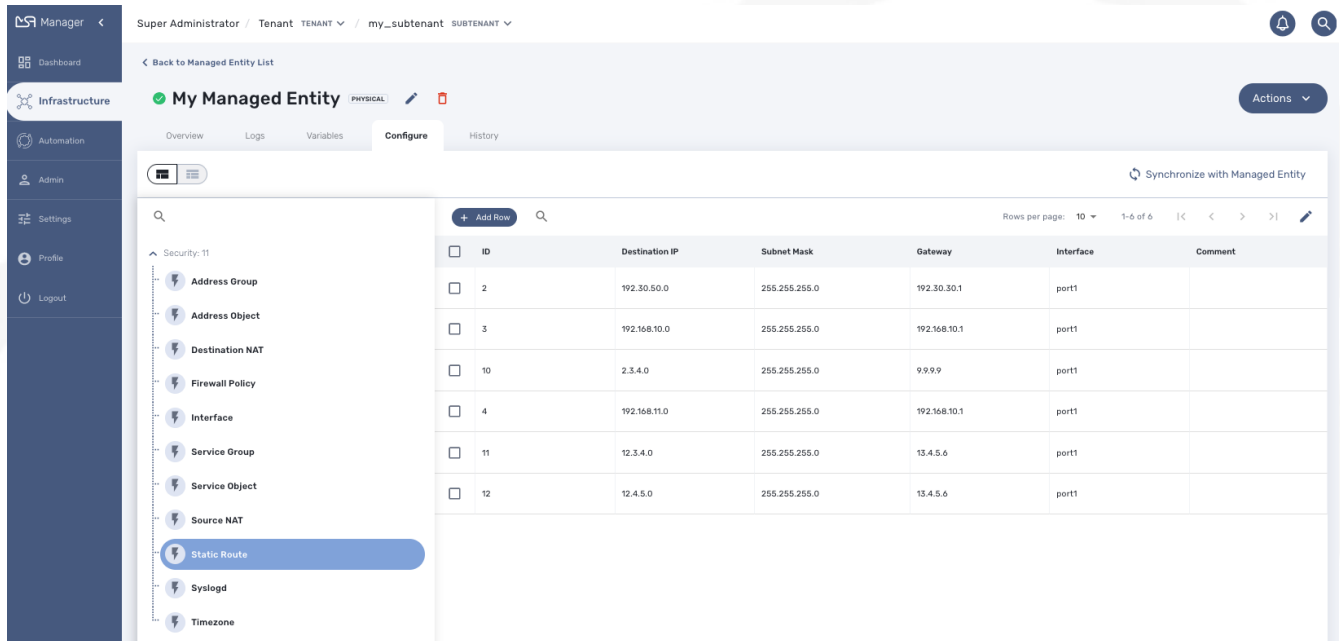
In order to use a microservice, it has to be associated to a managed entity via a deployment setting.

Microservice console

With the microservice console you will be able to use the microservices associated to a managed entity to configure the managed entity.

To access the console, select the managed entity and browse to the tab "Configure"

Microservice console



Calling the Microservice functions

Import

Click on "Synchronize With Managed Entity" to call the Import functions of the Microservices associated to the Managed Entity

Create

Select a Microservice on the left menu. If the Create function of the Microservice is implemented, you can use the button "+ Add Row".

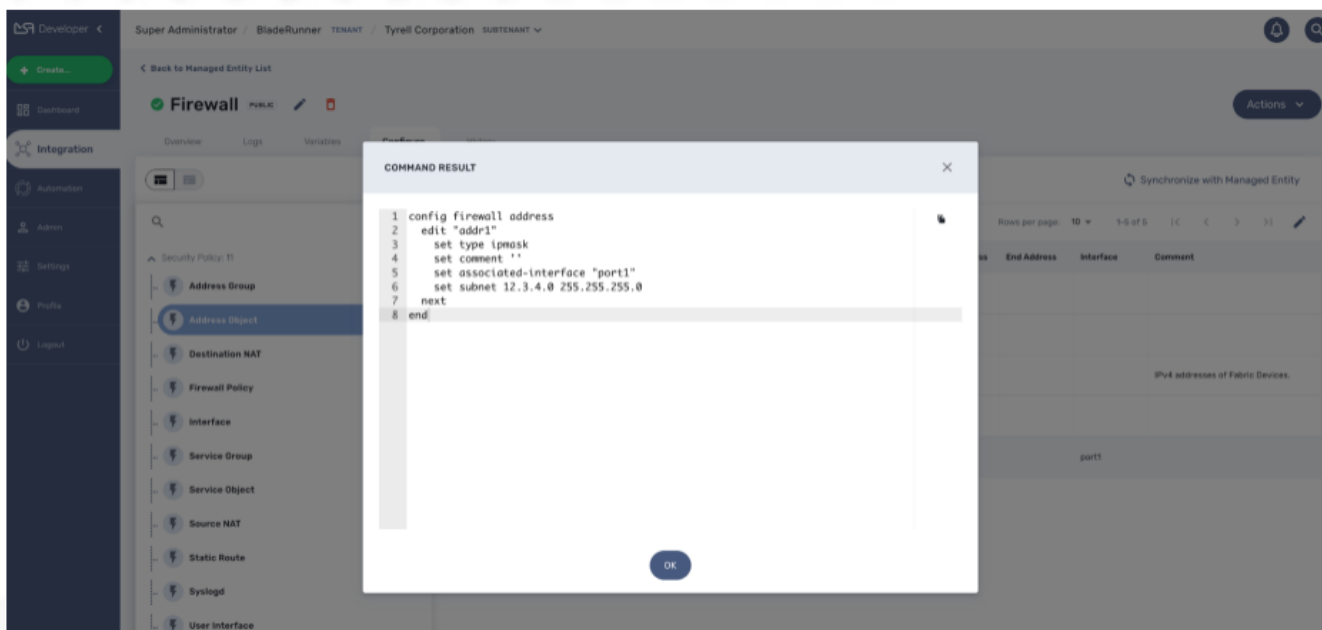
Use the form to provide the values to use and click "Save" to record the value in the execution OpenStack

Update and Delete

Select a Microservice on the left menu and select a Microservice instance to update or delete. A button "Edit" or "Remove" will be displayed if the UPDATE or the DELETE function is implemented for the Microservice.

Read

Select a Microservice on the left menu and select a Microservice instance to read. A button "Read" will be displayed if the READ function is implemented for the Microservice.



The read should be implemented by a Smarty template to generate a text file based on the microservice variable read in the database.



read more about this in the developer guide.

Execute the Microservice

You can stack multiple Create, Update and Delete orders for multiple Microservices. Once you are finished, you can either discard the changes or apply the changes.

If you discard the changes, the current order stack will be erased.

If you apply the changes, the configuration engine will go through the stack and apply the changes one by one on the Managed Entity.

Bulk Operations

With version 2.8.0, it is possible to execute bulk operations on the microservices.

Bulk operations allow you to select multiple instance to delete or update or create multiple instances.

Microservice bulk operation usually requires that some variables are configured to allow "Primary Composite Key". This is done by setting the parameter "Primary Composite Key" to true in the advanced parameter tab of the variable.

Primary Composite Key

In order to allow to bulk update a variable, the "Primary Composite Key" should be enabled for the variable.

When "Primary Composite Key" is enabled, you can assign multiple values to the variable field when creating or updating a microservice by clicking on the button "Edit Keys".



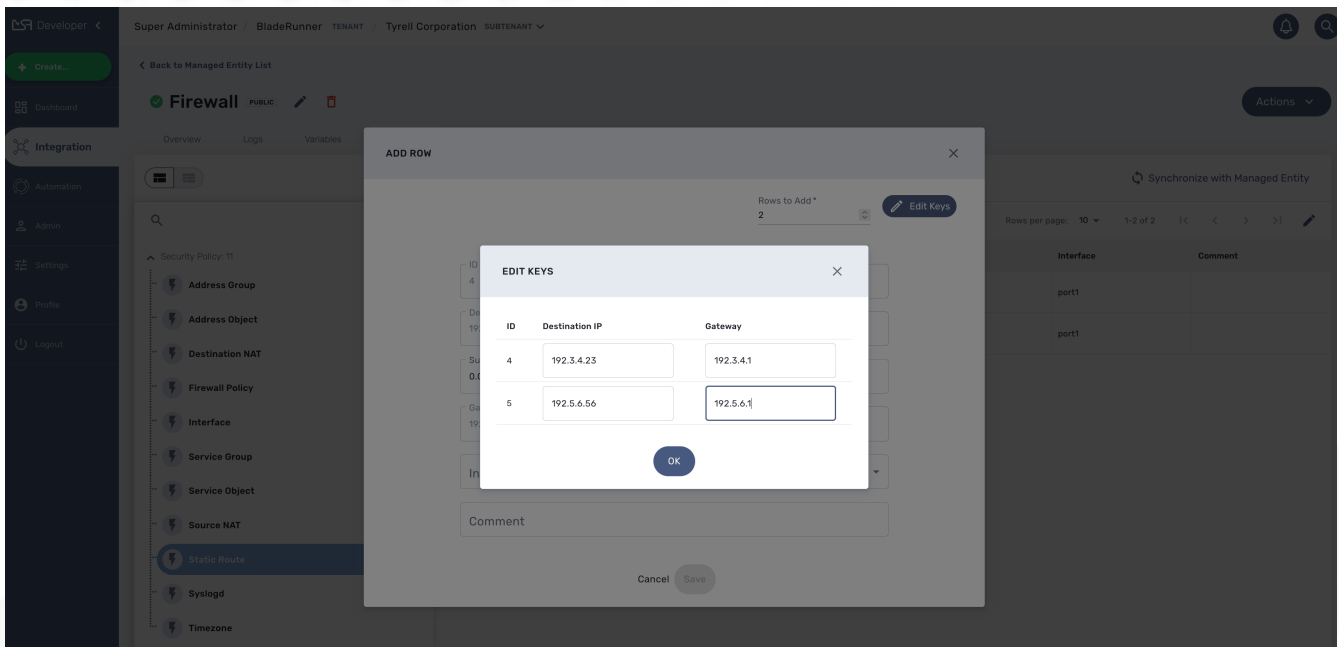
a composite key variable can only be edited by clicking on "Edit Keys" as the form input field is not editable in the parent screen.

Bulk creation

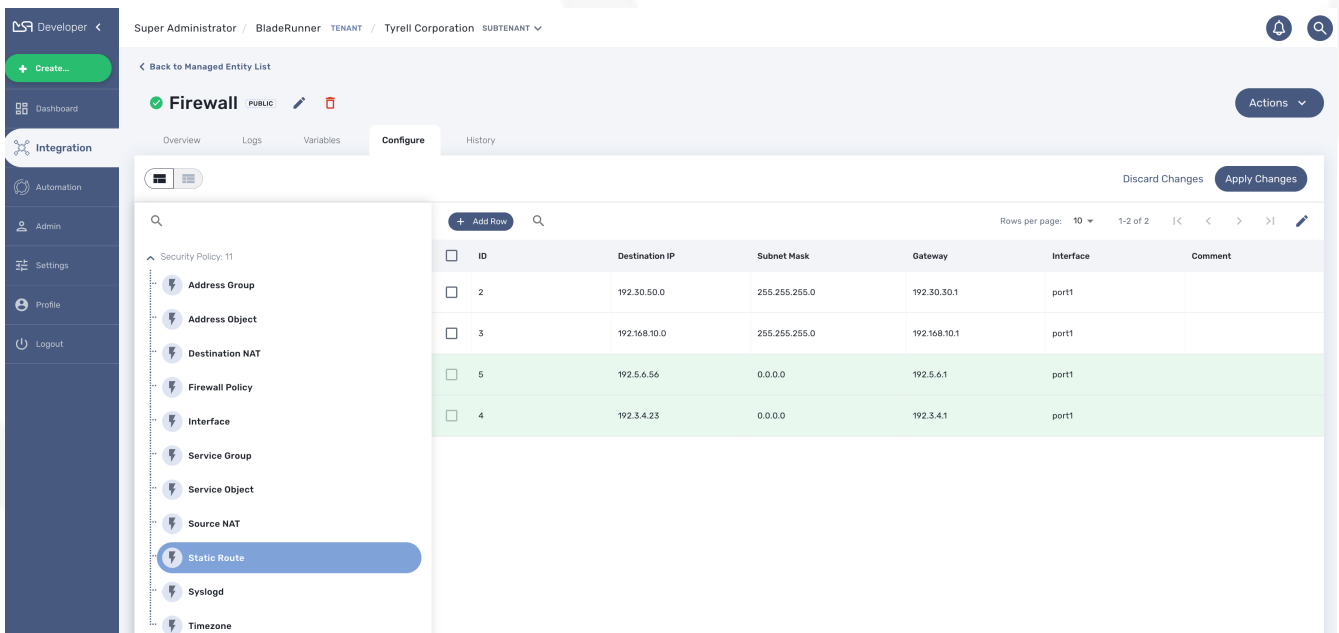
Select a microservice in the managed entity tab "Configure".

The microservice should have its Create function implemented with the "+ Add Row" button visible.

Click on "+ Add Row", by default the user form allows to create one instance. You can create more instances by changing the number of rows to add. This will show the button "Edit Keys".



Click on OK and save the form parameter.



You can create multiple instances for several microservice and once you are done, click on "Apply Changes" to trigger the configuration on the CoreEngine.

Bulk update

You can select multiple microservice instances and click on the edit button to change the parameters of these instance.



bulk edition can only be done on variables that are not set as primary composite key.

Bulk delete

Similarly as the update you can select multiple instances and delete them by using the "Remove"

button.

Microservice design

Microservice design is documented in the developer guide.



Deployment Settings

Deployment Settings will allow you to build your configurations and apply them to your managed entities.

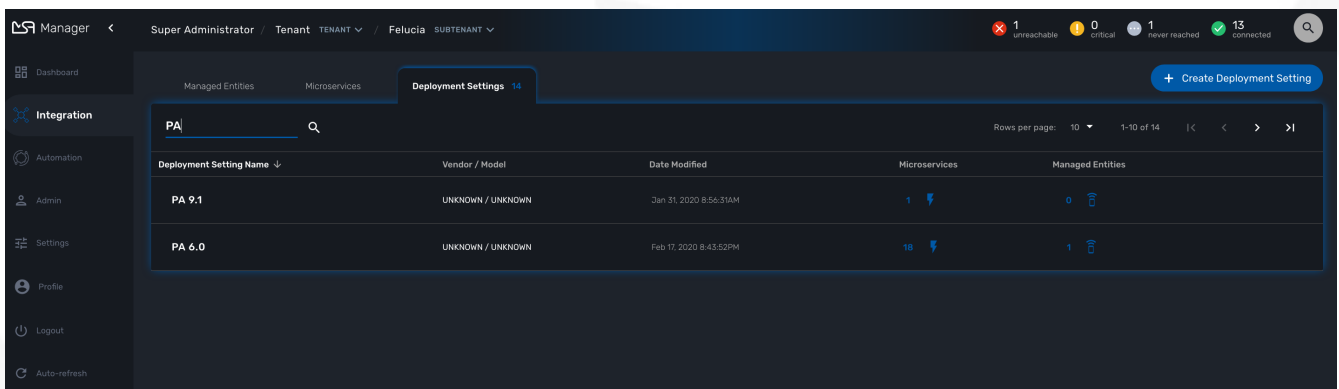
Deployment Settings will also ease any change to your configurations: you can add/remove a template or a microservice and be assured that the change will be applied in a consistent way across all your managed entities.

When using a deployment setting, you can ensure that your managed entities, associated with the deployment setting, have the same list of microservices, thus are all similar with regard to their managed services.

How to use deployment

You can view the deployment settings by clicking the "Integration" link on the left menu and select the tab "Deployment Settings"

This page shows the list of deployment settings, sortable and searchable by name.



The screenshot shows the Manager interface with the following data in the Deployment Settings table:

Deployment Setting Name	Vendor / Model	Date Modified	Microservices	Managed Entities
PA 9.1	UNKNOWN / UNKNOWN	Jan 31, 2020 8:56:31AM	1	0
PA 6.0	UNKNOWN / UNKNOWN	Feb 17, 2020 8:43:52PM	18	1

A Deployment setting acts as the intermediate layer between a set of managed entities and a set of microservices

Create, update, delete

Creation

To create a deployment setting you need to browse to the "Integration" panel, select the tab "Deployment Settings" and click on "+ Create Deployment Setting".

The first tab "Information" will let you set a name, an external reference, and vendor/model couple and optionally add a comment.

If you haven't selected a tenant and a subtenant yet, then you can do it at this stage.

The second tab is for selecting the microservices, the list is based on the vendor/model selected previously. If the list is empty it means that your repository doesn't have any microservice compatible with the vendor selected.

The third tab will let you select the managed entities that will be using the microservices. You can select several managed entities, only the ones from the subtenant, with the same vendor will be available.

Update

You can edit a deployment setting and change its configuration but the vendor/model selected at the creation time can't be changed. This will enforce consistency within your system.

Delete

You can delete a deployment setting any time. When you delete a deployment setting, the microservices won't be available to the managed entity but any configuration previously fetched from the managed entity will still be stored in the database.

External reference

When you save a new deployment setting, the information is stored in the database and a unique ID is assigned to this deployment setting. As it's commonly done in most applications, the database ID is immutable but there are cases where you need to be able to use your own unique identifier to identify a deployment setting (this also applies to managed entities for instance). For instance when integrating with a third party system with API it's convenient to decide on a common unique value to identify an object.

This is what external reference is made for. You can set it to your own value as long as it's unique in the {\$product_name} database.

Access Control

The scope of a deployment settings is the subtenant. In order to view the existing deployment settings you need first to select a subtenant. Once selected as shown below, this enables the user to change those settings appropriately.

Topology

The topology view is available on the portal and provides a graphical view of your network.

Topology view

The topology view is available in the "Infrastructure" section of the web user interface, in the tab "Managed Entities".

When you browse to the topology view for the first time, the topology will be calculated automatically based on the L3/SNMP topology mode (see below).

You can refresh the topology view, for instance after your infrastructure has been updated by clicking on the refresh button on the top right corner of the topology canvas.

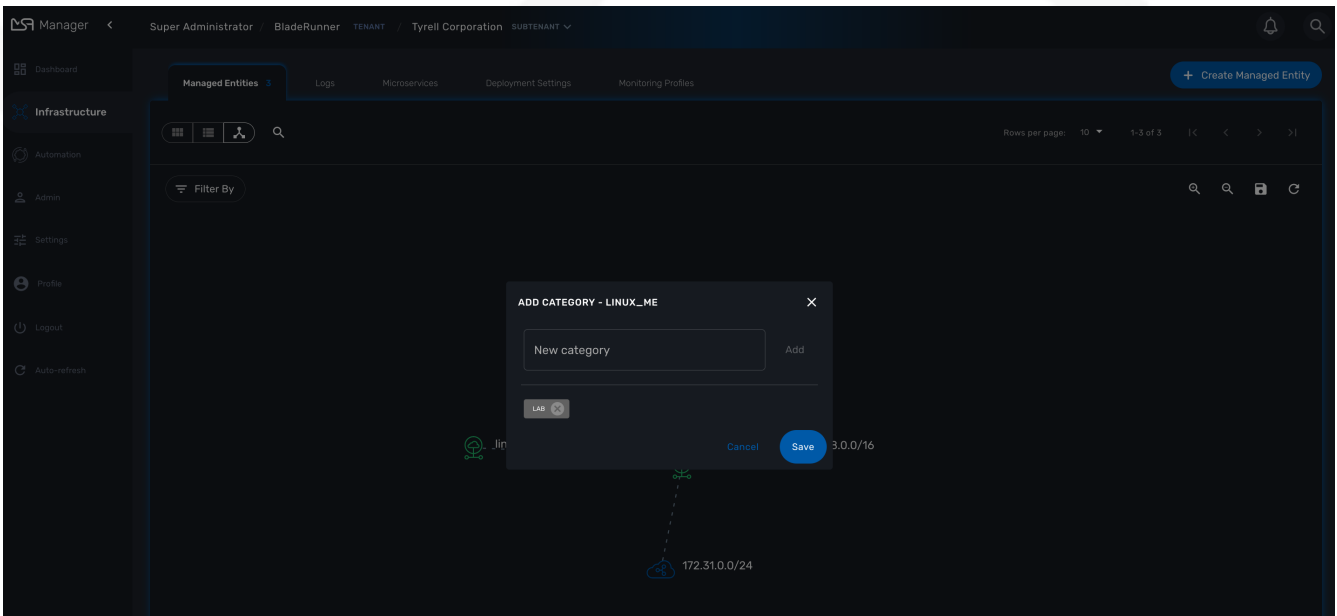
You can also zoom in and out and re-arrange the layout of the nodes by dragging them with your mouse.

If you want to persist the layout, you can save the topology with the save button on the top right corner of the topology canvas.

Managed Entity categories

On the topology view you can right-click on a managed entity icon and add categories to the managed entity.

This is useful to organize your infrastructure elements.

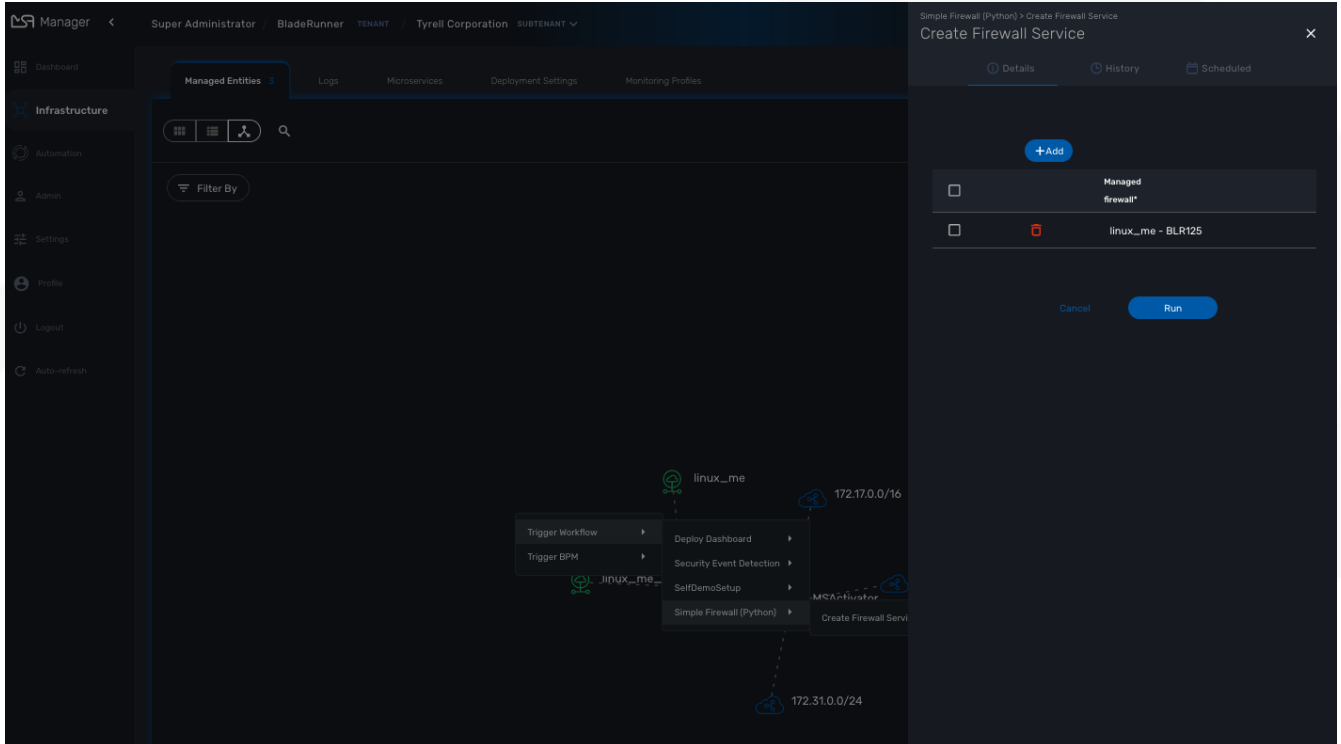


Use the "Filter By" action to filter your topology view and only display the elements you are interested in.

Workflow and BPM launcher

If you right-click anyway on the topology canvas, a contextual menu will pop-up and from there you have the possibility to trigger the execution of a workflow or a BPM.

This is a useful shortcut when you need to run some automated processes based a visual display of your infrastructure.



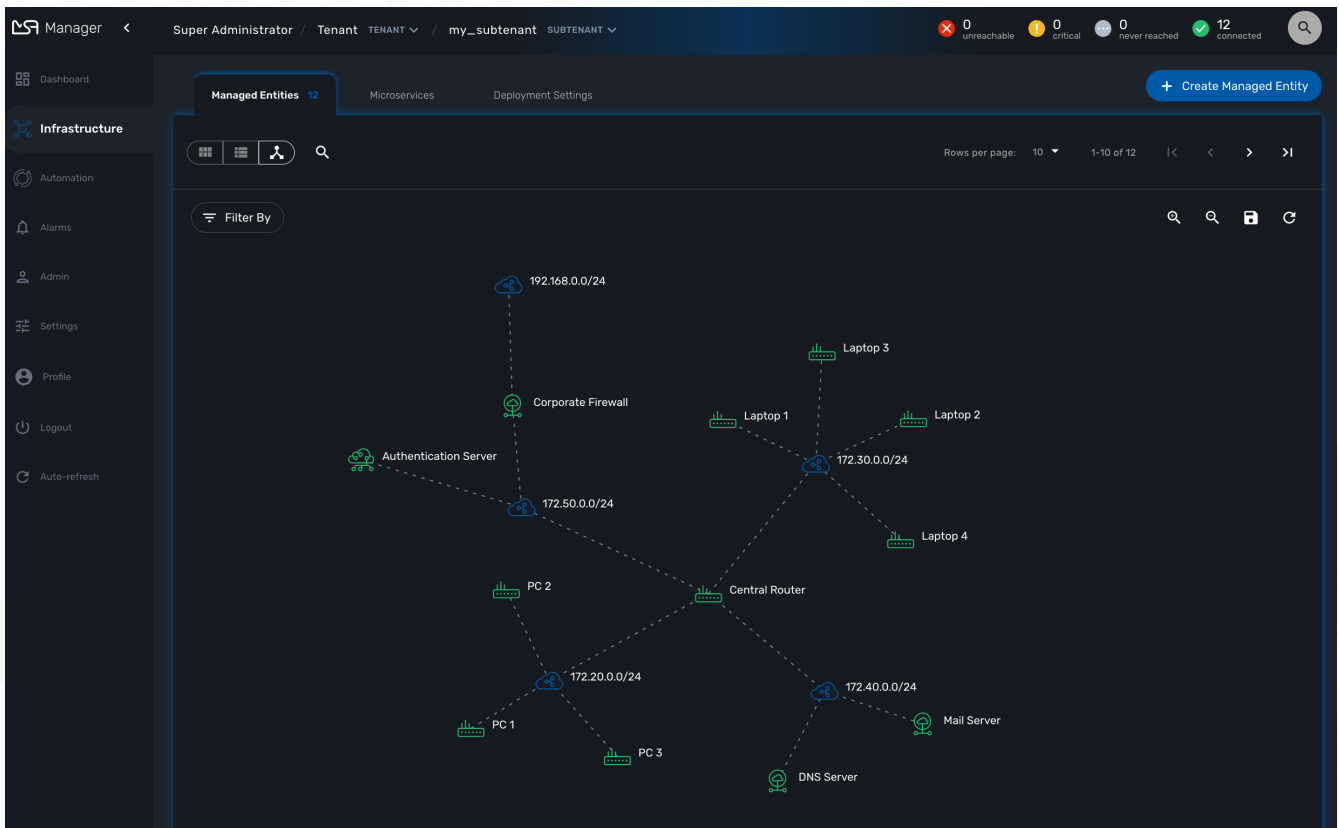
Topology types

2 types are available to build and display the topology view:

- Layer 3 view based on SNMP
- Layer 2 view based on VLAN

SNMP

The L3 SNMP mode relies on SNMP request to the managed entities to build the topology graph.



Prerequisites

SNMP must be enabled on the managed entities with a read-only community. The community must also be set on the managed entity on the `{${product_name}} managed entity form`.

How it works

The topology is calculated by a workflow [Topology](#). This workflow is automatically associated with the current subtenant when you browse to the topology screen in the "Infrastructure" section.

When you load or refresh the topology, the workflow will either create a new instance or update the last one that was created. It will loop through each managed entity of the subtenant and execute the CLI command below for each one.

```
snmpwalk -v2c -c <community> <address> IP-MIB::ipAdEntNetMask
```

The SNMP mode will rely on the CLI command `snmpwalk -v2c -c <community> <address> IP-MIB::ipAdEntNetMask` to get the list of IP addresses and network masks from the [IP MIB object](#).

```
ipAdEntNetMask OBJECT-TYPE
```

```
SYNTAX      IpAddress
```

```
MAX-ACCESS  read-only
```

```
STATUS      deprecated
```

```
DESCRIPTION
```

```
"The subnet mask associated with the IPv4 address of this
entry. The value of the mask is an IPv4 address with all
the network bits set to 1 and all the hosts bits set to 0."
```

```
::= { ipAddrEntry 3 }
```

For each managed entity, the topology workflow will get the list of IPv4 addresses of this MIB entry and it will build a data structure, stored in the {product_name} workflow database, to represent the topology as a graph with links and nodes.

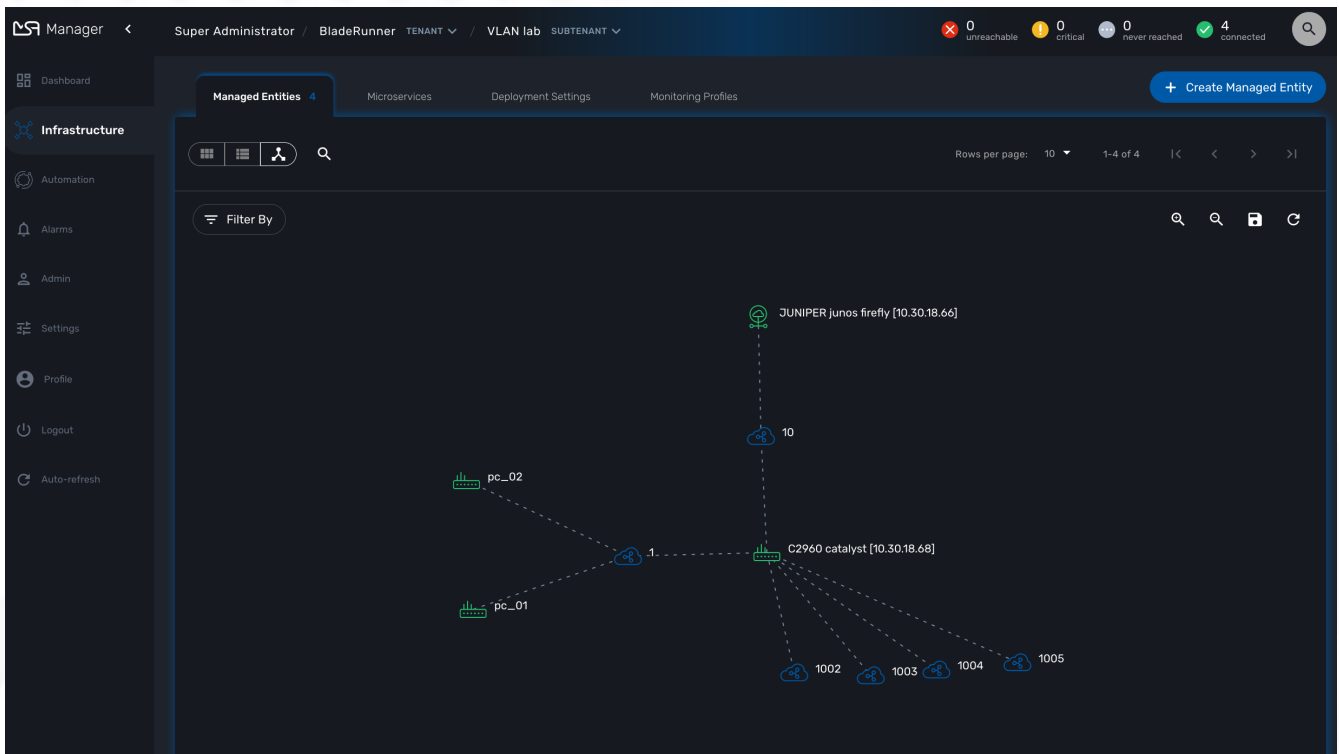
```
$cmd = "snmpwalk -v2c -c $community $address IP-MIB::ipAdEntNetMask 2>&1";  
exec($cmd, $value, $error);  
①  
if (!$error) {  
    foreach ($value as $search) {  
        if (searchAddress($search, $matches) != false) {  
            if ($matches [1] [0] != 127) {  
                $address_link = $matches [0] [0];  
                $maskAdr = $matches [0] [1];  
                $mask = calcMask($maskAdr);  
                $address_link_masked = getNetworkByAddressAndMask($address_link,  
$mask);  
  
                $addressAndMask = $address_link_masked . "/" . $mask;  
                createTopologyNetwork(str_replace(".", "_", $addressAndMask),  
$addressAndMask, "network", ""); ②  
                $context ['Nodes'] [$nodePlace] ["link"] [] ["id"] = $addressAndMask;  
            }  
        }  
    }  
} else {  
    logToFile($value, "Error : $value \n");  
}
```

- ① execute the snmpwalk command to list the IP addresses and masks
- ② create the topology links with the CIDR as the identifier

VLAN

The VLAN mode provides a layer 2 view of your infrastructure.

To generate this view you need first to create a new instance of the topology workflow and select "VLAN" for the topology type. Once this is done you will see the layer 2 topology in the topology screen of the infrastructure.



Prerequisites

The VLAN topology relies on microservices to get the vlan of you managed entities for a selected subtenant. It's therefore mandatory to have a microservice attached to every managed entity you need the vlan information for.

The microservice for vlan should have the following characteristics:

- be defined in a microservice file named vlan.xml
- the variable object_id should be set to the vlan ID

Any other variable such as the vlan name can be defined in the microservice for configuration purposes but it will not be used to generate the topology view.

A few examples are available on Github:

- [Linux](#)
- [Juniper JunOS](#)
- [Cisco Catalyst IOS](#)

How it works

When you load or refresh the topology, the topology workflow will either create a new instance or update the last one that was created. It will loop through each managed entity of the subtenant and import the vlan information based on the microservice implementation of the IMPORT function.

For example, with a linux based switch, the regex `:\svlan_(?<object_id>w+):\s\S+\s\S+\s\S+\s+\S+\s\S+\s\S+\s\S+\s(?<state>w+)` will be applied to the result of the CLI command `ip a`:

```
# ip a | grep vlan
4: eth4.200@eth4: <BROADCAST,MULTICAST,UP,LOWER_UP100> mtu 1500 qdisc noqueue master
vlan_200 state UP qlen 1000
5: vlan_default: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
qlen 1000
6: vlan_100: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP qlen
1000
7: vlan_200: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP qlen
1000
15: eth4@if16: <BROADCAST,MULTICAST,UP,LOWER_UP100,M-DOWN> mtu 1500 qdisc noqueue
master vlan_default state UP
41: eth1@if42: <BROADCAST,MULTICAST,UP,LOWER_UP100,M-DOWN> mtu 1500 qdisc noqueue
master vlan_default state UP
43: eth2@if44: <BROADCAST,MULTICAST,UP,LOWER_UP100,M-DOWN> mtu 1500 qdisc noqueue
master vlan_default state UP
45: eth3@if46: <BROADCAST,MULTICAST,UP,LOWER_UP100,M-DOWN> mtu 1500 qdisc noqueue
master vlan_100 state UP
#
```

and the result of the import will be 3 vlans, 100, 200 and default.

For non-linux managed entities the process to export the vlan information will be different but a similar result will be stored in the database and used by the workflow to build the data structure to represent the topology.

The code to build the topology node information will resemble to

```
foreach ($vlans as $vlan) {
    $vlan_id = $vlan->object_id;           ①
    createTopologyNetwork($vlan_id, $vlan_id, "network", "");           ②
    $context ['Nodes'] [$nodePlace] ["link"] [] ["id"] = $vlan_id;
}
```

① get the value of the microservice variable `object_id`. It's expected to be the vlan ID.

② create the topology link with the vlan ID

Create you custom topology

You can create your own topology view, either based on an existing one or you can create a completely new one based on the specifics of your infrastructure.

Here are the steps to add a new topology `my_topology` to your `{product_name}`

Step 1: prepare your development environment

The topology workflow is located under `/opt/fmc_repository/OpenMSA_WF/` in the container `msa_dev`, it's a git repository so you also need to make sure that it is up to date with `git status` and update your local repository with `git pull origin master` to get the latest updates.

Under `/opt/fmc_repository/Process`, there is a symlink to the git repo: `Topology` → `../OpenMSA_WF/Topology`

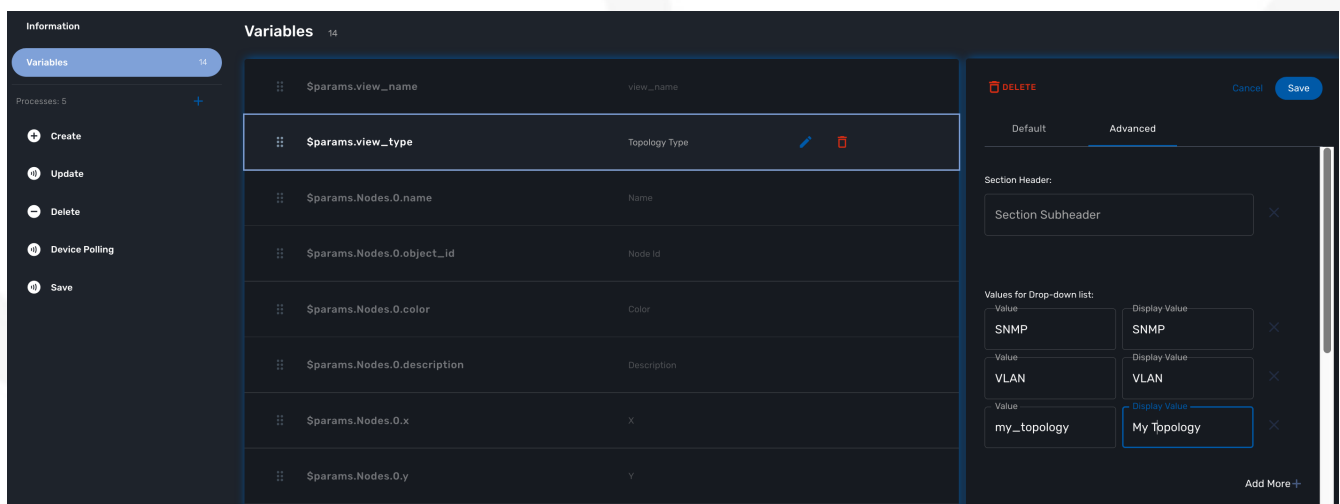
```
$ docker-compose exec msa-dev bash
[root@36f98599746a /]# cd /opt/fmc_repository/OpenMSA_WF/
[root@36f98599746a OpenMSA_WF]# git remote -v
origin https://github.com/openmsa/Workflows.git (fetch)
origin https://github.com/openmsa/Workflows.git (push)
```

You can add your own remote to your fork of the openmsa repository or work with the default one. Either way, you need to create a working branch that you will use later to initiate a pull request.

```
[root@36f98599746a OpenMSA_WF]# git checkout -b my_topology
Switched to a new branch 'my_topology'
```

Step 2: add a new topology type to the workflow

With the `{${product_name}}`, edit the topology workflow, edit the variable `view_type` and, in the "Advanced" section add `my_topology` to the values for the drop-down list.



The screenshot shows the configuration interface for a workflow. On the left, there is a sidebar with options: Variables (14), Processes (5), Create, Update, Delete, Device Polling, and Save. The main area is titled 'Variables' and contains a table of variables:

Variable Name	Value
<code>\$params.view_name</code>	view_name
<code>\$params.view_type</code>	Topology Type
<code>\$params.Nodes.0.name</code>	Name
<code>\$params.Nodes.0.object_id</code>	Node Id
<code>\$params.Nodes.0.color</code>	Color
<code>\$params.Nodes.0.description</code>	Description
<code>\$params.Nodes.0.x</code>	x
<code>\$params.Nodes.0.y</code>	y

On the right, the 'Advanced' section is visible, showing a 'Section Subheader' field and a 'Values for Drop-down list' section. The drop-down list contains three entries:

Value	Display Value
SNMP	SNMP
VLAN	VLAN
my_topology	My Topology

Save the workflow and use `git status` to see your change

```
[root@36f98599746a OpenMSA_WF]# git status
On branch my_topology
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
   modified:   Topology/.meta_Topology.xml
   modified:   Topology/Topology.xml

no changes added to commit (use "git add" and/or "git commit -a")
```

you can add and commit these files.

```
[root@36f98599746a OpenMSA_WF]# git lg
* c5f8bf6 - (HEAD -> my_topology) add a new topology view type <Antoine> (5 seconds ago)
```

Step 3: add a new PHP script to implement the new topology

Go to `/opt/fmc_repository/OpenMSA_WF/Topology/Topology_Types`

```
[root@36f98599746a Topology_Types]# pwd
/opt/fmc_repository/OpenMSA_WF/Topology/Topology_Types
[root@36f98599746a Topology_Types]# ll
total 12
-rwxr-xr-x 1 ncuser ncuser 3857 Sep 24 15:13 SNMP.php
-rwxr-xr-x 1 ncuser ncuser  419 Sep 24 15:13 Template.php
-rwxr-xr-x 1 ncuser ncuser 1516 Sep 24 15:13 VLAN.php
```

You can reuse any of these files to create your own script, we will use `Template.php` which is an "empty" implementation.

```
[root@36f98599746a Topology_Types]# cp Template.php my_topology.php
[root@36f98599746a Topology_Types]# chown ncuser.ncuser my_topology.php ①
[root@36f98599746a Topology_Types]# ll
total 16
-rwxr-xr-x 1 ncuser ncuser 3857 Sep 24 15:13 SNMP.php
-rwxr-xr-x 1 ncuser ncuser  419 Sep 24 15:13 Template.php
-rwxr-xr-x 1 ncuser ncuser 1516 Sep 24 15:13 VLAN.php
-rwxr-xr-x 1 ncuser ncuser  419 Sep 27 12:55 my_topology.php
```

① set the file user and group to ncuser

Add a new commit for this initial file

```
[root@36f98599746a Topology_Types]# git status
On branch my_topology
Untracked files:
  (use "git add <file>..." to include in what will be committed)
  my_topology.php

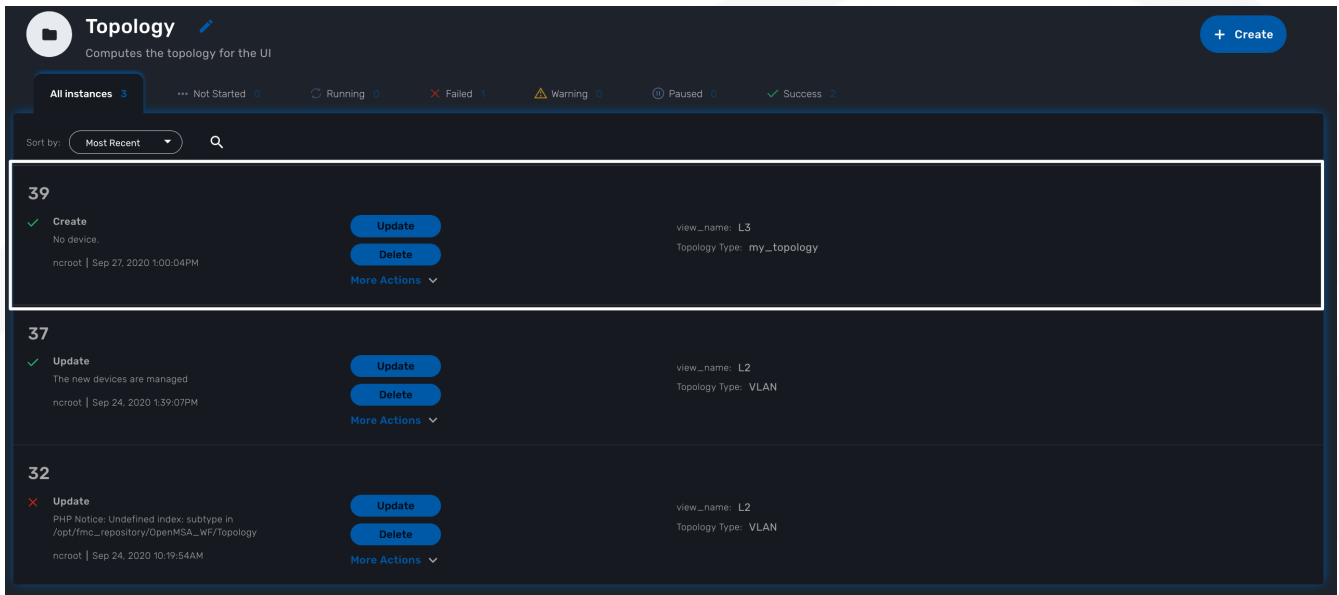
nothing added to commit but untracked files present (use "git add" to track)
[root@36f98599746a Topology_Types]# git add my_topology.php
[root@36f98599746a Topology_Types]# git commit -m "new empty implementation"
[my_topology 455ab85] new empty implementation
1 file changed, 15 insertions(+)
create mode 100755 Topology/Topology_Types/my_topology.php
```

Now you are ready to start implementing and testing your new topology.

Step 4: implementation and tests

On the workflow screen, create a new instance with your new topology view. At that point the implementation will be specific to your use case.

Whenever you create a new instance of the process, a dedicated log file is created in the API container, under `/opt/jboss/wildfly/standalone/log/process-<INSTANCE_ID>.log`. The workflow instance ID (39 in the screenshot below) is the one displayed at the top left corner of each instance.



You can monitor the log for debugging purpose: `docker-compose exec msa-api tail -F /opt/jboss/wildfly/standalone/log/process-39.log` (where 39 is the workflow instance ID)

Use the custom functions `logToFile` and `debug_dump` to output your debugging information in the log file.

With the code provided in `Template.php` you will get topology similar to this, without any links.

Manager < Super Administrator / Tenant TENANT / VLAN Simple Use Case SUBTENANT

0 unreachable 0 critical 0 power reached 5 connected

Dashboard

Infrastructure

Automation

Alarms

Admin

Settings

Profile

Logout

Auto-refresh

Managed Entities 5

Microservices

Deployment Settings

+ Create Managed Entity

Filter By

switch

pc_01

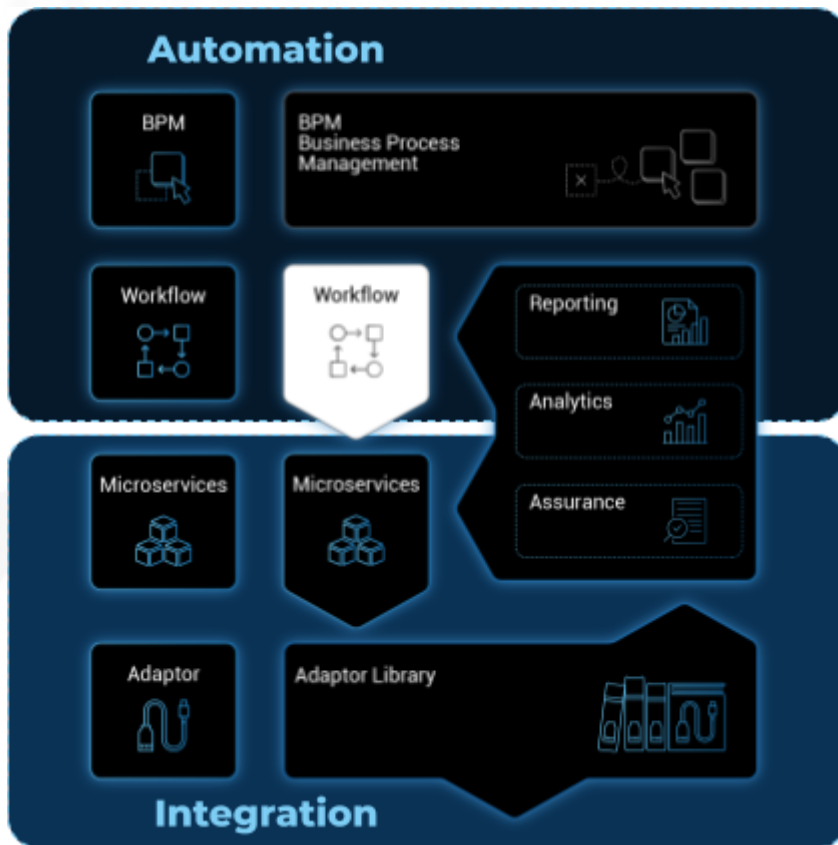
pc_02

pc_03

pc_04

Rows per page: 10 1-5 of 5

Workflows



Workflows allows the creation and management of complex automated processes.

Overview

This guide explains how to find, select and run workflows.

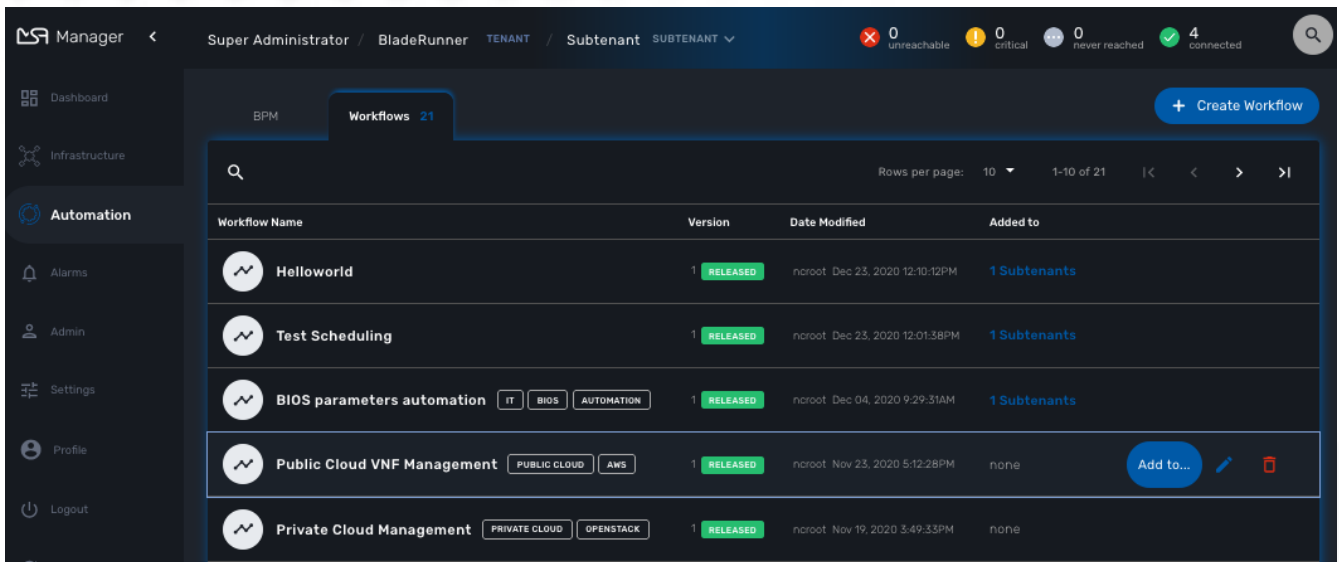
A workflow is composed of:

- A collection of processes, where each process is composed of a set of executable tasks implemented in Python or PHP.
- A list of variables stored in the database and are holding the state of a workflow instance.
- Some administrative information used to manage the service in the service console.

Workflow selection

In order to use a Workflow, it has first to be associated to a subtenant. To do so, you need to select a WF from the list and click on "Add to..."

Workflows available in the library



This will open a dialog popup where subtenant will be able to select the subtenant to add/remove to/from a workflow

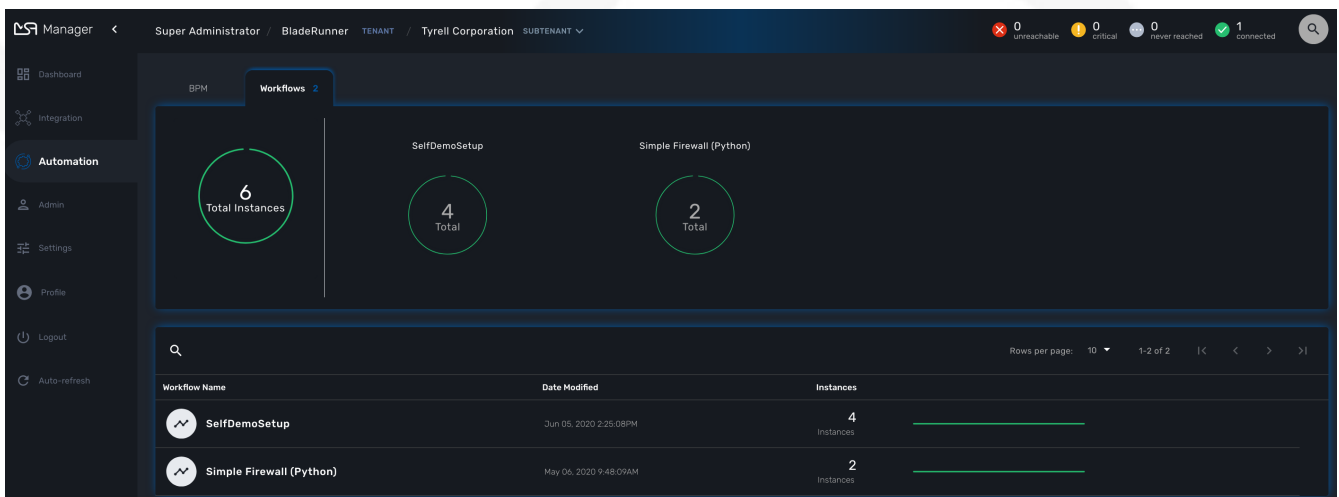
Workflow use

To run a workflow you must first select a subtenant from the subtenant selection list at the top of the screen.

This will display the subtenant management dashboard for the workflows.

This dashboard shows the overall status of process execution.

Workflow status dashboard

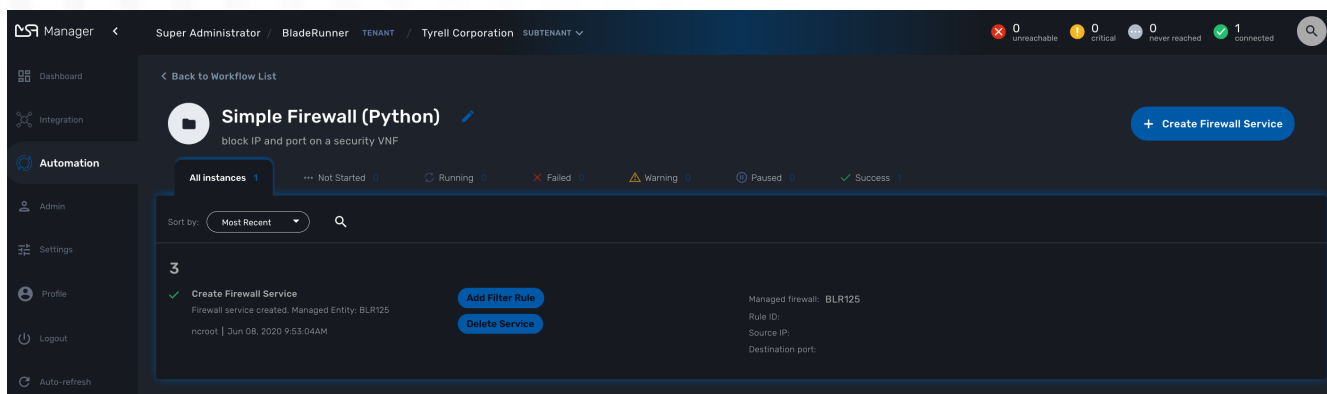


To use a workflow, you have to select it from the list at the bottom of the screen. This will open a screen with the list of the workflow instance and actions to create new instances, update or delete existing ones.

Create a workflow instance and run processes

Use the action on the top right to create a new instance of the workflow, select the actions available on an instance to call the processes available for this workflow.

Use "+ Create Firewall Service" to create a new instance of the workflow



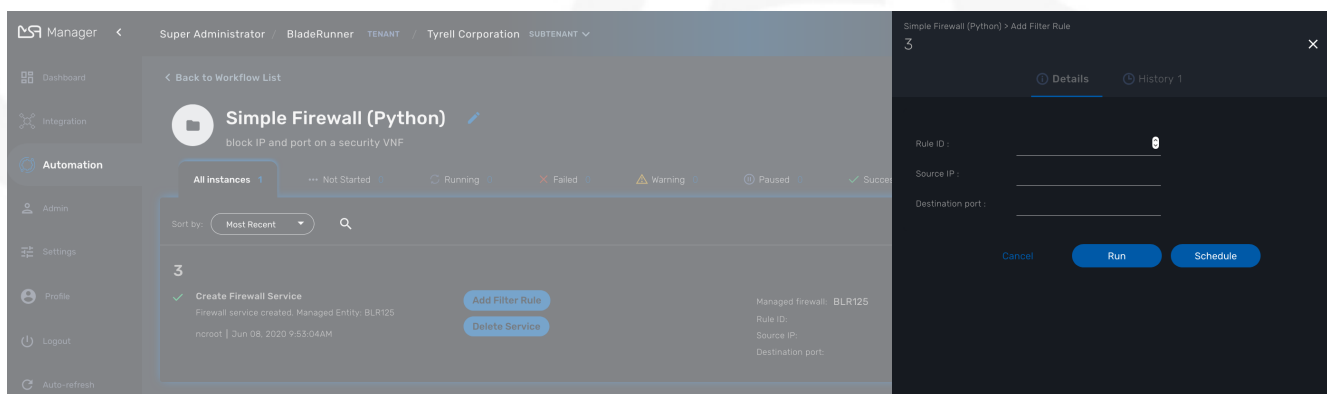
Instance lifecycle

Before you can start using a workflow, you need to create a new 'instance' of the workflow. (For programmers, this is akin to thinking of using a class to create an object instance in Object-Oriented Programming, or OOP).

The action on the top right will create a new instance and open a user form where you will be able to provide some parameters related to the creation of the instance (you can think of this as passing a parameter to the constructor in OOP). The form may not always require parameters (this would be the case of the default constructor in OOP).

The example below shows a user form with some network related information, scroll down and click on "Run" to execute the instance creation process.

Update the workflow instance by calling one of the update or delete processes



Once an instance is created, you can execute any process available to either update the instance state and run some automated task or delete the process instance. The process to delete an instance can also execute some automated tasks before removing the instance from the list.

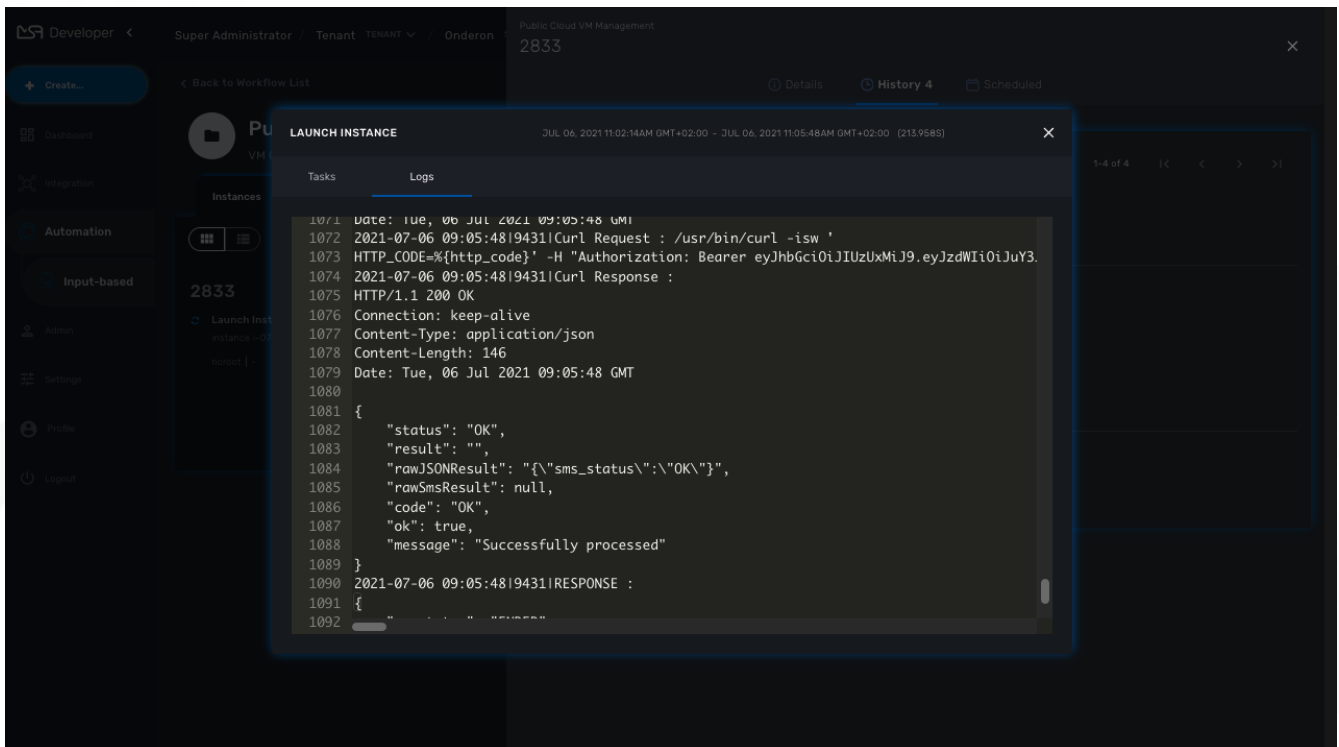
Example

A typical example of a workflow lifecycle is the one to manage VNF on a cloud:

- CREATE process: the user provide the VNF specific parameters and the process execute to create the VNF on the cloud, create and activate the Managed Entity on the MSactivator™.
- UPDATE processes: the user can ask for scale up/down or configuration changes of the VNF
- DELETE process: the VNF is removed as well as any related resources

Process execution logs

During the execution of a process you can view its execution logs in the "Logs" tab of the process execution screen.



Process execution scheduling

If a process has been configured to allow scheduling (see documentation about the workflow editor), it is possible to schedule the execution of a process.

A workflow scheduling can be deleted any time from the list of scheduled processes in the Workflow tab "Scheduled Processes"

Table 1. Workflow scheduling

Schedule	Execute Every	Pick at least one	Start date	End date
Once	NA	NA	define when the process should execute	NA
Minute	execution frequency	NA	define the start date	define the end date
Hourly	execution frequency	NA	define the start date	define the end date
Daily	execution frequency	Select the week day(s) for execution	define the start date	define the end date
Weekly	execution frequency	NA	define the start date	define the end date

Schedule	Execute Every	Pick at least one	Start date	End date
Monthly	execution frequency	Select the month(s) for execution	define the start date	define the end date

Retry a failed task

During the execution of a process, if a task fails to execute, you have the possibility to retry the execution of the process from the step where the task failed.

You can edit the process parameters before executing the process again.

Get information about workflow instance status

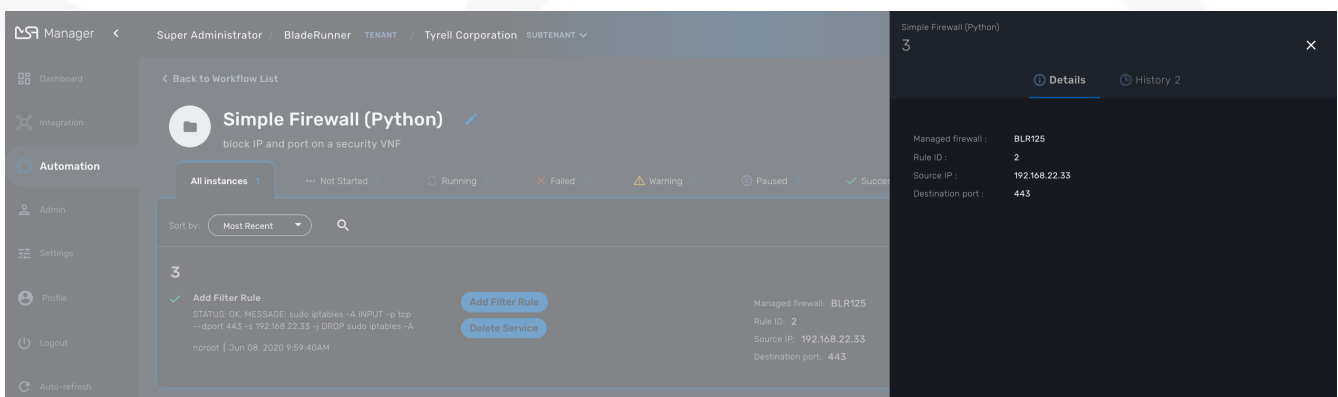
The list of workflow instances can be filtered by the status of the execution of their processes:

- All Instances: list all the instances
- Running: list the instances that have a process running
- Failed: list the instances that had a process execution failure
- Warning: list the instances where the last process execution ended with a warning
- Success: list the instances where the last process execution ended successfully

The status of a process and how a process can end with one of the possible statuses is defined by the process, in the tasks.

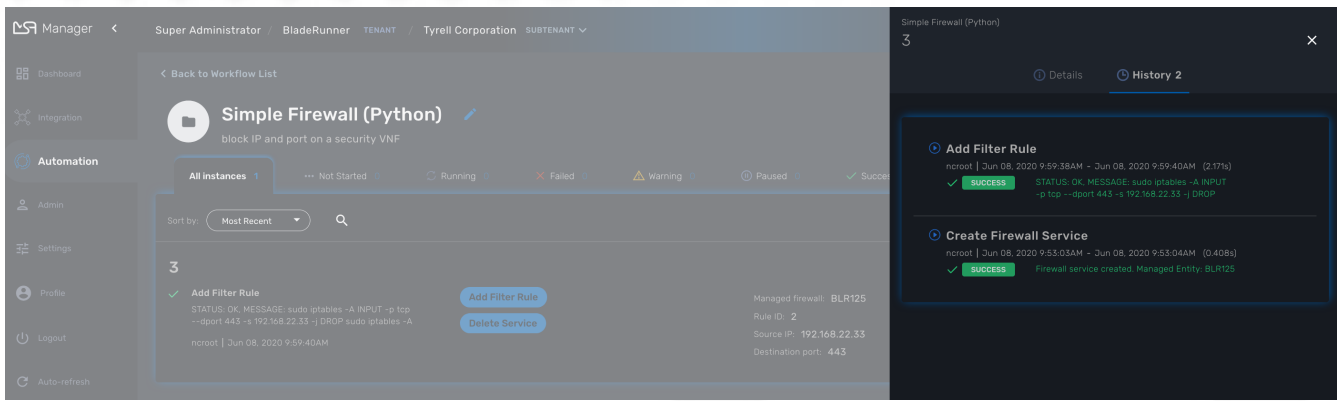
For each instance, a toolbar is available when you hover your mouse over it.

Each icon will give you some information about the instance:



- Details: lists the Workflow variable and their values. This is the state of the instance.
- History: lists the processes that were executed. For each process you can get the user that triggered the execution, the start and end time, the status of the execution.

The history will let you audit the process past executions and access all their the details.



Access rights

As privileged administrator (ncroot) or administrator, you have access to multiple tenants and their related subtenants. You can list the workflows that are in used (ie. associated to a subtenant) by clicking on the "Automation" link on the left menu.

As a manager you will only be able to select the subtenant in your tenant.

Workflow design

Workflow design is explained in the developer guide.

Workflows: utilities

Useful workflows to use as is or to extend based on your needs

Managed entities configuration variables

Configuration variables can be associated to any managed entity in order to add custom configuration.

In order to manage these configuration variables, you can use the workflow [Manage Device Variables](#).

The workflow provides a simple UI to create/update/delete and list the configuration variables associated to a managed entity.

To use it, first you need to associate it to your subtenant then execute the process **Init** to select a managed entity. **Init** will also read the database for any existing configuration variable.

Once created, you can use the workflow instance to manage the configuration variables.



If you use the process **Delete**, the workflow instance will be deleted but it **will not** delete the configuration variables

The screenshot displays the 'Manage Device Variables' workflow interface. The main view shows a list of instances for 'Instance: 49 / ME: BLR160'. A success message indicates that the variable 'PROTOCOL' with value 'HTTP' has been added to device 160. A modal window is open showing details for this instance, including a table of configuration variables.

Name	Value
Authorization:Token	0123456789abcdef0123456789abcdef01234567
Content-Type	application/json
HTTP_HEADER	
PROTOCOL	HTTP

The workflow instance is identified by its ID associated to the managed entity ID (ex: **Instance: 49 / ME: BLR160** in the screenshot above)

BPM

BPM (Business Process Management) allow the execution of complex business processes by automating a flow of workflow execution.

Overview

The integrated BPM engine can be accessed by clicking the "Automation" link in the left menu.

You need to select a subtenant to see the list of BPM that can be executed for a specific subtenant. BPM definition and instances work in a similar way as for workflows: you first need to associate a BPM to a subtenant and then each execution of a BPM will create a new instance that can be managed.

Use the "i" (information icon) to open a BPM instance and view it's detailed status.

A BPM instance can be deleted with the "trash" icon.

Execution management

Tracking

The BPM engine will start executing the BPM tasks one by one and the status of the current workflow process execution will be updated live in the view "LATEST EXECUTION RESULT".

Click "Show Tasks" to see the detail of the process execution.

BPM execution tracking

STATUS	TASK	START TIME	END TIME	DURATION
SUCCESS	task1 <small>Task OK</small>	Nov 06, 2020 9:17:55AM	Nov 06, 2020 9:18:05AM	(10.054s)
RUNNING	task2	Nov 06, 2020 9:18:05AM	Running	

Pause and resume

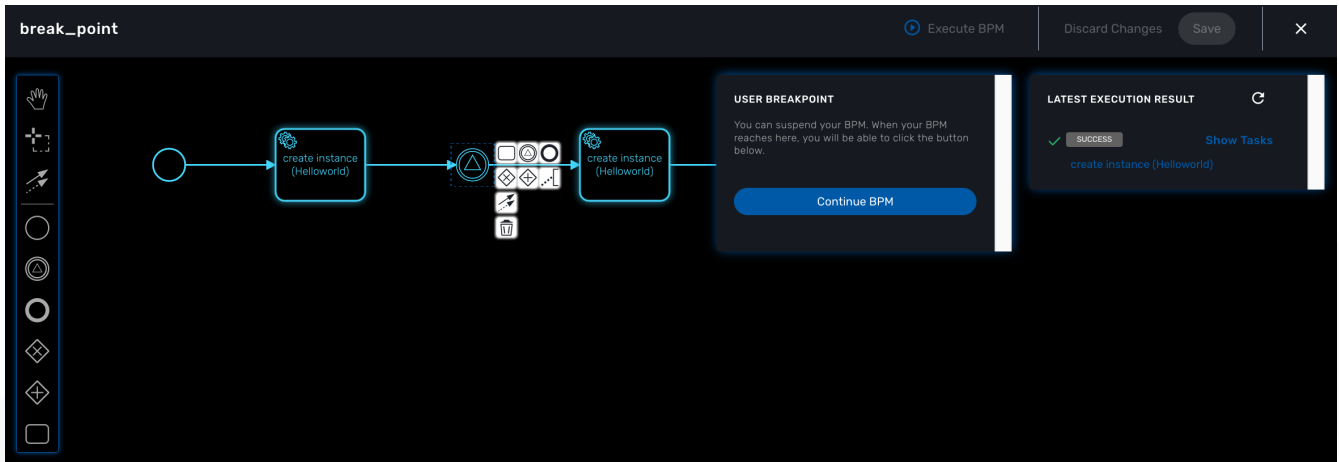
With the execution breakpoints the execution of a BPM can be paused until the user manually resume the execution

It can be used to execute complex BPM with several part and allow for manual validation of each

intermediate steps.

When a BPM execution is paused, the instance will be listed with an empty execution end date.

Resume a BPM execution



Terminating

The execution of a BPM can be cancelled any time by clicking on the "Terminate BPM" button at the top right of a BPM execution screen.

Scheduling

The execution of a BPM can be scheduled to run once at a predetermined date or in a recurring way for a predefined duration. The list of scheduled executions is available and any scheduled execution can be canceled

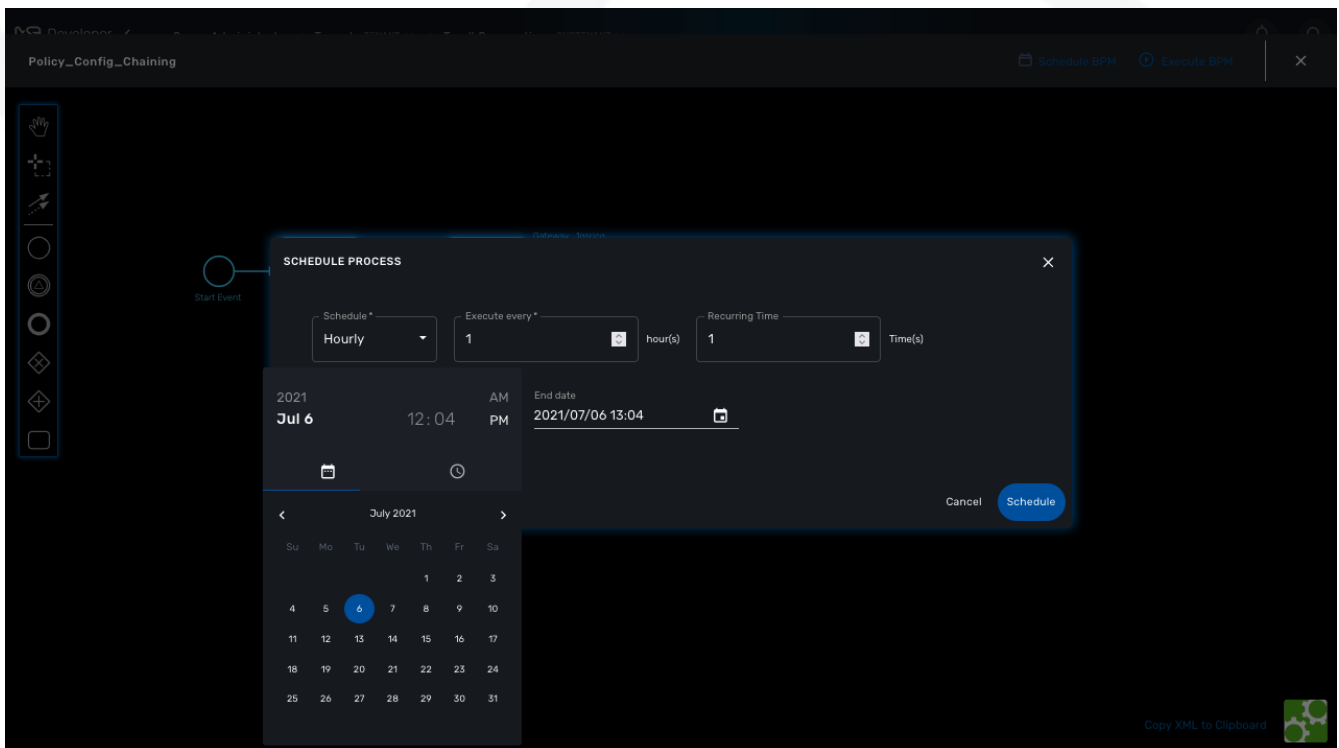


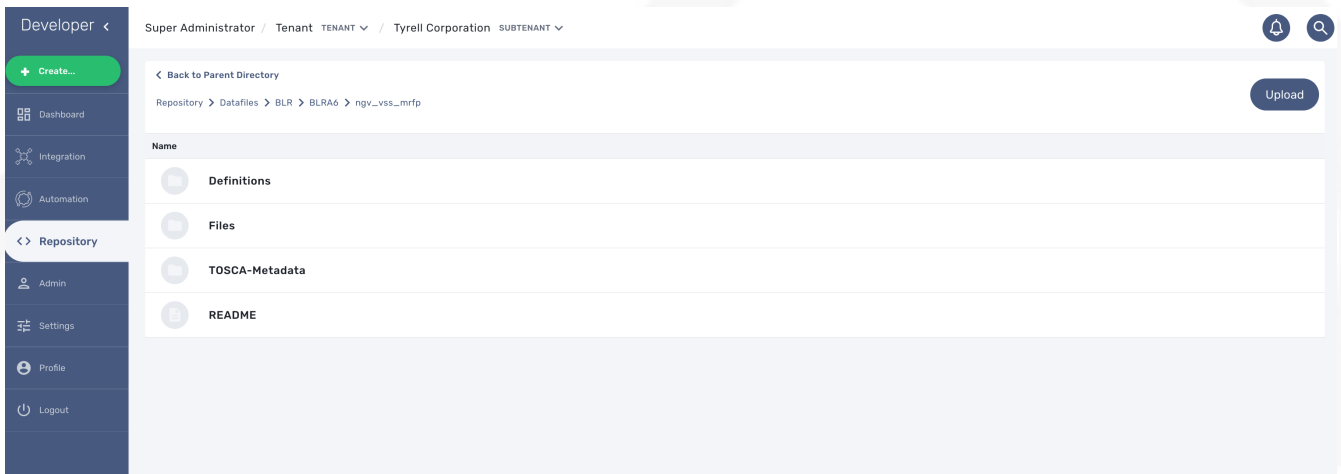
Table 2. BPM scheduling

Schedule	Execute Every	Pick at least one	Start date	End date
Once	NA	NA	define when the process should execute	NA
Minute	execution frequency	NA	define the start date	define the end date
Hourly	execution frequency	NA	define the start date	define the end date
Daily	execution frequency	Select the week day(s) for execution	define the start date	define the end date
Weekly	execution frequency	NA	define the start date	define the end date
Monthly	execution frequency	Select the month(s) for execution	define the start date	define the end date

Repository

The MSactivator™ repository contains the definition files for the workflows, microservices, BPM and various datafiles. Until version 2.8.3, these files could only be accessed either by the API or manually by connecting to the msa-dev container and using the CLI. These files are store under `/opt/fmc_repository/`

With version 2.8.3, you can use the UI to upload, delete, unzip and edit files in the DataFiles part of the repository. This feature is available for both developers and managers.



File upload

File will be uploaded based on the selected subtenant, therefore you need to select a subtenant in order to activate the upload button.

Settings

The settings screen provides information on the current version of your {\$product_name} version. This is also where you can upload and activate your product licence.

Details about license activation is available in the admin guide.