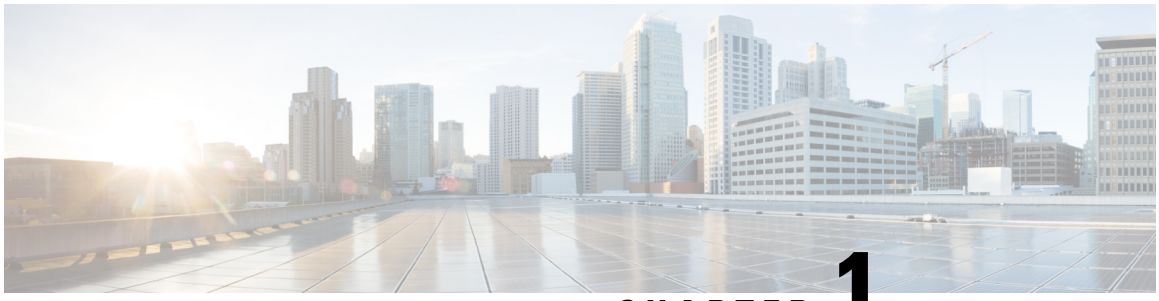
Cisco Virtual Managed Services (VMS) 3.3 Platform User Guide

First Published: 2018-05-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Getting Started with Cisco Virtual Managed Services (VMS)

Cisco Virtual Managed Services (VMS) is an open software platform that enables service providers to create and manage services across physical and virtual network elements. The VMS solution utilizes network function virtualization and enables service providers to provide their customers a flexible selection of services that are easily customized through a self-service portal. It reduces the costs for service creation, customer acquisition, service fulfillment, time to repair, and maintenance. With Cisco VMS solution, you can automate end-to-end provisioning for different use cases and service topologies. Each release of the VMS provides out-of-box capabilities to orchestrate particular use cases, also called service packs (such as, SDWAN, vBranch, and Managed Devices). The VMS service packs are a suite of prepackaged software capabilities that fully automate the end-to-end service creation including ordering, service chaining, orchestration, service assurance, user self care, real time performance reporting, and user-defined policy changes. With these fully validated service level packages, end customers can quickly turn on, control, and ensure cloud-based managed services offered by the service provider. For detailed information about VMS solution, see Cisco Virtual Managed Services (VMS) Solution Overview Guide.

For information on VMS platform or service pack installation, see the latest version of *Cisco VMS Installation Guide* on cisco.com.

This chapter contains the following topics:

Logging In and Out of the VMS Portal

To log into the VMS Portal, enter the following URL in your web browser address field, where server-ip is the IP address or fully qualified domain name (FQDN) name of the VMS server:

https://<server-ip>/vms or https://www.example.com/vms

Depending on your network configuration, the first time your browser connects to the Cisco VMS web server, you may have to update your client browser to trust the security certificate of the server. This ensures the security of the connection between your client and the Cisco VMS web server.

Your user account privileges determine what you can see and do in the user interface. For information on Cisco VMS users and the actions they can perform, see Managing User Roles.

To log out, in the left pane of the VMS Portal, click **Logout**.

Configuring Password Policies in Cisco VMS

In VMS, as an administrator user, you can define various settings for the password policies, such as password strength, password minimum/maximum length, account locking, password history, and password aging.

By default, there are two default policies available on VMS. An administrator user can modify these existing policies or create new policies. The default policies created at the deployment time are:

- *ppolicy_default*: Applicable for consumer user
- *ppolicy_strong*: Applicable for administrator accounts

To define the password policies, use the 'PwdPolicy' POST API in the IDM User Controller section of the **User Management Service API**. For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **VMS portal > Account Settings > Swagger > SFI SDK > User Management Service API**.

The following password policies settings are available in VMS:

- **Password strength (characterRule)** : This setting determines series of guidelines that are important for a strong password.
- **Password length (lengthRule)**: This determines minimum and maximum password length.
- **Account Locking (accountLocking)** : This setting controls the lockout of a user account. Using this setting you can control how may invalid password attempts (**lockoutFailCount**) are allowed within a time period (**lockoutFailIntervalSec**). If the number of attempts is exceeded, then account gets locked for a specified time (**lockoutDurationMin**).
- **Password History (historyRule):** This setting doesn't allow to reuse previous passwords within a predefined time period.
- **Password Aging Rules (agingRule):** This setting controls how long an existing password is valid. The following password aging settings are available in VMS.
  - **Password Expire Warning Period (expireWarningSec)**: With this setting, you can set the number of seconds before a password expires. In this policy, you can also set when an email notification is sent to the user before their password expires. Use the **pwdExpireWarning** parameter to define when the user starts to receive password expiration notifications. If this time interval is set to 0, no warning messages are sent out. The user can change their password at any time before the expiry. After expiry, they must change their password to continue using VMS.
  - **Password Grace Period (graceAuthNLimit)**: Use this setting to define the number of grace login attempts after the Password lifetime limit has exceeded. In this policy, you can set the number of times an expired password can be used to authenticate after the password lifetime limit has exceeded. Users attempting to log in to the account during this grace period will receive a warning message to change the password. If grace authentication is not defined for the user or the user has used all

allowed attempts , user login to the account fails, and the system displays the following error message, "Your password expired. Please Reset your password".

- **Maximum Password Age (maxAgesec)**: Using this setting, specify the number of seconds after which a password expires. Set the value to 0 if you want the password never to expire.
- **Minimum Password Age (minAgesec)**: Using this setting, you can set the minimum number of seconds between modifications to the password. Set the value to 0 if you want to reset/change password at any time.

The following is a sample implementation of the *ppolicy_default* .

```
{
  "policies": [
    {
      "name": "ppolicy_default",
      "description": "PHI ppolicy_default",
      "characterRule": {
        "enabled": true,
        "minDigit": 1,
        "minLowercasechars": 1,
        "minUppercasechars": 1,
        "minSpecialchars": 1
      },
      "lengthRule": {
        "enabled": true,
        "minLength": 8,
        "maxLength": 16
      },
      "accountLocking": {
        "enabled": true,
        "lockoutDurationMin": 30,
        "lockoutFailCount": 3,
        "lockoutFailIntervalSec": 60
      },
      "historyRule": {
        "enabled": true,
        "passwdhistorycount": 10,
        "passwdhistorydurationMonth": 60
      },
      "agingRule": {
        "enabled": true,
        "graceAuthNLimit": 3,
        "maxAgeSec": 10368000,
        "minAgeSec": 86400,
        "expireWarningSec": 1209600
      }
    }
]
```

Enabling Approval Process for a Service Request

The approval capability if enabled in Cisco Virtual Managed Services allows the user with relevant permissions to approve or reject a service request.

An approver can approve or reject the following request types:

- New service request
- Update to an existing service request
- Service cancellation request

For more information on permissions required to enable approvals for a user, see *Cisco Virtual Managed Services (VMS) 3.3 Platform and Service Pack Permissions Addendum*.

The approval metadata must be enabled at the service offer level. This metadata must be imported using the 'Import' service POST request in the Consume Service API.

To enable Approval, add the following metadata to the 'offers' section of the Import service POST request in the Consume Service API.

For more information on the API, refer to the Swagger documentation that can be accessed from the **VMS portal > Account Settings**.

```
"approvals": {
        "supportedApprovalOperations": [
            "NEW_ORDER","UPDATE_ORDER","DELETE_ORDER"
```

You can use the same API to edit the allowed operations (New service, Update Service, Unsubscribe) for Approvals. After enabling the Approval functionality for a service offering, any users with APPROVE_SERVICE permission can approve or reject a service request.

The following is a ConsumeService API sample that includes the Approvals metadata.

```
{
  "id": "16daba64-f788-4138-8977-6d5def97e16a",
  "name": "cloudvpn",
  "configuration": {},
  "options": [],
  "properties": [],
  "offers": [
    {
      "id": "17b1d14c-60ee-4cce-8475-b9e2bb0fa9a8",
      "name": "basic",
      "approvals": {
        "supportedApprovalOperations": [
            "NEW_ORDER","UPDATE_ORDER","DELETE_ORDER"
        ]
      }
    },
    {
      "id": "ab0ef666-965a-4c20-b97e-709ab66394f8",
      "name": "medium",
      "approvals": {
        "supportedApprovalOperations": [
             "NEW_ORDER","UPDATE_ORDER","DELETE_ORDER"
        ]
      }
    },

"offers": [
    {
      "id": "17b1d14c-60ee-4cce-8475-b9e2bb0fa9a8",
      "name": "basic",
      "approvals": {
        "supportedApprovalOperations": [
            "NEW_ORDER","UPDATE_ORDER","DELETE_ORDER"
```

]

Configuring Integrations for Outbound APIs

Using this procedure, you can enter the configuration details for the Business Support Set (BSS), Representational State Transfer (REST), and outbound API calls.

Procedure

Step 1 From the left pane of the Service Interface, click **Settings**.

Step 2 In the **Integrations** tab, you can enable or disable the following attributes:

- Support - Read knowledge articles and raise support tickets via the Cloud Services Portal.
- Manage Users - Add and remove portal users via the Cloud Services Portal.
- User and Tenant View (under **Identity**) - Disabling these attributes does not let you create, modify, or delete Users and Tenants respectively. You can only view the users and tenants. You can also enable the **Show Profile** option.

Step 3 Click the **REST Configuration** tab to set the authentication mode details for the Integrations system.

Step 4 Select **Basic** or **OAuth 2** based on your requirement.

- If you have selected **Basic**, enter the user ID and password of the Integrations system.
- If you have selected **OAuth 2**, enter the client ID, password, Token request URL, HTTP Method, Token Validation header, Token header format and other necessary details.

Step 5 Click **Save** to save the authentication details.

Step 6 In the **Outbound API** tab, under **API Context**, enter the base context URL for the outbound API calls in the **Base Context** attribute.

a) Under **APIs** area, you can modify the **Allowed Values**, **Pricing Options**, **Accessible Services**, **Service Cancellation**, **Notification URL** of APIs. Click **Update** to save changes.

Step 7 You can validate use case API operations in the **UseCase API** area.

Enabling Notification for Events

You can either enable notifications for various events through email or REST API. Cisco VMS provides support to trigger notifications when certain events occur:

Note

- Ensure you have configured Integrations, REST configuration details, and Outbound API details for sending REST notifications, if you want to use REST API rather than email notifications. For more information, see the section, Configuring Integrations for Outbound APIs.
- Both REST and Email communication modes are supported for all of the following list of events. However, only Email notification is supported (and not REST) for the event **End User Password Reset Link**.
- Email notifications are sent only when you have configured email client.

Table 1: List of Events

Recipients	Events
Consumer, operator, or administrator	Password is reset.
Remote user	• Remote user created or deleted. • User ID is activated or deactivated/suspended. • Password reset.
Service Provider End User	• Update Site • Delete Site • Add Site • Tenant Added. • Tenant Updated. • Tenant Deleted. • Approval Pending for Requester. • Approval Pending for Approver. • Service Approved or Rejected. • Device Added. • Device Deleted. • Device Only Purchase. • Device Updated. • Device Registered. • End User Added. • End User Deleted. • End User Password Reset Link (supports only Email notification).

Recipients	Events
Service Provider End User	• End User Password Success Confirmation. • End User Updated. • Confirmation for Service Order. • Service Order Failure. • Service Activation Success Confirmation. • Service Activation Failure. • Service Deprovisioned. • Service Deprovisioning Failure. • Service Unsubscribed. • Service Updated • Service Update Failure. • Configuration of Tenant VCE Required (indicating that the Cisco VCE is added to the Cloud VPN service). • SSL VPN User Added. • SSL VPN User Add Failure. • SSL VPN User Deleted. • SSL VPN User Password Reset Link (supports only Email notification). • SSL VPN Password Reset Success. • SSL VPN Password Reset Failure. • SSL VPN User Status Changed. • Enable Bandwidth Prioritization.

To enable notification for events:

Procedure

Step 1 From the left pane of the service interface, click **Notifications**.
Events related to Provider and End Users are displayed when you click the **Provider** and **End Users** tab respectively.

Step 2 Using the **Category** drop-down, you can further categorize events.

Step 3 For an event, you can edit the **Template** name, **Communication Mode** by clicking the Edit icon (located next to the Communication Mode value). You can also enable or disable the notification for a specific event.

Configuring an Announcement

Using this procedure, you can create an announcement text to display the alert messages such as planned maintenance alert and technical issues. These announcements are displayed for users upon login.

Procedure

Step 1 From the left pane of the VMS Portal, click **Settings > Announcements**.

Step 2 Enter the title and the message to be communicated.

Step 3 Choose an announcement style - **Danger**, **Warning**, **Info**, or **Success** from the **Visual Style** drop-down list, depending on the criticality or type of announcement to make.

Step 4 Optionally select the **Start Time** and **End Time** for the announcement.

If **Start Time** is not specified, the announcement is displayed immediately after it is saved. If an **End Time** is not specified, the announcement is displayed indefinitely after start time - You need to resolve the message for it to stop displaying.

Step 5 Choose either **Page Header Announcement** or **Ticker Announcement** to select the Announcement Type.

Step 6 Click **Save**. The newly added announcements are listed.

Once the issue is resolved, you can select the announcement that you want to delete from the list.

Defining Terms and Conditions for a Service

Cisco VMS allows you to define and maintain the terms for a service.

Procedure

Step 1 From the left pane of the VMS Portal, click **Configurations** and select the service pack.

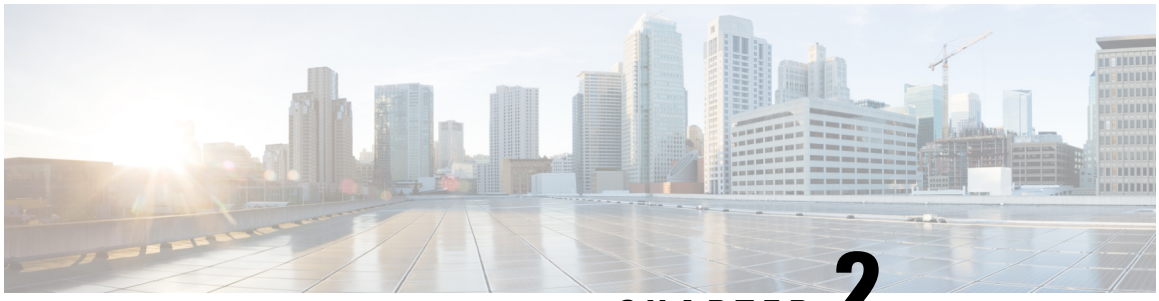
Step 2 Click **Terms**.

Step 3 Select one of the Cloud VPN offers from the "Offers" drop-down list.

Step 4 Select the desired format for the font.

Step 5 Enter details required for acceptance by a consumer while purchasing a service. This information is displayed while the consumer is placing an order for the service. The terms and conditions are defined specific to an offer in a service.

Step 6 Click **Save**.



CHAPTER 2

Role-Based Access in Cisco Virtual Managed Services

In Cisco Virtual Managed Services (VMS), user permissions are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes system access for users based on user roles. Based on the permissions assigned to a user by an administrator, a user can define and customize how their services are exposed to customers. The permissions allow to customize various aspects of a service workflow, such as managing tenants, notifications, integration with BSS systems, announcements, and so on. The role-based access permissions are categorized into the following categories:

- **Service Pack Specific Permissions**: Include permissions for controlling various settings for the service packs.
- **Services, Configurations, and Devices Specific Permissions**: Include permissions for configuring various settings for the devices and services.
- **Integrations, Settings, and Log Specific Permissions**: Include permissions for controlling integration, log, and SSO configurations.
- **Users, Roles, and Tenants Specific Permissions**: Include permissions to configure user, remote users, tenants, roles, provider settings, and so on.

For more information on all the available permissions in Cisco Virtual Managed Services (VMS) and to also see the minimum required permissions to perform various operations in VMS, see Cisco Virtual Managed Services (VMS) 3.3 Platform and Service Pack Permissions Addendum.

Note You will need Cisco Customer or Cisco Employee privileges to access the 3.3 documentation.

VMS provides out-of-the-box roles that have permissions applied by default. You can either modify the permissions associated with these out-of-box roles or add a new role. For the description of these permissions, see the table in the section, Cisco Virtual Managed Services Permissions and their Descriptions.

The following are the out-of-box roles available with VMS:

- **Service Provider Operators** support multiple customers by maintaining service information and settings, viewing, monitoring the SP-DNA platform, remediating basic customer issues, and escalating severe issues.

- **Service Provider Administrators** have Operator permissions and can also perform more advanced tasks like managing price plans, importing, and exporting service definitions, and configuring the service platform.
- **Service Provider API Administrators** update tenant data using API calls instead of the standard methods available through applications and platform web interface. This is a powerful role, as it bypasses Tenant RBAC checks.
- **Tenant Administrators** have Tenant Operator permissions and can also perform more advanced tasks like managing service policies and configurations.
- **Super User** supports all actions from user management to service management or operator.

For more information on how to add a new role or modify an existing role and to associate this role to a user, see Managing User Roles and Managing Users.

- Managing VMS Platform-Specific User Roles, on page 10
- Managing Tenants and Tenant Groups, on page 12

Managing VMS Platform-Specific User Roles

In Cisco VMS, you need to create a new role (such as Tenant Operator) and assign the permissions required to operate the platform tasks. To create a new role and assign it to users, do the following:.

Table 2: Overview Procedure for Creating Platform-Specific User Roles

	Task	Reference Topics
1	Log in to the Cisco VMS portal (as an Admin/Super user).	
2	Create the tenants.	Managing Tenants, on page 12
3	Create a new role (such as Tenant Operator) and assign the permissions required to operate the VMS application and the service packs.	• For more information on basic permissions required to perform the documented tasks for the VMS platform and the service packs, see *Cisco Virtual Managed Services (VMS) 3.3 Platform and Service Pack Permissions Addendum* • For more information on creating a new user role, see Managing User Roles, on page 11.
4	Create a user (such as Tenant Operator User), assign the role defined in Step 3 to this user, and select all the tenants that the user needs to access.	For more information on creating a new user, see Managing Users, on page 13

Managing User Roles

What you can see and do in the user interface is controlled by your user account privileges. In VMS 3.1 and later, the permission are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes system access for users based on user roles. A role defines the privileges of a user in the system. Since users are not directly assigned with privileges, management of individual user privileges is simply a matter of assigning the appropriate roles.

A user is granted access to desired system resources only if the assigned role grants the access privileges. For example, a user with the Service Extension Designer role can import service extension templates, define service extension parameters, define default parameter values, and so on. For more information on assigning roles to a user, see Managing Users, on page 13.

Adding a User Role

Procedure

Step 1 Log in to the Cisco VMS Portal.

Step 2 From the Left Hand Side menu, click **Roles**.

The Manage Roles screen appears.

Step 3 Click the **Add Role** button.

Step 4 Enter the role name, display name, and description.

Step 5 To assign the permission for the roles, click **Category** and select the corresponding check box(es) for the permission(s) that you want to grant to the role.

For more information on permissions required to perform a specific task on the VMS platform, see *Cisco Virtual Managed Services (VMS) 3.3 Platform and Service Pack Permissions Addendum*.

For more information on the complete list of VMS permissions, see *Cisco Virtual Managed Services (VMS) 3.3 Platform and Service Pack Permissions Addendum*.

The types of permission you can grant are:

Permission	Description
View	Provides only read-only access to the function.
Manage	Provides access to read and manage tasks associate with the function.

Step 6 Click **Save**.

Modifying an existing role

Procedure

Step 1 Log in to the Cisco VMS Portal.

Step 2 From the left pane of the **Service Interface**, click **Roles** to view the list of roles.

The Manage Roles screen appears.

Step 3 Select the role that you want to modify and click the **Edit** icon.

Step 4 To assign or revoke the permission for the roles, click **Category** and select or clear the corresponding check box for the permissions.
The types of permission you can grant are:

Permission	Description
View	Provides only read-only access to the function.
Manage	Provides access to read and manage tasks associate with the function.

Step 5 Click **Save**.

Managing Tenants and Tenant Groups

The multi-tenant architecture of VMS provides the ability to segment the data stored by tenant. When tenants are defined, data is partitioned by tenant. This provides data security and privacy for each tenant, while allowing cloud or managed service providers the flexibility to consolidate many smaller customer configurations on a set of infrastructure servers.

The following are the key points you must know while configuring tenants:

- Tenant administrators are linked to their data by a tenant object.
- Tenant objects must be consistent and unique across all clusters.
- A tenant administrator cannot view or modify the data of another tenant.

Managing Tenants

The multi-tenant architecture of VMS provides the ability to segment the data stored by tenant. When tenants are defined, data is partitioned by tenant. This provides data security and privacy for each tenant, while allowing cloud or managed service providers the flexibility to consolidate many smaller customer configurations on a set of infrastructure servers.

The following are the key points you should know while managing tenants:

- Tenant administrators are linked to their data by a tenant object.
- Tenant objects should be unique across all clusters.
- A tenant administrator cannot view or modify the data of another tenant.
- A tenant administrator can manage more than one tenant.

You can add new tenant details using this procedure. When you add a customer user, you need to associate the user with a tenant.

Procedure

Step 1 Login to the Cisco VMS Portal (Service Interface).

Step 2 From the Left Hand Side menu, click **Tenants** to view the list of existing tenants with their details in the **Manage Tenants** page.

Step 3 Click **Add Tenant** and enter the customer name and description, email address, website URL, and contact number.

Step 4 Click **Save**. The new customer details are listed in the **Manage Tenants** page.

You can also update the customer details (under **Action**), if required.

In addition, you can also disable the ability to create, modify or delete Tenants. For more details, see Configuring Integrations for Outbound APIs

Note You can delete a tenant only if the tenant is not associated with any user.

Managing Tenant Groups

After you create tenants, you can configure the tenant groups, which are a collection of tenants grouped for assigning a common list of functions such as, service extensions parameter values, and so on.

To manage tenant groups:

Before you begin

Procedure

Step 1 Log in to the Cisco VMS Portal.

Step 2 From the Left Hand Side menu, click **Tenant Groups** to view the list of tenant groups with their details in the Manage Tenant Groups window.

Step 3 Click **Add Tenant Group**.

Step 4 Enter the tenant group name and description.

Step 5 Select the tenants that you want to add to the tenant group.

Note A tenant can be associated with only one tenant group. The **Tenant** drop-down lists only those tenants that are not associated with any tenant group.

Step 6 Click **Save**.

Managing Users

Using this procedure you can add new user details, assign appropriate role to the user, and associate the new user to the tenant.

Note You can disable the creation and modification of users, if you choose **Single Sign-On** and use your Identity Provider. The following procedure, describes the use of local user accounts.

Procedure

Step 1 Log in to the Cisco VMS Portal.

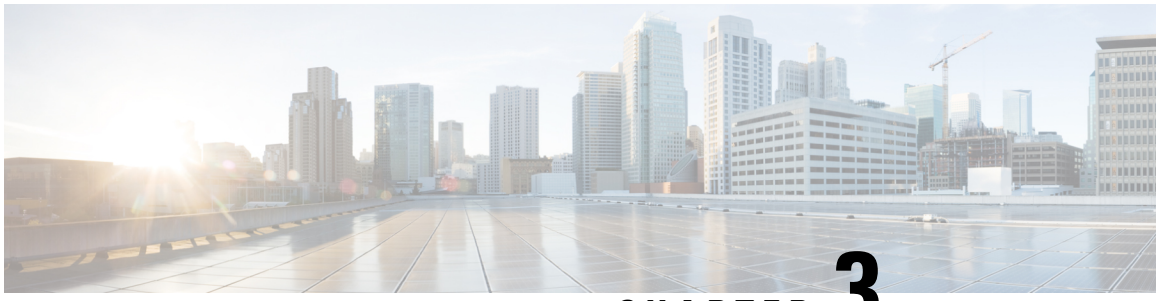
Step 2 From the Left Hand Side menu, click **Users** to view the list of users with their details in the **Manage Users** window.

Step 3 Click **Add User** and enter details such as first name, last name and user ID, email address, and contact number.

Step 4 To assign a role, you can choose from the available options in the drop-down by selecting them from the **Assigned Roles** drop-down. You can associate one or more roles to a user.

Step 5 Choose a tenant from the **Associate Tenants** drop-down list. You can associate one or more tenants to a user.

Step 6 Click **Save**. The new user details are displayed in the **Manage User** window.



CHAPTER 3

Monitoring VMS Services

This chapter describes how to monitor VMS services. Service dashboard displays at-a-glance views of the most important data in the service pack. The dashboard elements visually convey complex information in a simplified format. The dashboard allows you to quickly analyze data and drill down for an in-depth information.

This chapter contains the following sections:

Using the Dashboard

After logging into the Cisco Virtual Managed Services Portal, you can access dashboards that allows you to view your subscriptions, status of the services, and approval requests in a consolidated view. To access the dashboard, click **Dashboards** from the left pane of the Service Interface. You can only view the data in the dashlets that you have access to. If you are a user with an administrator privilege, you can view all the dashlets available in VMS with the data populated for all the users. Click on **Reload Dashlet** icon to refresh the data on the dashboards..

The following are the dashlets that are available on VMS:

- **Subscriptions**:

  By default, the dashboard will display all the subscriptions sorted by the service type, customers, status, number of issues, and status of the issues. This dashboard also displays the service pack specific subscriptions with details of the services, such as, Up, Down, Unregistered, Ordering, Updating, and Sites.

  Each of the service pack specific subscription page are also linked to their detailed services page. Click on **All Cloud VPN Services** to view Monthly Usage, Performance Metrics and Created/Provisioned Log for a service. For more details on this page, see Monitoring Status and Usage of a Service.

- **Approval**:

  When a new service order is submitted, the service request goes through an approval process before it is provisioned. Only an approver user or a user with approver privilege can approve or reject a request. If notifications are enabled, the approvers are notified of the pending approvals. This dashboard will show the list of pending approvals. For more information, see Approving or Rejecting a Service Request.

- **Device Management**:

This dashboard shows the type of devices ordered and their status and the deployed devices for each of the service types. The list of devices in various status such as Unregistered, Registering, Provisioned, Ordering, Updating, Provisioning Failed, Up, Down, Unknown are displayed. For information on how to manage your devices, see the Service Pack Guides .

Monitoring Status and Usage of a Service

Using this procedure, you can monitor key performance metrics for your services in the VMS Portal. You can set the level of monitoring to minimal and can customize the monitoring displays. If you have purchased a service, you can also monitor monthly usage and performance metrics of a service, for a specific period.

You can monitor services as follows:

Procedure

Step 1 From the left pane of the VMS Portal, select **Dashboard** on the left pane.

Step 2 In the Subscriptions dashlet, click any of the Service Packs.

Step 3 Click on **All Services** to display Services along with the status such as *Provisioned, Ordering, Update Failed, Provisioning failed* and *Unknown*.

Step 4 To filter services, select a status from the drop-down.

Step 5 Expand the Service name to view the Performance Metrics, Monthly Usage and other necessary information for the selected service.

Step 6 You can view **Monthly Usage**, **Performance Metrics** and **Created/Provisioned Log** for a service (displayed on the right pane). You can further expand the service offer and click the device name under the service offer (for instance, click Cisco 881 Integrated Service Router) to view the serial number and location on the right pane.

Step 7 Under **Performance Metrics**, slide the **Timeframe** slidebar to view performance metrics such as **Internet Traffic**, **On Network Traffic**, and **Connected Remote Access Users** over a specific time frame. You can also view the date when the service was created, modified and provisioned in the **Created/Provisioned Log** in the right pane, when you select a services

Example

Note When logged in as an Admin or Operator for operations and troubleshooting, it is useful to have a view of what any customer can access. You could achieve this by clicking **Login as Customer** in (bottom) left pane. From the drop-down list provided, select the customer to view and the user to login as. Click **Start**.

This provides a central location for the Service Provider administrator or the operator to login as any customer without the need to remember login credentials for all customers.

Approving or Rejecting a Service Request

When a new service order is submitted, the service request goes through an approval process before it is provisioned. For information on how to order a new service for a Managed Device, SDWAN, vBranch service packs, see the service pack user guides on cisco.com.

Only an approver user or a user with approver privilege can approve or reject a request. If notifications are enabled, the approvers are notified of the pending approvals. An approver can approve or reject the following request types:

- New service request
- Update to an existing service request
- Service cancellation request

For a service provider user, the status of the submitted order will stay in pending state until it is approved or rejected. If the notifications are configured for the service provider, the user will be notified of the status through an email or REST API.

Note Only an approver user or a user with approver privileges can perform this process.

Before you begin

Configure notifications if you want to notify approvers or service provider users about the status of the approvals. See Enabling Notification for Events.

Procedure

Step 1 Log in to the Cisco VMS Portal.

Step 2 From the left pane, click **Approvals** to view a list of pending service requests.

Step 3 Select a request and click **Approve** or **Reject**. If rejected, provide a reason for rejection.

The user will be notified about the status.

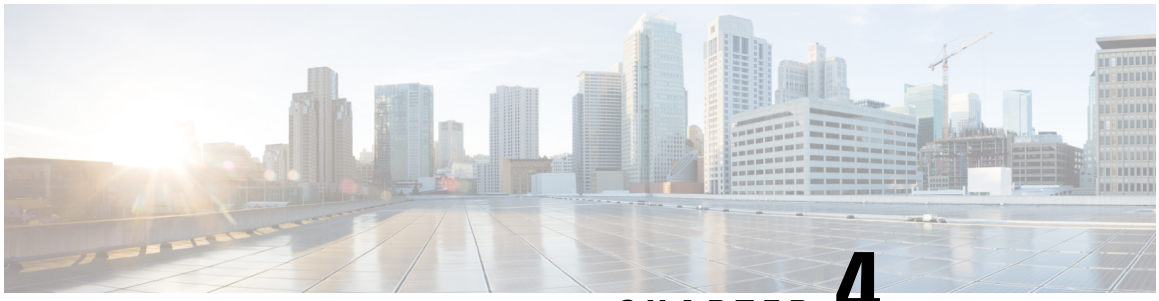
Viewing an Event Log

Procedure

Step 1 Log in to the VMS Portal using your credentials. If a user belongs to many tenants, a drop-down is displayed to select the tenant.

Step 2 From the Left Hand Side menu, click **Event Log**.

Step 3 From the Event Log screen, filter the event log records. Select the filter type from the drop-down. You can filter these events by severity and time frame. To list event logs for a specific duration, select the **Custom Range** check box and specify the dates.



CHAPTER 4

Cisco VMS Service Extensions

This chapter provides an overview of VMS service extensions and also describes the process to create, import, and apply service extension template to a service workflow.

This chapter contains the following topics:

Understanding How Cisco VMS Service Extensions Work

VMS service extensions simplifies how configuration snippets can be applied to a service or a device. VMS leverages the underlying capability of Cisco Network Services Orchestrator (NSO) custom templates, which get pushed along with the derived configuration templates. Service extensions can be used, in most cases, to map services to device configurations, without the need for any additional programming.

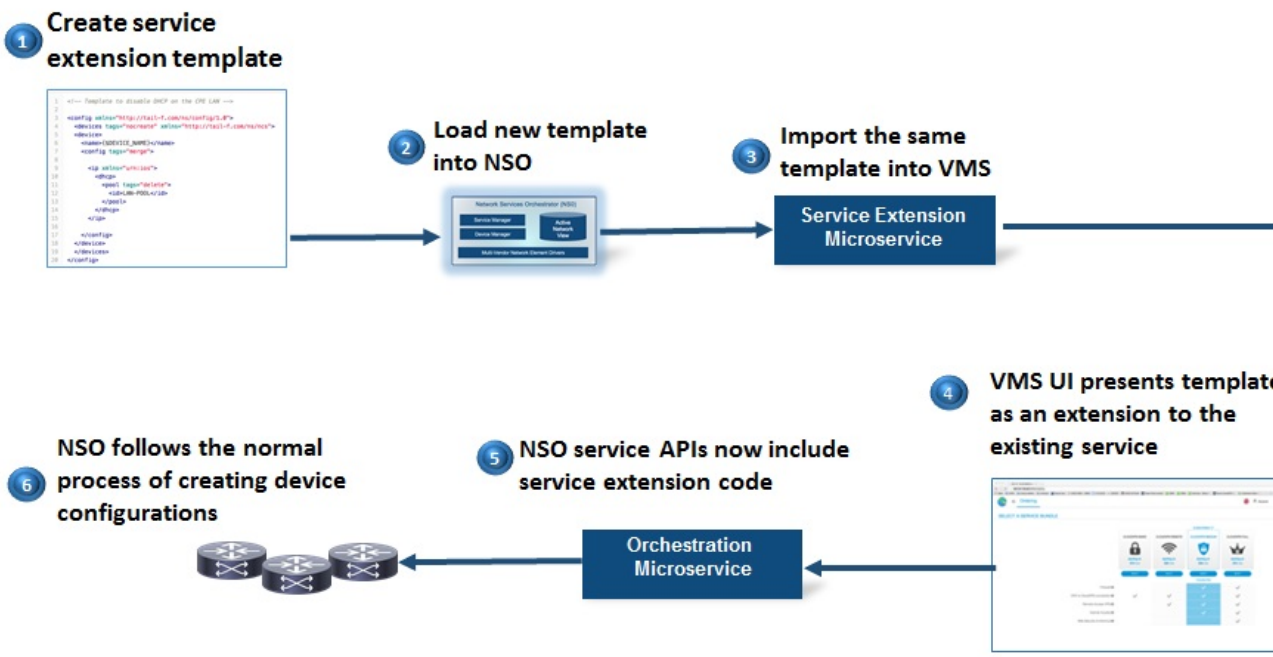
VMS service extension templates use variables to map service attributes to the corresponding device configurations and are applied. The service extensions allow a declarative way to describe such manipulations. The VMS operator can apply a service extension template to an existing service chain in VMS or to a device, without having to manually go into the NSO CLI. This service extension template is used by NSO to add, modify, or delete service configuration snippets before NSO pushes the configuration to the devices.

You can apply VMS service extension templates to a service ordering workflow or a single device. When you import a service extension template into VMS, you can specify if the template is to be applied to a service workflow or a device.

When a service extension template is applied to service ordering workflow, VMS service workflow gathers the parameter values the tenant users enter during service ordering process. These values are passed to NSO, which further uses these values in the device configurations.

The following illustration depicts the end-to-end workflow that needs to be followed to work with service extension templates in VMS.

Figure 1: VMS Service Extensions Workflow



Creating a VMS Service Extension Template XML File

The VMS service extension template is an XML file. The structure of that file is defined by the YANG model.

The basic principles of defining a template are as following:

1. A template is an XML file (for example **mytemplate.xml**) that corresponds to a node in the device tree.
2. Each value in a template is stored as a string. This string value is converted to the actual value type of the YANG model when the template is applied.
3. The value part of the XML tag that needs to be configured must be represented with a variable name prefixed with '$' literal.
4. The templates allow for defining different behavior while applying the template. This is accomplished by setting tags such as **merge, replace, delete, create or nocreate** on the relevant nodes in the template.

For example, to create a template to set the NTP server on a device, the sample template XML file should be:

```
<config
    xmlns="http://tail-f.com/ns/config/1.0">
    <device
        xmlns="http://tail-f.com/ns/ncs">
        <name>ntp</name>
        <config tags="merge">
            <system xmlns="http://pica8.org/yang">
                <ntp-server-ip>{$NTP}</ntp-server-ip>
            </system>
            <ntp xmlns="urn:ios">
                <server>
```

```
                    <server-list>
                        <ip-address>{$NTP}</ip-address>
                    </server-list>
                </server>
            </ntp>
        </config>
    </devices>
</config>
```

After you create a service extension template, you need to do the following:

Import the template XML file into NSO. For details see, Importing the Template XML File into NSO, on page 21.

Import the template XML file into VMS. For details see, Creating a Service Extension in the VMS Portal, on page 25.

Importing the Template XML File into NSO

To import a template XML file into NSO, you need to:

Procedure

Step 1 Log in to the Cisco Network Services Orchestrator (NSO) server.

Step 2 Create the Custom templates folder (only first time).

```
admin@ncs%sudo mkdir /var/opt/ncs/packages/custom-templates/templates/
```

Step 3 Create package-meta-data.xml file in `/var/opt/ncs/packages/custom-templates` folder (only first time).

```
admin@ncs%sudo vi package-meta-data.xml   <== copy content below

<ncs-package
    xmlns="http://tail-f.com/ns/ncs-packages">
    <name>custom-templates</name>
    <package-version>1.0</package-version>
    <description>Custom template store</description>
    <ncs-min-version>4.1</ncs-min-version>
</ncs-package>
```

Step 4 Verify the contents of the **package-meta-data.xml** file (only first time).

```
admin@ncs%/var/opt/ncs/packages$ cat
/var/opt/ncs/packages/custom-templates/package-meta-data.xml

<ncs-package
    xmlns="http://tail-f.com/ns/ncs-packages">
    <name>custom-templates</name>
    <package-version>1.0</package-version>
    <description>Custom Template Store</description>
    <ncs-min-version>4.1</ncs-min-version>
</ncs-package>
```

Step 5 Add service extensions custom templates to NSO, in the **/var/opt/ncs/packages/custom-templates/templates** folder.

Step 6 Enable NSO custom templates:

```
admin@ncs%set globals custom-template true
admin@ncs%commit
```

Step 7 Reload NSO.

```
admin@vms-ncs-tmepoc1-sm% request packages reload
```

Note
- When you reload NSO, ensure that the new template is present in the `/var/opt/ncs/packages/custom-templates/templates` folder.
- When the packages reload, ensure that all the CLI sessions are in operational mode and none of them are open in the Config mode.

Defining Service Extension Parameters for a Provider, Tenant Group, or Tenant

When a service extension template is imported into VMS, the operator needs to specify the metadata for each service extension parameter. In addition, the value of some of these parameters could be common across all devices for a service provider or for a tenant. In Cisco VMS 3.1 and later, when a service extension template is imported you can map the metadata and default values for service extension parameters. This is done by mapping template parameters to the predefined service extensions provider or tenant parameters during the template import process. The three types of service extension parameters are:

- **Provider Parameters** - Defined at the service provider level. The provider parameters are available across all the tenants.
- **Tenant Group Parameters** – Defined at the service provider level but the default value can be set for each tenant group.
- **Tenant Parameters** - Defined by the service extension designer and the default value can be set for each tenant.

Note When you define a tenant service extension parameter, you need to associate the parameter to a tenant or tenant group and can provide separate default values for each tenant or tenant group. For more information, seeSpecifying Default Value for a Service Extension Tenant Parameter , on page 24 .

The service extension parameters provide the following advantages:

- Can be defined at the service provider or the tenant group or the tenant level.
- Parameters are auto-mapped when a template XML file is imported into VMS and the parameter metadata gets inherited.
- Follows the order of precedence—First tenant parameters are used, if one exists. Otherwise the provider parameter is used.
- Set the default parameter values for provider or tenant parameter in service ord ering process.

To define service extension parameter, you need to:

Procedure

Step 1 Log in to the Cisco VMS Portal.

Note Cisco Virtual Managed Services now includes a new predefined role: Service Extension Designer. Service extension designers can import service extension templates, define service extension parameters, define default parameter values, and so on.

Step 2 From the Left Hand Side menu, choose **Setting**, and **Extensions**.

Step 3 To add service provider level parameters, do the following:

1. Click the **Provider** tab.
2. Click the **Add Extension Parameter** button.
3. Enter the parameter name.
4. Enter the parameter label that is displayed on the VMS portal.
5. Select the input type.
6. Select the display type.
7. Enter the default value for the parameter.
8. Click **Save**.

Step 4 To add Tenant Group parameters, do the following:

1. Click the **Tenant Group** tab.
2. Click the **Add Extension Parameter** button.
3. Enter the parameter name.
4. Enter the parameter label that is displayed on the VMS portal.
5. Select the input type.
6. Select the display type.
7. Click **Save**.

Step 5 To add tenant level parameters, do the following:

1. Click the **Tenant** tab.
2. Click the **Add Extension Parameter** button.
3. Enter the parameter name.
4. Enter the parameter label that is displayed on the VMS portal.
5. Select the input type.
6. Select the display type.

7. Click **Save**.

Specifying Default Value for a Service Extension Tenant Parameter

When you define service extension tenant parameter, you need to specify the default value for each tenant. This default value is inherited by the parameter when the service extension template is applied to a service workflow.

To specify service extension tenant parameter value, you need to:

Specify Service Extension Parameter Default Value for Tenants

Procedure

Step 1 Log in to the Cisco VMS Portal.

Note Cisco Virtual Managed Services now includes a new predefined role: Service Extension Designer. Service extension designers can import service extension templates, define service extension parameters, define default parameter values, and so on.

Step 2 From the Left Hand Side menu, choose **Tenants**.

The Manage Tenants screen appears.

Step 3 To specify the parameter default value, select the tenant user on the list and click the **Edit** icon.

Step 4 Specify the default value for the service extension parameter.

Step 5 Click **Save**.

Specify Service Extension Parameter Default Value for Tenant Groups

Procedure

Step 1 Log in to the Cisco VMS Portal.

Note Cisco Virtual Managed Services now includes a new predefined role: Service Extension Designer. Service extension designers can import service extension templates, define service extension parameters, define default parameter values, and so on.

Step 2 From the Left Hand Side menu, choose **Tenants Group**.

The Manage Tenants Groups screen appears.

Step 3 To specify the parameter default value, select the tenant user on the list and click the **Edit** icon.

Step 4 Specify the default value for the service extension parameter.

Step 5 Click **Save**.

Creating a Service Extension in the VMS Portal

Before you import service extension templates into VMS, you can define the service extensions global or tenant group or tenant parameters. For more information, see Defining Service Extension Parameters for a Provider, Tenant Group, or Tenant, on page 22.

To create a Service Extension, you need to:

Procedure

Step 1 Log in to the Cisco VMS Portal.

Note Cisco Virtual Managed Services now includes a new predefined role: Service Extension Designer. Service extension designers can import service extension templates, define service extension parameters, define default parameter values, and so on.

Step 2 From the Left Hand Side menu, choose **Configurations**.

Step 3 Click the service for which you want to import the service extension template.

Step 4 Click the **Service Extensions** tab.

Step 5 Click the **Add Service Extension** button.

Step 6 Click the **Upload File** button, to import the service extension template XML file.

Note The template name should match the exact name uploaded into NSO.

Step 7 Enter the template name and the description.

Step 8 Click **Next**.

Step 9 Do one of the following:

- To apply the template to all the tenant, select **All Tenants**.
- To apply the template to specific tenants, select **Specific Tenants** and select one or more tenant.

Step 10 Specify the XPATH that the service extension applies to. For more information, see table below.

Service Pack	XPATH	Device Type
cVPN Service Pack		
	/cloudvpn	Hub Router
	/cloudvpn/cpe	CPEs
	/cloudvpn/firewall	ASA Firewall

	/cloudvpn/wsa	WSA Services
	/cloudvpn/cpe[id='{DEVICE-ID}'] **Note** This XPATH must be specified for device templates.	Corresponding device
IWAN Service Pack		
	/iwan/hub-sites/	Border Routers
	/iwan/hub-sites/	Master Controllers
	/iwan/sites/cpes	Branch Devices
	/iwan/sites[./name='SITE2']/cpes	Only Branch Device SITE2
	/iwan/sites[contains(name, 'SITE1')]/cpes	Branch Device Name Contains “SITE1”
	/iwan/hub-sites/border-routes[name='{$ROUTER-ID}']	Specific router
	/iwan/sites/cpes[name='{$CPE-ID}'] **Note** This XPATH must be specified for device templates.	Corresponding device

Step 11 To apply a service extension template to a service order or a device, do one of the following:

- To enable the service extension template for a service order, select **Yes**.
- To enable the service extension template for a device, select **No**.

Step 12 Click **Next**.

The service extensions parameters are displayed.

VMS auto-maps the template parameters if the parameter name matches with the predefined service extension parameters, see Defining Service Extension Parameters for a Provider, Tenant Group, or Tenant, on page 22.

Note If you are enabling service extensions on a device, it is not mandatory to define the service extension parameters for a device. In this scenario, skip Step 13 and 14 and proceed directly to Step 15.

Step 13 To edit the parameter auto-mapping attributes, click the parameter and do the following:

1. Select the Function Pack Context check box.

   Note
   - If functional pack context check box is selected, then the parameter will not be seen in the form when applying the extension. The value will be resolved by NSO.
   - If the check box is not selected, then the value should be provided by the user either by mapping it to a predefined (provider, tenant, tenant-group) parameter or by providing it when applying the extension.

2. Click **Edit extension parameter mapping** link to disassociate the auto-mapping.
3. Click **Done**.

Step 14 Specify the Input Type and Display Type attributes for the service extension parameters.

Note If the Input Type and Display Type attribute is not specified for a parameter it is considered as a text field in the service ordering form.

Step 15 Click **Save and Enable**.

The service extension template is available to customers while they order the service.

Service Extensions on a Device

In addition to applying VMS service extension templates to a service ordering workflow, Cisco VMS provides you the capability to also apply these templates on a device. When you are importing a service extension template to VMS, you can specify whether the template has to be applied on a service workflow or on a device.

When a service extension template is applied to a device after the service is ordered, the service extension template is applied to the device outside the service ordering workflow and is available for the use of individual devices. The following table lists the various steps involved before applying the service extension templates to a device.

Steps	Related Section	Notes
1. Create a VMS Service Extension Template XML File.	Creating a VMS Service Extension Template XML File	
2. Import the Template XML File into NSO.	Importing the Template XML File into NSO	

Steps	Related Section	Notes
3. Create a Service Extension in the VMS Portal.	Creating a Service Extension in the VMS Portal	While performing this procedure, make sure that you: • Specify the XPATH of the device where the Service Extension has to be applied. For example, the XPATH for IWAN can be /iwan/hub-sites/border-routers[name='{$ID}'] or any other device where you want to apply the service extension. Adding a dollar parameter in the XPATH for a device ID automatically converts the Service Extension into a Device Extension. • Enable the service extension template for a device by setting the service extension template option for a service order as 'No'. • Skip Step 13 and 14 and proceed directly to Step 15, as it is not mandatory to define the service extension parameters for a device.
4. Apply Service Extensions on a Device.	Applying Service Extensions on a Device	

Applying Service Extensions on a Device

To apply a service extension template to a device:

Procedure

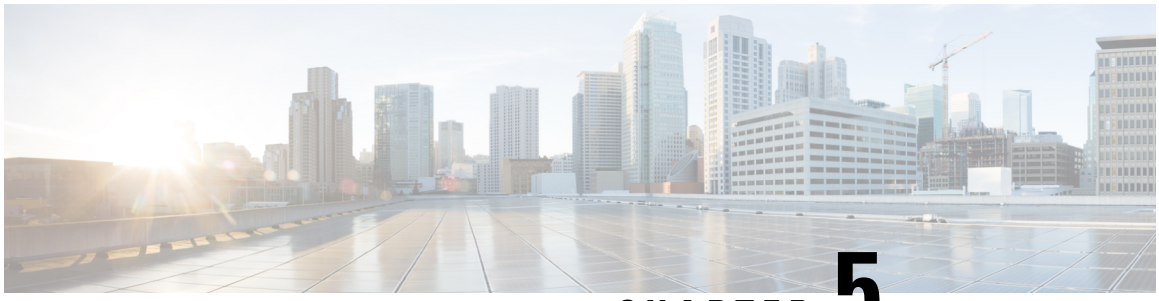
Step 1 Log in to the Cisco VMS Portal.

Step 2 From the left pane of the **Service Interface**, click **Devices** to view the list of devices you have purchased in the **Register Device** window.

Step 3 Click the device for which you want to apply service extension template and click **Device Extensions**. The Device Extension dialog box appears.

Step 4 Click the service extension and specify the corresponding parameter value.

Step 5 Click **Update**.



CHAPTER 5

Troubleshooting VMS Issues

To troubleshoot an issue, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

The following steps provide guidelines to use in the problem-solving process.

- Analyze the problem and create a clear problem statement. Define symptoms and potential causes.
- Gather the facts that you need to help isolate possible causes.
- Consider possible causes based on the facts that you gathered.

This section describes problems, possible causes, recommended actions, and error messages, if applicable to the problem.

Order Fails During Provisioning

Problem

When you place an order and the order goes into provisioning but fails during provisioning. VMS service interface indicates that the order provisioning has failed.

Solution

1. Review the tenant event logs UI to confirm the error occurred during provisioning and not initial validation.
2. The tenant user needs to escalate this issue to the service provider operator.

Note The system will not self-recover even if the unplugged devices are plugged back in.

3. The service provider operator has to login to NSO directly and fix the problem.
   - Ensure that the malfunctioning devices are taken offline.
   - Retry the provisioning operation.

When the NSO provisioning operation completes successfully, it sends the correct notification to the northbound interface, and resets the VMS service interface to the provisioned state.

Order Failed Error Message

Problem

When you place an order and get an order failed message right away (due to first-level call to NSO failing), it means that the order has failed.

Solution

1. Review the tenant Event logs and confirm the error is caused due to first-level call to NSO failing.
2. Deletes the order from the VMS service interface.
3. Place a new order.

Service Ordering Fails

Problem

When you try to order a service, the service ordering fails.

Solution

- Verify if all microservices are running
- Verify orchestration microservice is sending the appropriate provider name to NSO. Confirm that the "Provider Name" is populated correctly by navigating to **Settings** as an Admin.
- Check NSO netconf-north.log. If not, check connectivity between the VMS Portal and the NSO.

Device Registration Fails Due to Incorrect Serial Number

Problem

The device does not get registered with the PnP server and does not return any error if the tenant user enters an incorrect serial number during registration.

NSO PnP server zero touch provisioning works as:

- Tenant users register a device serial number against a device, which associates a device with a tenant, a site and a device, so VMS knows what type of configurations to push to this device.
- The connected devices call home to the PnP server, register themselves, and wait for the PnP server to push the configuration.

These events happen in any order and if the tenant user registers a device with a serial number that has not called home to the PnP server, the server waits for the device to call the PnP server. If this device never calls (because the serial number is invalid), the PnP server continues to wait.

Solution

Tenant user needs to register the device with the correct serial number. For more information, see the service pack guides on cisco.com.

Device Registration Fails Due to Incorrect CPE Day -1 Configuration

Problem

When you order a service, the service comprises of devices for sites. These devices must be registered with the VMS service interface. For more information, see Registering Devices.

If the device fails to register with the PnP server, you need to verify that the Day -1 configuration on the CPE allows it to call home to the PnP server.

Solution

1. Log in to the device and verify to which PNP server the device is connected to.
2. Run command show run | s pnp to list the current PnP server that this device is talking to, and examine the output:

```
Router#show run | s pnp pnp
Router#profile zero-touch transport https ipv4 <IP address> port 443 remotecert ncs
```

3. To change the IP address of the PNP server, switch to the configuration mode.

```
Router#config terminal
Router(config)#
```

4. Enter text that you received as output in Step 2o, replacing the IP address with the new one.

```
Router(config)#pnp profile zero-touchtransport https ipv4 <IP address> port 443 remotecert
 ncs
```

5. Exit out of Router(config-pnp-init) mode and then out of Router(config) mode.
6. Copy the configuration into flash configuration, by running the following command:

```
Router#copy running-config flash:day--1-config
Destination filename [day--1-config]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
4609 bytes copied in 0.876 secs (5261 bytes/sec)
```

Obtaining CPE Password

If a CPE is in True/True/True state, then it should be possible to SSH from the NSO to the CPE. Required information (CPE Management IP Address, username, password) can be obtained from NSO by executing the `show pnp-state device` command as shown below.

```
admin@vms-ncs-sm> show pnp-state device XXX194326WW
pnp-state device XXX194326WW
udi PID:C881-K9,VID:V01,SN:XXX194326WW
device-info 15.5(3)M1
ip-address 11.156.141.167
mgmt-ip 10.254.0.29
port 22
name cpe-XXX194326WW
username admin
password cpe_password
sec-password cpe_password
salt ABCD
remote-node vms-ncs-dm
wan-interface FastEthernet4
lan-interface FastEthernet0
configured true
request backoff
added true
synced true
is-netsim false
need-clean false
pending-exec ""
last-contact 2015-12-09 01:53:33
last-clean 0
[ok][2015-12-09 01:54:14]
```

From NSO, establish an SSH session to the CPE.

```
admin@vms-ncs-sm> ssh 10.254.0.29
Password:cpe_password
router line 11
router#
```

Physical or Virtual CPE status

If you want to check the CPE status, execute the following command:

```
admin@ncs-sm> show pnp list
SERIAL        IP ADDRESS       CONFIGURED  ADDED  SYNCED  LAST CONTACT
-------------------------------------------------------------------------------
FJC2012A29P   11.255.255.35    false       false  false   2016-06-08 16:16:28
FJC2013L1SZ   11.255.255.42    false       false  false   2016-06-08 16:17:13
FJC2020L11L   11.255.255.25    false       false  false   2016-06-06 16:27:12


CONFIGURED: Day-0 config. Pushed onto CPE device
ADDED: CPE device is added into NCS
SYNCED: Service configs pushed into device
```

Display Core Data

If you want to check if the firewall, router and such Cloud VPN components are provisioned, you can execute the `show core-data` command as follows. The following example is for a Cloud VPN Advanced Service with Web Security offer:

```
 admin@ncs-sm% show core-data eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1
offering      CVPN;
service-type  FULL;
provider      vms-ottpod1;
tenant        eb272672-e0e4-4344-9a52-68cc3c1d1be1;
remote-node   ncs-dm;
geo-redundant false;
nfv cpe-FJC2027L1NQ {
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-ASA-dev1-esc-device {
    type          vFirewall;
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    type          vRouter;
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-WSA-dev1-esc-device {
    type          vWSA;
    isProvisioned true;
}
allocations eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    pool-name loopback;
}
```

Core data for VCE

```
 admin@ncs-sm% show core-data eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-2
offering     VCE;
service-type converged;
provider     vms-ottpod1;
tenant       eb272672-e0e4-4344-9a52-68cc3c1d1be1;
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    type          vRouter;
    isProvisioned true;
}
```

Device Registration Fails Due to Incorrect CPE Day -1 Configuration

Problem When you place an order for a service, the service comprises of devices for sites. These devices must be registered with the VMS service interface.

Problem If the device fails to register with the PnP server, you need to verify that the Day -1 configuration on the CPE allows it to call home to the PnP server.

Solution

1. **Solution** Log in to the device and verify to which PNP server the device is connected to.
2. **Solution** Run command show run | s pnp to list the current PnP server that this device is talking to, and examine the output:

   ```
   Router#show run | s pnp pnp
   Router#profile zero-touch transport https ipv4 <IP address> port 443 remotecert ncs
   ```

3. **Solution** To change the IP address of the PNP server, switch to the configuration mode.

   ```
   Router#config terminal
   Router(config)#
   ```

4. **Solution** Enter text that you received as output in Step 2, replacing the IP address with the new one.

   ```
   Router(config)#pnp profile zero-touchtransport https ipv4 <IP address> port 443 remotecert
   ncs
   ```

5. **Solution** Exit out of Router(config-pnp-init) mode and then out of Router(config) mode.
6. **Solution** Copy the configuration into flash configuration, by running the following command:

   ```
   Router#copy running-config flash:day--1-config
   Destination filename [day--1-config]?
   %Warning:There is a file already existing with this name
   Do you want to over write? [confirm]
   4609 bytes copied in 0.876 secs (5261 bytes/sec)
   ```

Note **Solution** The digital certificate supplied to the “crypto pki certificate chain ncs” should be updated to match the certificate installed on the PNP proxy of the Edge Server.

PnP Server CLI Command

Solution PnP Server to IP Device

```
show run | s pnp
Router#show run | s pnp pnp profile zero-touch transport https ipv4 203.35.248.89 port 443
remotecert ncs
```

Solution PnP Server configured with HTTPS and SSL

```
admin@ncs-sm-vbranch> show configuration pnp server
port 443;
use-ssl true;
[ok][2016-05-31 19:33:28]
```

Solution List of devices and states in contact with the PnP Server

```
admin@ncs-sm-vbranch> show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
------------------------------------------------------------------------------
FTX1738AJME 173.36.207.85 true true true 2016-05-23 23:44:44
FTX1738AJMG 173.36.207.81 true true true 2016-05-23 23:43:50
FTX1740ALBX 173.36.207.80 true true true 2016-05-23 23:44:21
SSI184904LG 173.36.207.82 true true true 2016-05-23 23:43:56
SSI185104LT 173.36.207.84 true true true 2016-05-23 23:43:57
[ok][2016-05-23 23:44:49]
```

Solution PNP commands to reset the CPE

```
request pnp reset clean serial xxxxxx
request pnp delete serial xxxxxx
```

If the day-1-config file need changing on CPE use the commands to create a new file and overwrite the existing:

```
tclsh
puts [open "flash:day--1-config" w+] {
aaa new-model
aaa authentication login default none
interface GigabitEthernet0
…..
pnp profile zero-touch
transport https ipv4 x.x.x.x port 443 remotecert ncs
}
Tclquit
```

Solution Viewing device-info through PnP-state

```
admin@ncs-sm-vbranch> show pnp-state device FTX1738AJME
pnp-state device FTX1738AJME
udi PID:ISR4451-X/K9,VID:V02,SN:FTX1738AJME
device-info 15.5(3)S2
ip-address 173.36.207.81
mgmt-ip 10.254.0.1
port 22
name FTX1738AJME
username user-site2
password cisco223
sec-password priv-cisco222
snmp-community-ro cisco
salt ABCD
remote-node ""
wan-interface GigabitEthernet0/0/1
lan-interface GigabitEthernet0/0/0
configured true
request config
added false
synced false
is-netsim false
need-clean false
pending-exec ""
last-contact 2016-05-31 19:29:18
last-clean 0
reload-upon-delete false
[ok][2016-05-31 19:29:23]
```