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**.