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 2
- Managing Tenants and Tenant Groups, on page 4

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 1: 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 4
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 3.
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 5

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 5.

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 Configure Integrations

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.