VMM USER ROLES

How to Add Users to the Administrator User Role in VMM

Applies To: System Center 2012 SP1 - Virtual Machine Manager, System Center 2012 R2 Virtual Machine Manager, System Center 2012 - Virtual Machine Manager

The Administrator user role is created when you install Virtual Machine Manager (VMM). The user who performs the VMM installation and all domain users in the Local Administrators group are added to the Administrator user role.

Use this procedure to add users to the Administrator user role in VMM or remove users from the user role.

Account requirements Administrators can add new users to the Administrator user role or remove users from that user role.

Creating User Roles in VMM

Applies To: System Center 2012 SP1 - Virtual Machine Manager, System Center 2012 R2 Virtual Machine Manager, System Center 2012 - Virtual Machine Manager

You can create user roles in Virtual Machine Manager (VMM) to define the objects that users can manage and the management operations that users can perform. The following table summarizes the capabilities of each user role in VMM.

User Role Descriptions for VMM

VMM User Role	Capabilities
Administrator	Members of the Administrators user role can perform all administrative actions on all objects that VMM manages. Administrators have sole responsibility for these features of VMM: - Only administrators can add stand-alone XenServer hosts and XenServer clusters (known as pools) to VMM management. - Only administrators can add a Windows Server Update Services (WSUS) server to VMM to enable updates of the VMM fabric through VMM. .

Use this procedure to add users to the Administrator user role in VMM or remove users from the user role.

Account requirements Administrators can add new users to the Administrator user role or remove users from that user role.

To add users to the Administrator user role

1. In the **Settings** workspace, click **Security**, then click **User Roles**. Under **User Roles**, click the **Administrator** user role to select it.
2. In the **Home** tab, in the **Properties** group, click **Properties**
3. In the **Administrator Properties** dialog box, click **Members** to access the **Members** page, and then click **Add** to open the **Select Users, Computers, or Groups** dialog box.
4. Enter a user or Active Directory group of users and click **OK** to continue. The dialog box verifies that your selections are valid users.

   Note

   You can delete members from the **Members** page by selecting an entry and then clicking **Remove**.

5. Click **OK** to save your changes.

Members of the **Delegated Administrator user role** can perform all administrative tasks within their assigned host groups, clouds, and library servers, except for adding XenServer and adding WSUS servers. Delegated Administrators cannot modify VMM settings, and cannot add or remove members of the Administrators user role.

Fabric Administrator (Delegated Administrator)

How to Create a Delegated Administrator User Role in VMM

Use this procedure to create a Delegated Administrator user role in Virtual Machine Manager (VMM).

Account requirements Administrators and delegated administrators can create a Delegated Administrator user role. Delegated administrators can create Delegated Administrator user roles that include a subset of their scope, library servers, and Run As accounts.

To create a Delegated Administrator user role

1. In the **Settings** workspace, on the **Home** tab in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard**, enter a name and optional description for this Delegated Administrator user role. Click **Next** to continue.
3. On the **Profile** page, select **Delegated Administrator**, and then click **Next**.
4. On the **Members** page, click **Add** to add user accounts and Active Directory groups to the user role with the **Select Users, Computers, or Groups** dialog box. After you have added the members, click **Next**.
5. On the **Scope** page, select private clouds or host groups for this Delegated Administrator, and then click **Next**. A delegated administrator differs from an administrator by having a defined scope in which the delegated administrator can make changes.
6. On the **Library servers** page, click **Add** to select one or more library servers with the **Select a Library server** dialog box. Click **OK** to select a server, and then click **Next**.
7. On the **Run As accounts** page, click **Add** to open the **Select a Run As account** dialog box. Select one or more accounts and click **OK** to add the account to the **Run As accounts** page.
    - Use the Ctrl key to select multiple accounts.
    - Click the **Create Run As Account** button to access the **Create Run As Account** dialog box.

    After selecting accounts, click **Next** to continue.

8. Review the settings you have entered and then click **Finish** to create the Delegated Administrator user role.

After you create a delegated administrator, you can change **Members**, **Scope**, **Library servers**, and **Run As accounts** in the **Properties** dialog box for the Delegated Administrator user role.

Read-Only Administrator

Read-only administrators can view properties, status, and job status of objects within their assigned host groups, clouds, and library servers, but they cannot modify the objects. Also, the read-only administrator can view Run As accounts that administrators or delegated administrators have specified for that read-only administrator user role.

How to Create a Read-Only Administrator User Role in VMM

Use this procedure to create a Read-Only Administrator user role in Virtual Machine Manager (VMM).

Account requirements Administrators and delegated administrators can create a Read-Only Administrator role. Delegated administrators can create Read-Only Administrator user roles that include a subset of the Delegated Administrator user role's scope, library servers, and Run As accounts.

To create a Read-Only Administrator user role

1. In the Settings workspace, on the Home tab in the Create group, click Create User Role.
2. In the Create User Role Wizard, enter a name and optional description for this Read-Only Administrator. Click Next to continue.
3. On the Profile page, select Read-Only Administrator and then click Next.
4. On the Members page, click Add to add user accounts and Active Directory groups to the user role with the Select Users, Computers, or Groups dialog box. After you have added the members, click Next.
5. On the Scope page, select private clouds or host groups for this read-only administrator, and then click Next. A read-only administrator can only view items within this defined scope.
6. On the Library servers page, click Add to select one or more library server with the Select a Library server dialog box. Click OK to select a server, and then click Next.
7. On the Run As accounts page, click Add to open the Select a Run As account dialog box. Select one or more accounts and click OK to add the account to the Run As accounts page.
    - Use the Ctrl key to select multiple accounts.
    - Click the Create Run As Account button to access the Create Run As Account dialog box.

    After selecting accounts, click Next to continue.

8. Review the settings you have entered and then click Finish to create the Read-Only Administrator user role.

After you create a read-only administrator, you can change its Members, Scope, Library servers, and Run As accounts in the Properties dialog box for the Read-Only Administrator user role.

As of VMM in System Center 2012 Service Pack 1 (SP1), you can create Tenant Administrator user roles.

Members of the Tenant Administrator user role can manage self-service users and VM networks. Tenant administrators can create, deploy, and manage their own virtual machines and services by using the VMM console or a web portal. Tenant administrators can also specify which tasks the self-service users can perform on their virtual machines and services. Tenant administrators can place quotas on computing resources and virtual machines.

How to Create a Tenant Administrator User Role in VMM

Tenant Administrator

As of Virtual Machine Manager (VMM) in System Center 2012 Service Pack 1 (SP1), you can create a Tenant Administrator user role. Tenant administrators can create and manage self-service users and VM networks. Tenant administrators can create, deploy, and manage their own virtual machines and services by using the VMM console or a web portal. A tenant administrator can specify which tasks the self-service users can perform on their virtual machines and services, and can place quotas on computing resources and virtual machines.

Account requirements Administrators and delegated administrators can create a Tenant Administrator user role.

To create a Tenant Administrator user role

1. In the **Settings** workspace, on the **Home** tab in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard**, enter a name and optional description for this Tenant Administrator user role, and then click **Next**.
3. On the **Profile** page, select **Tenant Administrator**, and then click **Next**.
4. On the **Members** page, click **Add** to add user accounts and Active Directory groups to the user role. Add the members by using the **Select Users, Computers, or Groups** dialog box, and then click **Next**.
5. On the **Scope** page, select the private clouds that the members of this Tenant Administrator role can use. If you want to allow members of this role to receive and implement Performance and Resource Optimization (PRO) tips, select **Show PRO tips**. Then click **Next**.

6. If one or more **Quotas** pages appear (based on whether you selected private clouds on the previous wizard page), review and specify quotas as needed for each private cloud. Otherwise, skip to the next step.

   To set quotas for the combined use of all members of this user role, use the upper list. To set quotas for each individual member of this user role, use the lower list. By default, quotas are unlimited. To create a limit, clear the appropriate check box under **Use Maximum** and then, under **Assigned Quota**, select a limit. When you have completed all settings, click **Next**.

7. On the **Networking** page, to add the VM networks that the members of this Tenant Administrator role can use, click the **Add** button, select one or more VM networks, and then click **OK**. Then click **Next**.
8. On the **Resources** page, do the following:
   1. Under **Resources**, click **Add** to select resources by using the **Add Resources** dialog box, and then click **OK**.
   2. Under **Specify user role data path**, click **Browse** to specify a library path that members of this user role can use to upload data.
   3. Click **Next**.
9. Select one or more actions that the members of this role can perform, as follows:
   - As of System Center 2012 R2, on the **Permissions** page, select global actions, and any cloud-specific actions.
   - Otherwise, select global actions.

   Click **Next**.

10. If the **Run As accounts** page appears (based on whether you selected the **Author** action on the **Actions** page), add Run As accounts that you want the members of this user role to be able to use. Otherwise, skip to the next step.
11. If the **Quotas for VM networks** page appears (based on whether you selected the **Author VMNetwork** action on the **Actions** page), review and specify quotas to limit the number of VM networks that members of this user role can create. Otherwise, skip to the next step.

    To limit the combined number of VM networks that can be created by all members of this user role, use the upper setting. To limit the number of VM networks that can be created by each individual member of this user role, use the lower setting.

12. On the **Summary** page, review the settings you have entered. Click **Finish** to create the Tenant Administrator user role, or click **Previous**

to change any settings.

13. In the **Settings** pane, expand **Security** and then click **User Roles**. Verify that the Tenant Administrator user role that you created appears in the User Roles pane.

After you create a Tenant Administrator user role, you can change **Members**, **Scope**, **Networking**, **Resources**, and **Actions** in the **Properties** dialog box for the Tenant Administrator user role.

Application Administrator (Self-Service User)	Members of the Self-Service User role can create, deploy, and manage their own virtual machines and services by using the VMM console or a Web portal.

C

How to Create a Self-Service User Role in VMM

You can use this procedure to create a Self-Service User role in Virtual Machine Manager (VMM).

Account requirements Administrators and delegated administrators can create Self-Service User roles. Delegated administrators can create Self-Service User roles for private clouds that are in the scope of their user role.

To create a Self-Service User role

1. In the **Settings** workspace, on the **Home** tab, in the **Create** group, click **Create User Role**.
2. In the **Create User Role Wizard** on the **Name and description** page, enter a name and optional description of the Self-Service User role, and then click **Next**.
3. On the **Profile** page, click **Self-Service User**, and then click **Next**.
4. On the **Members** page, add user accounts and Active Directory groups to the role, and then click **Next**.

Note

If you want all role members to share ownership of all virtual machines that any member creates, create a security group in Active Directory and assign that group to the user role. An alternate method for sharing resources among Self-Service User role members is to use the **Share** and **Receive** actions, discussed later, which enable resource owners

who are self-service users to share individual resources with one or all members of a Self-Service User role.

If you plan to use this user role to test deploying virtual machines and services to a private cloud, be sure to add yourself as a member.

5. On the **Scope** page, select at least one private cloud for the Self-Service User role, and then click **Next**.
6. On the **Quotas** page, set quotas for each private cloud that is in the scope of the user role, and then click **Next**. If multiple private clouds are assigned to a Self-Service User role, you will see a **Quotas** page for each private cloud.

Note

Each quota sets an individual limit for each member of the user role. If you want all role members to share overall quotas, create a security group in Active Directory and assign that group to the user role.

7. Quota Types Supported for Self-Service in VMM

Quota Type	Description
Virtual CPUs	Limits the total number of virtual machine CPUs that can be consumed from the private cloud.
Memory (MB)	Limits the amount of virtual machine memory (in megabytes) that can be consumed from the private cloud.
Storage (GB)	Limits the amount of virtual machine storage (in Gigabytes) that can be consumed from the private cloud.
Custom quota (points)	Sets a quota on virtual machines deployed on the private cloud based on total quota points assigned to the virtual machines via their virtual machine templates. Quota points are an arbitrary value that can be assigned to a virtual machine template based on the anticipated "size" of the virtual machines. Custom quotas are provided for backward compatibility with self-service user roles created in VMM 2008 R2.
Virtual machines	Limits the total number of virtual machines that can be deployed on a private cloud.

8. Quotas only apply to deployed virtual machines. If a Self-Service User role has permission to store virtual machines, the quota does not apply to virtual machines that are stored in the library.

9. On the **Resources** page, click **Add** to open the **Add Resources** dialog box. Assign hardware profiles, operating system profiles, virtual machine templates, application profiles, SQL server profiles, and service templates for the self-service users to use during virtual machine creation.
10. Under **Specify user role data path**, use the **Browse** button to select a path on a library share where user role members can upload and share their own resources. The user data path also is a good place to store prepared resources that should be shared only with members of this Self-Service User role.

    Click **Next** to continue.

11. On the **Actions** page, select the actions that the self-service users need to perform on their own virtual machines and services, and then click **Next**. To select all actions, click **Select all**.

Actions Available to Self-Service User Roles in VMM

Action	Description
Author	Grants members permission to author templates and profiles. Users with authoring rights can create hardware profiles, operating system profiles, application profiles, SQL Server profiles, virtual machine templates and service templates.
Checkpoint	Grants members permission to create, edit, and delete checkpoints for their own virtual machines and to restore their virtual machine to a previous checkpoint. **Note:** VMM does not support checkpoint actions on services.
Checkpoint (Restore only)	Grants members permission to restore their own virtual machines to a checkpoint but not to create, edit, and delete checkpoints.
Deploy	Grants members permission to deploy virtual machines and services from templates and virtual hard disks that are assigned to their user role. However, they do not have the right to author templates and profiles. (Expanded in VMM to include creation of services)
Deploy (From template only)	Grants members permission to deploy virtual machines and services from templates that are assigned to their user role. However, they do not have any authoring rights. (Expanded in VMM to include creation of services)
Local Administrator	Grants members permission to serve as a local Administrator on their own virtual machines. **Important:** Be sure to select the **Local Administrator** action on any Self-Service User role that has the

	Deploy (From Template) action selected. This action enables those users to set the local Administrator password during virtual machine and service deployment. Self-service users who are granted the **Deploy** action do not need this action to be able to set local Administrator credentials.
Pause and resume	Grants members permission to pause and resume their own virtual machines and services.
Receive	Allows members to receive resources that are shared by members of other Self-Service User roles.
Remote connection	Grants members permission to connect to their virtual machines from the VMM console, the VMM Self-Service Portal, or App Controller. **Note:** As of System Center 2012 Service Pack 1 (SP1), the VMM Self-Service Portal has been removed. If you need a self-service portal solution, we recommend that you use App Controller. For more information, see App Controller.
Remove	Grants members permission to remove their own virtual machines and services.
Save	Grants members permission to save their own virtual machines and services.
Share	Allows members to grant resources that they own to other Self-Service User roles. Sharable resources include hardware profiles, operating system profiles, application profiles, SQL Server profiles, virtual machine templates, virtual machines, service templates, and services. A self-service user must be the owner of a resource to share it. The Self-Service User role that receives the shared resource must be assigned the **Receive** action.
Shut down	Grants members permission to perform an orderly shutdown of their own virtual machines and services.
Start	Grants members permission to start their own virtual machines and services.
Stop	Grants members permission to stop their own virtual machines and services.
Store and re-deploy	Grants members permission to store their own virtual machines in the VMM library, and re-deploy those virtual machines. Virtual machines stored in the library do not count against a user's virtual machine

quotas. **Note:** VMM does not support storing services.

12. If you selected the **Author** action, the **Run As accounts** page opens. Select Run As accounts for the Self-Service User role to use in the templates and profiles that they use to create virtual machines and services, and then click **Next**.
13. Review the settings you have entered on the **Summary** page, and then click **Finish**.

After you create a Self-Service User role, you can change settings using the **Properties** dialog box for the user role.

If you grant rights for a particular template to a user that does not have rights to the Run As

account that the template is configured with, then the user can potentially extract the credentials for the Run As account from the template.

As of System Center 2012 R2, VMM administrators can use the Create User Role Wizard **to configure user roles with a set of permitted actions on a per-cloud basis in addition to the global settings. These settings apply only to the tenant administrator and the self-service user roles. With these settings, the user's effective permitted actions for a given cloud are the combination of their global permitted actions and cloud permitted actions**.