Configuring a Super User

The Super User feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization, and if necessary, remove the protection or change the protection that was previously applied. The Super User feature is a feature to access all protected content of your tenant. It must be activated manually (it is not enabled by default), and it is possible to assign the rights to single users or groups.

When to use the Super User feature?

The Super User feature is not only required for data recovery but also for any operation that processes protected documents, files and emails and that needs access to the content. There are different situations where the Super User feature is required to access protected documents, including:

- An employee leaves the organization and you need to read the files that they protected.
- An IT administrator needs to remove the current protection policy that was configured for files and apply a new protection policy
- Exchange Server needs to index mailboxes for search operations
- You have existing IT services for data loss prevention (DLP) solutions, content encryption gateways (CEG), and anti-malware products that need to inspect files that are already protected
- You need to bulk decrypt files for auditing, legal, or other compliance reasons

It does not matter at which point you activate a Super User. Even if you activate it after you are protecting certain files, you can still unprotect and decrypt them at a later point.

Configuring the Super User

By default, the super user feature is not enabled, and no users are assigned this role. It is enabled for you automatically if you configure the Rights Management connector for Exchange, and it is not required for standard services that run Exchange Online, SharePoint Online, or SharePoint Server.

The Super User is configured with the PowerShell cmdlets from the AADRM module. It is not possible to configure it through any of the products' GUI.

To manually enable the super user feature, use the PowerShell cmdlet **Enable-AadrmSuperUserFeature**, and then assign users (or service accounts) as needed by using the **Add-AadrmSuperUser** cmdlet or the **Set-AadrmSuperUserGroup** cmdlet and add users (or other groups) as needed to this group.

It is possible to add Azure AD users and mail-activated groups to the Super User feature. By default, the Super User feature is not enabled and neither a user nor a group is assigned to it.

To activate and configure the Super User feature, you must use the AADRM PowerShell modules as follows:

1. Connect to the Azure RMS service by running the following cmdlet:Connect-AadrmService

2. Check the activation status of the Super User by running the following cmdlet:Get-AadrmSuperUserFeature
3. If the function is not “enabled” yet, activate it with the following cmdlet:Enable-AadrmSuperUserFeature
4. You can now add a single Azure AD user or an Azure AD group through the following cmdlets, respectively:Add-AadrmSuperUser -EmailAddress <emailaddress>orSet-AadrmSuperUserGroup -GroupEmailAddress <emailaddress>

The following table identifies the cmdlets that are needed to configure a Super User:

PowerShell Cmdlet	**Description**
Get-AadrmSuperUserFeature	Check the status of the super user feature.
Enable-AadrmSuperUserFeature	Enables the super user feature.
Disable-AadrmSuperUserFeature	Disables the super user feature.
Add-AadrmSuperUser	Adds an individual account to the super user list for your organization.
Set-AadrmSuperUserGroup	Specifies a group to use as the super user group.
Get-AadrmSuperUser	Check the currently configured Super Users.
Get-AadrmSuperUserGroup	Check the currently configured Super User Group.
Get-AadrmAdminLog	Generates logs for all administrative commands. You

	can specify a start time and stop time of entries to include.

Note: Using a group for the Super Users is easier to manage, but be aware that for performance reasons, Azure Rights Management caches the group membership. So if you need to assign a new user to be a super user to decrypt content immediately, add that user by using **Add-AadrmSuperUser**, rather than adding the user to an existing group that you have configured by using **Set-AadrmSuperUserGroup**.