Filename: microsoft-ms101-10-6-1-configure-super-user
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Azure Information Protection (AIP)
EpisodeName: Configure Super User
Description: Adam and Wes discuss the steps necessary to help you successfully plan for configuring the super user functionality.

Configure Super User

Manage Microsoft 365 Governance and Compliance (35-40%)

Implement Azure Information Protection (AIP)
• Plan AIP Solution
• Plan for Deployment On-Prem Rights Management Connector
• Plan for Windows Information Protection (WIP) Implementation
• Plan for Classification Labeling
• Configure Information Rights Management (IRM) for Workloads
• Configure Super User
• Deploy AIP Clients
• Implement Azure Information Protection Policies
• Implement AIP Tenant Key

==========

Configure 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.

If necessary, the protection can then be removed or changed.

A super user always has the Rights Management Full Control usage right for documents and emails that have been protected by your organization's Azure Information Protection tenant.

For example, you would use this feature for any of the following scenarios:

```
• 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.

Configuration for the super user feature

NOTE: 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.

If you need to manually enable the super user feature, use the PowerShell cmdlet Enable-AipServiceSuperUserFeature, and then assign users (or service accounts) as needed by using the Add-AipServiceSuperUser cmdlet or the Set-AipServiceSuperUserGroup cmdlet and add users (or other groups) as needed to this group.

Although using a group for your super users is easier to manage, 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-AipServiceSuperUser, rather than adding the user to an existing group that you have configured by using Set-AipServiceSuperUserGroup.

Security best practices for the super user feature:

```
• Restrict and monitor the administrators who are assigned a global
```

administrator for your Office 365 or Azure Information Protection tenant, or who are assigned the GlobalAdministrator role by using the Add-AipServiceRoleBasedAdministrator cmdlet. These users can enable the super user feature and assign users (and themselves) as super users, and potentially decrypt all files that your organization protects.

• To see which users and service accounts are individually assigned as super users, use the Get-AipServiceSuperUser cmdlet. To see whether a super user group is configured, use the Get-AipServiceSuperUserGroup cmdlet and your standard user management tools to check which users are a member of this group. Like all administration actions, enabling or disabling the super feature, and adding or removing super users are logged and can be audited by using the Get-AipServiceAdminLog command.

• If you do not need the super user feature for everyday services, enable the

feature only when you need it, and disable it again by using the Disable-AipServiceSuperUserFeature cmdlet.