DocAve®
Governance Automation Online

Administrator Guide

Service Pack 9, Cumulative Update 6

Issued December 2017

Table of Contents

What's New in this Release

- Office 365 customers can now extend their governance strategy to Microsoft Teams.

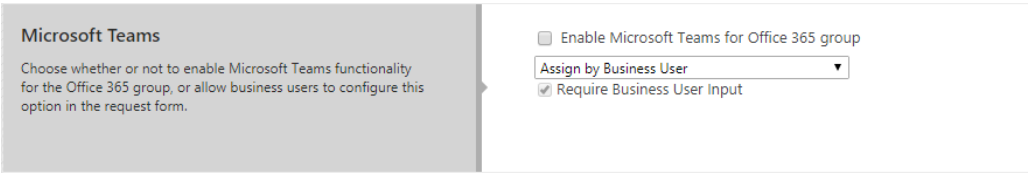

Figure 1:The Microsoft Teams functionality.

- IT Admins can configure the e-mail template language to specify the display language of e-mails sent to recipients, when configuring the e-mail template.
- IT Admins can choose to use the default recipient mailbox settings, or choose to send e-mails to custom mailboxes, when configuring the e-mail settings.
- The Create Site Collection service now supports adding suffix to the URL of the site collection created via this service request.

For more information, refer to the Release Notes.

The following updates have been made to this user guide for this release:

- Added information about the **E-mail Template Language** field in the Configuring E-mail Templates section.
- Added information about the **Microsoft Teams** field in the Configuring Create Group Services section.
- Added information about the **Microsoft Teams** field in the Configuring Change Group Settings Services section.
- Added information about the **Recipient Settings** field in the Configuring E-mail Settings section.
- Added information about the suffix for the site collection URL in the **URL** field of the Configuring Create Site Collection Services section.

About DocAve Governance Automation Online

DocAve Governance Automation Online is an online version of DocAve Governance Automation that supports the need for organizations to use Microsoft SharePoint as a service by automating the ways users request configurable services including, but not limited to: content management, lifecycle management, permissions management, and provisioning.

Governance Automation Online provides ways to create and govern your SharePoint Online objects automatically, by submitting rich and customizable predefined service requests which can trigger corresponding approval processes and policies to accomplish the processes. This automation results in more speed, overall effectiveness of the interactions and often a reduction in errors.

Governance Automation Online is available both commercially and for the U.S. Government Public Sector.

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. You can Submit Your Feedback on our website.

Integration with AvePoint Online Services

Governance Automation Online is integrated with AvePoint Online Services. To sign up for a Governance Automation Online account, you must first sign up an account in AvePoint Online Services. AvePoint provides the following methods to sign up for an AvePoint Online Services account:

- Sign up on the AvePoint Online Services website.
- Visit the AvePoint Online Services page or the DocAve Governance Automation Online page on the AvePoint official website.
- To sign up for AvePoint Online Services for U.S. Government Public Sector, access the following URL: https://usgov.avepointonlineservices.com.

To access Governance Automation Online, use one of the entries above to sign in to AvePoint Online Services. For details, refer to the AvePoint Online Services User Guide.

From any page within Governance Automation Online, you can open a new tab to access AvePoint Online Services or another AvePoint service. Click the change to a different service ( ) button on the upper-right corner, and then click **AvePoint Online Services** or a service.

AvePoint Online Services Versions: Commercial and U.S. Government Public Sector

There are two versions of AvePoint Online Services: a version for Commercial use, and a version available on Microsoft's Cloud Platform for U.S. Government. The U.S. Government Public Sector version of AvePoint Online Services offers most of the same functionality as the Commercial version. For details, refer to the AvePoint Online Services User Guide. The Governance Automation Online for the U.S. Government Public Sector version differs from the Commercial version in the following ways:

- The link to download the Governance Automation Online App file is different. For details, refer to Downloading the Governance Automation Online App.
- The app domain and redirect URI used to register the Governance Automation Online App are different. For details, refer to Registering the Governance Automation Online App.
- The APIs used to log into Governance Automation Online and to get a list of requests created by the login user are different. For details, refer to Implementing Governance Automation Online API.

Browser Support Information

The following table provides the supported browser versions:

Browser	Version
Internet Explorer	Any version of IE 11
Google Chrome	The latest version
Mozilla Firefox	The latest version
Microsoft Edge	The latest version

Before You Begin

Refer to the sections below for important information on Governance Automation Online.

Understanding Governance Automation Online

If you are new to Governance Automation Online, it may be helpful to review the Governance Automation Online Key Terms and Phrases to familiarize yourself with the key terms that are used throughout this user guide.

Once you are familiar with Governance Automation Online terminology, it is important to understand how the different features and functionalities work together. This knowledge is essential to properly configure the software for your organization.

In Governance Automation Online, administrators can set up services that perform SharePoint Online or DocAve Online operations. These services can be made available and customized for specific departments/purposes. A service may have a policy associated with it so that if your organization has specific rules on certain SharePoint Online operations, you can ensure that all services with the same associated policy will be compliant with your organization's standards. Services will also have at least one approval process associated with it so that when a user submits a request for a specific service, the appropriate parties are notified and can provide the necessary approval. Once the service request has been fully approved, Governance Automation Online performs the SharePoint Online and/or DocAve Online processes according to the customized settings configured for that service.

Familiarizing Yourself with the Interface

In the administrator landing page, the following tiles are available for you to manage:

- Settings
- Start a Request
- View My Requests
- View My To-Do List
- Public Site Collection Directory
- My Sites

Use the tiles to navigate through the software. At any point, click **MENU** on the upper-left corner to display the navigation bar on the top of the interface. You are able to go to your desired section by clicking the section name on the navigation bar. You can also click the pin ( ) button on the lower-right corner on the navigation bar to pin the navigation bar. The navigation bar will always display on the top of the interface until you click the unpin ( ) button.

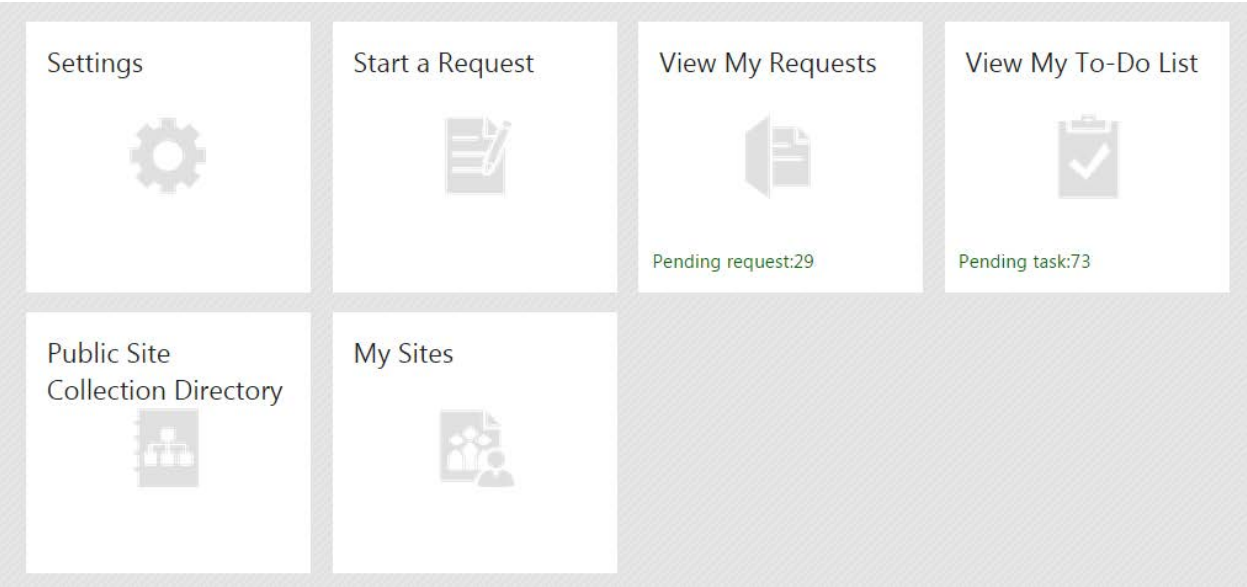

Figure 1: The administrator landing page.

Governance Automation Online Key Terms and Phrases

To help better understand how to use the features and functions in Governance Automation Online, refer to the following list of key terms and phrases:

- Administrator – An Administrator in Governance Automation Online has full control to all settings, reports and applications in Governance Automation Online, as well as full control to their organization's Office 365 tenant.
- Administrator Contact – The Administrator Contact is the IT administrator to be contacted if the service request is unable to properly complete.
- Approval Process – An approval process is a defined process to obtain approval in order for an Office 365 or DocAve Online procedure to start.
- Category – Categories are used for organizational purposes. For example, by placing policies used for SharePoint Online administration purposes in the Administration category, you can then sort policies by categories, and more easily find the policy of your choice.
- Site Collection Inactivity Threshold – The inactivity threshold is the amount of time you allow for a site collection to not have been modified by anyone before Governance Automation Online notifies the designated contact.
- Office 365 Group Inactivity Threshold – The inactivity threshold is the amount of time that Office 365 group settings have not been changed or that any content in the corresponding group team sites, files, notebook, calendar, mailbox, or conversations has been added or modified. Note that changes to a group's plan in Planner are not regarded as activities since Office 365 does not provide API to retrieve a plan's last modified time.

- Site Collection Lease Period – A lease period is the amount of time a site collection is expected to be used. Once the lease period has reached its expiration date, the designated user will be prompted to decide on the action to perform on the site collection. This allows for the automation of content lifecycle management.
- Office 365 Group Lease Period – A lease period is the amount of time allotted wherein an Office 365 group is valid in Office 365. Once the lease period has reached its expiration date, the designated user will be prompted to decide on the action to perform on the Office 365 group. This allows for the automation of Office 365 group lifecycle management.
- Office 365 User Contract Term – A contract term is the amount of time allotted wherein a user is a valid account in Office 365. Once the contract term has reached its expiration date, the designated user will be prompted to decide on the action to perform on the Office 365 user. This allows for the automation of Office 365 user lifecycle management.
- Policy – A policy is an organization-wide rule or standard that can be applied to a site collection, Office 365 user, or Office 365 group. Policies are configured by Governance Automation Online Administrators.
- References – References are information about the Service Request. References include: Request Summary, Requester, Task Created Time, Rejecter, Approver, Rejected Time, Approved Time, Comments, Request Object URL, Lease Expiration Warning Period, Task Link, Governance Automation Online Link, etc.
- Service – A service is a set of configured settings for a management operation in Office 365 that can be leveraged by business users, when submitting a service request. Services are configured by Governance Automation Online Administrators.
- Service Request – A service request is a request for a management operation in Office 365. Service requests are submitted by business users, and depending on the service that is requested, they may require approval from both business users and Governance Automation Online Administrators.
- Service Contact – The Service Contact is the business user who owns the business process for a service.

User Roles for Governance Automation Online

Since Governance Automation Online is integrated with AvePoint Online Services, Governance Automation Online user roles are integrated with the AvePoint Online Services Tenant Users role. The AvePoint Online Services Tenant User role consists of an Application Administrator and Standard Users.

- Application Administrator – The Application Administrator fulfills the role of the Governance Automation Online IT Administrator. IT Administrators are able to access both the IT Administrator and Business User interface of Governance Automation Online, giving them the ability to configure system settings, monitor requests/tasks/system processes/site collections/sites, and maintain services, as well as submit and approve requests for services.

- Standard User – A Standard User fulfills the role of a Governance Automation Online Business User. Business Users are only able to access the Business User interface of Governance Automation Online, allowing them to submit and approve requests for allowed services.

For more information about the user role management in AvePoint Online Services, refer to the AvePoint Online Services User Guide.

In Governance Automation Online, the IT Administrator can also create custom Business User groups to allow designated users to also view Governance Automation Online reports for monitoring requests, tasks, system processes, site collections, or sites.

For more information about managing Governance Automation Online groups and users, refer to Configuring Account Manager.

Required Permissions

Refer to the section below for the required permissions for using Governance Automation Online properly.

- To properly use the following functionalities in Governance Automation Online, the Office 365 account used to register SharePoint Online site collections in DocAve Online or AvePoint Online Services must have the **SharePoint Administrator** role. For details about this role, refer to the Microsoft article About the SharePoint Online admin role.
    - Create Site Collection services and requests
    - Change Site Collection Contact or Administrator services and requests
    - Change Site Collection Settings services and requests
    - Site Collection Lifecycle Management services and requests
    - Create Site services and requests
    - Change Site Contact services and requests
    - Change Site Settings services and requests
    - Site Lifecycle Management services and requests
    - Create Library/List services and requests
    - Change Library/List Settings services and requests
    - Content Move services and requests
    - Change Permissions services and requests
    - Grant Permissions services and requests
    - Clone or Transfer User Permissions services and requests

- To properly use the following functionalities in Governance Automation Online, you must create a Microsoft Azure AD app profile in AvePoint Online Services first. When you create the app profile, the **AvePoint Online Services Administration for Azure** app is automatically created. The Office 365 account used to consent the app must have the **Global Administrator** role, which is a requirement from Microsoft. For details about this role, refer to the Microsoft article About Office 365 admin roles.
    - Create User services and requests
    - Change User Properties services and requests
    - User Lifecycle Management services and requests
    - Create Group services and requests
    - Change Group Settings services and requests
    - Group Lifecycle Management services and requests
    - Import existing groups via the **Import Existing Office 365 Objects** functionality.

  ***Note**: If the **Retrieve Outlook Web App mailbox policy from Office 365** checkbox is selected in the **Outlook Web App Policy** section in a user policy, the account configured in the Office 365 service account profile must have the **Exchange Administrator** role. For details about this role, refer to the Microsoft article About the Exchange Online admin role.

- To import existing site collections and sites via the **Import Existing Office 365 Objects** functionality, the account used to register the SharePoint Online admin center via the **Single Site Collection** method in DocAve Online Control Panel must have the **SharePoint Administrator** role. For details about this role, refer to the Microsoft article About the SharePoint Online admin role.

Configuring the Account Pool

AvePoint recommends that you configure the account pool in AvePoint Online Services. The account pool can contain multiple Office 365 accounts. With the credentials of these accounts, Governance Automation Online can process multiple requests simultaneously. The SharePoint Online throttling, which limits the number of concurrent requests, can be reduced. For more information about configuring the account pool, refer to the **Manage Office 365 Account Pool** section in the AvePoint Online Services User Guide.

Registering SharePoint Online Admin Centers/Site Collections

To use Governance Automation Online to manage content in SharePoint Online, you must first register the SharePoint Online admin centers or site collections in AvePoint Online Services. For more information, refer to the **Manage Dynamic Object Registration** section in the AvePoint Online Services User Guide.

***Note**: To register a SharePoint Online admin center, you must use the **Batch Import** method in **Dynamic Object Registration** > **Manage Containers**.

Configuring the Quick Start Wizard

When you first log into DocAve Governance Automation Online, the **Governance Automation Online Quick Start Wizard** window appears. Enter the information as instructed by the wizard to allow Governance Automation Online to create sample data that allows you to quickly get started using the product.

***Note**: To use the sample policies and services created by the quick start wizard, you must first import SharePoint Online site collections through **Settings** > **Import Existing Site Collections and Sites**. For more information, refer to Importing Existing Office 365 Objects.

Configure the following settings in the wizard:

1. Configure the administrator and the department.
    - **Administrator** – The administrator has the Full Control permission to Governance Automation Online. Enter a username to set as the administrator. Press **Enter** to check whether or not the name is valid.
    - **Department** – A department is used as a report condition that provides statistics on the amount of actions performed by users. Enter a customized department name in the text box.
2. Click the arrow on the right-hand side to proceed to the next step.
3. Configure the following options to retrieve data from SharePoint Online:
    a. **Username** – Enter an Office 365 global administrator or SharePoint administrator account in the format of **someone@example.com**.
    b. **Password** – Enter the password of the account above.
    c. **SharePoint Online admin center URL** – Enter a SharePoint Online admin center URL. The admin center will be added into the **Default SharePoint Sites Group** in DocAve Online.
    d. Click **Test** to test the validation.
4. Click **Save** to save your configurations. A window appears to display the real-time process of creating sample data. You can close the window and the sample data will be created in the background.

Getting Started with Governance Automation Online

The sections below detail what you must configure in order to use Governance Automation Online (Account Manager, Departments, Approval Processes, Policies, and Services). These instructions should be followed in order, from Configuring Account Manager through Configuring Services. Additional optional configurations are described in Additional Governance Automation Online Configurations.

Configuring Account Manager

Account Manager allows you to manage user accounts and groups for Governance Automation Online. There are two default groups for Governance Automation Online:

- **Administrator Group** – Users in this group are able to access both the administrator and business user interface of Governance Automation Online, giving them the ability to configure system settings, monitor requests and tasks, and maintain services, as well as submit and approve requests for services.

  ***Note**: Users of this group are managed through AvePoint Online Services. If you want to add users or remove users from this group, go to **AvePoint Online Services** > **User Management** by using one of the following types of AvePoint Online Services account:

  - Service Administrator
  - Tenant User: Service Administrator of Governance Automation Online

- **Business User Group** – Users in this group are only able to access the business user interface of Governance Automation Online, allowing them to submit and approve requests for allowed services. Custom Business User Groups may be created allowing designated users to also view Governance Automation Online reports for monitoring processes and ownership of site collections.

Note the following:

- If a Governance Automation Online Service Administrator is demoted to a Standard User in AvePoint Online Services, this user will be removed from the Administrator Group and be added to the Business User Group.
- AvePoint Online Services supports adding the **Everyone** role to AvePoint Online Services users. **Everyone** refers to all available users in your Office 365 tenant's Azure AD. If the Service Administrator of AvePoint Online Services assigns Governance Automation Online to **Everyone**, all available users can sign into AvePoint Online Services and use Governance Automation Online.

Additional custom user groups can be created to allow certain users to view reports and monitor all requests and tasks.

To configure Account Manager for Governance Automation Online, click **Account Manager** in the **System** group within the **Settings** interface.

Managing Governance Automation Online Groups

In Account Manager, you can change the number of groups displayed per page by selecting the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the groups, click the sort (⬇) button in a column heading such as **Group Name** and **Description**.

You can perform the following actions in the **Account Manager** interface:

- **Create Group** – Create groups of user accounts for Governance Automation Online. For more information, refer to Creating New User Groups.
- **Edit Group** – Modify user group information or reassign group permissions. For more information, refer to Creating New User Groups.
- **View User(s)** – View the user accounts within a selected group. Within the groups, you can add or remove user accounts. For more information, refer to Adding Users into Custom Groups or Removing Users from Groups.
- **Delete Group** – Remove a group from Governance Automation Online. A confirmation window appears when you click **Delete Group**. Click **OK** to delete the selected group, or click **Cancel** to return to the **Account Manager** interface without deleting the selected group.

***Note**: The Administrator Group and Business User Group cannot be deleted.

Viewing Administrator Accounts

To view the administrators for Governance Automation Online, select the **Administrator Group** and click **View User(s)** on the ribbon. Click **Back** on the ribbon to return to the **Account Manager** interface. All previously configured administrators will be listed in the **Administrator Group** interface.

In this interface, you can change the number of administrator accounts displayed per page by selecting the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the user accounts, click the sort (⬇) button in a column heading **Username** and then choose **Ascending** or **Descending**.

Managing Business Users

To view and manage the business users for Governance Automation Online, select the **Business User Group** and click **View User(s)** on the ribbon. Click **Back** on the ribbon to return to the **Account Manager** interface. All previously configured business users will be listed in the **Business User Group** interface and you can perform the following actions.

- **Add User** – To add users or Office 365 groups to the Business User Group, click **Add User** on the ribbon. You are be brought to the **Add User** interface.
    i. **Add User(s)** – Enter the names of the users or Office 365 groups you wish to add in the text box. Press **Enter** to check whether or not the name is valid.

***Note:** Click the **AvePoint Online Services** link in the description to add external users into Governance Automation Online through AvePoint Online Services.

ii. Click **Save** on the ribbon to save the configurations, or click **Cancel** to return to the Business User Group interface without saving any configurations.

- **Remove User from Group**– To remove business users from Governance Automation Online, select the usernames or Office 365 group names, and then click **Remove User from Group** on the ribbon. A confirmation window will appear. Click **OK** to delete the selected users or groups, or click **Cancel** to return to the **Business User Group** interface without deleting the selected users or groups.

Creating New User Groups

To create a new user group for Governance Automation Online, click **Create Group** on the ribbon. To modify a previously configured group, select the desired group, and click **Edit Group** on the ribbon. These groups are aimed to give the business users' permissions to view the reports, activities, requests, and tasks.

In the **Create Group** or **Edit Group** interface, configure the following settings:

1. **Group Information** – Enter a **Group Name** in the provided text box. Then, enter an optional **Group Description** for future reference.
2. **Permissions** – Assign the permissions to the group by selecting corresponding checkboxes.
3. Click **Save** to save the configurations, or click **Cancel** to return the **Account Manager** interface without creating the group.

Adding Users into Custom Groups

To add users or Office 365 groups into a Governance Automation Online custom group, refer to the instructions below:

1. In the **Account Manager** interface, select a group by clicking the group name, and then click **View User(s)** on the ribbon.
2. Within the group, click **Add User** on the ribbon. You will be brought to the **Add User** interface.
3. Enter the names of the users or Office 365 groups you wish to add in the text box. Press **Enter** to check whether or not the name is valid.

   ***Note:** Click the **AvePoint Online Services** link in the description to add external users into Governance Automation Online through AvePoint Online Services.

4. Click **Save** on the ribbon to save the configurations, or click **Cancel** to return to the group interface without adding any users or groups.

Removing Users from Groups

To remove users from a group, complete the following steps:

1. In the **Account Manager** interface, select a group by clicking the group name, and then click **View User(s)** on the ribbon.
2. Within the group, select the desired usernames or Office 365 group names, and then click **Remove User from Group** on the ribbon. A confirmation window appears.
3. Click **OK** to delete the selected users or groups, or click **Cancel** to return to group interface without deleting the selected users or groups.

Configuring Departments

Departments with specific responsibilities in an organization can be associated with corresponding services in order to organize services to help create custom service catalogs catered to the needs of different users.

You can retrieve the department information from Azure Active Directory properties or SharePoint Online User Profile Service, or add new departments manually. Both methods are described in the sections below:

Retrieving Existing Departments

To retrieve a requesters' department information from the Azure AD properties or from a SharePoint Online User Profile Service, follow the instructions below:

1. Click **Department** in the **System** group within **Settings**.
2. In the **Department** interface, choose the **Use department in Azure Active Directory properties or in SharePoint Online user profile** option.
3. Click **Save** on the ribbon to save the configurations, or click **Cancel** to return to the **Settings** interface without saving any configurations.

***Note**: The department information will be retrieved from the Azure AD properties first. If no department information is retrieved from Azure AD properties, the department information will be retrieved from SharePoint Online User Profile Service.

Manually Adding New Departments

To add new departments in Governance Automation Online, follow the instructions below:

1. Click **Department** in the **System** group within **Settings**.
2. In the **Department** window, click **Add New**.
3. Enter a department name in the text box under the **Value** column heading.

4. Click **Insert** next to the text box to add the desired department.
5. Repeat the steps above to add more departments.

   Click the edit ( ) button next to the text box to modify the department name, and then click **Update** to save the modifications or click **Cancel** to exit the editing mode without saving any modifications.

   Click the delete ( ) button to delete the unnecessary departments.

6. Click **Save** on the ribbon to save all of the configurations, or click **Cancel** to return to the **Settings** interface without saving any configurations.

Configuring Approval Processes

A Governance Automation Online approval process is a defined process to automatically obtain approval for a SharePoint Online or DocAve Online management operation. With approval processes properly configured, these operations can be completed efficiently by standardizing the process, without human error.

To create or manage approval processes, click **Approval Process** in the **Request Management** group within **Settings**. The **Approval Process Management** interface appears.

Managing Approval Processes

In Approval Process Management, all of the Governance Automation Online approval processes you have configured are displayed. You may change the number of approval processes displayed per page, as well the order they are displayed in. To change the number of approval processes displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the approval processes, click the sort ( ) button in a column heading such as **Approval Process**, **Category**, **Last Modified Time**, and **Created By**.

You can customize how the approval processes are displayed in a number of different ways:

- Search – Allows you to filter approval processes displayed by the keyword you designate. The **Approval Process** column and the **Created By** column support to search for the desired approval process, and only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – You can manage which columns are displayed in the list so that only information you want to see is displayed. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list. Click **All** to select the checkboxes of all columns and have all columns displayed in the list or click **None** to uncheck the checkboxes of all columns and have none columns displayed in the list.

- Filter item ( ) – This allows you to filter which item in the list is displayed. Click the filter ( ) button of the column you want to filter, and then select the checkbox next to the item name to have that item shown in the list.

You can perform the following actions in **Approval Process Management**:

- **Create** – Click **Create** on the ribbon to go to the **Approval Process Management** interface. For more information, refer to Creating or Editing Approval Processes.
- View Details – Click an approval process name for detailed information about the approval process.
- **Deactivate** – Select the approval processes you want to deactivate, and click **Deactivate** on the ribbon.
- **Edit** –An approval process is available to edit only when its status is **Inactive**. If the status of an approval process is **Active**, deactivate the approval process first. Then, select the approval process, and click **Edit** on the ribbon. See Creating or Editing Approval Processes for details on editing an existing approval process.
- **Activate** – Select the approval processes you want to activate, and click **Activate** on the ribbon. Active approval processes can be used in policies and services.
- **Delete** – Select an inactive approval process, and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to delete the selected approval process, or click **Cancel** to return to the **Approval Process Management** interface without deleting the selected approval process.

Creating or Editing Approval Processes

Follow the instructions below to configure an approval process:

1. **Approval Process Name** – Enter a **Name** and an optional **Description** for this approval process in the corresponding text boxes.
2. **Approval Process Category** – Categories are used to organize your Governance Automation Online approval processes. Select an existing category from the drop-down list or create a new category for this approval process by clicking **Create New** then configuring the new category in the **Create Category** interface.
3. **Approval Process Stages** – Choose the approval method:
   - **Use approval stages** – Select **Use approval stages** and select the number of approval stages. Having multiple approval stages provides flexibility based on your governance needs. You can select the **Automatically approve the request if the requester and the approver are the same user** checkbox to skip the approval.
   - **Auto-approve** – Select **Auto-approve** and services using this approval process will be performed automatically upon request.
4. **CC** – Specify additional users and/or groups that you want to be notified when the service request is completed without assigning tasks to them. They can be AvePoint Online Services

local users, Office 365 users, and Azure Active Directory groups. By default, Governance Automation Online will notify all of the approvers and the requester upon request completion.

a. Enter the name of the users and/or groups in the provided text box. Press Enter to check whether or not the name is valid.

   You can also enter the following roles:

   - **$Manager of Approver** – The manager of the approver of the service request will be notified.
   - **$Administrator Contact** – The administrator contact defined in the service will be notified.
   - **$Primary Site Collection Administrator** – The primary site collection administrator will be notified.
   - **$Primary Site Collection Contact** – The primary site collection contact will be notified.
   - **$Secondary Site Collection Contact** – The secondary site collection contact will be notified.
   - **$Primary Site Contact** – The primary site contact will be notified.
   - **$Secondary Site Contact** – The secondary site contact will be notified.

b. Select a **Completion E-mail Template** for this notification from the drop-down list. The Completion E-mail Template can be configured in the **System** group within **Settings**.

5. If you select **Auto-approve**, skip the following steps and click **Save** to save all of the configurations and return to the **Approval Process Management** interface. Click **Save and Activate** to save all of the configurations and activate this approval process. Click **Cancel** to return to the **Approval Process Management** interface without saving any changes.

6. If you chose to use approval stages, continue to the **Stage One Configurations**. Configure the following for the first stage of approval:

   a. **Stage Name** – Enter a **Name** for the first level stage. By default, its name is **First Stage Approval**. Then, enter an optional **Description** for future reference.

   b. **Approver(s)** – Enter the first stage approvers. All approvers will be assigned a task when this approval process starts.

      - Specify roles – Specify the approver relevant to the user making the request. This may be preferable to entering specific users since role based approval can adapt to personnel shifts in your organization.

        Enter the role of the person designated to be the approver for this approval stage in the text box. You can enter more than one role, but if more than one role is appointed for a given stage, all approvers of all specified roles for that stage must approve the request in order to proceed to the next approval stage.

The following roles are available:

- **$Requester** – The requester of service request will be assigned to deal with the task.
- **$Manager of Requester** – The manager of the requester of the service request will be assigned to deal with the task.
- **$Primary Site Collection Contact** – The Primary Site Collection Contact will be assigned to deal with the task. The Site Collection Contacts are assigned when configuring the services.
- **$Secondary Site Collection Contact** – The Secondary Site Collection Contact will be assigned to deal with the task. The Site Collection Contacts are assigned when configuring the services.
- **$Primary Site Contact** – The Primary Site Contact will be assigned to deal with the task. The Site Contacts are assigned when configuring the services.
- **$Secondary Site Contact** – The Secondary Site Contact will be assigned to deal with the task. The Site Contacts are assigned when configuring the services.
- **$Primary Site Collection Administrator** – The Primary Site Collection Administrator will be assigned to deal with the task.
- **$Manager of Previous Stage Approver** (this option is only available for second or third stage approval) – The manager of the previous stage's approver will be assigned to deal with the task.
- **$Source User** – The user to clone permissions from.
- **$Target User** – The user to clone permissions to.
- **$New Site Collection Contact** – The user that takes over the role of Site Collection Contact.
- **$Primary Site Contact of Source** – The Primary Site Contact of the source node will be assigned to deal with the task.
- **$Secondary Site Contact of Source** – The Secondary Site Contact of the source node will be assigned to deal with the task.
- **$Primary Site Contact of Target** – The Primary Site Contact of the target node will be assigned to deal with the task.
- **$Secondary Site Contact of Target** – The Secondary Site Contact of the target node will be assigned to deal with the task.
- **$New Site Contact** – The user that takes over the role of Site Contact.
- **$Manager of User** – The manager of the Office 365 user will be assigned to deal with the task.

- **$Group Owners** – The owners of the Office 365 group will be assigned to deal with the task.
- **$Service Metadata ("Metadata Name")** – The person or group specified in the metadata will be assigned as an approver to approve or reject the task. Enter the role in this format. Replace **Metadata Name** with the name of the Person or Group type of metadata. The metadata must be added to the service that will be applied with this approval process. Make sure that **Allow a variable role referred to this metadata in the approval process** is enabled on the Person or Group type of metadata.
- **$Primary Group Contact** – The Primary Group Contact will be assigned to handle the task. The Group Contacts are assigned when configuring the services.
- **$Secondary Group Contact** – The Secondary Group Contact will be assigned to handle the task. The Group Contacts are assigned when configuring the services.

If multiple roles are entered, choose the order in which those tasks are assigned from the **Order** drop-down list:

- **One at a time (serial)** – The users of your specified roles must approve one after another. If an approver of one role rejects the request, the approver of next role will not be asked for approval.
- **All at once (parallel)** – The users of all specified roles will be notified at the same time. If an approver of any role rejects the request, the request will be rejected.

  ***Note**: If this approval method is selected, you can further choose whether to select **Allow the approval stage to complete when one approver approves**. If one of the specified users approves it, the request will be complete.

- Specify users – Enter the names of the AvePoint Online Services local users and/or Office 365 users you wish to designate as approvers for this stage of the approval process. Press **Enter** to check whether or not the names are valid.

  If multiple users are entered, choose the order in which those tasks are assigned from the Order drop-down list:

  - **One at a time (serial)** – The users you have specified must approve one after another. If an approver rejects the request, the next approver will not be asked for approval.
  - **All at once (parallel)** – All specified users will be notified at the same time. If any approver rejects the request, the request will be rejected.

- Specify groups – Enter the names of the Azure Active Directory groups you wish to designate as approvers for this stage of the approval process Press **Enter** to check whether or not the names are valid. Governance Automation Online will

assign the task to the groups. If the login user is a member of the groups, the task will be displayed in the **My To-Do List** > **My Tasks** page. The task will be approved once any single member of the groups approves it.

If multiple groups are entered, choose the order in which those tasks are assigned from the **Order** drop-down list:

One at a time (serial) – The groups you have specified must approve one after another. When a user of the first group approves the task, the task will be assigned to the next group. If a group member rejects the request, the next group will not be asked for approval.

All at once (parallel) – All specified groups will be notified at the same time. If any group member rejects the request, the request will be rejected.

You can also choose **Allow approvers to reassign tasks to others**. If the checkbox is selected, the approver can reassign the task to another user or group.

c. **E-mail Settings** – Configure settings for e-mail notifications for this approval process. By default, the **Notify the approver when the task is assigned** checkbox and the **Notify the requester when the request is rejected** checkbox are selected. You can also choose to notify the requester once the request is approved by selecting the **Notify the requester when the request is approved** checkbox. Select the e-mail template you wish to use for each notification from the corresponding drop-down list.

   ***Note:** E-mail templates are configured in the **E-Mail Template** section of the **System** group within **Settings**.

d. **Duration and Escalation** – Select the **Enable Duration and Escalation** checkbox to notify the escalation user or group that the original task has not been handled within the specified amount of time. They can be AvePoint Online Services local users, Office 365 users, and Azure Active Directory groups. A task will be assigned to the escalation user or group to continue the approval process. Make sure that the user or group receiving the escalated task has the right permissions to handle the task.

   i. **Duration** – Enter a number in the **Duration** text box for the amount of time allowed before the task is escalated, and select either **Day(s)**, **Week(s)** as the time unit for the duration.

      You can select the **Enable reminder before the escalation** checkbox to remind the approver before the task expires. Select a reminder profile from the drop-down list or click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

   ii. **Escalation** – Choose the action that the escalation will trigger from the drop-down list.

- **Notify** – The specified user or group will be notified when the task is escalated. Enter the name of the user or of the group in the text box. This user or group is the one that you want to notify to be responsible for this case. Press **Enter** to check whether or not the name is valid. This user or group will be notified once the amount of time specified as the duration passes.
- **Re-assign to** – The task will be re-assigned to the specified user or group when the task is escalated. Enter the name of the user or of the group in the text box. This user or group is the one that you want this task to be re-assigned to. Press **Enter** to check whether or not the name is valid. The task will be re-assigned to this user or group once the amount of time specified as the duration passes, and this user or group will receive a notification e-mail that the task is re-assigned to them. If a group is selected here, the task will be completed once any of the users in the group handles the task.

  ***Note**: The task can only be re-assigned to one user or one group.

iii. Select an **E-mail Template** for the notification sent when this approval task is escalated from the drop-down list.

7. If more than one approval stage was selected, follow the instructions for Stage One Configurations for the remaining stages.
8. At any time, click the arrow on the left-hand side to return to the previous step to check or modify your configurations. When you have finished, choose one of the following options:
   - Click **Save** to save all of the configurations and return to the **Approval Process Management** interface.
   - Click **Save and Activate** to save all of the configurations and change the status to Active.
   - Click **Cancel** to return to the **Approval Process Management** interface without saving any changes.

Configuring Policies

A policy is an organization-wide set of rules and standards for governing specific Office 365 objects (SharePoint Online site collections, Office 365 groups, or Office 365 users) and DocAve Online operations. Policies can be applied to services to enable automatic provisioning of Office 365 objects. This allows for greater efficiency in provisioning Office 365 objects as identical Office 365 and DocAve Online operations can be carried out and repeated by Governance Automation Online rather than by an administrator. This also helps reduce human error since a correctly set policy will apply the same settings to all services associated with that policy.

To create or manage policies, click **Policy** in the **Request Management** group within **Settings**. The **Policy Management** interface appears.

Managing Policies

In **Policy Management**, all of the Governance Automation Online policies you have configured are displayed. You may change the number of policies displayed per page, as well the order they are displayed. To change the number of policies displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the policies, click the sort ( ) button in a column heading such as **Policy**, **Category**, **Last Modified Time**, and **Created By** then select **Ascending** or **Descending**.

You can customize how the policies are displayed in a number of different ways:

- **Search** – Find policies based on the keywords entered. The Policy column and the Created By column support to search for the desired policies, and only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – You can manage which columns are displayed in the list so that only information you want to see is displayed. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter item ( ) – This allows you to filter which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, and then select the checkbox next to the item name to have that item shown in the list.

You can perform the following actions in **Policy Management**:

- **Create** – Click **Create** on the ribbon to display the **Create New** interface. Then, select **Site Collection Policy**, **User Policy**, or **Group Policy**. For more information about configuring policy settings, refer to the sections below.
- View Details –Click the policy name to see detailed information.
- **Deactivate** – Select active policies, and click **Deactivate** on the ribbon to deactivate them. Make sure to deactivate all services that use the policies you want to deactivate.
- **Edit** – A policy is available to edit only when its status is **Inactive**. If the status of a policy is **Active**, deactivate the policy first. Then, select the policy, and click **Edit** on the ribbon. For more information about configuring policy settings, refer to the sections below.
- **Activate** – Select inactive policies, and click **Activate** on the ribbon to activate them.
- **Delete** – Select an inactive policy, and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to delete the selected policy, or click **Cancel** to return to the **Policy Management** interface without deleting the selected policy.
- **Copy** – Duplicate the existing policy to make minor changes in order to save as a new policy. Select a desired policy by selecting the corresponding checkbox. Click **Copy** on the ribbon, and make the desired modifications. When you have finished making changes, click **Save** to save all of the settings or click **Save and Activate** to save all of the

configurations and activate the policy which means this policy might be used in the service. Click **Cancel** to return to the **Policy Management** interface without saving any configurations.

Creating or Editing Site Collection Policies

Site collection policy allows you to customize rules to automatically manage your site collection and integrate DocAve Online features with the site collection once it is created successfully. Site collection policies can be used in the Create Site Collection service. Site collection policies work in conjunction with Site Collection Lifecycle Management services to not only automatically govern site collections associated with each policy, but also empowers business users to easily manage the lifecycle of the site collections they own.

In the interface for creating or editing a site collection policy, configure the following settings:

1. **Policy Name and Description** – Enter a **Name** for the new policy. Then, enter an optional **Description** for future reference.
2. **Policy Category** – Categories are used to organize Governance Automation Online policies. Select an existing category from the drop-down list or create a new category for this policy by clicking **Create New** then configuring the new category in the **Create Category** interface.
3. Click the arrow on the right-hand side to continue, or click **Cancel** to return to the **Policy Management** interface without saving any configurations.
4. **Quota** – Enter the storage quota and server resource quota for the site collection.

   ***Note**: A storage quota less than 25600 GB will take effect only if storage limit is required for each site collection in your SharePoint Online environment. Otherwise, 25600 GB will be used as the default value.

5. **Sharing** – Choose whether or not to enable sharing on site collections with this policy applied. When sharing is enabled on a site collection, sharing is also enabled on all sites in this site collection. If you select the **Enable sharing** checkbox, configure the following settings:
   - **Sharing outside your company** – Allows you to control how users invite people outside your organization to access site collection content and site content. Choose one of the following options:
     - **Don't allow sharing outside your organization**
     - **Allow sharing only with the external users that already exist in your organization's directory**
     - **Allow external users who accept sharing invitations and sign in as authenticated users**
     - **Allow sharing with all external users, and by using anonymous access links**
   - **Access request settings** – Select the **Allow access requests** checkbox to allow users to request access to the site collection applied with this policy. Then, you can enter the e-mail address of the approver in the **Send all requests for access to the following e-mail**

address text box. The approver will process the request. You can also enter the **$PrimarySiteCollectionContact** role and/or the **$SecondarySiteCollectionContact** role. The site collection contacts will process the access requests. Note that if you enter both roles, separate them with a comma.

You can allow members to share the site and individual files and folders by selecting the corresponding checkbox. With this checkbox selected, the **Allow members to invite others to the site members group. This setting must be enabled to let members share the site** checkbox is automatically selected. You can also choose to only allow members to share the site and individual files and folders, or to only allow members to invite others to the site members group.

6. **SharePoint Designer Configuration** – Select the **Enable SharePoint Designer** checkbox to allow Site Owners and Designers to edit the sites in this site collection using SharePoint Designer. Site Collection Administrators will always be able to edit sites regardless of this configuration.
7. **Site Maximum Depth Limit** – Site Depth limits the layers of sites that can be created under a site collection. Select **Maximum depth** and then enter a positive number which is smaller than 12 in the provided text box.
8. **Site Collection Policy Icon** – Configure the settings for displaying the site collection policy icon on the chrome bar within SharePoint Online site collections. If you select the **Display site collection policy icon within SharePoint Online site collections** checkbox, configure the following settings:
    - **Policy icon image URL** – You must enter the policy icon image URL in the text box to retrieve the image.
    - **Policy details reference URL** – Enter the policy details reference URL in the text box for users to view details of the policy.
9. **DocAve Online Configurations** – Configure this policy to utilize DocAve Online products.
    - **Enable Policy Enforcer** – Select this checkbox to have DocAve Online Policy Enforcer rules applied to the site collections. Policy Enforcer ensures that all actions and changes to the site collections fall within your previously configured rules by continuously monitoring and taking action on the site collections. Select a Policy Enforcer profile from the drop-down list. For more information, refer to the DocAve Administrator User Guide.
    - **Enable Deployment Manager** – Select this checkbox to include the site collection in a DocAve Online Deployment Manager plan. Select a plan from the drop-down list. For more information on how to configure Deployment Manager plans, refer to the DocAve Deployment Manager User Guide.

      Deployment Manager plans that meet all of the following conditions are available in the drop-down list:

      i. The deployment type of the mappings in the plan is **Design Element** or the source nodes in the mappings are within the **User Solution Gallery** node.

ii. The destination nodes in the mappings are site collections.

iii. All of the mappings in the plan meet all of the conditions above.

***Note**: To avoid performance issues, the enabled Deployment Manager plan will not be applied to the site collections that are imported through the Import Existing Site Collections and Sites function.

- **Enable Granular Backup** – Select this checkbox to include the site collection in a Granular Backup plan to provide data protection for site collection associated with this policy.

  ***Note**: If this option is enabled, do not activate this policy until you have configured the appropriate filter policy and added it to the selected Granular Backup plan. For more information on how to configure filter policies for DocAve Online Granular Backup and Restore to provide data protection for site collection created by Governance Automation Online that are associated with this policy, refer to Configuring Filter Policy to Use DocAve Online Granular Backup.

- **Enable Auditing** – Select this checkbox to include the site collection into an Audit Controller plan in DocAve Online Report Center to record all events of site collections associated with this policy.

  ***Note**: If this option is enabled, do not activate this policy until you have configured the appropriate filter policy and added it to the selected Audit Controller plan. For more information on how to configure the filter policy, refer to Configuring Filter Policy to Use Audit Controller in DocAve Online Report Center.

- **Enable site collection content archival using DocAve Online Archiver** – Select this checkbox to allow content in the site collections associated with this policy to be archived by DocAve Online Archiver after manual approval. You must then select an Archiver profile and an approval process from the corresponding checkboxes.

  When there is site collection content that meets the Archiver rule, a manual archiver task (which contains a report of all content that meets the archive rules) will be generated. The task will be assigned to the approver with a report, allowing the approver to select on the report which content to be archived. When the manual archive task is approved, the selected content will be archived. For more information about the manual archive task, refer to Managing Manual Archive Tasks.

10. **Site Collection Lifecycle Management Request Types** – Choose whether or not to enable the request types for the Site Collection Lifecycle Management service. The request types that you select in this section will be available for business users in the following situations:

    - If **Enable deletion of entire site collection** is selected here, **Delete Site Collection** will be the available lifecycle action in the site collection automated locking profiles applied to the following sections: **Site Collection Inactivity Threshold Management** and **Site Collection Lease Period Management**.

- Business users can submit Site Collection Lifecycle Management service requests for the corresponding site collections based on the enabled request types.
- Business users can manage lifecycle of site collections in **My Sites**.

Enable the following request types by selecting the corresponding checkboxes. For each request type, you can choose to **Use the default approval process**, select a created approval process from the drop-down list, or click **Create New** to create a new approval process. If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new approval process on the basis of the selected approval process. The approval process will be triggered when service requests to manage site collection lifecycle are submitted.

- **Enable archiving of entire site collection** – Allows the entire site collection to be archived upon request.

  To notify the selected users when the archiving is completed, select the **Notify the following people when the lifecycle action is completed** checkbox, and then enter their usernames or Office 365 group names in the text box. You can also enter the following roles: **$Primary Site Collection Contact**, **$Secondary Site Collection Contact**, and **$Primary Site Collection Administrator**.

  The notification e-mail uses the e-mail template selected from the **E-mail template** drop-down list.

- **Enable deletion of entire site collection** – Allows the entire site collection to be deleted upon request.

  To notify the selected users when the deletion is completed, select the **Notify the following people when the lifecycle action is completed** checkbox, and then enter their usernames or Office 365 group names in the text box. You can also enter the following roles: **$Primary Site Collection Contact**, **$Secondary Site Collection Contact**, and **$Primary Site Collection Administrator**.

  The notification e-mail uses the e-mail template selected from the **E-mail template** drop-down list.

- **Enable extension of site collection lease** –Allows the lease of this site collection to be extended upon request. You can choose one of the following methods to set limitations on the extension:

  - Each extension must be a specific period of time – Enter a number in the text box and select **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the time unit.
  - Each extension cannot exceed a specific period of time – Enter a number in the text box and select **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the time unit.

  ***Note**: If the extension request of this site collection's lease is approved, the expiration date of the site collection's new lease will be the original expiration date plus the specific period of time of the new extension.

- **Enable site collection policy change** –Allows business users to request a different policy for site collections created with this policy.
- **Enable site collection unlocking** – Allows business user to request to unlock a locked site collection.
- **Enable site collection locking** – Allows business users to request to lock a site collection. If you enable site collection locking, select one or both of the following locking types:
    - **Lock the site collection in "no access" status**
    - **Lock the site collection in "read-only" status**

  To notify the selected users when the locking is completed, select the **Notify the following people when the site collection is locked** checkbox, and then enter their usernames or Office 365 group names in the text box. You can also enter the following roles: **$Primary Site Collection Contact**, **$Secondary Site Collection Contact**, and **$Primary Site Collection Administrator**.

  The notification e-mail uses the e-mail template selected from the **E-mail template** drop-down list.

- **Enable site collection quota change** – Allow business users to request to change the site collection quota. If you enable site collection quota change, select one of the following quota change options:
    - **Allow quota change to any available size** – Allows business users to request to change site collection quota to any available size.
    - **Allow quota upgrade or downgrade within [Specific Size] GB** – Allows business users to increase or decrease site collection quota, and the change cannot exceed the size defined here.

11. **Site Collection Inactivity Threshold Management** – Site collection lifecycle management helps reduce the number of unused or expired site collections in your SharePoint Online environment. Configure the following lifecycle management settings:

    a. **Enable Site Collection Inactivity Threshold** – Select this checkbox to enable the inactivity threshold for the site collection. If the site collection is not accessed within the amount of time entered here, a site collection inactivity threshold task will be assigned to the business user.

    For more information about how site collection inactivity is calculated by Governance Automation and Governance Automation Online, refer to the AvePoint Knowledge Base article http://www.avepoint.com/community/kb/how-site-collection-inactivity-is-calculated-by-governance-automation/.

    Enter a number in the text box and select **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as a time unit.

b. **Approval process** – Select a created approval process from the drop-down list for the inactivity threshold task, or click **Create New** to create a new one. Note that multiple-stage approval is supported for the inactivity threshold task.

   If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.

c. **Enable automated locking** – You can select **Enable automated locking** to lock the site collection if the inactivity threshold task is not completed within the amount of time configured in a site collection automated locking profile. Select a site collection automated locking profile from the drop-down list or click **Create New** to create a new one. For more information about how to configure a site collection automated locking profile, refer to Configuring Site Collection Automated Locking Profiles.

12. **Site Collection Lease Period Management** – A site collection lease period is the amount of time a site collection is available for use. **Site Collection Lease Period Management** helps manage the expired site collection in your SharePoint Online environment. Configure the following lease period management settings:

    a. **Enable Site Collection Lease Period** – Select this checkbox to enable the lease period for the site collection. When the lease period expires or when the last lease extension expires, a site collection lease period task will be assigned to the business user. Configure the site collection lease period by entering a number in the text box and then selecting **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as a time unit.

    b. **Approval process** – Select a created approval process from the drop-down list for the lease period task, or click **Create New** to create a new one. Note that multiple stage approval process is supported for the lease period task.

       If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.

    c. **Notify the approver of expiration** – Select this checkbox to notify the approver when the site collection lease has expired. The notification e-mail uses the e-mail template selected from the drop-down list.

    d. **Enable automated locking** – You can select **Enable automated locking** to lock the site collection if the lease period task is not completed within the amount of time configured in a site collection automated locking profile. Select a site collection automated locking profile from the drop-down list or click **Create New** to create a new one. For more information about how to configure a site collection automated locking profile, refer to Configuring Site Collection Automated Locking Profiles.

13. **Deactivated Site Collection Contact Election**– You can choose whether or not to have the automated ownership election process to begin if either of the site collection contacts is deactivated. If enabled, configure the following settings:

    - **Specify the users you want to exclude** – Enter the names of the users that will be excluded during the election process.
    - **E-mail Settings** – Choose to enable the following notifications by selecting the corresponding checkboxes:
        - **Notify the user when the election task is assigned** – Select this checkbox to send a notification e-mail to a user when the election task is assigned to them.
        - **Notify the primary contact when the site collection is assigned** – Select this checkbox to send a notification e-mail to a user when they become the primary site collection contact.
        - **Notify the secondary contact when the site collection is assigned** – Select this checkbox to send a notification e-mail to a user when they become the secondary site collection contact.

      Each notification has a default e-mail template. You can also select a custom e-mail template.

    - **Duration** – Set the duration for each election stage. If the nominee does not complete the election task during the duration, the election task will be assigned to the next stage's nominee. Enter a number in the text box, then select **Day (s)** or **Week (s)** as the unit.

      You can also notify the nominee before the assigned time is reached. Select **the Remind the nominated user before each nomination task expires** checkbox and select a reminder profile from the drop-down list. You can also click **Create New** to create a reminder profile. For more information, refer to Creating or Editing Reminder Profiles.

    For more information about the election process, refer to Managing the Election Process.

14. **Recertification** – You can choose whether or not to enable recertification to check site collection permission, metadata, or ownership. If enabled, select a recertification profile from the drop-down list or click **Create New** to create a new recertification profile. For more information about configuring a recertification profile, refer to Creating or Editing Recertification Profiles. Then, the recertification settings will be applied to the site collection.
15. Click the arrow on the right-hand side to proceed the next step.
16. View the timelines below for the site collection lifecycle management configured in this policy:
    - **Lease Period Timeline** – View the site collection lease period timeline and/or configurations in this timeline.
    - **Inactivity Threshold Timeline** – View the site collection inactivity threshold timeline and/or configurations in this timeline.

For each timeline, **Show Details** is selected as the default view. You can also select **Timeline Only** from the drop-down list to only view the timeline without viewing detailed configurations. Note the following:

- If you select **Show Details** from the drop-down list as the view, you can click icons within the timeline to hide the detailed configurations.
- If you select **Timeline Only** from the drop-down list as the view, you can click icons within the timeline to display the detailed configurations.

17. When you have finished configuring this policy, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous step to check and modify your configurations.
    - Click **Save** to save all of the configurations.
    - Click **Save and Activate** to save all of the configurations and activate the policy, which allows this policy to be used in services.
    - Click **Cancel** to return to the **Policy Management** interface without saving any changes.

Creating or Editing Office 365 User Policies

The Office 365 user policy allows you to customize rules to automatically manage your Office 365 users and integrate your Outlook Web App mailbox policy with the Office 365 users once it is created or imported successfully. Office 365 user policies are required in Create User services and in **Import Existing Objects** – **Users**. Office 365 user policies work in conjunction with User Lifecycle Management services to not only automatically govern Office 365 users associated with each policy, but also empowers business users to easily manage the lifecycle of the Office 365 users.

In the interface for creating or editing an Office 365 user policy, configure the following settings:

1. **Policy Name and Description** – Enter a **Name** for the new policy. Then, enter an optional **Description** for future reference.
2. **Policy Category** – Categories are used to organize Governance Automation Online policies. Select an existing category from the drop-down list or create a new category for this policy by clicking **Create New** then configuring the new category in the **Create Category** interface.
3. **Azure Active Directory App Profile** – Select an Azure AD app profile that you wish this policy to apply to from the drop-down list. An Azure AD app profile represents your Office 365 tenant. The app profiles displayed here are the ones that you have created in AvePoint Online Services. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide.
4. Click the arrow on the right-hand side to continue, or click **Cancel** to return to the **Policy Management** interface without saving any configurations.
5. **DocAve Online Configuration** – Configure this policy to use the DocAve Online Granular Backup for the Office 365 user's One Drive for Business, which was created via Governance Automation Online and is associated with this policy. Select the **Enable Granular Backup for OneDrive for**

Business checkbox to include the OneDrive for Business into a Granular Backup plan to provide data protection for the OneDrive for Business associated with the Office 365 user applied with this policy.

***Note**: If this option is enabled, do not activate this policy until you have configured the appropriate filter policy and added it to the selected Granular Backup plan. For more information on how to configure filter policies for DocAve Online Granular Backup and Restore, refer to Configuring Filter Policy to Use DocAve Online Granular Backup.

6. **Outlook Web App Mailbox Policy** – The Outlook Web App mailbox policy defines feature availability and file access settings. Note that before you create an Office 365 user policy, you must navigate to **AvePoint Online Services** > **Settings** > **Office 365 Service Account** to create an Office 365 Service account profile. The credentials in the Office 365 service account profile will be used to invoke Exchange Online PowerShell. Governance Automation Online will retrieve the Outlook Web App mailbox policy via Exchange Online PowerShell.

   Choose whether to retrieve the Outlook Web App mailbox policy from Office 365 by selecting the corresponding checkbox. If you enable this option, you must select a policy from the drop-down list. You can also click **View Outlook Web App Mailbox Policy Settings** to view or modify the settings of the policy. In the **Outlook Web App Mailbox Policy Settings** window, the Outlook Web App mailbox policy settings are based on the default policy features enabled in Office 365. You can choose to enable or disable the following features by selecting or deselecting the corresponding checkboxes:

   - **Enable group creation** – Allows Office 365 users to create groups in Office 365.
   - **Enable LinkedIn contact sync** – Allows Office 365 users to add their LinkedIn connections to their mailboxes as contacts. When a user's connection updates their information in LinkedIn, the contact will be automatically updated.

7. **Office Graph/Delve** – Select the **Enable Office Graph/Delve** checkbox to allow the user's documents to be visible to other users in Delve and in the Discover view in OneDrive for Business.

8. **Office 365 User Lifecycle Management Request Types** – Choose whether or not to enable the request types for the User Lifecycle Management service. Business users can submit User Lifecycle Management service requests for the corresponding Office 365 users based on the enabled request types.

   Enable the following request types by selecting the corresponding checkboxes. For each request type, you can choose to **Use the default approval process**, select a created approval process from the drop-down list, or click **Create New** to create a new approval process. If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new approval process on the basis of the selected approval process. The approval process will be triggered when service requests to manage user lifecycle are submitted.

- **Enable offboarding of Office 365 user** – Select this checkbox to allow business users to delete or block the Office 365 user, or to reset the password of the Office 365 user account upon request.
- **Enable extension of Office 365 user contract term** – Select this checkbox to allow the contract of Office 365 users to be extended upon request. You can choose one of the following methods to set limitations on the extension:
    - Each extension must be a specific period of time – Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** as the time unit.
    - Each extension cannot exceed a specific period of time – Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** as the time unit.

  ***Note**: If the extension request of an Office 365 user's contract is approved, the expiration date of the Office 365 user's new contract will be the original expiration date plus the specific period of time of the new extension.

- **Enable Office 365 user policy change** – Select this checkbox to allow business users to request a different policy for Office 365 users that have this policy applied.
- **Enable Office 365 user unblocking** – Select this checkbox to allow business users to request to unblock blocked Office 365 users.

9. **Office 365 User Contract Term Management** – An Office 365 user contract term is the amount of time allotted wherein the user is a valid account in Office 365. **Office 365 User Contract Term Management** helps manage the expired Office 365 user in your Office 365 environment. Configure the following contract term management settings:

    a. **Enable Office 365 user contract term management** – Select this checkbox to enable the contract term for Office 365 users. Configure the user contract term by entering a number in the text box and then selecting **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit. When the contract term expires or when the last contract extension expires, an Office 365 user contract expiration task will be automatically generated and assigned to the business user. The business user can choose to delete or offboard the user.

    b. **Approval Process** – Select an approval process from the drop-down list for the user contract expiration task, or click **Create New** to create a new one.

    If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.

    c. You can configure the following settings:

        - **Enable user contract expiration warning** – Select this checkbox to notify the approvers before the user contract expiration task is generated. Then, you must select a reminder profile from the **Reminder profile** drop-down list. You can also click **Create New** to create a new reminder profile. For detailed information

about creating reminder profiles, refer to the Configuring Reminder Profiles for Upcoming Expiration section.

- **Enable automated user blocking** – Select this checkbox to block the user if the automated user contract expiration task is not completed after a specific amount of time. Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit.

  ***Note**: If you enable this option, you must select the **Enable offboarding of Office 365 user** checkbox in the **Office 365 User Lifecycle Management Request Types** field above.

  You can configure the settings below:

  Notify the following people when the user is blocked – Select this checkbox to notify specific users when the Office 365 user is blocked. Enter the names of the users in the text box and press **Enter** to check whether or not the names are valid. Then, you must select an e-mail template from the **E-mail template** drop-down list.

  Start an additional user lifecycle action to escalate – Select this checkbox to generate an Office 365 user deletion task after the user is blocked at a certain time. Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit.

  Enable reminder for the approvers about the user escalation before generating the lifecycle action task – Select this checkbox to send notification e-mails to approvers about the user escalation before the additional lifecycle action task is generated. Then, you must select a reminder profile from the drop-down list. You can also click **Create New** to create a new reminder profile. For detailed information about creating reminder profiles, refer to the Configuring Reminder Profiles for Upcoming Expiration section.

10. When you have finished configuring this policy, choose one of the following options:

    - Click the arrow on the left-hand side to go to the previous step to check and modify your configurations.
    - Click **Save** to save all of the configurations.
    - Click **Save and Activate** to save all of the configurations and activate the policy, which allows this policy to be used in services.
    - Click **Cancel** to return to the **Policy Management** interface without saving any changes.

Creating or Editing Office 365 Group Policies

The Office 365 group policy allows you to customize rules to automatically manage your Office 365 group. Office 365 group policies are required in Create Group services and in **Import Existing Objects – Group**. Office 365 group policies work in conjunction with Group Lifecycle Management services to not

only automatically govern Office 365 groups associated with each policy, but also empowers business users to easily manage the lifecycle of the Office 365 groups.

In the interface for creating or editing an Office 365 group policy, configure the following settings:

1. **Policy Name and Description** – Enter a **Name** for the new policy. Then, enter an optional **Description** for future reference.
2. **Policy Category** – Categories are used to organize Governance Automation Online policies. Select an existing category from the drop-down list or create a new category for this policy by clicking **Create New** then configuring the new category in the **Create Category** interface.
3. **Azure Active Directory App Profile** – Select an Azure AD app profile that you wish this policy to apply to from the drop-down list. An Azure AD app profile represents your Office 365 tenant. The app profiles displayed here are the ones that you have created in AvePoint Online Services. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide.
4. Click the arrow on the right-hand side to continue, or click **Cancel** to return to the **Policy Management** interface without saving any configurations.
5. **Office 365 Group Lifecycle Management Request Types** – Choose whether or not to enable the request types for the Group Lifecycle Management service. Business users can submit Group Lifecycle Management service requests for the corresponding Office 365 groups based on the enabled request types.

   Enable the following request types by selecting the corresponding checkboxes. For each request type, you can choose to **Use the default approval process**, select a created approval process from the drop-down list, or click **Create New** to create a new approval process. If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new approval process on the basis of the selected approval process. The approval process will be triggered when service requests to manage Office 365 groups are submitted.

   - **Enable deletion of Office 365 group** – Select this checkbox allow business users to delete the Office 365 group upon request.
   - **Enable extension of Office 365 group lease** – Select this checkbox to allow the lease of an Office 365 group to be extended upon request. You can choose one of the following methods to set limitations on the extension:
     - Each extension must be a specific period of time – Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit.
     - Each extension cannot exceed a specific period of time – Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit.
   - **Enable Office 365 group policy change** – Select this checkbox to allow business users to request a different policy for Office 365 groups that have this policy applied.

- **Enable Office 365 group team site quota change** – Select this checkbox to allow business users to request to change the Office 365 group team site quota. Choose from the following methods to set limitations on the group team site quota change:
    - **Allow quota change to any available size** – Choose this option to allow business users to request to change group team site quota to any available size.
    - **Allow additional quota to the maximum of [Specified Size] GB** – Choose this option to allow business users to add additional group team site quota, and the additional quota size cannot exceed the size defined here. Enter a number in the text box.

      Note the following:

      The maximum group team site quota cannot exceed 25600 GB.

      The group team site quota cannot be reduced to be less than its current size.

6. **Office 365 Group Inactivity Threshold** – An Office 365 group inactivity threshold is the amount of time that the group settings have not been changed or that any content in the corresponding group team sites, files, notebook, calendar, mailbox, or conversations has been added or modified. Note that changes to a group's plan in Planner are not regarded as activities since Office 365 does not provide API to retrieve a plan's last modified time. **Office 365 Group Inactivity Threshold** helps reduce the number of unused groups and group team sites in your Office 365 environment. Configure the following inactivity threshold settings:

    a. **Enable Office 365 group inactivity threshold** – Select this checkbox to enable the inactivity threshold for Office 365 groups. Configure the Office 365 group inactivity threshold by entering a number in the text box and selecting **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit. When the group settings have not been changed and the group team sites have not been accessed within the specified amount of time, an Office 365 group inactivity threshold task will be automatically generated and assigned to business users. Business users can choose to keep or delete the groups and corresponding team sites.

    b. **Approval Process** – Select an approval process from the drop-down list for the group inactivity threshold task or click **Create New** to create a new approval process.

       If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.

    c. You can configure the following settings:

       - **Enable group inactivity threshold warning** – Select this checkbox to notify the approvers before the group inactivity threshold task is generated. Then, you must select a reminder profile from the **Reminder profile** drop-down list. You can also click **Create New** to create a new reminder profile. For detailed

information about creating reminder profiles, refer to the Configuring Reminder Profiles for Upcoming Expiration section.

- **Enable automatic deletion of Office 365 group** – Select this checkbox to delete the group if the group inactivity threshold task is not completed after a specific amount of time. Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit.

  ***Note**: If you enable this option, you must select the **Enable deletion of Office 365 group** checkbox in the **Office 365 Group Lifecycle Management Request Types** field above.

  Enable a reminder for the approvers before the group inactivity threshold task is generated – Select this checkbox to send notification e-mails to approvers before the group inactivity threshold task is generated. Select a reminder profile from the drop-down list. You can also click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Configuring Reminder Profiles for Upcoming Expiration.

  Notify the following people upon the deletion of the group – Select this checkbox to notify specific users when the group is deleted. Enter the names of the users in the text box and press **Enter** to check whether or not the names are valid. Then, you must select an e-mail template from the **E-mail template** drop-down list.

7. **Office 365 Group Lease Period Management** – An Office 365 group lease period is the amount of time allotted wherein the group is valid in Office 365. **Office 365 Group Lease Period Management** helps manage the expired Office 365 group in your Office 365 environment. Configure the following lease period management settings:

   a. **Enable Office 365 group lease management** – Select this checkbox to enable the lease period for Office 365 groups. Configure the Office 365 group lease period by entering a number in the text box and selecting **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit. When the group lease expires or when the last lease extension expires, an Office 365 group lease expiration task will be automatically generated and assigned to the business user. The business user can choose to extend the group lease or delete the group.

   b. **Approval Process** – Select an approval process from the drop-down list for the group lease expiration task, or click **Create New** to create a new one.

      If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.

   c. You can configure the following settings:

      - **Enable group lease expiration warning** – Select this checkbox to notify the approvers before the group lease expiration task is generated. Then, you must

select a reminder profile from the **Reminder profile** drop-down list. You can also click **Create New** to create a new reminder profile. For detailed information about creating reminder profiles, refer to the Configuring Reminder Profiles for Upcoming Expiration section.

- **Enable automatic deletion of Office 365 group** – Select this checkbox to delete the group if the group lease expiration task is not completed after a specific amount of time. Enter a number in the text box and select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the unit.

  ***Note**: If you enable this option, you must select the **Enable deletion of Office 365 group** checkbox in the **Office 365 Group Lifecycle Management Request Types** field above.

  Enable a reminder for the approvers before the group is deleted – Select this checkbox to send notification e-mails to approvers before the group deletion task is generated. Select a reminder profile from the drop-down list. You can also click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Configuring Reminder Profiles for Upcoming Expiration.

  You can select the **Notify the following people upon the deletion of the group** checkbox to notify specific users when the group is deleted. Enter the names of the users in the text box and press **Enter** to check whether or not the names are valid. Then, you must select an e-mail template from the **E-mail template** drop-down list.

8. **Office 365 Group Team Site Quota Threshold** – Select the **Enable Office 365 group team site quota threshold** checkbox to enable a quota threshold for Office 365 group team sites. A quota threshold is the maximum resources that a group team site can use. If you select the checkbox, set the threshold by entering a number in the text box. Once a group team site's storage reaches the quota threshold, a notification e-mail will be sent to the group owners.

9. **Recertification** – You can choose whether or not to enable recertification to check group permission or membership. If enabled, select a recertification profile from the drop-down list or click **Create New** to create a new recertification profile. For more information about configuring a recertification profile, refer to Creating or Editing Recertification Profiles. Then, the recertification settings will be applied to the group.

10. When you have finished configuring this policy, choose one of the following options:

    - Click the arrow on the left-hand side to go to the previous step to check and modify your configurations.
    - Click **Save** to save all of the configurations.
    - Click **Save and Activate** to save all of the configurations and activate the policy, which allows this policy to be used in services.
    - Click **Cancel** to return to the **Policy Management** interface without saving any changes.

Configuring Services

A service is a set of configured settings for a management operation in SharePoint Online that can be leveraged by business users when submitting a service request. Administrators can limit what options are available to Business Users based on the standards of practice of the organization.

To create or manage services, click **Service** in the **Request Management** group within **Settings**. The **Service Management** interface appears.

Managing Services

In **Service Management**, all of the Governance Automation Online services you have configured are displayed. You may change the number of services displayed per page, as well the order they are displayed in. To change the number of services displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the services, click the sort ( ) button in a column heading such as **Service**, **Category**, **Last Modified Time**, and **Created By** then select **Ascending** or **Descending**.

You can customize how the services are displayed in a number of different ways:

- **Search** – Allows you to filter services displayed by the keyword you designate. The **Service** column and the **Created By** column support to search for the desired services, and only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – You can manage which columns are displayed in the list so that only information you want to see is displayed. Click the manage columns ( ) button, and then select the checkbox next to the column name to have that column shown in the list.
- Filter item ( ) – This allows you to filter which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

You can perform the following actions in **Service Management**:

- **Create** – Click **Create** on the ribbon to display the **Create New** interface. For more information about configuring service settings, refer to the sections below.
- **View Details** – Click a service name to see the detailed information.
- **Deactivate** – Select the services you want to deactivate and click **Deactivate** on the ribbon. Inactive services will not be shown to business users and cannot be requested.
- **Edit** – A service is available to edit only when its status is **Inactive**. If the status of a service is **Active**, deactivate the service first. Then, select the service, and click **Edit** on the ribbon. For more information about configuring service settings, refer to the sections below.
- **Activate** – Select the services you want to activate and click **Activate** on the ribbon. Active services are available to be requested.

- **Copy** – Duplicate an existing service to make minor changes in order to save as a new service. Select a desired service by selecting corresponding checkbox. Click **Copy** on the ribbon, and enter the related information required. When completing the configurations, click **Save** to save all of the settings or click **Save and Activate** to save all of the configurations and activate this service which makes this service available to be requested. Click **Cancel** to return to the Service Management interface without saving any configurations.
- **Delete** – Select an inactive service, and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to delete the selected service, or click **Cancel** to return to the **Service Management** interface without deleting the selected service.

Instructions on configuring each type of service are provided in the sections below.

Configuring Common Service Settings

The following fields are common service settings in all types of services:

1. **Service Name and Description** – Enter a **Name** for the service and an optional **Description** for future reference. You can also select to **Hide the Request Summary field from the request form and use the service and timestamp to automatically generate the request summary**.
2. **Language** – Choose the language for this service. When starting a request, you can filter the services according to their languages.
3. **Service Category** – Categories are used to organize your Governance Automation Online services. Select an existing category from the drop-down list or create a new category for this service by clicking **Create New** then configuring the new category in the **Create Category** interface.
4. **Department** – Departments help organize services as well as provide essential Governance Automation Online reporting information for sorting and understanding your organization's SharePoint Online usage. Select a **Department** you wish this service to belong to from the drop-down list or click **Create New** to create a new one.

   Choose whether to assign a department to this service, or allow the business user to choose the department when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The department selected in the preceding drop-down list will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to choose the department when submitting a service request for this service.

   ***Note**: If **Use department in Azure Active Directory properties or in SharePoint Online user profile** was chosen when an IT Admin configured departments in the **System** group, Governance Automation Online will retrieve the requesters' departments from Azure AD properties or from SharePoint Online User Profile Service.

5. **Service Initiation** – Choose how users will be able to initiate requests for this service.
    - **Available in service catalog (the Start a Request page)** – Select this checkbox to allow business users to access this service via the service catalog (the **Start a Request** page).
    - **Available as a questionnaire result** – Select this checkbox to allow business users to access this service via questionnaire results. Then, choose one of the following options:
        - **Users must meet the service permissions below** – Allows business users who meet the permission conditions in the **Service Permissions** field below to access this service via questionnaire results.
        - **Allow all users to use this service from questionnaire results (Regardless of the service permission conditions)** – Allows all business users to access this service via questionnaire results regardless of the service permission conditions.
6. **Service Permissions** – Choose what kind of users have permission to use this service. Note that local users, Office 365 users, or Office 365 groups entered here must be existing AvePoint Online Services users.
    - **Allow all users to use this service** – Allow this service to be requested by any user.
    - **Define conditions for users who can use this service** – Allows business users who meet certain conditions to use this service. Refer to the following steps:
        i. Select one of the following options from the **Users/Groups/Roles** drop-down list:

        ***Note**: The supported conditions vary with service types.

        Local Users or Office 365 Users/Groups – The AvePoint Online Services local users or Office 365 users/groups entered in the text box below can view this service in the **Start a Request** page and can submit requests via this service.

        Site Roles – The site roles entered in the text box below can submit requests via this service.

        SharePoint Online Groups – The users of the entered SharePoint Online groups can submit requests via this service.

        Office 365 Group Roles – The Office 365 group roles entered in the text box can submit requests via this service.

        ii. Configure the **Allowed values** field.

        Enter the usernames or group names in the text box. Press **Enter** to check whether or not the names are valid.

        If you selected **Site Roles** or **Office 365 Group Roles** from the **Users/Groups/Roles** drop-down list, enter **$** and select a role from the drop-down list.

        If you selected **SharePoint Online Groups** from the **Users/Groups/Roles** drop-down list, you can also enter the **$SiteName Group Name Suffix**

role in the text box. Note that you must replace **Group Name Suffix** with your desired value. The **SiteName** part will be automatically replaced with the corresponding site title.

iii. Click **Add to List** to add the entered users/groups/roles to the table or click **Clear Settings** to reset your configurations of conditions.

After the users/groups/roles are added to the table, you can also perform the following actions:

Click **Clear Table** to remove the added users/groups/roles from the table.

Click the edit ( ) button to fill the users/groups/roles added to the table back in the text box and edit them.

Click the delete ( ) button to remove the users/groups/roles from the table.

iv. Optionally, select the **Require a user to meet all conditions above for using this service** checkbox to allow business users who meet all conditions above to use this service.

7. **Service Contact** – Specify a user to be the Service Contact. This should be a business user who is the owner of the business process for this service. Enter the username in the **Service Contact** text box. Press **Enter** to check whether or not the name is valid.

8. **Administrator Contact** –Specify a user or an Azure Active Directory group to be the Administrator Contact. This user or group should be an administrator of Governance Automation Online and is responsible for service management. Governance Automation Online will assign a task to the Administrator Contact when an error occurs after the approval process starts. Enter a username or a group name in the **Administrator Contact** text box. Press **Enter** to check whether or not the name is valid. To also have an e-mail notification be sent to the Administrator Contact when this service encounters an error, configure the **Administrator Notification** section of the **System** group within **Settings**. For more information, refer to Configuring Administrator Notification.

9. **Metadata** – Select the metadata to be made available to users when submitting a request for this service. Click the **Add Metadata** to go to the **Add Metadata** window. In the **Add Metadata** window:

   - **Create** – Click **Create** to create new metadata in the **Create Metadata** window. For more information about how to configure metadata, refer to Creating or Editing Metadata.
   - **Edit** – Select metadata and click **Edit**. For more information about how to configure metadata, refer to Creating or Editing Metadata.
   - **Add to List** – Select desired metadata and click **Add to List**. The metadata displayed here is configured in **Settings** > **Request Management** > **Metadata**.

10. **Approval Process** – Choose **Single approval process** or **Multiple approval processes** that will be used for the service. Follow the instructions below:

- **Single approval process** – Select this option and then select an approval process from the drop-down list.

  Optionally, select the **Allow all approvers to edit this service request** checkbox to allow all of the approvers to edit the service request for this service when viewing the service request. You can **Notify the requester when the service request is edited** by selecting the corresponding checkbox, then, select an **E-mail template** from the drop-down list.

  ***Note**: If you select an approval process with **Auto-approve** enabled, the **Allow all approvers to edit this service request** option is invisible.

- **Multiple approval process** – Select this option to add one or more conditional approval processes, which determines which approval process will be used for requests for this service according to the metadata criteria. Click **Add Conditional Approval Process** and the **Add Conditional Approval Process** window appears. Complete the following settings:

  i. **Name** – Enter a name for the conditional approval process in the text box.

  ii. **Conditional Settings** – Choose to **Always run this approval process** or **Run this approval process if the conditions below are met**. If you chose the latter option, you must complete the following settings that will be combined with an approval process.

  Metadata source – Select a metadata source from the drop-down list. The metadata within this source will be a condition of the conditional approval process.

  Metadata name – Select a metadata name within the metadata source selected above from the drop-down list.

  Condition – Select a condition from the drop-down list.

  Metadata value – Enter a metadata value in the text box or select a metadata value from the drop-down list.

  Add to List – Click **Add to List** to add the criterion configured above to the table. You can repeat the settings above to add more criteria.

  If you add multiple criteria, select **And** or **Or** from the **Logic Option** drop-down list. If you select **And**, the approval process will be applied to the service request when all of the criteria is met. If you select **Or**, the approval process will be applied to the service request when any of the criteria is met.

  You can also perform the following actions:

  Clear Settings – Click **Clear Settings** to clear all of the condition settings configured above.

Clear Table – Click **Clear Table** to clear all of the conditions you added to the table.

iii. **Approval Process** – Select an approval process from the drop-down list that will be combined with the conditions configured above to create a conditional approval process.

iv. Click **Save** on the ribbon to save your configurations or click **Cancel** to return to the service settings page without saving any configurations.

v. You can repeat the steps above to create multiple conditional approval process. You can also click the **Order** drop-down list of an added approval process, then, select a number from the drop-down list to set the order of the approval process.

vi. You can click **Preview** to preview the conditional approval process.

vii. **Default approval process** – Select a default approval process from the drop-down list and select one of the following circumstances that will use the default approval process:

Use the default approval process if none of the conditions above is met

Use the default approval process as the last approval stage for all of the requests submitted via this service

viii. **Notify the requester and the approvers upon the request completion** – You can select this option to notify the requester and the approvers when the request completes. Then, select an e-mail template used for sending notification e-mail to the requester and approvers.

***Note**: If you select the **Allow all approvers to edit this service request** option, but the default approval process or the approval process within the conditional approval process has **Auto-approve** enabled, this option will not take effect.

When you select a single approval process from the drop-down list or a default approval process for multiple approval processes from the drop-down list, you can also click **Create New** to create a new approval process. This will bring you to the **Approval Process Settings** interface without saving any of the configurations you have made for this service. After selecting the approval process, you can click the information (ⓘ) icon to view the approval stage, approver, and approval order in a pop-up window.

If the configurations of the selected approval process do not meet your requirements, you can create a new approval process on the basis of the selected approval process. Click **Create from This Existing Approval Process** and the **Approval Process Settings** window appears. Configure the settings, and then save and activate the approval process. For more information on configuring the approval process, refer to Creating or Editing Approval Processes.

11. **Custom Action** – Allows you to define custom actions that can be taken during pending validation, before approving, after approving, and after executing a request via the methods that exist in a published Web Service.

    - **Pending validation** – After business users submit the request, the defined custom action will be executed to validate the request. If the request is valid, a task will be generated and assigned to an approver.
    - **Before approval** – After business users submit the request, the defined custom action will be executed. Then, a task will be generated and assigned to an approver.
    - **After approval** – After business users submit the request, a task will be generated and assigned to an approver. After the approver approves the task, the defined custom action will be executed.
    - **After execution** – After business users submit the request and all of the settings configured in this service are executed, the defined custom action will be executed.

    Note the following:

    - Custom Services only support custom actions for **Before approval** and **After approval**.
    - The **Pending submission** is only supported in Create Site Collection services.

    Select the corresponding checkboxes and complete the following steps:

    a. Enter the URL of your published Web Service in the **Web Service Address** text box.

    b. Select **Anonymous Access** or **Azure Active Directory Authentication** as the authentication type that will be used to access the Web service from the drop-down list. If you select **Azure Active Directory Authentication** as the authentication type, you must enter the Client ID of Azure Active Directory application in the text box.

    ***Note**: In order to use the Azure Active Directory account to access the Web service, you must configure your App service application first. Refer to the following Microsoft technical article to configure your App service application: https://azure.microsoft.com/en-us/documentation/articles/app-service-mobile-how-to-configure-active-directory-authentication/

    c. Click **Retrieve** to retrieve the methods in the Web Service.

    d. Select your desired method from the drop-down list.

    e. If there are parameters defined in the selected method, the parameters are displayed in a table. Enter the value for each parameter in the corresponding text box.

12. **Run During** – Select **Enable service request execution schedule** to define when Governance Automation Online executes the service request. Then choose a previously configured execution schedule from the drop-down list or click **Create New** to create a new one.

Configuring Create Site Collection Services

Configure Create Site Collection services to define the Create Site Collection service request template for business users. You can customize the settings for site collections created by this service as well as configure available options for business users to choose from when requesting this service. Create Site Collection services also allow you to apply data protection and content retention policies on the site collections with full auditing to monitor compliance with your corporate standards.

In the interface for creating or editing a Create Site Collection service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Admin Centers and Managed Paths** – Specify the SharePoint Online admin center and associated managed path where you wish to create a site collection.

   Expand the site collection group tree to select the desired admin center by selecting the corresponding option. Specify a default admin center and managed path for the site collection you wish to create by selecting from drop-down lists under the tree.

   You can choose to **Use SharePoint Online context to automatically populate the service request scope**. With this option selected, SharePoint Online context will be retrieved and used in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the admin center and managed path of the site collection where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The admin center and managed path will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The admin center and managed path will be automatically filled into the text box, and the requester can edit them.
   - **Show as Read-Only to Business User** – The admin center and managed path will be displayed as read-only, and the requester cannot edit them.
   - **Hide from Business User** – The admin center and managed path will be hidden from the requester.

2. **Policy** – Specify the site collection policies to provision the site collections created by this service by selecting the corresponding checkboxes or click **Create New** to be brought to the **Policy Management** interface to create a new policy. Configure this section as follows:

   a. Select the policies to be made available for business users to choose from by selecting the corresponding checkbox of each policy in the **Select Policies** configuration area. All policies selected here will be made available to business users if you select **Assign by Business User** in the Assign by drop-down list. If no existing policy is appropriate for this service, you may click **Create New** to create a new one.

b. Select a default policy in the **Default Selection** drop-down list. If **Assign by Business User** is selected in the Assign by drop-down list, this policy will be selected in the service request, but the business user will be able to select another policy out of the policies you have selected in the **Select the Policies** configuration area. If **Assign by IT Admin** is selected in the Assign by drop-down list, this will be the only available policy in the service request and the business user will not be able to choose another policy.

Choose whether to assign a policy to site collections created by this service, or allow the business user to choose the policy when submitting a service request for this service from the policies selected in the **Select the Policies** configuration area. Choose from the following:

- **Assign by IT Admin** – The policy selected in the **Default Selection** drop-down list will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business user to choose from the policies you have selected in the **Select the Policies** configuration area.

3. **Language** – Select the language for the site collection. If more than one language is selected, choose a default language from the **Default Selection** drop-down list.

   Choose whether to assign a language to site collections created by this service, or allow the business user to choose the language when submitting a service request for this service from the languages selected in the **Select Language** configuration area. Choose from the following:

   - **Assign by IT Admin** – The language selected in the **Default Selection** drop-down list will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to choose from the languages you have selected in the **Select Language** configuration area.

4. **Site Collection Template** – Specify the site collection template to use for site collections created by this service. Configure this section as follows:

   - **Retrieve custom site template from an external data source** – Select this option to use a custom template to create a site collection.

     i. **Get custom site template from a library** – Enter the URL of the SharePoint Online library where the information of the custom templates is stored.

     ii. **Get template name from the following column** – Select a column whose values are the custom template names.

   - **Select templates** – In this field, select which site collection templates will be made available for business users by selecting the corresponding checkbox.

5. Select the default site collection template in the **Default Selection** drop-down list.

6. Choose to use the default site collection template to create site collections, or to allow business users to choose the site collection template from the available templates when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The site collection template selected in the **Default Selection** drop-down list will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows business user to choose from the site collection templates you have selected in the **Select the templates** configuration area.

7. **Communication Site Classification** (for the Communication Site template only) – Select site classifications for communication sites created by this service. If you select multiple site classifications, select a default one from the **Default site classification** drop-down list.

    Choose whether to assign a site classification to communication sites created by this service, or allow the business to select the site classification when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The site classification selected in the **Default site classification** drop-down list will be applied to communication sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows business users to choose from the site classifications you selected in the service. The default site classification selected in this service will become the default option, and business users can change it to another site classification.

8. **Communication Site Design** (for the Communication Site template only) – Select the site design for communication sites created by this service.

    Choose whether to assign the site design to communication sites created by this service, or allow business users to select the site design when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The site design selected here will be applied to communication sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows business users to select the site design.

9. Click the arrow on the right-hand side to proceed to the next step.

10. **Time Zone** – Select the time zone for the site collections created by this service.

    Choose whether to assign the time zone to site collections created by this service, or allow the business user to select the time zone when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The time zone selected here will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

- **Assign by Business User** – Allows business users to select the time zone in the **Time Zone** configuration area.

11. **Site Collection Permissions** (the **Common** tab) – Configure the common permission settings to assign permissions to specific groups and users. By default, the common groups are displayed. Click the edit ( ) button to edit the settings of a group or click the delete ( ) button to delete a group.

    - **Create Group** – Click **Create Group** to create a new group and add it into the common permission settings. In the **Add a Group** window, configure the following settings:

        i. **Custom Group Name** – Enter a name for the group and enter an optional description for future reference. Enter **$SiteName** to automatically add the site collection title as the group name prefix in Create Site Collection service request.

        ii. **Group Owner** – Choose to assign an Office 365 user or a SharePoint Online group to be the group owner. Configure the following settings:

            Office 365 user – Choose this option and enter the username of an Office 365 user in the text box as the group owner. Press **Enter** to check whether or not the name is valid. By default, the **$Primary Site Collection Administrator** role is automatically populated into the text box as the group owner.

            SharePoint Online group – Choose this option and select a SharePoint Online group from the drop-down list as the group owner.

            Choose to assign the group owner to the custom group that will be created together with the site collection created via this service, or allow business users to assign the group owner when submitting requests for this service. Choose from the following:

            Assign by IT Admin – The group owner assigned here will be the group owner. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

            Assign by Business User – Allows business users to assign the group owner when submitting requests for this service.

        iii. **Select Users** – Select your desired users to add into the group. Click **Add a User** and enter the usernames in the pop-up window. You can also enter the following roles: **$Requester**, **$Manager of Requester**, **$Primary Site Collection Contact**, and **$Secondary Site Collection Contact**. Then, click **OK** to save your configurations.

            Optionally, select the **Enforce Permission** checkbox after a username. In the request page, the user cannot be deleted and the user permissions cannot be modified. For the enforced permission user, you can hide the enforced permission user from the request page by selecting the **Hide** checkbox.

Choose to assign group members to the custom group that will be created together with the site collection created via this service, or allow business users to assign group members when submitting requests for this service. Choose from the following:

Assign by IT Admin – The users assigned here will be the group members. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

Assign by Business User – Allows business users to assign the users as group members when submitting requests for this service.

iv. **Permissions** – Configure the permissions for this group. Select your desired permission levels by selecting the corresponding checkboxes.

Optionally, select the **Allow Business User to change the permission level of this group** checkbox, so that the business users can modify the permission level when creating a request.

v. Click **Save** to save the group settings.

- **Grant Permissions** – Click **Grant Permissions** to grant permissions to specific users. In the **Grant User Permissions** window, configure the following settings:

  i. **Select Users** – Enter the names of the users that you are about to grant permissions.

  ii. **Assign By** – Choose who will assign the user permissions, IT Admin or Business User.

  iii. **Permissions** – Configure the permissions for the users. Select your desired permission levels by selecting the corresponding checkboxes.

  iv. Click **Save** to save your configurations.

12. **Site Collection Permissions** (the specific template tab) – The template tab depends on the selected site collection template. The default groups of the site collection template are displayed. Click the edit ( ) button to edit the settings of a custom group or click the delete ( ) button to delete a custom group.

    - **Use common permission settings** – Select the checkbox to apply the permission settings in the **Common** tab. If there are group names that already exist in the **Common** tab, the group settings will be replaced by those of the **Common** tab.

    - **Create Group** – Click **Create Group** to create a new group and add it into the specific template permission settings. In the **Add a Group** window, configure the following settings:

      i. **Custom Group Name** – Enter a name for the group and enter an optional description for future reference. Enter **$SiteName** to automatically add the site

collection title as the group name prefix in Create Site Collection service request.

ii. **Group Owner** – Choose to assign an Office 365 User or a SharePoint Online group to be the group owner. Configure the following settings:

Office 365 user – Choose this option and enter the username of an Office 365 user in the text box as the group owner. Press **Enter** to check whether or not the name is valid. By default, the **$Primary Site Collection Administrator** role is automatically populated into the text box as the group owner.

SharePoint Online group – Choose this option and select a SharePoint Online group from the drop-down list as the group owner.

Choose to assign the group owner to the custom group that will be created together with the site collection created via this service, or allow business users to assign the group owner when submitting requests for this service. Choose from the following:

Assign by IT Admin – The group owner assigned here will be the group owner. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

Assign by Business User – Allows business users to assign the group owner when submitting requests for this service.

iii. **Select Users** – Select your desired users to add into the group. Click **Add a User** and enter the usernames in the pop-up window. You can also enter the following roles: **$Requester**, **$Manager of Requester**, **$Primary Site Collection Contact**, and **$Secondary Site Collection Contact**. Then, click **OK** to save your configurations.

Optionally, select the **Enforce Permission** checkbox after a username. In the request page, the user cannot be deleted and the user permissions cannot be modified. For the enforced permission user, you can hide the enforced permission user from the request page by selecting the **Hide** checkbox.

Choose to assign group members to the custom group that will be created together with the site collection created via this service, or allow business users to assign group members when submitting requests for this service. Choose from the following:

Assign by IT Admin – The users assigned here will be the group members. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

Assign by Business User – Allows business users to assign the users as group members when submitting requests for this service.

iv. **Permissions** – Configure the permissions for this group. Select your desired permission levels by selecting the corresponding checkboxes.

Optionally, select the **Allow Business User to change the permission level of this group** checkbox, so that the business users can modify the permission level when creating a request.

v. Click **Save** to save the group settings.

- **Grant Permissions** – Click **Grant Permissions** to grant permissions to specific users. In the **Grant User Permissions** window, configure the following settings:

  i. **Select Users** – Enter the names of the users that you are about to grant permissions.

  ii. **Assign By** – Choose who will assign the user permissions, IT Admin or Business User.

  iii. **Permissions** – Configure the permissions for the users. Select your desired permission levels by selecting the corresponding checkboxes.

  iv. Click **Save** to save your configurations.

- **Reset All** – Click **Reset All** to clear your configurations and reset all configured security groups settings to the initial state.
- **Business User action control** – Choose how to control the business user actions on the security group.
  - **Allow Business User to grant user permissions directly** – Select this checkbox to allow business users to directly grant permissions to specific users in the request.
  - **Prevent Business User from requesting to grant permissions with the following permission levels** – Select this checkbox and select your desired permission levels. The selected permission levels will not be displayed in the request.

13. Click the arrow on the right-hand side to proceed to the next step.
14. **Primary Site Collection Administrator** – Assign a user to be the primary site collection administrator by entering the username into the text box. Press **Enter** to check whether or not the name is valid.

    You can also enter one of the following roles:

    - **$Requester** – The requester will become the primary site collection administrator.
    - **$Manager of Requester** – The manager of the requester will become the primary site collection administrator.
    - **$Primary Site Collection Contact** – The primary site collection contact for the site collection created via the service request will become the primary site collection administrator.

- **$Secondary Site Collection Contact** – The secondary site collection contact for the site collection created via the service request will become the primary site collection administrator.

Choose whether to assign the primary site collection administrator to site collections created by this service, or allow the business user to choose the primary site collection administrator when submitting a service request for this service. By default, it is **Assign by IT Admin** and **Hide from Business User**. Choose from the following:

- **Assign by IT Admin** – The primary site collection administrator configured here will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows the business user to configure the primary site collection administrator.

15. **Additional Site Collection Administrators** – Assign one or more users to be the additional site collection administrators of the new site collection by entering the usernames into the text box. Press **Enter** to check whether or not the name is valid.

    You can also enter one of the following roles:

    - **$Requester** – The requester will become the additional site collection administrator.
    - **$Manager of Requester** – The requester's manager will become the additional site collection administrator.
    - **$Primary Site Collection Contact** – The primary site collection contact of the site collection created via the service request will become the additional site collection administrator.
    - **$Secondary Site Collection Contact** – The secondary site collection contact of the site collection created via the service request will become the additional site collection administrator.

    Choose whether to assign the additional site collection administrators to site collections created by this service, or allow the business user to choose the additional site collection administrators when submitting a service request for this service. The default settings are **Assign by IT Admin** and **Hide from Business User**. Choose from the following:

    - **Assign by IT Admin** – The additional site collection administrators configured here will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows the business user to configure the additional site collection administrators.

16. **Primary Site Collection Contact** – The primary site collection contact will be the user designated for managing the lifecycle of the site collection created by this service. Assign a user to be the primary site collection contact by entering the username into the text box. Press **Enter** to check whether or not the name is valid.

You can also enter one of the following roles:

- **$Requester** – The requester will become the primary site collection contact.
- **$Manager of Requester** – The manager of the requester will become the primary site collection contact.

Choose whether to assign the primary site collection contact to site collections created by this service, or allow the business user to choose the primary site collection contact when submitting a service request for this service. Choose from the following:

- **Assign by IT Admin** – The primary site collection contact configured here will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows the business user to configure the primary site collection contact.

You can send an e-mail to notify the primary site collection contact when the site collection is created successfully. Select the **Notify the contact upon site collection creation** checkbox and select an e-mail template from the drop-down list.

17. **Secondary Site Collection Contact** – The secondary site collection contact will be the user designated for managing the lifecycle of the site collection created by this service if the primary site collection contact is unable to respond to a notification. Assign a user to be the secondary site collection contact by entering the username into the text box. Press **Enter** to check whether or not the name is valid.

    You can also enter one of the following roles:

    - **$Requester** – The requester will become the secondary site collection contact.
    - **$Manager of Requester** – The manager of the requester will become the secondary site collection contact.

    Choose whether to assign the secondary site collection contact to site collections created by this service, or allow the business user to choose the secondary site collection contact when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The secondary site collection contact configured here will be associated with all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows the business user to configure the secondary site collection contact.

    You can send an e-mail to notify the secondary site collection contact when the site collection is created successfully. Select the **Notify the contact upon site collection creation** checkbox and select an e-mail template from the drop-down list.

18. Click the arrow on the right-hand side to proceed to the next step.

19. **DocAve Online Deployment Manager Plan** – Select the **Apply DocAve Online Deployment Manager Plan** checkbox to apply a DocAve Manager plan to the new site collection. The pattern in the Deployment Manager plan will be used to create the new site collection. Deployment Manger plans will be displayed in the table if they meet all of the following conditions:

    a. The deployment type of the mappings in the plan is **Design Element** or the source nodes in the mappings are within the **User Solution Gallery** node.

    b. The destination nodes in the mappings are site collections.

    c. All of the mappings in the plan meet all of the conditions above.

    If more than one Deployment Manager plan is selected, you must choose a default Deployment Manager plan from the **Default Selection** drop-down list.

    You can assign the selected Deployment Manager plan to site collections created by this service, or allow the business user to choose the Deployment Manager plan when submitting a service request. Choose from the following:

    - **Assign by IT Admin** – The Deployment Manager plan selected in the **Default Selection** drop-down list will be applied to all site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows the business user to choose from the Deployment Manager plans you have selected in the **Select plans** area.

20. **Manage Site Collection Lifecycle** – Select the **Enable Site Collection Lease Period** checkbox to enable a lease period for the site collection. Specify the lease period by entering a number in the provided text box and choose **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** from the drop-down list.

    Choose whether to assign the site collection lease period to site collections created by this service, or allow the business user to choose the site collection lease period when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The site collection lease period configured here will be associated with the site collection created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows the business user to configure the site collection lease period.

    When the site collection lease period is enabled, you can choose to enable lease expiration warning to configure when to send the warning e-mail before the site collection reaches expiration by selecting the **Enable lease expiration warning** checkbox. Then, enter a number in the provided text box and choose **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** from the drop-down list.

    Choose whether to assign the lease expiration warning to site collections created by this service, or allow the business user to choose the lease expiration warning when submitting a service request for this service. Choose from the following:

- **Assign by IT Admin** – The lease expiration warning configured here will be associated with the site collection created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows the business user to configure the lease expiration warning.

Select an approval process from the drop-down list or click **Create New** to create a new one. This approval process will be triggered when the site collection lease period is exceeded. A task will be assigned to the business users specified in the selected approval process asking if they would like to extend site collection lease or delete the site collection. Note that the multiple-stage approval process is supported for the site collection lease period task.

If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.

21. **Governance Automation Online App and App Part** – Choose to automatically enable the Governance Automation Online App during site collection creation. If enabling this feature, first make sure that the Governance Automation Online App has been properly deployed to your SharePoint Online environment. For more information about the environment configuration and deployment, refer to Installing the Governance Automation Online App. If you choose **Automatically enable Governance Automation Online App**, you can select the app parts: **Site Information Card** and/or **Site Lifecycle Timeline**. Governance Automation Online will automatically add the selected app parts into the homepage of the site collection that is created by this service.

    ***Note**: If you want to share a site collection's top-level site that contains the Governance Automation Online app parts to other users, make sure you have invited them in AvePoint Online Services **Settings** > **User Management**. Otherwise, they cannot view the app parts.

22. **Yammer Integration** – Choose to enable the integration of Governance Automation Online and Yammer. If you enable it, you must create a Yammer app profile in AvePoint Online Services first, and then configure the following settings:

    a. **Yammer network** – Select a Yammer network from the drop-down list to connect Governance Automation Online to a Yammer tenant.

    b. **Add a Yammer group feed to the site collection homepage** – Allows to add a Yammer group feed to the site collection homepage via one of the following methods:

        - **Allow business users to create a new Yammer internal group** – Choose this option to allow business users to create a new Yammer internal group when submitting a request for this service. The feed of the new Yammer internal group will be added to the site collection homepage. Then, configure the following settings:

            Group Type – Allows you to choose who can view the group content. Choose **Public – Anyone in this network** to allow every user in this network to view the group content, or choose **Private – Only approved**

members to allow users approved by members of this group to view the group content. If you choose the **Private – Only approved members** option, you can select the **List in group directory** checkbox to have the approved members listed in the group directory.

Group Permission – Allows you to choose who can join the group. Choose **Anyone in this network** to allow every user in this network to join the group, or choose **Only those approved by an admin** to allow users approved by a group administrator to join the group.

Choose to apply the new Yammer internal group settings configured here to the site collections created by this service, or allow business users to configure the new Yammer internal group settings when submitting requests via this service. Choose from the following:

Assign by IT Admin – Apply the new Yammer internal group settings configured here to the site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

Assign by Business User – Allows business users to configure the new Yammer internal group settings.

- **Allow business users to use an existing Yammer group** – Choose this option to allow business users to use an existing Yammer group when submitting a request for this service. The feed of the existing Yammer group will be added to the site collection homepage.

  If you did not select the **Allow business users to create a new Yammer internal group** checkbox above, you can select the **Apply an existing Yammer group** checkbox to apply an existing Yammer group to the site collection created via this service. Then, you must enter the name or ID of an existing Yammer group in the text box and click **Validation Test** to validate the group name or group ID.

23. **URL** – Choose one of the following methods to define the site collection URL.

- **Manually input URL** – Allows the requester to manually enter the site collection URL. You can choose the following options:
  - **Construct URL** – Select the checkbox to build the site collection URL using specific rules. Click **Add** and select a rule from the drop-down list. The following rules are available:

    Site Collection Title

    Department

    Custom metadata with the types of Single line of text, Choice, Person or Group, and Managed Metadata.

    ***Note**: If the metadata with the type of Choice - Checkboxes, Person or Group, or Managed Metadata has multiple values, the values will be separated with semicolons in the constructed URL.

You can also define the suffix for the site collection URL as the one of the following formats:

{01} – The suffix in the site collection URL will increase from **01** to **99** in numerical value.

{01*} – The suffix in the site collection URL will increase from **01** to **999999999** in numerical value.

If you add multiple rules, you can enter one or more connection characters for connecting the values of those rules. If you choose to not define a connection character, the rule values will be connected by spaces.

Choose whether to allow business users to modify the site collection URL when submitting requests via this service. Choose from the following:

Assign by IT Admin – The URL rules configured here will be used to generate the URL of the site collection created via this service. The generated site collection URL will be displayed to business users as read-only in the request form.

Assign by Business User – The URL rules configured here will be used to generate the URL of the site collection created via this service. In the request form, the generated site collection URL will be displayed to business users as the default URL, and business users can modify the URL if desired.

- **URL validation** – Select the checkbox to enable site collection URL validation. Then, select a text validation rule from the drop-down list. The site collection URL defined by the requester will be validated according to the regular expression set in the text validation rule.

- **Automatically generate URL** – Allows Governance Automation Online to automatically generate the site collection URL. Choose one of the following methods:
  - **Sequential numbering** – Define the prefix, delimiter, and sequence number. Refer to the following examples:

Prefix	Sequence Number	Note
abc{d}		**abc** will be used fixedly as a part of the site collection URL prefix. The part **{d}** will increase in alphabetical order from **d** to **z**.
	{01}	The sequence number in the site collection URL will increase from **01** to **99** in numerical value.
abc	{01}	**abc** will be used fixedly as the site collection URL prefix. The sequence number in the site collection URL will increase from **01** to **99** in numerical value.
abc	{01*}	The sequence number in the site collection URL will increase from **01** to **999999999** in numerical value.
{abc}	{01}	After the sequence number increases to **99**, the prefix will increase to **abd** and the sequence number will be initialized to **00**.
{abcz}	{01}	After the sequence number increases to **99**, the prefix will increase to **abdz** and the sequence number will be initialized to **00**.

- **Random string** – Choose this method to automatically generate site collection URL by randomly adding letters and numbers. Define the **Minimum length of the URL name** and **Maximum length of the URL name**. You can also enter a prefix, and the URL name will be prefix + random string.

  A site collection URL is in the following format:

  https://domain name/managed path/prefix + random string

  For example, **https://contoso.sharepoint.com/sites/us_kb824**. Here **us_** is the prefix and **kb824** is the random string.

  When you define the maximum and minimum length of the URL name, note that the length of a site collection URL cannot exceed 136 characters.

24. Click the arrow on the right-hand side to proceed to the next step.
25. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.

- Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
- Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Create Site Services

Configure Create Site services to define the Create Site service request template for business users. You can customize the settings for sites created by this service as well as configure available options for business users to choose from when requesting this service. Sites created by Governance Automation Online inherit data protection and content retention policies from the site collection they live in.

On the interface for creating or editing a Create Site service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Choose the site collections you wish to be made available in this service. Business users will be able to choose which site collection to create the new site under.
    a. Choose one of the following methods to configure the scope:
        - **Manually input URL** - Select this option and click **Add Your Own URL** to enter the URL of the site collection in the text box. To add more site collections, click **Add Your Own URL** after entering a URL.
        - **Select scope from tree** – Select this option and then select the site collections from the data tree.
    b. **Use SharePoint Online context to automatically populate the service request scope** – Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:
        - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
        - **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
        - **Hide from Business User** – The site URL will be hidden from the requester.
    c. **Site URL** – You can choose the following options:
        - **Use site title in URL** – Select this checkbox to have the site URL filled automatically after entering the site title in the service request.

- **URL validation** – Select this checkbox to enable site URL validation. Then, select a text validation rule from the drop-down list. The site URL defined by the requester will be validated according to the regular expression set in the text validation rule.

2. **Language** – Specify the language for the sites. If more than one language is selected, choose a default language from the **Default Selection** drop-down list.

   Choose whether to assign a language to sites created by this service, or allow the business user to choose the language when submitting a service request for this service from the languages selected in the **Language** configuration area. Choose from the following:

   - **Assign by IT Admin** – The language selected in the **Default Selection** drop-down list will be associated with all sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to choose from the languages you have selected in the **Language** configuration area.

3. **Site Template** – Specify the templates which can be used to create the site. In the **Select templates** text box, enter the site collection URL where all of your site templates are centrally stored. Then click **Retrieve** to retrieve the available templates and select the desired templates by selecting corresponding checkboxes. Select a template as the default template from the drop-down list in the **Default Selection** section.

   Choose whether to assign a template to sites created by this service, or allow the business user to choose the site template when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The site template selected in the **Default Selection** drop-down list will be associated with all sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to choose from the site templates you have selected in the **Template Selection** configuration area.

4. Click the arrow on the right-hand side to proceed to the next step.

5. **Security Groups** – Select to inherit permissions from parent site or use the unique permissions.

   - **Use same permissions as parent site** – Select this option to inherit the parent site's permissions settings. **Assign by IT Admin** will be the default selection for the Assign by drop-down list. Choose whether to **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Use unique permissions** – Select this option, and refer to the instructions in step 6 and step 7 to customize the site permissions for sites created by this service:

6. **Site Permissions**: **Use unique permissions** (the **Common** tab) – Configure the common permission settings to assign permissions to specific groups and users. By default, the common groups are displayed. Click the edit ( ) button to edit the settings of a specific group or click the delete ( ) button to delete a specific group.

- **Create Group** – Click **Create Group** to create a new group and add it into the common permission settings. In the **Add a Group** window, configure the following settings:

  i. **Custom Group Name** – Enter a name for the group and enter an optional description for future reference. Enter **$SiteName** to automatically add the site title as the group name prefix in Create Site service request.

  ii. **Group Owner** – Choose to assign an Office 365 user or a SharePoint Online group to be the group owner. Configure the following settings:

  Office 365 user – Choose this option and enter the username of an Office 365 user in the text box as the group owner. Press **Enter** to check whether or not the name is valid. By default, the **$Primary Site Collection Administrator** role is automatically populated into the text box as the group owner.

  SharePoint Online group – Choose this option and select a SharePoint Online group from the drop-down list as the group owner.

  Choose to assign the group owner to the custom group that will be created together with the site created via this service, or allow business users to assign the group owner when submitting requests for this service. Choose from the following:

  Assign by IT Admin – The group owner assigned here will be the group owner. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

  Assign by Business User – Allows business users to assign the group owner when submitting requests for this service.

  iii. **Select Users** – Select your desired users to add into the group. Click **Add a User** and enter the usernames in the pop-up window. You can also enter the following roles: **$Requester**, **$Manager of Requester**, **$Primary Site Collection Contact**, **$Secondary Site Collection Contact**, **$Primary Site Contact**, and **$Secondary Site Contact**. Then, click **OK** to save your configurations.

  Optionally, select the **Enforce Permission** checkbox after a username. In the request page, the user cannot be deleted and the user permissions cannot be modified. For the enforced permission user, you can hide the enforced permission user from the request page by selecting the **Hide** checkbox.

  Choose to assign group members to the custom group that will be created together with the site collection created via this service, or allow business users to assign group members when submitting requests for this service. Choose from the following:

Assign by IT Admin – The users assigned here will be the group members. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

Assign by Business User – Allows business users to assign the users as group members when submitting requests for this service.

iv. **Permissions** – Configure the permissions for this group. Select your desired permission levels by selecting the corresponding checkboxes.

Optionally, select the **Allow Business User to change the permission level of this group** checkbox, so that the business users can modify the permission level when creating a request.

v. Click **Save** to save the group settings.

- **Grant Permissions** – Click **Grant Permissions** to grant permissions to specific users. In the **Grant User Permissions** window, configure the following settings:

  i. **Select Users** – Enter the names of the users that you are about to grant permissions.

  ii. **Assign By** – Choose who will assign the user permissions, IT Admin or Business User.

  iii. **Permissions** – Configure the permissions for the users. Select your desired permission levels by selecting the corresponding checkboxes.

  iv. Click **Save** to save your configurations.

7. **Site Permissions**: **Use unique permissions** (the specific template tab) – The template tab depends on the selected site template. The default groups of the site template are displayed. Click the edit ( ) button to edit the settings of a custom group or click the delete ( ) button to delete a custom group.

   - **Use common permission settings** – Select the checkbox to apply the permission settings in the **Common** tab. If there are group names that already exist in the **Common** tab, the group settings will be replaced by those of the **Common** tab.

   - **Create Group** – Click **Create Group** to create a new group and add it into the specific template permission settings. In the **Add a Group** window, configure the following settings:

     i. **Custom Group Name** – Enter a name for the group and enter an optional description for future reference. Enter **$SiteName** to automatically add the site title as the group name prefix in Create Site service request.

     ii. **Group Owner** – Choose to assign an Office 365 user or a SharePoint Online group to be the group owner. Configure the following settings:

Office 365 user – Choose this option and enter the username of an Office 365 user in the text box as the group owner. Press **Enter** to check

whether or not the name is valid. By default, the **$Primary Site Collection Administrator** role is automatically populated into the text box as the group owner.

SharePoint Online group – Choose this option and select a SharePoint Online group from the drop-down list as the group owner.

Choose to assign the group owner to the custom group that will be created together with the site created via this service, or allow business users to assign the group owner when submitting requests for this service. Choose from the following:

Assign by IT Admin – The group owner assigned here will be the group owner. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

Assign by Business User – Allows business users to assign the group owner when submitting requests for this service.

iii. **Select Users** – Select your desired users to add into the group. Click **Add a User** and enter the usernames in the pop-up window. You can also enter the following roles: **$Requester**, **$Manager of Requester**, **$Primary Site Collection Contact**, and **$Secondary Site Collection Contact**. Then, click **OK** to save your configurations.

Optionally, select the **Enforce Permission** checkbox after a username. In the request page, the user cannot be deleted and the user permissions cannot be modified. For the enforced permission user, you can hide the enforced permission user from the request page by selecting the **Hide** checkbox.

iv. **Permissions** – Configure the permissions for this group. Select your desired permission levels by selecting the corresponding checkboxes.

Optionally, select the **Allow Business User to change the permission level of this group** checkbox, so that the business users can modify the permission level when creating a request.

v. Click **Save** to save the group settings.

- **Grant Permissions** – Click **Grant Permissions** to grant permissions to specific users. In the **Grant User Permissions** window, configure the following settings:

i. **Select Users** – Enter the names of the users that you are about to grant permissions.

ii. **Assign By** – Choose who will assign the user permissions, IT Admin or Business User.

iii. **Permissions** – Configure the permissions for the users. Select your desired permission levels by selecting the corresponding checkboxes.

iv. Click **Save** to save your configurations.

- **Business User action control** – Choose how to control the business user actions on the security group.
  - **Allow Business User to grant user permissions directly** – Select this checkbox to allow business users to directly grant permissions to specific users in the request.
  - **Prevent Business User from requesting to grant permissions with the following permission levels** – Select this checkbox and select your desired permission levels. The selected permission levels will not be displayed in the request.

8. **Navigation** – Configure navigation options for sites created using this service:

   - Choose whether or not to **Display this site on the Quick Launch bar of the parent site**.
   - Choose whether or not to **Display this site on the top link bar of the parent site**.

   Choose whether to apply this option to sites created by this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The navigation options configured here will be associated with all sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows the business user to configure the navigation options.

9. **Navigation Inheritance** – Choose whether or not to have sites created by this service **Use the top link bar from the parent site** by choosing the corresponding option.

   Choose whether to apply the option to this service and sites created by this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

   - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
   - **Assign by IT Admin** – The selected option will be applied for this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

10. Click the arrow on the right-hand side to proceed to the next step.

11. **Primary Site Contact** – The primary site contact will be the user designated for managing the site created by this service. Assign a user to be the primary site contact by entering the username into the text box. Press **Enter** to check whether or not the name is valid.

    You can also enter one of the following roles:

    - **$Requester** – The requester will become the primary site contact.
    - **$Manager of Requester** – The manager of the requester will become the primary site contact.

- **$Primary Site Collection Contact** – The primary site collection contact of this service will become the primary site contact.
- **$Secondary Site Collection Contact** – The secondary site collection contact of this service will become the primary site contact.

Choose whether to assign the primary site contact to sites created by this service, or allow the business user to designate one when submitting a service request for this service. Choose from the following:

- **Assign by IT Admin** – The primary site contact configured here will be associated with all sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows the business user to configure the primary site contact.

You can send an e-mail to notify the primary site contact when the site is created successfully. Select the **Notify the contact upon site creation** checkbox and select an e-mail template from the drop-down list.

12. **Secondary Site Contact** – The secondary site contact will be the user designated for managing sites created by this service in case the primary site contact is unable to respond to a notification. Assign a user to be the secondary site contact by entering the username into the text box. Press **Enter** to check whether or not the name is valid.

    You can also enter one of the following roles:

    - **$Requester** – The requester will become the secondary site contact.
    - **$Manager of Requester** – The manager of the requester will become the secondary site contact.
    - **$Primary Site Collection Contact** – The primary site collection contact of this service will become the secondary site contact.
    - **$Secondary Site Collection Contact** – The secondary site collection contact of this service will become the secondary site contact.

    Choose whether to assign the secondary site contact to sites created by this service, or allow the business user to designate one when submitting a service request for this service. Choose from the following:

    - **Assign by IT Admin** – The secondary site contact configured here will be associated with all sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows the business user to configure the secondary site contact.

You can send an e-mail to notify the primary site contact when the site is created successfully. Select the **Notify the contact upon site creation** checkbox and select an e-mail template from the drop-down list.

13. **DocAve Online Deployment Manager Plan** – Select the **Apply DocAve Online Deployment Manager Plan** checkbox to apply a DocAve Manager plan to the new site. The pattern in the Deployment Manager plan will be used to create the new site. Deployment Manger plans will be displayed in the table if they meet all of the following conditions:

    a. The deployment type of the mappings in the plan is **Design Element** or the source nodes in the mappings are within the **User Solution Gallery** node.

    b. The destination nodes in the mappings are sites.

    c. All of the mappings in the plan meet all of the conditions above.

    If more than one Deployment Manager plan is selected, you must choose a default Deployment Manager plan from the **Default Selection** drop-down list.

    You can assign the selected Deployment Manager plan to sites created by this service, or allow the business user to choose the Deployment Manager plan when submitting a service request. Choose from the following:

    - **Assign by IT Admin** – The Deployment Manager plan selected in the **Default Selection** drop-down list will be applied to all sites created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows the business user to choose from the Deployment Manager plans you have selected in the **Select plans** area.

14. **Governance Automation Online App and App Part** – Choose to automatically enable the Governance Automation Online App during site creation. If enabling this feature, first make sure that the Governance Automation Online App has been properly deployed to your SharePoint Online environment. For more information about the environment configuration and deployment, refer to Installing the Governance Automation Online App. If you choose **Automatically enable Governance Automation Online App**, you can select the app parts: **Site Information Card** and/or **Site Lifecycle Timeline**. Governance Automation Online will automatically add the selected app parts into the homepage of the site that will be created by this service.

    ***Note**: If you want to share the sites that contain the Governance Automation Online app parts to other users, make sure you have invited them in AvePoint Online Services **Settings** > **User Management**. Otherwise, they cannot view the app parts.

15. **Yammer Integration** – Choose to enable the integration of Governance Automation Online and Yammer. If you enable it, you must create a Yammer app profile in AvePoint Online Services first. Note that when an approver approves a request via this service, the site users who will have unique permissions to the site will be automatically added to the new Yammer internal group or the existing Yammer group. Configure the following settings:

a. **Yammer network** – Select a Yammer network from the drop-down list to connect Governance Automation Online to a Yammer tenant.

b. **Add a Yammer group feed to the site homepage** – Allows to add a Yammer group feed to the site homepage via one of the following methods:

   - **Allow business uses to create a Yammer internal group** – Choose this option to allow business users to create a new Yammer internal group when submitting a request for this service. The feed of the new Yammer internal group will be added to the site homepage. Then, configure the following settings:

     Group Type – Allows you to choose who can view the group content. Choose **Public – Anyone in this network** to allow every user in this network to view the group content, or choose **Private – Only approved members** to allow users approved by members of this group to view the group content. If you choose the **Private – Only approved members** option, you can select the **List in group directory** checkbox to have the approved members listed in the group directory.

     Group Permission – Allows you to choose who can join the group. Choose **Anyone in this network** to allow every user in this network to join the group, or choose **Only those approved by an admin** to allow users approved by a group administrator to join the group.

     Choose to apply the new Yammer internal group settings configured here to the site collections created by this service, or allow business users to configure the new Yammer internal group settings when submitting requests via this service. Choose from the following:

     Assign by IT Admin – Apply the new Yammer internal group settings configured here to the site collections created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

     Assign by Business User – Allows business users to configure the new Yammer internal group settings.

   - **Allow business users to use an existing Yammer group** – Choose this option to allow business users to use an existing Yammer group when submitting a request for this service. The feed of the existing Yammer group will be added to the site homepage.

     If you did not select the **Allow business users to create a new Yammer internal group** checkbox above, you can select the **Apply an existing Yammer group** checkbox to apply an existing Yammer group to the site collection created via this service. Then, you must enter the name or ID of an existing Yammer group in the text box and click **Validation Test** to validate the group name or group ID.

16. When you have finished configuring settings for this service, choose one of the following options:

- Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
- Click **Save** to save all of the configurations and return to the **Service Management** interface.
- Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
- Click **Cancel** to return to the **Service Managemen**t interface without saving any configurations.

Configuring Create Library/List Services

Configure Create Library/List services to define the Create Library/List service request templates for business users. You can predefine the settings for libraries or lists created by this service as well as configure available options for business users to choose from when requesting this service. Libraries or lists created by Governance Automation Online are included in the data protection plan and content retention rules of the site collection they live in.

On the interface for creating or editing a Create Library/List service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Choose the site collections you wish to be made available in this service. Business users will be able to choose which site collection to create the new library or list under.

   Choose one of the following methods to configure the scope:

   - **Manually input URL** – Select this option and click **Add Your Own URL** to enter the site collection URL in the **URL** text box. To add more site collections click **Add Your Own URL** after entering a URL.
   - **Select scope from tree** – Select this option and then select the site collections from the data tree.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
   - **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.

- **Hide from Business User** – The site URL will be hidden from the requester.

2. **Navigation** – Specify whether to display this library or list in the Quick Launch of its parent site.

   Choose whether to assign the navigation option to the library or list created by this service, or allow the business user to choose this option when submitting a service request for this service in the **Navigation** configuration area. Choose from the following:

   - **Assign by IT Admin** – The option selected here will be associated with all libraries or lists created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to choose the option in the **Navigation** configuration area.

3. **Type** – Select the type of the object that you allow to be create, **Library** or **List**.

   Choose whether to assign the type to the library or list created by this service, or allow the business user to choose the type when submitting a service request for this service in the **Type** configuration area. Choose from the following:

   - **Assign by IT Admin** – The type selected here will be associated with all service requests created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to choose the type in the **Type** configuration area.

4. Click the arrow on the right-hand side to proceed to the next step.

5. **Library/List Template** – Enter the address in which the templates are stored in the **Templates store** text box to load the templates. Click **Retrieve** to retrieve the templates. Then, select the template for the library or list that you are about to create by selecting the corresponding checkboxes.

   Select a template from the **Default template** drop-down list to set it as the default template. Choose whether to assign the selected templates to the library or list created by this service, or allow the business user to select templates when submitting a service request for this service in the **Library/List Template** configuration area. Choose from the following:

   - **Assign by IT Admin** – The templates selected here will be associated with all libraries or lists created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to select templates in the **Library/List Template** configuration area.

6. **Document Version History** (This section appears when you select **Library** as the Type.) – Specify whether a version is created each time you edit a file in this library.

   - **Require content approval for submitted files?** – Specify whether new files or changes to existing files should remain in a draft state until they have been approved.

- **Create a version each time you edit a file in this library?**
    - **No versioning** – Do not create a version when a file in this library is edited.
    - **Create major versions** – Create a major version each time a file in this library is edited.
    - **Create major and minor (draft) versions** – Create major and minor versions each time a file in this library is edited.
- **Optionally limit the number of versions to retain** – Allows you to limit the number of versions that you wish to retain. To limit the number of major versions, select the checkbox before **Keep the following number of major versions** and enter a number in the provided text box. You can also keep drafts for major versions by selecting the checkbox before **Keep drafts for the following number of major versions** and enter a number in the provided text box.

Choose whether to assign the configured settings to the library created by this service, or allow the business user to configure these settings when submitting a service request for this service in the **Document Version History** configuration area. Choose from the following:

- **Assign by IT Admin** – The settings configured here will be associated with all libraries created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business user to configure the settings in the **Document Version History** configuration area.

7. **Item Version History** (This section appears when you select **List** as the **Type**.) – Specify whether a version is created each time you edit an item in this list.
    - **Require content approval for submitted items?** – Specify whether new items or changes to existing items should remain in a draft state until they have been approved.
    - Choose whether to **Create a version each time you edit an item in this list**.
    - **Optionally limit the number of versions to retain** – Allows you to limit the number of versions that you wish to retain. To limit the number of versions, select the **Keep the following number of versions** checkbox and enter a number in the provided text box. You can also keep drafts for approved versions by selecting the **Keep drafts for the following number of approved versions** checkbox and entering a number in the provided text box.

Choose whether to assign the configured settings to the list created by this service, or allow the business user to configure these settings when submitting a service request for this service in the **Item Version History** configuration area. Choose from the following:

- **Assign by IT Admin** – The settings configured here will be associated with all lists created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

- **Assign by Business User** – Allows business user to configure the settings in the **Item Version History** configuration area.

8. Click the arrow on the right-hand side to proceed to the next step.
9. **Library or List Address** – You can choose the following options to validate or construct the library or list URL:
    - **Construct URL** – Select the checkbox to build the library or list URL using specific rules. Click **Add** and select a rule from the drop-down list. The following rules are available:
        - **Library or List Name**
        - **Department**
        - Custom metadata with the types of Single line of text, Choice, Person or Group, and Managed Metadata.

          ***Note**: If the metadata with the type of Choice - Checkboxes, Person or Group, or Managed Metadata has multiple values, the values will be separated with semicolons in the constructed URL.

      If you add multiple rules, you can enter one or more connection characters for connecting the values of those rules. If you choose to not define a connection character, the rule values will be connected by spaces.

      Choose whether to business users to modify the library/list URL when submitting requests via this service. Choose from the following:

        - **Assign by IT Admin** – The URL rules configured here will be used to generate the URL of the library/list created via this service. The generated library/list URL will be displayed to business users as read-only in the request form.
        - **Assign by Business User** – The URL rules configured here will be used to generate the URL of the library/list created via this service. In the request form, the generated library/list URL will be displayed to business users as the default URL, and business users can modify the URL if desired.
    - **URL validation** – Select the checkbox to enable library or list URL validation. Then, select a text validation rule form the drop-down list. The library or list URL defined by the requester will be validated according to the regular expression set in the text validation rule.
10. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.

- Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
- Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Create User Services

Configure Create User services are used to define the Create User service request template for business users. You can customize the settings for the Office 365 user created by this service as well as configure available options for business users to choose from when requesting this service.

On the interface for creating or editing a Create User service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Domain** – Create an app profile for Microsoft Azure Active Directory in AvePoint Online Services first. An Azure AD app profile represents your Office 365 tenant. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide. Then, select an app profile and one or more domains from the tree. The domain that will be applied to a request for this service determines where the new Office 365 user will reside, and the domain name will be used as the suffix of the user's Office 365 login ID.

   If you selected multiple domains, select a default domain from the drop-down list.

   Choose whether or not to assign a domain for Office 365 users created via this service, or allow business user to select a domain when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The domain selected from the **Default domain** drop-down list will be used as the domain for new Office 365 users. **Show as Read-Only to Business User** is chosen to allow the business users to see the domain in the service request.
   - **Assign by Business User** – Allows business users to select a domain when submitting requests for this service. The default domain selected in this service will become the default option, and business users can change it to another domain.
2. **Locations and Licenses** – Select the location and optionally select the license for the new Office 365 user. Then, configure the following settings:

   - If more than one location is selected, select a default location from the **Default location** drop-down list.

     Choose whether to assign the location to Office 365 users created via this service, or allow business users to select the location when submitting requests for this service. Choose from the following:

- **Assign by IT Admin** – The default location selected from the drop-down list will be used for Office 365 users created via this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business users to select a location when submitting requests for this service. The default location selected in this service will become the default option, and business users can change it to another location.

- Select one or more licenses that will be assigned to Office 365 users created via this service.

  Choose whether to assign licenses to Office 365 users or allow business users to select licenses when submitting service requests for this service. Choose from the following:

  - **Assign by IT Admin** – The licenses selected here will be assigned to Office 365 users created via this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
  - **Assign by Business User** – Allows business users to select licenses when submitting requests for this service. You can also select the **Require Business User Input** checkbox to require business users to select licenses in the service request.

3. **Manager of Office 365 User** – Enter a username in the text box to be the manager of new Office 365 users. Then, press **Enter** to check whether or not the name is valid. You can also enter the **$Requester** role or the **$Manager of Requester** role in the text box to be the manager of new Office 365 users.

   Choose to assign the manager to new Office 365 users created via this service, or allow business users to assign the manager when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – The user or role assigned in this service will be the manager of new Office 365 users. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business users to assign the user or role as the manager of new Office 365 users when submitting requests for this service. You can also select the **Require Business User Input** checkbox to require business users to assign the manager in the service request.

4. **Group Assignment** – Enter one or more names of Office 365 groups that new Office 365 users will belong to in the text box. Then, press **Enter** to check whether or not the names are valid.

   Choose to assign the group for new Office 365 users created via this service, or allow business users to assign the group when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – New Office 365 users created via this service will become members of the group you defined in this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

- **Assign by Business User** – Allows business users to assign the group that new Office 365 users will belong to when submitting requests for this service. You can also select the **Require Business User Input** checkbox to require business users to assign the group in the service request.

***Note**: If you want to only allow the Office 365 user who belongs to the defined groups having permissions to create OneDrive for Business, complete the following settings:

a. In the **SharePoint admin center** interface, navigate to **user profiles** > **Manage User Permissions**.

b. Select the **Everyone except external users** group, then, deselect the **Create Personal Site (required for personal storage, newsfeed, and followed content)** checkbox to remove the permission of creating personal site from every Office 365 user.

c. Enter one or more group names in the text box that you defined for the **Group Assignment** field of the Create User service. Then, click **Add**.

d. Select the groups whose members are allowed to create OneDrive for Business. Then, select the **Create Personal Site (required for personal storage, newsfeed, and followed content)** checkbox, the **Follow People and Edit Profile** checkbox, and the **Use Tags and Notes** checkbox.

e. Click **OK** to save the changes, or click **Cancel** to return to the **SharePoint admin center** without saving any changes.

5. Click the arrow on the right-hand side to proceed to the next step.

6. **Password** – Choose whether to enable sending password of the new user's Office 365 account to specific users via a notification e-mail by selecting the **Send password** checkbox. If you enable it, you must select an e-mail template from the **E-mail template** drop-down list. Business users will provide the e-mail addresses of desired recipients in the request for this service.

7. **Office 365 User Policy** – Select one or more Office 365 user policies that you wish to apply to this service by selecting the corresponding checkboxes. If you select more than one Office 365 user policies, you must select a default Office 365 user policy from the **Default policy** drop-down list.

   Choose to apply an Office 365 user policy to new Office 365 users created via this service, or allow business users to select the policies when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – The policy selected in the **Default policy** drop-down list will be associated with Office 365 users created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business user to select from the policies you have selected in this service when submitting requests for this service. The default policy selected in this service will become the default option, and business users can change it to another policy.

Optionally, select the **Allow requesters to configure user contract term** checkbox to allow requesters to configure the user contract term of an Office 365 user when submitting requests for this service.

8. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Managemen**t interface without saving any configurations.

Configuring Create Group Services

Configure Create Group services to define the Create Group service request template for business users. You can customize the settings for Office 365 groups created by this service as well as configure available options for business users to choose from when requesting this service.

On the interface for creating or editing a Create Group service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **App Profile** – Create an app profile for a Microsoft Azure AD in AvePoint Online Services first. An Azure AD app profile represents your Office 365 tenant. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide. Then, select the app profile. This app profile provides the scope where new Office 365 groups will reside.

    ***Note**: Governance Automation Online uses Exchange Online Web Service to create Office 365 groups. To ensure Office 365 groups can be created successfully, make sure the user whose credentials are used to create the selected app profile has an Exchange Online mailbox.

2. **Privacy** – Configure the privacy settings for new Office 365 groups. Choose one of the following privacy settings, or allow business users to configure this when submitting requests via this service:
    - **Public – Anyone can see group content** – Allows any user to see the group content.
    - **Private – Only members can see group content** – Only allows group members to see the group content.

    Choose to apply the privacy settings to the request form or allow business users to configure this when submitting requests via this service. Choose from the following:

- **Assign by IT Admin** – The privacy settings configured here will be applied to new Office 365 groups. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business users to configure the privacy settings when submitting requests for this service.

3. **Subscribe Members** – Configure the settings for subscribing members to decide whether to allow group members to receive copies of group conversations and events, or allow business users to configure this when submitting requests for this service. Choose from the following options:

   - **Send copies of group conversations and events to group members' inboxes** – Choose this option to allow group members to receive copies of group conversations and events.
   - **Don't send copies of group conversations and events to group members' inboxes** – Choose this option to not allow group members to receive copies of group conversations and events.

   Choose to apply the settings of subscribing members to the request form or allow business users to configure this when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – The settings of subscribing members configured here will be applied to new Office 365 groups. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business users to configure the settings of subscribing members when submitting requests for this service.

4. **Outside Senders** – Configure the outside senders settings to decide whether to allow users outside the organization to send e-mails to new Office 365 groups, or allow business users to configure this when submitting requests for this service. Choose from the following options:

   - **Allow outside senders** – Choose this option to allow users outside the organization to send e-mails to new Office 365 groups.
   - **Don't allow outside senders** – Choose this option to not allow users outside the organization to send e-mails to new Office 365 groups.

   Choose to apply the outside senders settings to the request form or allow business users to configure this when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – The outside senders settings configured here will be applied to new Office 365 groups. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business users to configure the outside senders settings when submitting requests for this service.

5. **Microsoft Teams** – Choose whether or not to enable Microsoft Teams functionality for the Office 365 group created via this service, or allow business users to configure this in the service request form. Choose from the following:

- **Assign by IT Admin** – New Office 365 groups created via this service will have the Microsoft Teams functionality enabled. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business users to choose to enable Microsoft Teams for new Office 365 groups when submitting requests for this service.

6. **Language** – Select one or more languages for the new Office 365 groups from the table. If more than one language is selected, you must select a default language from the **Default language** drop-down list.

   Choose whether to assign a language to Office 365 groups created via this service, or allow business users to select languages when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – The language selected from the **Default language** drop-down list will be used as the language for new Office 365 groups. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business users to select languages when submitting requests for this service. The default language selected in this service will become the default option, and business users can change it to another language.

7. Click the arrow on the right-hand side to proceed to the next step.
8. **Group Classification** – Select one or more group classifications that you wish to apply to new Office 365 groups created via this service. If you select more than one group classifications, you must select a default group classification from the **Default group classification** drop-down list.

   Choose to apply the group classification to new Office 365 groups created via this service, or allow business users to select the classifications when submitting requests for this service. Choose from the following:

   - **Assign by IT Admin** – The group classification selected from the **Default group classification** drop-down list will be associated with new Office 365 groups created via this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows business users to select from the group classifications you have selected in this service when submitting requests for this service. The default group classification selected in this service will become the default option, and business users can change it to another group classification.

9. **Primary Group Contact** – The primary group contact will be the user designated to manage the lifecycle of new Office 365 groups created via this service. Assign a user to be the primary group contact by entering their username into the text box. Press **Enter** to check whether or not the name is valid.

   Choose to either assign the primary group contact to Office 365 groups created via this service, or allow business users to assign the primary group contact when submitting requests for this service. Choose from the following:

- **Assign by IT Admin** – The primary group contact assigned here will be associated with all of the new Office 365 groups created via this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business users to assign the primary group contact when submitting requests for this service.

10. **Secondary Group Contact** – The secondary group contact will be the user designated for managing the lifecycle of new Office 365 groups created via this service if the primary group contact is unable to respond to a notification. Assign a user to be the secondary group contact by entering the username into the text box. Press **Enter** to check whether or not the name is valid.

    Choose either to assign the secondary group contact to Office 365 groups created via this service, or allow business users to assign the secondary group contact when submitting requests for this service. Choose from the following:

    - **Assign by IT Admin** – The secondary group contact assigned here will be associated with all of the new Office 365 groups created via this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows business users to assign the secondary group contact when submitting requests for this service.

11. **Group Owner** – Enter one or more usernames in the text box that will be assigned as the owners of new Office 365 groups. Then, press **Enter** to check whether or not the names are valid. You can also enter the following roles in the text box to be the owners of new Office 365 groups:

    - **$Requester**
    - **$Manager of Requester**
    - **$Primary Group Contact**
    - **$Secondary Group Contact**

    Choose to assign the group owner to new Office 365 groups created via this service, or allow business users to assign the group owner when submitting requests for this service. Choose from the following:

    - **Assign by IT Admin** – The user or role assigned in this service will be the owner of new Office 365 groups. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows business users to assign the owner of new Office 365 groups when submitting requests for this service. You can also select the **Require Business User Input** checkbox to require business users to assign the owner in the service request.

12. **Group Members** – Choose one of the following methods to assign group members:

- **Select group members manually** – Enter one or more usernames in the text box to be the members of new Office 365 groups. Then, press **Enter** to check whether or not the names are valid. You can also enter the following roles in the text box to be the members of new Office 365 groups:
    - **$Requester**
    - **$Manager of Requester**
    - **$Primary Group Contact**
    - **$Secondary Group Contact**

  Choose to assign the group members to new Office 365 groups created via this service, or allow business users to assign the group members when submitting requests for this service. Choose from the following:

    - **Assign by IT Admin** – The users or roles assigned in this service will be members of new Office 365 groups. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
    - **Assign by Business User** – Allows business users to assign the members of new Office 365 groups when submitting requests for this service. You can also select the **Require Business User Input** checkbox to require business users to assign members in the service request.
- **Business users define rules to get group members dynamically** – If you select this option, business users will define dynamic group membership rules in the service request. Office 365 users who meet the rules will automatically become members of new Office 365 groups.

You can also choose whether to **Enable hidden group membership to hide the members of the Office 365 group from users who are not members of the group**. Choose to apply the option to new Office 365 groups created via this service, or allow business users to select the option when submitting requests for this service. Choose from the following:

- **Assign by IT Admin** – The enabled or disabled hidden group membership will be applied to new Office 365 groups created via this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allow business users to choose whether to enable hidden group membership.

13. **Office 365 Group Policy** – Select one more Office 365 group policies that you wish to apply to this service by selecting the corresponding checkboxes. If you select more than one Office 365 group policies, you must select a default Office 365 group policy from the **Default policy** drop-down list.

    Choose to apply an Office 365 group policy to new Office 365 groups created via this service, or allow business users to select the policies when submitting requests for this service. Choose from the following:

- **Assign by IT Admin** – The policy selected in the **Default policy** drop-down list will be associated with Office 365 groups created by this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business user to select from the policies you have selected in this service when submitting requests for this service. The default policy selected in this service will become the default option, and business users can change it to another policy.
- Optionally, select the **Allow requesters to configure the group lease period** checkbox to allow requesters to configure the group lease period of a new Office 365 group when submitting requests for this service.

14. **Group Name/ID** – If groups names/group IDs of your tenant's Office 365 groups require rules, select the **Construct Office 365 group name** checkbox and/or the **Construct Office 365 group ID** checkbox. Otherwise, leave the checkbox as deselected and business users can enter desired content as groups names and group IDs.

    If you select the checkboxes, refer to the following steps to construct group name and/or group ID:

    a. Click **Add** for the prefix and/or suffix of the group name/group ID.

    b. Select **Text**, **Metadata**, or **Attribute** as a rule from the drop-down list, and then define the value for the selected rule.

    c. You can repeat the steps above to add more rules that will be used to build the group name and/or group ID.

    Choose to define group names/group IDs for Office 365 groups created via this service, or allow business users to define group names/group IDs based on the prefixes/suffixes in your rules. Choose from the following:

    - **Assign by IT Admin** – The prefixes/suffixes you set here will be used to build group names/group IDs for Office 365 groups created via this service. Group names/group IDs will be displayed to business users as read-only.
    - **Assign by Business User** – The prefixes/suffixes you set here will be displayed to business users as read-only. Apart from the prefixes/suffixes, business users can enter additional content to build groups names/group IDs. You can select the **Require Business User Input** checkbox to require business users to enter additional content for groups names/group IDs.

15. **Links in Request/Task Details Page** – Choose whether to display links of **Planner**, **Site**, **Files**, **Conversations**, and/or **Notebook** that will be created together with the Office 365 group.

16. When you have finished configuring settings for this service, choose one of the following options:

    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.

- Click **Save** to save all of the configurations and return to the **Service Management** interface.
- Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
- Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Site Collection Lifecycle Management Services

Site Collection Lifecycle Management services provide business users with control over the lifecycle of their site collections created/managed by Governance Automation Online. You can configure the settings to notify site collection owners of lease expiration and lack of use of their site collections.

On the interface for creating or editing a Site Collection Lifecycle Management service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Lifecycle Management Actions** – Select the type of lifecycle management service to create:
    - **Extend Site Collection lease** – Allows business users to request an extension to the lease of their site collections. Note that an extension to a site collection's lease will grant the site collection the amount of time indicated in the lease from the site collection's old lease expiration date.
    - **Delete Site Collection** – Allows business users to request their site collections to be deleted.
    - **Archive Site Collection** – Allows business users to request their site collections to be archived.
    - **Change Site Collection Policy** – Allows business users to request a different site collection policy be associated with the site collection they own.
    - **Unlock Site Collection** – Allows business users to request locked site collections to be unlocked.
    - **Lock Site Collection** – Allows business users to request their site collections to be locked.
    - **Change Site Collection Quota** – Allows business users to request changes of storage quota for site collections.
2. **Scope** – Expand the tree to select your desired nodes by selecting the corresponding checkboxes.

    You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the

Governance Automation Online App page, the URL of the site collection where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site collection URL will be automatically used as the request scope. Choose one of the following options:

- **Allow Business User to Edit the URL** – The site collection URL will be automatically filled into the text box, and the requester can edit it.
- **Show as Read-Only to Business User** – The site collection URL will be displayed as read-only, and the requester cannot edit it.
- **Hide from Business User** – The site collection URL will be hidden from the requester.

3. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Site Lifecycle Management Services

Site Lifecycle Management services provide business users with control over the lifecycle of their sites created/managed by Governance Automation Online.

On the interface for creating or editing a Site Lifecycle Management service, configure the following settings:

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Configure the scope for this service. Choose one of the following methods:
    - **Manually input URL** – Click **Add Your Own URL** to add the URL, then enter the URL in the text box. Repeat the step to add multiple URLs.
    - **Select scope from tree** – Expand the tree and select your desired nodes by selecting the corresponding checkboxes.

    You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card

or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

- **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
- **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
- **Hide from Business User** – The site URL will be hidden from the requester.

2. **Lifecycle Management Actions** – Allows business users to request to delete or archive their site by choosing the corresponding option. If you choose the **Archive Site** option, you must select an Archiver profile that was created in DocAve Online from the drop-down list.
3. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring User Lifecycle Management Services

User Lifecycle Management services provide business users with control over the lifecycle of their Office 365 users managed by Governance Automation Online.

On the interface for creating or editing an Office 365 Group Lifecycle Management service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **App Profile** – Create an app profile for Microsoft Azure AD in AvePoint Online Services first. An Azure AD app profile represents your Office 365 tenant. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide. Then, select the app profile. This app profile provides the scope for the Office 365 users whose lifecycle can be managed.
2. **Lifecycle Management Action** – Select the lifecycle management action that you allow business users to request for.
    - **Offboard Office 365 User** – Allows business users to request to offboard Office 365 users via one of the following methods:

- **Enable deletion of Office 365 user** – Select this checkbox to allow business users to delete Office 365 users. You can also choose to **Change the administrator of the deleted Office 365 user's OneDrive for Business**. With this option enabled, business users need must assign a user as the administrator in the request form.
- **Enable Office 365 user blocking** – Select this checkbox to allow business users to request to block Office 365 users. You can also choose to **Forward the blocked Office 365 user's e-mail to another user**. With this option enabled, business users must assign a user to receive the e-mails.
- **Enable reset of Office 365 user's password** – Select this checkbox to allow business users to reset Office 365 users' passwords. You can also choose to **Send the Office 365 user's password to another user**. Then, you must select an e-mail template from the drop-down list. With this option enabled, business users must provide the recipients in the e-mail address.

If you select multiple options for offboarding user, you must select a default action for business users from the **Default action** drop-down list.

- **Extend Office 365 User Contract** – Allows business users to request to extend the contract term of Office 365 users. Note that an extension to an Office 365 user's contract term will grant the user the amount of time indicated in the contract from the user's old contract expiration date.
- **Change Office 365 User Policy** – Allows business users to request a different user policy be associated with Office 365 users.
- **Unblock Office 365 User** – Allows business users to request to unblock Office 365 users.

3. When you have finished configuring settings for this service, choose one of the following options:
   - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
   - Click **Save** to save all of the configurations and return to the **Service Management** interface.
   - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
   - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Group Lifecycle Management Services

Group Lifecycle Management services provide business users with control over the lifecycle of their Office 365 groups managed by Governance Automation Online.

On the interface for creating or editing an Office 365 Group Lifecycle Management service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **App Profile** – Create an app profile for Microsoft Azure AD in AvePoint Online Services first. An Azure AD app profile represents your Office 365 tenant. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide. Then, select the app profile. This app profile provides the scope for the Office 365 groups whose lifecycle can be managed.
2. **Lifecycle Management Action** – Select the lifecycle management action that you allow business users to request for.
    - **Delete Office 365 Group** – Allows business users to request to delete Office 365 groups.
    - **Extend Office 365 Group Lease** – Allows business users to request to extend the lease of Office 365 groups. Note that an extension to an Office 365 group's lease will grant the group the amount of time indicated in the lease from the group's old lease expiration date.
    - **Change Office 365 Group Policy** – Allows business users to request a different group policy be associated with the Office 365 group.
    - **Change Office 365 Group Team Site Quota** – Allows business users to request to change the quota of the Office 365 group team site.
3. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Site Collection Contact or Administrator Services

Configure Change Site Collection Contact or Administrator services to define the Change Site Collection Contact or Administrator service request for business users. You can change the site collection contact or site collection administrator when the site collection expires to transfer the responsibilities to another user.

On the interface for creating or editing a Change Site Collection Contact or Administrator service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Expand the tree to select your desired nodes by selecting the corresponding checkboxes.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site collection where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site collection URL will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The site collection URL will be automatically filled into the text box, and the requester can edit it.
   - **Show as Read-Only to Business User** – The site collection URL will be displayed as read-only, and the requester cannot edit it.
   - **Hide from Business User** – The site collection URL will be hidden from the requester.

2. **Change Site Collection Contact/Administrator Settings** – Choose to allow business users to change the primary and secondary site collection contacts, or site collection administrators. You can also choose to notify the new contacts or the new administrators by selecting the **Notify the new contacts** or the **Notify the new administrators** checkbox. If you enable the notification, select an e-mail template from the corresponding drop-down list. By default, the **Built-in Object Ownership Notification E-mail Template** is selected.

3. **Change Method** – Choose **By URL** or **By User** as a change method for this service, or allow business user to decide when submitting requests for this service.

   - **Assign by Business User** – Allows business user to choose the change method when submitting a request for this service.
   - **Assign by IT Admin** – The selected change method will be applied to requests for this service. The selected change method will be shown as read-only to business user.

4. When you have finished configuring settings for this service, choose one of the following options:

   - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
   - Click **Save** to save all of the configurations and return to the **Service Management** interface.
   - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
   - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Site Collection Settings Services

Configure Change Site Collection Settings services to define the Change Site Collection Settings service request template for business users. You can change the title, description, and metadata of site collections.

On the interface for creating or editing a Change Site Collection Settings service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Expand the tree to select the scope that contains the site collections whose settings are allowed to change.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site collection where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site collection URL will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The site collection URL will be automatically filled into the text box, and the requester can edit it.
   - **Show as Read-Only to Business User** – The site collection URL will be displayed as read-only, and the requester cannot edit it.
   - **Hide from Business User** – The site collection URL will be hidden from the requester.

2. **Changed Site Collection Settings** – Choose whether to allow business users to change the **Title**, **Description**, **Metadata** of site collections, and/or **Apply DocAve Online Deployment Manager Plan** by selecting the corresponding checkboxes. Note the following:

   - If you select the **Metadata** checkbox, click **Add Metadata** to go the **Add Metadata** window. In the **Add Metadata** window, select desired metadata and click **Add to List**. The metadata displayed here is configured in **Settings** > **Request Management** > **Metadata**. You can also create or edit metadata first, and then add the metadata to the list. The metadata you added can be edited by business users in the request form.

     You can also select the **Enable adding or deleting metadata** checkbox to allow business users to add or delete metadata when submitting request for this service.

     ***Note**: If you do not select the **Enable adding or deleting metadata** checkbox, you are only able to add metadata whose values are assigned by business users to the grid. Otherwise, business users cannot modify the metadata values in the service request form.

- If you selected the **Apply DocAve Online Deployment Manager Plan** checkbox, select one or more Deployment Manager plans from the table. If you select multiple plans, you must select a default plan from the drop-down list.

  Choose whether or not to assign a plan for the site collection whose settings will be changed via this service, or allows business users to select a plan when submitting a request for this service. Choose from the following:

  - **Assign by IT Admin** – The plan selected from the **Default Selection** drop-down list will be applied to site collections. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
  - **Assign by Business User** – Allows business users to select a plan when submitting requests for this service. The default plan selected in this service will become the default option, and business users can change it to another plan. You can also select the **Require Business User Input** checkbox to require business users to select a plan in the service request.

3. When you have finished configuring settings for this service, choose one of the following options:
   - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
   - Click **Save** to save all of the configurations and return to the **Service Management** interface.
   - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
   - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Site Contact Services

You can change the Site Contact when the corresponding site collection expires to transfer the responsibilities to another user.

On the interface for creating or editing a Change Site Contact service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Specify the scope by manually inputting URLs or selecting from the tree.
   - **Manually input URL** – Click **Add Your Own URL** and then enter the URL in the text box. Repeat to add more URLs.
   - **Select from tree** – Expand the tree to select the desired nodes by selecting the corresponding checkboxes.

You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

- **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
- **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
- **Hide from Business User** – The site URL will be hidden from the requester.

2. **Notify New Contacts** – Choose whether to notify the new site contacts by selecting the **Notify the new contact** checkbox. If you enable this option, select an e-mail template from the drop-down list. By default, the **Built-in Object Ownership Notification E-mail Template** is selected.
3. **Change Method** – Choose **By URL** or **By User** as a change method for this service, or allow business users to decide when submitting requests for this service.
    - **Assign by Business User** – Allows business users to choose the change method when submitting requests for this service.
    - **Assign by IT Admin** – The selected change method will be applied to requests for this service. The selected change method will be shown as read-only to business users.
4. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Site Settings Services

Configure Change Site Settings services to define the Change Site Settings service request template for business users. You can change the site settings when you want to update the site information.

On the interface for creating or editing a Change Site Settings service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Specify the scope by manually inputting URLs or selecting from the tree.
    - **Manually input URL** – Click **Add Your Own URL** and then enter the URL in the text box. Repeat to add more URLs.
    - **Select scope from tree** – Expand the tree to select the desired nodes by selecting the corresponding checkboxes.

    You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

    - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
    - **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
    - **Hide from Business User** – The site URL will be hidden from the requester.
2. Click the arrow on the right-hand side to proceed to the next step.
3. **Change Site Settings** – Choose to allow business users to change the **Title**, **Description**, **Metadata** of the site, and/or to **Apply DocAve Online Deployment Manager Plan** by selecting the corresponding checkboxes. Note the following:
    - If you selected the **Metadata** checkbox, click **Add Metadata** to go the **Add Metadata** window. In the **Add Metadata** window, select desired metadata and click **Add to List**. The metadata displayed here is configured in **Settings** > **Request Management** > **Metadata**. You can also create or edit metadata first, and then add the metadata to the list. The metadata you added can be edited by business users in the request form.

      You can also select the **Enable adding or deleting metadata** checkbox to allow business users to add or delete metadata when submitting request for this service.

    - If you selected the **Apply DocAve Online Deployment Manager Plan** checkbox, select one or more Deployment Manager plans from the table. If you select multiple plans, you must select a default plan from the drop-down list.

      Choose whether to assign a plan for the site whose settings will be changed via this service, or allows business users to select a plan when submitting a request for this service. Choose from the following:

        - **Assign by IT Admin** – The plan selected from the **Default Selection** drop-down list will be applied to the site defined in the request page. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
        - **Assign by Business User** – Allows business users to select a plan when submitting requests for this service. The default plan selected in this service will

become the default option, and business users can change it to another plan. You can also select the **Require Business User Input** checkbox to require business users to select a plan in the service request.

4. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Library/List Settings Services

Configure Change Library/List Settings services to define the Change Library/List Settings service request templates for business users. You can choose the library/list settings that are available for business users to choose from when requesting this service. Library/list settings include name, description, navigation, and versioning settings.

On the interface for creating or editing a Change Library/List Settings service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Specify the scope by manually inputting URLs or selecting from the tree.
    - **Manually input URL** – Click **Add Your Own URL** and then enter the URL in the text box. Repeat to add more URLs.
    - **Select scope from tree** – Expand the tree to select the desired nodes by selecting the corresponding checkboxes.

    You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

    - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.

- **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
- **Hide from Business User** – The site URL will be hidden from the requester.

2. **Change Library/List Settings** – Select the library/list settings that you allow business users to change by selecting the corresponding checkboxes, including **Name**, **Description**, **Navigation**, and **Versioning settings**.
3. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change User Properties Services

Configure Change User Properties services to define the Change User Properties service request template for business users. You can change the user properties when you want to update the user information.

On the interface for creating or editing a Change User Properties service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **App Profile** – Create an app profile for Microsoft Azure AD in AvePoint Online Services first. An Azure AD app profile represents your Office 365 tenant. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide. Then, select the app profile. This app profile provides the scope for the Office 365 users whose properties can be changed.
2. **User Scope** – Define the scope of Office 365 users whose properties can be changed. Choose one of the following options:
    - **Allow any user** – Choose this option to allow business users to change any Office 365 user's properties in the request form.
    - **Allow peers and direct or indirect reports** – Choose this option to:
        - Allow a business user to change the properties of the Office 365 user who shares the same manager as the business user.

    - Allow a business user to change the properties of the Office 365 user who directly reports to the business.
    - Allow a business user to change the properties of the Office 365 user who indirectly reports to the business user.
  - **Allow direct or indirect reports** – Choose this option to:
    - Allow a business user to change the properties of the Office 365 user who directly reports to the business user.
    - Allow a business user to change the properties of the Office 365 user who indirectly reports to the business user.

3. **Change Basic Information** – Choose whether or not to allow business users to change the **First name**, **Last name**, **Display name**, **Username**, and/or **Domain** of Office 365 users.
4. **Change Contact Information** – Choose whether or not to allow business users to change contact information of Office 365 users by selecting the **Contact information** checkbox.
5. **Change License and Location** – Choose whether or not to allow business users to change the **Location** and/or **License** of Office 365 users.
6. **Change Manager** – Choose whether or not to allow business users to change the **Manager of Office 365 user**.
7. **Change Group Assignment Settings** – Choose whether or not to allow business users to add Office 365 users to Office 365 groups and/or remove Office 365 users from Office 365 groups:
   - **Add users to groups** – Allows business users to add users to groups in the request form. Choose one of the following options to set limitations on groups:
     - **Allow adding an Office 365 user into any group**
     - **Allow adding an Office 365 user into groups owned by business users**
   - **Remove users from groups** – Allows business users to remove users from groups in the request form.
8. **Change OneDrive for Business Metadata Settings** – Choose whether to allow business users to change the metadata of the Office 365 user's OneDrive for Business. If you select the **Metadata** checkbox, you can also select the **Enable adding or deleting metadata** checkbox to allow business users to add or delete metadata in the service request form. Then, click **Add Metadata** to go the **Add Metadata** window. In the **Add Metadata** window, select desired metadata and click **Add to List**. The metadata displayed here is configured in **Settings** > **Request Management** > **Metadata**. You can also create or edit metadata first, and then add the metadata to the list.

   ***Note**: If you do not select the **Enable adding or deleting metadata** checkbox, you are only allowed to add metadata whose values are assigned by business users to the grid. Otherwise, business users cannot modify the metadata values in the service request form.

9. When you have finished configuring settings for this service, choose one of the following options:

- Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
- Click **Save** to save all of the configurations and return to the **Service Management** interface.
- Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
- Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Group Settings Services

Configure Change Group Settings services to define the Change Group Settings service request template for business users. You can change the group settings when you want to update the group information.

On the interface for creating or editing a Change Group Settings service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **App Profile** – Create an app profile for Microsoft Azure AD in AvePoint Online Services first. An Azure AD app profile represents your Office 365 tenant. For more information about how to create an Azure AD app profile, refer to the **Creating an App Profile for Microsoft Azure AD** section in the AvePoint Online Services User Guide. Then, select the app profile. This app profile provides the scope for the Office 365 groups whose settings can be changed.
2. **Group Scope** – Define the scope of Office 365 groups whose settings can be changed. Choose one of the following options:
    - **Allow changes to any group** – Allows business users to change settings of any Office 365 group.
    - **Allow changes to groups owned by requester** – Only allows business users to change settings of the Office 365 groups they own.
3. **Change Office 365 Group Name and Description** – Choose whether or not to allow business users to change the **Name** and/or **Description** of the Office 365 group.
4. **Change Member Subscription Settings** – Choose whether or not to allow business users to change the **Send copies of group conversations and events to group members' inboxes** setting.
5. **Change Outside Senders Settings** – Choose whether or not to allow business users to change settings for outside senders by selecting the **Change outside senders** checkbox.
6. **Change Group Contact** – Choose whether or not to allow business users to change the **Primary group contact** and/or **Secondary group contact**.
7. **Change Group Owner Settings** – Choose whether to allow business users to add or remove Office 365 group owners.

- **Add group owners** – Select this option to allow business users to add new owners to Office 365 groups. Then, you must choose the scope for the new group owners. Choose one of the following options:
    - **Allow any user** – Allows business user to add any user as the new group owner.
    - **Allow peers and direct or indirect reports** – Allows business user to add Office 365 users as new group owners when:

      The requester shares the same manager as the Office 365 user.

      The requester is the manager of the Office 365 user.

      The requester is a higher level manager of the Office 365 user.
    - **Allow direct or indirect reports** – Allows business user to add Office 365 users as new group owners when:

      The requester is the manager of the Office 365 user.

      The requester is a higher level manager to the Office 365 user's manager.
- **Remove group owners** – Select this option to allow business user to remove group owners from Office 365 groups.

8. **Change Group Assignment Settings** – Choose whether or not to allow business users to change group assignment for classic group membership and dynamic group membership:

   For **Classic group membership**, choose whether or not to allow business users to add or remove Office 365 group members.

   - **Add users to groups** – Allows business users to add Office 365 users to Office 365 groups in the request form. Choose one of the following options to set the scope for group members:
     - **Allow any user** – Allows business users to add any Office 365 user to a group.
     - **Allow peers and direct or indirect reports** – Allow business users to add Office 365 users to groups when:

       The requester shares the same manager as the Office 365 user.

       The requester is the manager of the Office 365 user.

       The requester is a higher level manager to the Office 365 user's manager.
     - **Allow direct or indirect reports** – Allow business users to add Office 365 users to groups when:

       The requester is the manager of the Office 365 user.

       The requester is a higher level manager to the Office 365 user's manager.
   - **Remove users from groups** – Allows business users to remove Office 365 users from Office 365 groups in the request form.

For **Dynamic group membership**, choose whether or not to allow business users to **Change dynamic group membership rules**.

9. **Microsoft Teams** – Choose whether or not to allow business users to enable Microsoft Teams functionality for the requested Office 365 group.
10. **Change Group Classification Settings** – Choose whether or not to allow business users to change group classifications for the Office 365 group specified in the service request form. If you select the **Change group classification** checkbox, you must select one or more of the classifications from the table.
11. **Change Group Metadata** – Choose whether or not to allow business users to change group metadata for the Office 365 group specified in the service request form. If you select the **Metadata** checkbox, you can also select the **Enable adding or deleting metadata** checkbox to allow business users to add or delete metadata in the service request form. Then, click **Add Metadata** to go the **Add Metadata** window. In the **Add Metadata** window, select desired metadata and click **Add to List**. The metadata displayed here is configured in **Settings** > **Request Management** > **Metadata**. You can also create or edit metadata first, and then add the metadata to the list.

    ***Note**: If you deselect the **Enable adding or deleting metadata** checkbox, you are only allowed to add metadata whose values are assigned by business users to the grid. Otherwise, business users cannot modify the metadata values in the service request form.

12. When you have finished configuring settings for this service, choose one of the following options:
    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Content Move Services

Configure Content Move services to define the Content Move service request template for business users. You can configure the settings to copy or move SharePoint Online contents, so the content and topology of your SharePoint Online environment can be restructured easily and accurately.

On the interface for creating or editing a Content Move service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Select your desired nodes in the **Source Scope** and **Destination Scope** and they can be identified as a source or destination in a Content Move request.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
   - **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
   - **Hide from Business User** – The site URL will be hidden from the requester.

2. **Method** – Select **Copy** or **Move** for this service, or allow the business user to decide when submitting the request:

   - **Assign by Business User** – Allows business user to choose the method when submitting a service request for this service.
   - **Assign by IT Admin** – The selected method will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

   If you select **Move**, you may also configure the following settings:

   - **Source Documents/Items Deleted Method** – Select **Manually** to delete the source content yourself once the move job is complete in DocAve Online (select the move job in **Job Monitor**, then click **Delete** on the ribbon and select **Delete Content** from the drop-down list), or select **Automatically** to have DocAve Online delete the source content once the move job is complete.

     Choose whether to assign the method to this service, or allow the business user to choose the method when submitting a service request for this service. Choose from the following:

     - **Assign by Business User** – Allows business user to choose the method when submitting a service request for this service.
     - **Assign by IT Admin** – The selected method will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

   - **Delete Checked Out Documents From Source** – By default, **No** is selected. Select **Yes** if you want to have the checked out documents on the source node deleted when the source content is deleted.

     Choose whether to assign this option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

- **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
- **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

3. **Action** – Select **Attach** to transfer the source node as a child node underneath the destination node, or select **Merge** to add the content, securities, and configurations of the source node to the destination node.

   Choose whether to assign the action to this service, or allow the business user to choose the action when submitting a service request for this service. Choose from the following:

   - **Assign by Business User** – Allows business user to choose the action when submitting a service request for this service.
   - **Assign by IT Admin** – The selected action will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

4. Click the arrow on the right-hand side to proceed to the next step.
5. **Filter Policy** – Select a filter policy you previously created in DocAve Online from the drop-down list. Filter policies allow you to select specific objects or data within each SharePoint Online level from site collection down to the item level.

   Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

   - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
   - **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

6. **Configuration** – Choose whether to migrate configuration to the destination.

   - Select **Copy configuration** or **Move configuration** to copy or move the properties, descriptions, titles, settings, and features from the source node to the destination node.
     - If you want to keep the look and feel of the source site, including the quick launch, top link bar, tree view, site themes, and master page, select the **Keep look and feel** checkbox.

       ***Note**: This function will only take effect if the source node is a site, the destination node is a top-level site or a site collection, and **Merge** is chosen as the action.

   - Select **Do not copy configuration** or **Do not move configuration** if you do not want to migrate configuration to the destination. Then, choose from the following options:
   - Select **Copy the item-dependent columns and content types to maintain item integrity** or **Move the item-dependent columns and content types to maintain item integrity**.

Then, select a conflict resolution method for these items' columns and content types from the drop-down list:

- **Ignore the differences of the columns and content types, and copy/move the items** – Ignore the differences of the columns and content types in the destination node from those in the source node, and copy/move the items of the source node to the destination node.
- **Do not copy/move the columns and content types, or the corresponding items** – Ignore the conflicting columns, content types, and the corresponding items, and do nothing on the source and destination node.
- **Overwrite the columns and content types** – Overwrite the destination columns and content types with the source node.
- **Append the columns and content types to destination** – Keep the destination columns and content types when there is a conflict. In addition, copy the source columns and content types to the destination node with a numerical suffix added (for example, ColumnName_1, ColumnName_2, etc.).

- Select **Do not copy the item-dependent columns or content types**. Report the items if the corresponding column or content type is not found in destination or **Do not move the item-dependent columns or content types**. Report the items if the corresponding column or content type is not found in destination. The corresponding items are not copied or moved to the destination. The job report will show items if the corresponding column or content type is not found in the destination node.

***Note**: If a source node is associated with a Managed Metadata column and there is no Managed Metadata column in the destination node, Governance Automation Online do not copy or move the source Managed Metadata column to the destination.

Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

- **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
- **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

7. **Security** – Select the **Copy security** or **Move security** checkbox to copy or move the user and/or group permissions from the source node to the destination node, including SharePoint Online permission level and permission inheritance of SharePoint Online objects.

   Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

   - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
   - Assign by IT Admin – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

8. **Content** – Select the **Copy content** or **Move content** checkbox to copy or move content from the source node to the destination node, including files and items. Select the **Include list attachment** checkbox to also copy or move attached content in lists from the source node to the destination node.

   Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

   - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
   - **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

9. **Include Versions** – Select the **Include versions** checkbox to copy or move the versions of files and list items.

10. **Workflow** – Select the **Include workflow definition** checkbox to copy or move the definition of existing workflows for the selected content from the source node to the destination node.

    Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

    - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
    - **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

11. **Information Rights Management (IRM) Settings** – If the Information Rights Management Settings are enabled in SharePoint Online and the **Disable Information Rights Management (IRM) settings** checkbox is:

    - Selected, IRM Settings will be disabled temporarily on the individual list/library while it is being copied or moved and re-enabled once the operation on this list/library is complete.
    - Deselected, Content Manager does not work with the IRM Settings enabled library/list and the library/list cannot be copied or moved.

    Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

    - **Assign by Business User** – Allows business users to choose the option when submitting requests for this service.
    - **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

12. Click the arrow on the right-hand side to proceed to the next step.

13. **Preserve the Null Column Values** – Select **Yes** to preserve the null values of item columns even if the columns on the destination have default values configured, or select **No** to replace null values with default values in the destination node.

    Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

    - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
    - **Assign by IT Admin** – The selected option will be applied for this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

14. **Mappings** – Select previously configured profiles for content type mapping, user mapping, and language mapping. Mapping profiles are created in DocAve Online and are optional.

    - **Column mapping** – Allows you to map source columns to the configured columns in the destination, or change the column name to another one. The specified source columns will be mapped according to the selected column type, and the column values will be mapped according to the added value mappings.
    - **Content type mapping** – Allows you to map source content types to the specified content types in destination, or change the content type name to another one, according to the condition that you set up.
    - **User mapping** – Allows you to replace an existing source node username with an existing destination node username or a default username in the destination, or add a place holder account to keep user metadata even if the user no longer exists.
    - **Language mapping** – Allows you to choose if you want to display destination node in a different language than source node after the plan has been executed.

    Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

    - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
    - **Assign by IT Admin** – The selected option will be applied for this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

15. **Back Up Environment Before Running Plan** – Allows you to keep a copy of the source or destination node before copying/moving content.

    - **Back up the source environment** (for Move only) – Create a copy of the source node prior to performing the move.
    - **Back up the destination environment** – Create a copy of the destination node prior to performing the copy. This allows you to undo the copy.

    ***Note**: If you choose **Back up the source environment** and/or **Back up the destination environment**, you must select a storage policy from the drop-down list.

Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

- **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
- **Assign by IT Admin** – The selected option will be applied for this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

16. **Conflict Resolution** – If the item name in the source node is the same as that of an existing item in the destination node, a conflict occurs. This setting allows you to handle conflicts of the container level, the content level, and the apps. Configure the following settings:

    - **Container level conflict resolution** – Contains **Skip**, **Merge**, and **Replace**. Select one of these conflict resolutions for the container level from the drop-down list:
        - **Skip** – Keeps the destination container as is and you can choose to set content level conflict resolution by clicking the checkbox next to **Check lower objects**.
        - **Merge** – Adds the source container to the destination, but you must set content level conflict resolution.
        - **Replace** – Substitutes the container in the destination with the one in source and you cannot set content level conflict resolution.
    - **Content level conflict resolution** – Contains **Skip**, **Overwrite**, and **Overwrite by Last Modified Time**. Select one of these conflict resolutions for the content level from the drop-down list:
        - **Skip** – Keeps the destination content as is.
        - **Overwrite** – Substitutes the destination content with the source content.
        - **Overwrite by Last Modified Time** – Substitutes the destination content with the content that has the latest modification.
    - **Apps conflict resolution** – Contains **Skip** and **Overwrite**. Select one of these conflict resolutions for the Apps from the drop-down list:
        - **Skip** – If the apps in the source and destination conflict, the conflict will be skipped. The destination app and AppData will remain unchanged.
        - **Overwrite** – If the apps in the source and destination conflict, the destination app and AppData will be removed, an app in the latest version will be downloaded and installed from app store, and the backed up AppData will be restored to the destination.

    Choose whether to apply the option to this service, or allow the business user to choose the option when submitting a service request for this service. Choose from the following:

    - **Assign by Business User** – Allows business user to choose the option when submitting a service request for this service.
    - **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

17. **Preserve Modified By and Modified Time** – Choose whether to preserve the source documents' column values of **Modified By** and **Modified** when copying or moving documents to the destination by selecting **Yes** or **No**. Note that this setting only takes effect for the destination library in which **Create major and minor (draft) version** is enabled.

    Choose whether to apply the option to this service, or allow business users to choose the option when submitting requests for this service. Choose from the following:

    - **Assign by Business User** – Allows business users to choose the option when submitting requests for this service.
    - **Assign by IT Admin** – The selected option will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

18. When you have finished configuring settings for this service, choose one of the following options:

    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Grant Permissions Services

Configure Grant Permissions services to define the Grant Permissions service request template for the business users. You can specify users in a specified site or a library who you wish to grant permissions to.

On the interface for creating or editing a Grant Permissions service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** –Expand the tree to select your desired nodes by selecting the corresponding checkboxes.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.

- **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
- **Hide from Business User** – The site URL will be hidden from the requester.

2. **Select Users** – Specify the users to which you want to grant permissions. Choose from the following:

   - **Allow any user/group** – Select this option to allow the business user to grant permissions to any SharePoint Online users and security groups of the selected scope.
   - **Allow peers and direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to grant permissions the users managed by the requester and the users of the same title as the requester.
   - **Allow direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to grant permissions the users managed by the requester.

   Optionally, select the **Set requester as the default user** checkbox to add the requester as the default user when starting a Grant Permissions request.

   ***Note**: Granting permissions to users outside your company depends on the corresponding site collection's sharing settings in the site collection policy or in SharePoint Online.

3. **Permission Duration** – Choose the permission duration for the selected users/groups.

   - **Permanent permissions** – The permissions will be granted to the selected users/groups permanently.
   - **Temporary permissions** – The permissions will be granted to the selected users/groups temporarily.

   Choose whether to assign the Permission Duration option to this service, or allow the business user to choose the Permission Duration option when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The Permission Duration option configured here will be applied on the Grant Permission service request.
   - **Assign by Business User** – Allows the business user to configure the Permission Duration option.

   If **Temporary permissions** is selected, you can further configure the **Temporary permissions settings**:

   - When **Permission Duration** is assigned by IT Admin, you must define the permission duration by entering a number in the text box and selecting **Day(s)**, **Month(s)**, or **Year(s)** from the drop-down list. Then, choose from the following options:
     - **Allow business users to specify the duration** – When submitting a request for this service, business users can enter desired permission duration, regardless of the default duration. You must define the maximum permission duration that

the business user can request for. Enter a number in the text box and select **Day(s)**, **Month(s)**, or **Year(s)** from the drop-down list.

  - **Business users can only request with the default duration** – When submitting a request for this service, the default duration is mandatory and business users cannot change the permission duration.

- When **Permission Duration** is assigned by Business User, you can configure the following options:
  - **Specify the default duration** – Define a default permission duration by entering a number in the text box and selecting **Day(s)**, **Month(s)**, or **Year(s)** from the drop-down list.
  - **The permission cannot be granted longer than** – Define the maximum permission duration that the business user can request for. Select this checkbox, then enter a number in the text box and select **Day(s)**, **Month(s)**, or **Year(s)** from the drop-down list.

Optionally, choose whether to **Notify the person who was granted the permissions about permission expiration**. Select the checkbox and define the time that the person will be notified in advance. Enter a number and select **Day(s)** or **Month(s)** from the drop-down list.

4. **Grant Permissions** – Specify the permissions to the selected users/groups.

   - **Add users to a SharePoint group** – Grants the group permission to a user by adding the user into this group.
   - **Grant users permission directly** – Assigns the explicit permission to a user.

   Choose whether to assign the Grant Permissions option by this service, or allow the business user to choose the Grant Permissions option when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The Grant Permissions option configured here will be applied on the Grant Permission service request.
   - **Assign by Business User** – Allows the business user to configure the Grant Permissions option.

   Optionally, select **Exclude specified permission levels from the request page** and then select your desired permission levels by selecting the corresponding checkboxes. The selected permission levels will be excluded from the permission level list if the requester grants the user permission. If the requester adds users to a SharePoint group, the group that contains the selected permission levels will not be displayed.

   ***Note**: The displayed permission levels are retrieved from Governance Automation Online **Settings** > **SharePoint Permission Level Management**.

5. **Send E-mail** – Choose whether or not to send an e-mail to the new users for notifying his or her new permission. Select the **Send welcome e-mail to the new users** checkbox, and then enter the subject and the body of the e-mail to be a template.

   Choose whether to assign the Send E-mail option by this service, or allow the business user to choose the Send E-mail option when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The Send E-mail option configured here will be applied on the Grant Permission service request. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows the business user to configure the Send E-mail option.

6. When you have finished configuring settings for this service, choose one of the following options:

   - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
   - Click **Save** to save all of the configurations and return to the **Service Management** interface.
   - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
   - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Clone or Transfer User Permission Services

Configure Clone or Transfer User Permission services to request having one person's permissions be the same as another user. Role changes happen frequently in most organizations. This puts permission control in the hands of business users based on predefined settings set by IT administrators.

On the interface for creating or editing a Clone or Transfer User Permissions service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Expand the tree to select the desired nodes by selecting the corresponding checkboxes.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

- **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
- **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
- **Hide from Business User** – The site URL will be hidden from the requester.

2. **Restrict Source User Selection** – Specify the users from which can be selected as the source user to clone permissions. Choose from the following:
    - **Allow any user/group** – Select this option to allow the business user to select any user and group of the selected scope as the source user.
    - **Allow peers and direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to select the users managed by the requester and the users of the same title as the requester to be the source user.
    - **Allow direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to select the users managed by the requester to be the source user.
3. **Restrict Target User Selection** – Specify the users to which can be selected as the target user to clone permissions. Choose from the following:
    - **Allow any user/group** – Select this option to allow the business user to select any user and group of the selected scope as the target user.
    - **Allow peers and direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to select the users managed by the requester and the users of the same title as the requester to be the target user.
    - **Allow direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to select the users managed by the requester to be the target user.
4. Click the arrow on the right-hand side to proceed to the next step.
5. **Permission Option** – Select a method from the drop-down list to determine how you will assign the source user's/group's permission to the target user/group.
    - **Append** – Adds the permission of the source user/group to the destination user/group.
    - **Replace** – Replaces the permission of the target user/group with the source user's/group's permission.

    Choose whether to assign the Permission Option by this service, or allow the business user to choose the Permission Option when submitting a service request for this service. Choose from the following:

- **Assign by IT Admin** – The Permission Option configured here will be applied on the Clone User Permission service request. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows the business user to configure the Permission Option.

6. **Additional Option** – Choose how to deal with the permissions of the source user that resides in a SharePoint Online security group. Choose from the following:

   - **Add target user to the same group in destination** – Adds the target user into the SharePoint Online security group where the source user resides.
   - **Clone source user's permissions to the target user directly** – Copies the permissions of the group where the source user resides to the target user.

   Choose whether to assign the Additional Option directly by this service, or allow the business user to choose the Additional Option when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The Additional Option configured here will be associated with all of the site collections selected in the scope of the Clone User Permission service request. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows the business user to configure the Additional Option.

7. **Options for Transfer** – Specify the options to manage the source user/group when transferring permissions. The selected options will be the default selections when submitting a service request. Choose from the following:

   - **Remove source user's explicit permission** – Removes the source user's or group's permission after cloning the permission successfully.
   - **Remove source user from SharePoint groups** – Deletes the source user from SharePoint Online security groups that he resides after cloning the permission successfully.
   - **Delete source user from site collection** – Deletes the source user or group from the site collection after cloning the permission successfully.

   Choose whether to assign the Options for Transfer directly by this service, or allow the business user to choose the Options for Transfer when submitting a service request for this service. Choose from the following:

   - **Assign by IT Admin** – The Options for Transfer configured here will be associated with all of the site collections selected in the scope of the Clone User Permission service request. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
   - **Assign by Business User** – Allows the business user to configure the Options for Transfer.

8. When you have finished configuring settings for this service, choose one of the following options:

   - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.

- Click **Save** to save all of the configurations and return to the **Service Management** interface.
- Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
- Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Change Permissions Services

Configure Change Permissions services to define the Change Permissions service request template for the business users. You can specify the users in a certain site collection whose permission you wish to change.

On the interface for creating or editing a Change Permissions service, configure the following settings.

***Note**: For information about common service settings that exist in all types of services, refer to Configuring Common Service Settings.

1. **Scope** – Expand the tree to select your desired nodes by selecting the corresponding checkboxes.

   You can also choose to **Use SharePoint Online context to automatically populate the service request scope**. Select this checkbox to retrieve and use SharePoint Online context in the service request scope. In the request triggered from the Site Information Card app part or from the Governance Automation Online App page, the URL of the site where the Site Information Card or the Governance Automation Online App page resides will be retrieved. The site URL will be automatically used as the request scope. Choose one of the following options:

   - **Allow Business User to Edit the URL** – The site URL will be automatically filled into the text box, and the requester can edit it.
   - **Show as Read-Only to Business User** – The site URL will be displayed as read-only, and the requester cannot edit it.
   - **Hide from Business User** – The site URL will be hidden from the requester.
2. **Select Users** – Select the users for which you want to change the permissions. Choose from the following:
   - **Allow any user/ group** – Select this option to allow the business user to change permissions of any SharePoint Online users and security groups of the selected scope.
   - **Allow peers and direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user to change permissions of users managed by the requester and the users of the same title as the requester.
   - **Allow direct or indirect reports** (only supports SharePoint Online standard instance user) – Select this option to allow the business user change permissions of users managed by the requester.

3. **Change Type** – Choose to **Remove Permissions** from users/groups or **Change Permissions** of users/groups.

   Choose whether to assign the selected change type to this service, or allow the business user to choose the change type when submitting a service request for this service. Choose from the following:

   - **Assign by Business User** – Allows business user to choose the change type when submitting a service request for this service.
   - **Assign by IT Admin** – The selected change type will be applied to this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

   In the **Advanced settings**, select an e-mail template to send the notification e-mail that notifies the requester to review or change permissions in the generated permission review task.

4. When you have finished configuring settings for this service, choose one of the following options:

   - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
   - Click **Save** to save all of the configurations and return to the **Service Management** interface.
   - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
   - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Configuring Custom Services

Use the Custom Service to capture required service information using metadata and to execute your desired action via the methods that exist in a published Web Service.

On the interface for creating or editing a Custom service, configure the following settings:

1. **Service Name and Description** – Enter a **Name** for the service and an optional **Description** for future reference.
2. **Language** – Choose a language for this service. When starting a request, a requester can filter the services according to their languages**.**
3. **Service Category** – Categories are used to organize your Governance Automation Online services. Select an existing category from the drop-down list or create a new category for this service by clicking **Create New** then configuring the new category in the **Create Category** interface.
4. **Department** – Departments help organize services as well as provide essential Governance Automation Online reporting information for sorting and understanding your organization's

SharePoint Online usage. Select a department you wish this service to belong to from the drop-down list or click **Create New** to create a new one.

Choose to assign a department to this service, or allow the business user to choose the department when submitting a request for this service. Choose from the following:

- **Assign by IT Admin** – The users in the department selected in the preceding drop-down list will be the intended requesters of this service. Select either **Show as Read-Only to Business User** or **Hide from Business User**.
- **Assign by Business User** – Allows business users to choose the department when submitting a request for this service.

***Note**: If **Use department in Azure Active Directory properties or in SharePoint Online user profile** was chosen when an IT Admin configured departments in the **System** group, Governance Automation Online will retrieve the requester's departments from Azure AD properties or from SharePoint Online User Profile Service.

5. **Service Permissions** – Choose how users will get to this service and who has permission to access it. Note that Office 365 users or groups entered here must exist in the AvePoint Online Services users.
   - **Display this service in the service catalog** – This service will be displayed in the service catalog.
     - **Allow all users to use this service** – Allow this service to be requested by any user.
     - **Select users of groups to use this service** – Select the users or Office 365 groups to have permission to submit requests for this service. Enter the names of users or groups in the text box. Press **Enter** to check whether or not the names are valid.
   - **Users may access this service via a questionnaire even if not listed in the permissions above** – Allow users to request this service after they finish answering the questionnaire, even if they are not listed in the service permissions above.
6. **Service Contact** – Specify a user to be the Service Contact. This should be a business user who is the owner of the business process for this service. Enter the username in the **Service Contact** text box. Press **Enter** to check whether or not the name is valid.
7. **Administrator Contact** – Specify a user or an Azure Active Directory group to be the Administrator Contact. This user or group should be an IT administrator of Governance Automation Online and is responsible for service management. Governance Automation Online will assign a task to the Administrator Contact when an error occurs after the approval process starts. Enter a username or a group name in the **Administrator Contact** text box. Press **Enter** to check whether or not the name is valid. To also have an e-mail notification be sent to the Administrator Contact when this service encounters an error, configure the **Administrator Notification** section of the **System** group within **Settings.** For more information, refer to Configuring Administrator Notification.
8. Click the arrow on the right-hand side to proceed to the next step.

9. **Metadata** – Select the metadata to be made available to users when submitting a request for this service. Click **Add Metadata** to go to the **Add Metadata** window. In the **Add Metadata** window:

    - **Create** – Click **Create** to create new metadata in the **Create Metadata** window. For more information about how to configure metadata, refer to Configuring Metadata.
    - **Edit** – Select metadata and click **Edit**. For more information about how to configure metadata, refer to Configuring Metadata.
    - **Add to List** – Select metadata and click **Add to List**. The metadata displayed here is configured in **Settings** > **Request Management** > **Metadata**.

10. **Approval Process** – Select an approval process from the drop-down list or click **Create New**. The **Approval Process Settings** interface appears. After selecting the approval process, the approval stage, approver, and approval order are displayed. You can create a new approval process from an existing approval process by clicking **Create From This Existing Approval Process.** The **Approval Process Settings** window appears. Configure the settings, and then save and activate the approval process. For more information on configuring the approval process, refer to Creating or Editing Approval Processes. This approval process will be triggered when a service request to remove the permission of a specific user is submitted.

    Select the **Allow approvers to edit this service request** checkbox to allow the approvers to edit the service request for this service. You can also choose to **Notify the requester when the service request is edited** by selecting the checkbox and then selecting an **E-mail template**

11. **Custom Action** – Allows you to define custom actions before approval and after approval of the request via the methods that exist in a published Web Service. Select the corresponding checkboxes and complete the following steps:

    a. Enter the URL of your published Web Service in the **Web Service Address** text box.

    b. Select **Anonymous Access** or **Azure Active Directory Authentication** as the authentication type that will be used to access the Web service from the drop-down list. If you select **Azure Active Directory Authentication** as the authentication type, you must provide the following client IDs:

        - **Client ID of Azure Active Directory application**
        - **Client ID of Azure Active Directory native client application**

        ***Note**: In order to use the Azure Active Directory account to access the Web service, you must configure your App service application first. Refer to the following Microsoft technical article to configure your App service application: https://azure.microsoft.com/en-us/documentation/articles/app-service-mobile-how-to-configure-active-directory-authentication/

    c. Click **Retrieve** to retrieve the methods in the Web Service.

    d. Select your desired method from the drop-down list.

e. If there are parameters defined in the selected method, the parameters are displayed in a table. Enter the value for each parameter in the corresponding text box.

12. **Run During** – Select **Enable service request execution schedule** to define when Governance Automation executes the service request. Then, choose a previously configured execution schedule from the drop-down list or click **Create New** to create a new one.

13. When you have finished configuring settings for this service, choose one of the following options:

    - Click the arrow on the left-hand side to go to the previous steps to review and modify your configurations.
    - Click **Save** to save all of the configurations and return to the **Service Management** interface.
    - Click **Save and Activate** to save all of the configurations and activate this service, which allows users to submit requests for this service.
    - Click **Cancel** to return to the **Service Management** interface without saving any configurations.

Additional Governance Automation Online Configurations

The following sections detail additional configurations you can make to Governance Automation Online. Additional configurations include the following:

- The Governance Automation Online App.
- The optional settings in the following groups within the **Settings** interface: **System**, **SharePoint**, **Request Management**, **Monitoring Reports**, **Audit Reports**, and **Administration Reports**. These settings may affect the entire Governance Automation Online platform or be only relevant to certain features.

Installing the Governance Automation Online App

Governance Automation Online App, an app for SharePoint Online, provides SharePoint Online end-users with easier access to Governance Automation Online without having to leave their SharePoint Online interface. With the Governance Automation Online App configured, the Site Information Card app part and the Site Lifecycle Timeline app part are available for SharePoint Online sites.

Downloading the Governance Automation Online App

To install and use the Governance Automation Online App, download the app file: http://download2.avepoint.com/Governance Automation Online App File/Governance_Automation_Online_App_1.1.2.0.app.

If you are using Governance Automation Online version for U.S. Government Public Sector, download the app file: http://download2.avepoint.com/Governance Automation Online App File/Governance_Automation_Online_App_USGov_1.1.2.0.app.

Required Permissions

To install and use the Governance Automation Online App, ensure that the following permissions are in place.

Uploading the Governance Automation Online App to App Catalog

The user who uploads the Governance Automation Online App to the app catalog site collection must have Design or above permission to the app catalog site collection.

Registering the Governance Automation Online App

The user who registers the Governance Automation Online App must be the administrator of the site collection or site from which the **Register an App** page is started.

Adding the Governance Automation Online App to a SharePoint Online Site

The user who adds the Governance Automation Online App to a SharePoint Online site must be the administrator of the site.

Inserting a Governance Automation Online App Part to a SharePoint Online Site

The user who inserts a Governance Automation Online app part to a SharePoint Online site must have Contribute or above permission to the site.

Uploading the Governance Automation Online App to App Catalog

Before adding the Governance Automation Online App to any SharePoint Online site, you must upload the Governance Automation Online App to the app catalog site collection.

Complete the following steps to upload the Governance Automation Online App to the app catalog site collection:

1. In the **SharePoint admin center** interface, navigate to **apps** > **App Catalog**.
2. Click **Apps for SharePoint** on the left pane.
3. In the **Apps for SharePoint** interface, click **Upload**.
4. In the **Add a document** window, click **Browse…**.
5. In the **Choose File to Upload** window, select the downloaded app file and click **Open**.
6. In the **Add a document** window, click **OK**. The app file is successfully uploaded to the app catalog.

Registering the Governance Automation Online App

To use the Governance Automation Online App, you must register the app in SharePoint Online.

Complete the following steps to register the Governance Automation Online App:

1. Go to any site collection or site that is in the same tenant of the app catalog site collection where the Governance Automation Online App is uploaded.
2. Modify the site collection or site URL to …**/_layouts/15/appregnew.aspx**. The **Register an App** page appears.
3. Configure the following settings in the **Register an App** page:
    a. **Client Id** – Enter **efbb98fd-e154-42b8-96df-f552bc3a862d** in the text box.
    b. **Client Secret** – Enter **bFilTPqDzKpUmzJhy+ykSokPHIJdNM09WtK0DuPpnSk=** in the text box.
    c. **Title** – Enter a desired title for the Governance Automation Online App.
    d. **App Domain** – Enter **gaoapp.avepointonlineservices.com** in the text box.

If you are using the Governance Automation Online version for U.S. Government Public Sector, enter **gausgovapp.avepointonlineservices.com**.

e. **Redirect URI** – Enter **https://gaoapp.avepointonlineservices.com/home/index** in the text box.

   If you are using the Governance Automation Online version for U.S. Government Public Sector, enter **https://gausgovapp.avepointonlineservices.com/home/index**.

f. Click **Create** to register the Governance Automation Online App.

Adding the Governance Automation Online App to a SharePoint Online Site

Complete the following steps to add the Governance Automation Online App to any SharePoint Online site that exists in the same tenant as the app catalog site collection.

1. Log into the SharePoint Online site where you want to add the Governance Automation Online App.
2. Click the Settings ( ) button on the upper-right corner of the site, and then click **Add an app**. You can also navigate to the **Site Contents** interface and click **add an app**. The **Your Apps** interface appears.
3. In the **Apps you can add** section, click **Governance Automation Online**.
4. When asked if you want to trust Governance Automation Online, click **Trust It**.
5. The Governance Automation Online App is added to the site and a **Governance Automation Online** link is added on the Quick Launch. Click the **Governance Automation Online** link and you are brought to a new page. By default, the following tiles are displayed in the page:
   - **Start a Request**
   - **View My Requests**
   - **View My To-Do List**
   - **Public Site Collection Directory**
   - **My Sites**

   ***Note**: If you want to share the Governance Automation Online App interface to other users, make sure you have invited them in AvePoint Online Services **Settings** > **User Management**. Otherwise, they cannot view the tiles above.

Inserting a Governance Automation Online App Part

Governance Automation Online App provides the following app parts that can be inserted to SharePoint Online sites:

- **Site Information Card** – Displays key information about the site, such as ownership, classification, policy, and available service requests.

  ***Note**: This app part can be inserted to a top-level site of a site collection, or be inserted to an individual site. In a top-level site, the app part displays the site collection information. In a site, the app part displays the site information.

- **Site Lifecycle Timeline** – Displays governance activities during the lifecycle of the site collection or the site.

  ***Note**: This app part can be inserted to a top-level site of a site collection, or be inserted an individual site. In a top-level site, the app part displays the site collection lifecycle timeline. In a site, the app part displays the site lifecycle timeline.

To insert an app part to a site, complete the following steps:

1. Go to the site and click the **PAGE** tab on the ribbon.
2. In the **PAGE** tab, click **Edit**.
3. Click the **INSERT** tab and click **App Part**.
4. In the **Parts** section, select **Site Information Card** or **Site Lifecycle Timeline**.
5. Click **Add** to add this app part to the site.
6. Click **Save** on the ribbon to save your configurations.

***Note**: If you want to share the sites that contain the Governance Automation Online app parts to other users, make sure you have invited them in AvePoint Online Services **Settings** > **User Management**. Otherwise, they cannot view the app parts.

Directing Business Users to Certain Pages via Links

In a SharePoint Online site where you have added the Governance Automation Online app, you can refer allow business users to be directed to certain pages directly by clicking the configured links. To configure this functionality, follow the steps below.

1. Navigate to **Site Contents** > **Contents** > **Site Pages**. The **Site Pages** interface appears. Note that if the style of the page is **Modern Library**, you must refer to the following instructions to modify the list experience, so that the Site Information Card app part can be successfully inserted. The URL of the Site Information Card app part will be obtained to constitute the URLs of custom links.

   

   Figure 2: The style of Modern Library.

   a. Click the settings (⚙) button on the upper-right corner and select **Library Settings**. The **Settings** page appears.

   b. In the **Settings** page, click **Advanced settings**. The **Advanced Settings** page appears.

c. In the **Advanced Settings** page, navigate to the **List experience** field, then, choose the **Classic experience** option.

d. Click **OK** to save your configurations.

2. Navigate to the **Site Pages** interface, then click **New** to create a new page. The **New Item** page appears.
3. Enter a **New page name** in the text box. Then, click **Create** to create the new page.
4. In the **Edit Item** page, click the **INSERT** tab on the ribbon, then, click **App Part**.
5. Select **Site Information Card**, then, click **Add** to add this app part.
6. Right-click the added Site Information Card app part, and select **Inspect Element**.
7. In the **DOM Explorer** tab, find the first **iframe id** node. Then, double-click the value of the **src** node below this **iframe id** node to copy the URL of the Site Information Card app part.

   ***Note**: You can delete the newly created page, after you obtain the URL of the Site Information Card app part.

8. Navigate back to the SharePoint Online site where you have added the Governance Automation Online app, click **EDIT** on the upper-right corner. The **Edit Item** page appears.
9. Click the **INSERT** tab and click **Link**. Then, select the **From Address** option. The **Insert Hyperlink** window appears.
10. In the **Insert Hyperlink** window, enter a text to be displayed in the SharePoint site in the **Text to display** text box. Then, paste the URL of the Site Information Card app part into the **Address** text box.
11. In the URL of the Site Information Card app part, add a certain value before the **AppAction%3d0** value. The value you add represents the action that you want business users to perform directly via this link.

    The value you are about to add can be obtained from the URL of the tile within the Governance Automation Online app. Below are two examples of how you can add the value:

    - If you want business users to be directed to the **Start a Request** page via the link, complete the following steps:

      i. Click **DocAve Governance Automation Online** on the Quick Launch.

      ii. Click the **Start a Request** tile.

      iii. In the browser address bar, find the **/App/Request/StartRequest** value, which is between Governance Automation Online URL and **?SPHostUrl**.

      iv. In the pasted Site Information Card app part URL, add **url%3d/App/Request/StartRequest%26** before **AppAction%3d0**.

    - If you want business users to be directed to a service request form directly via the link, add the value in the format of **url%3d/App/Request/New/Service ID**. Note that you can obtain the service ID from the browser address bar when you edit the service.

12. Click **OK** to insert the hyperlink. You can repeat the steps above to insert more links.
13. Click **Save** to save your configurations.

Updating the Governance Automation Online App

Governance Automation Online provides the Governance Automation Online App of a new version. The new version provides new features for the app part **Site Lifecycle Timeline**. If you want to use this new app part, follow the sections below to update your Governance Automation Online App to the new version.

Downloading the Governance Automation Online App of the New Version

To update the Governance Automation Online App, download the app file of the new version first: http://download2.avepoint.com/Governance Automation Online App File/Governance_Automation_Online_App_1.1.2.0.app.

If you are using Governance Automation Online version for the U.S. Government Public Sector, download the app file: http://download2.avepoint.com/Governance Automation Online App File/Governance_Automation_Online_App_USGov_1.1.2.0.app.

Uploading the Governance Automation Online App of the New Version to App Catalog

After downloading the app file of the new version, you must upload the Governance Automation Online App of the new version to the app catalog site collection. Note that the permissions required to upload the new version of the Governance Automation Online app are the same as that of the old version. Complete the following steps to upload the new Governance Automation Online App to the app catalog site collection:

1. In the **SharePoint admin center** interface, navigate to **apps** > **App Catalog**.
2. Click **Apps for SharePoint** on the left pane.
3. In the **Apps for SharePoint** interface, click **Upload**.
4. In the **Add a document** window, click **Browse…**.
5. In the **Choose File to Upload** window, select the **Governance_Automation_Online_App_1.1.2.0.app** file or the **Governance_Automation_Online_App_USGov_1.1.2.0.app** file and click **Open**.
6. In the **Add a document** window, click **OK**. The app file is successfully uploaded to the app catalog.

Updating the Governance Automation Online App

After uploading the app file of the new version to the app catalog site collection, complete the following steps to update the Governance Automation Online App:

1. Navigate to the SharePoint Online site where you have added the Governance Automation Online App of the old version.
2. Fine the **DocAve Governance Automation Online** app and click the **Click for more information** (···) button, then, click **ABOUT**.
3. In the **Add Apps** interface, click **GET IT** in the right pane.
4. In the pop-up window, click **Trust it** to update the app to the new version or click **Cancel** to return to the **Add Apps** interface without updating the app.

Updating the Client Secret of the Governance Automation Online App

When you registered the Governance Automation Online App in SharePoint Online, you provided a client secret. This client secret is available for one year. One year later, this client secret will expire, and you cannot access the Governance Automation Online App and app parts. You can complete the following steps to update the client secret:

1. Download and install SharePoint Online Management Shell: https://www.microsoft.com/en-us/download/details.aspx?id=35588
2. Download the .ps1 file for setting a new client secret: http://download2.avepoint.com/Governance%20Automation%20Online%20App%20File/Governance_Automation_Online_Set_New_Client_Secret.ps1
3. Use an Office 365 Global Administrator account to execute the **Governance_Automation_Online_Set_New_Client_Secret.ps1** file via SharePoint Online Management Shell. It takes up to 24 hours to take effect.

   ***Note**: The new client secret will be available for three years. AvePoint will update the .ps1 file every three years. Three years later, you can download the .ps1 file again and execute it to update the client secret.

***Note**: If you want to know the expiration date of the current client secret, execute the following command via SharePoint Online Management Shell:

```
Connect-msolservice

 get-msolserviceprincipalcredential -appprincipalid 'efbb98fd-e154-42b8-96df-f552bc3a862d' -returnkeyvalues $false
```

Installing the Site Governance Web Part

The Site Governance Web part is a panel that displays key information of the site collection using the communication site template, such as ownership, classification, policy, site lifecycle timeline, and available service requests.

***Note**: Make sure the intended users have the correct permissions to access the communication sites where this Web part is installed.

Downloading the Site Governance Web Part

To install and use the Site Governance Web part, download the app file:

http://download2.avepoint.com/Governance Automation Online App File/Site_Governance_Panel.sppkg

If you are using Governance Automation Online version for the U.S. Government Public Sector, download the app file: http://download2.avepoint.com/Governance Automation Online App File/Site_Governance_Panel_USGov.sppkg

Required Permissions

To install and use the Site Governance Web part, ensure that the permissions for the following are in place:

Uploading the Site Governance Web Part to App Catalog

The user who uploads the Site Governance Web part to the app catalog site collection must have Design or above permission to the app catalog site collection.

Registering the Site Governance Web Part

The user who registers the Site Governance Web part must be the administrator of the site collection or site from which the **Register an App** is started.

Inserting a Site Governance Web Part to a SharePoint Online Site

The user who inserts the Site Governance Web part to a communication site must have Contribute or above permission to the site.

Uploading the Site Governance Web Part to App Catalog

Before adding the Site Governance Web part to any communication sites, you must upload the Web part to the app catalog site collection.

Complete the following steps to upload the Site Governance Web part to the app catalog site collection:

1. In the **SharePoint admin center** interface, navigate to **apps** > **App Catalog**.

2. Click **Apps for SharePoint** on the left pane.
3. In the **Apps for SharePoint** interface, click **Upload**.
4. In the **Add a document** window, click **Browse…**.
5. In the **Choose File to Upload** window, select the downloaded app file and click **Open**.
6. In the **Add a document** window, click **OK**. The app file is successfully uploaded to the app catalog.
7. In the **Do you trust Site Governance Panel** window, select the **Make this solution available to all sites in the organization** checkbox, then, click **Deploy**.

Registering the Site Governance Web Part

To use the Site Governance Web part, you must register the Web part in SharePoint Online.

Complete the following steps to register the Web part:

1. Go to any communicate site in the same tenant of the app catalog site collection where the Site Governance Web part is uploaded.
2. Modify the communication site URL to …**/_layouts/15/appregnew.aspx**. The **Register an App** page appears.
3. Configure the following settings on the **Register an App** page:
    a. **Client Id** – Enter **efbb98fd-e154-42b8-96df-f552bc3a862d** in the text box.
    b. **Client Secret** – Enter **bFilTPqDzKpUmzJhy+ykSokPHIJdNM09WtK0DuPpnSk=** in the text box.
    c. **Title** – Enter a desired title for the Site Governance Web part.
    d. **App Domain** – Enter **gaoapp.avepointonlineservices.com** in the text box.

    If you are using the Governance Automation Online version for U.S. Government Public Sector, enter **gausgovapp.avepointonlineservices.com**.

    e. **Redirect URI** – Enter **https://gaoapp.avepointonlineservices.com/home/index** in the text box.

    If you are using the Governance Automation Online version for U.S. Government Public Sector, enter **https://gausgovapp.avepointonlineservices.com/home/index**.

    f. Click **Create** to register the Site Governance Web part.

Inserting the Site Governance Web Part

To insert the Site Governance Web part to a communication site, complete the following steps:

1. Go to the communication site and click **Edit** (Edit).

2. Click **Add the new section or a Web part** ( ) in the middle of the page.
3. Select **Site Governance** under **Other**.
4. Click **Save and close** on the ribbon to insert the Site Governance Web part.

***Note**: If you want to share the sites that contain the Site Governance Web part with other users, make sure you have invited them in AvePoint Online Services **Settings** > **User** > **Management**. Otherwise, they cannot view this Web part.

Configuring Language and Time Zone Settings

To configure the language and time zone for your Governance Automation Online platform, click the login ID on the navigation bar. Then, click **Configure Personal Settings**.

In the pop-up **Configure Personal Settings** interface, configure the following settings:

1. **Language** – Select a language from the drop-down list to set it as the display language.
2. **Time Zone** – Select a time zone from the drop-down list to set it as the display time zone. The time zone selected here decides the display time of data in Governance Automation Online interface.
3. Click **Save** on the ribbon to save your configuration. The display language and time zone are changed automatically. Click **Cancel** to exit the **Configure Personal Settings** interface.

Configuring Settings in the System Group

The System group allows you to configure the optional system settings of Governance Automation Online, including **E-mail Templates**, **Administrator Notification**, **Timer Service Configuration Management**, **Report Export Location**, **Category Management**, and **Recertification Profile Management**.

Refer to the following instructions for details of these sections.

Configuring E-mail Templates

E-mail Templates allow you to customize notification e-mails sent by Governance Automation Online, such as when a request is approved or when a task is assigned. Different e-mail templates are used for different notifications.

To access **E-mail Templates** settings, click **E-mail Templates** in the **System** group within the **Settings** interface.

Searching and Filtering E-mail Templates

To change the number of rows displayed, use the **Show rows** drop-down list in the upper-right corner. To sort the e-mail templates, click the sort ( ) button in a column heading such as **E-mail Template** and

Description. You can also filter the **E-mail Template Type** by clicking the filter ( ) button in the column heading.

To search displayed e-mail template, enter the keyword in the **Search** text box and then click the search ( ) button.

Creating or Editing E-mail Templates

To create a new e-mail template, click **Create** on the ribbon. To modify a previously configured e-mail template, select the e-mail template, and click **Edit** on the ribbon.

In the interface for creating or editing an e-mail template, configure the following settings:

1. Enter a desired **E-mail Template Name** for the e-mail template. Then, enter an optional **Description** for the e-mail template for future reference.
2. Select an **E-mail Template Type** from the drop-down list to designate when the e-mail template can be used in Governance Automation Online.
3. **E-mail Template Language** – The e-mail template language will be used as the display language of the e-mail sent to recipients. Complete the following steps to configure the e-mail template language:
    a. Click the edit ( ) button of a language that you want to define for the e-mail template you are about to create.
    b. In the **Edit** window, complete the following steps:
        i. **Subject** – Enter the subject of the e-mail notification for the e-mail template. You can insert a reference in the Subject by clicking **Insert Reference**. A reference is a parameter that will call up the corresponding bit of information for which it is named for each individual service request.
        ii. **Message Body** – Customize the message body of the e-mail notification for the e-mail template. You can insert a reference in the Message Body by clicking **Insert Reference**. A reference is a parameter that will call up the corresponding bit of information for which it is named for each individual service request.
        iii. Click **Save** to save your configurations, or click **Cancel** to return to the **E-mail Templates** window.
    c. Click **Not Enabled** in the table to have the status switched to **Enabled**. The language will be enabled as the display language for this e-mail template.
    d. You can repeat the steps above to enable multiple languages for the e-mail template.

    If you enabled multiple languages, select a default language from the drop-down list. Note the following:

- The display language of the e-mail sent to recipients follows the language defined in the Governance Automation Online Personal Settings of the recipients, if the language selected in Governance Automation Online Personal Settings is enabled here.
- The default language will be used as the display language of the e-mail, if the language selected in Governance Automation Online Personal Settings is not enabled here.

4. Click **Save** to save the configurations and return to the **E-mail Templates** interface, or click **Cancel** to return to the **E-mail Templates** interface without saving any configurations.

Deleting E-mail Templates

To delete an e-mail template from Governance Automation Online, select an e-mail template from the e-mail template list, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected e-mail template, or click **Cancel** to return to the **E-mail Template** interface without deleting the selected e-mail template.

Configuring Administrator Notification

Administrator Notification allows you to configure a notification to inform the Administrator Contact should any service request encounter an error.

To access **Administrator Notification** settings, click **Administrator Notification** in the **System** group within the **Settings** interface.

Follow the instructions below to configure the Administrator Notification settings:

1. **Alternate Administrator Contact** – Specify a user or an Azure Active Directory group to be an alternate Administrator Contact in case that the Administrator Contact is unavailable. Enter the username or the group name in the text box. Press **Enter** to check whether or not the name is valid.
2. **E-mail Settings** – Allows you to send an e-mail to the Administrator Contact once a task has been assigned to that Administrator Contact when an error occurs. Select the **Notify the Service Request Administrator Contact when the task is assigned** checkbox, and select an e-mail template from the drop-down list for this e-mail notification.
3. **Duration and Escalation** – Select the **Enable Duration and Escalation** checkbox to notify another administrator contact if an error task has not been handled within the specified amount of time. Make sure that the user receiving the escalated tasks has enough permission to handle all tasks.

    a. **Duration** – Enter a number in the text box for the deadline, and select **Day(s)** or **Week(s)** as the time unit for the duration.

    You can select the **Enable reminder before the escalation** checkbox to remind the administrator contact before the error task expires. Select a reminder profile from the drop-down list or click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

    b. **Escalation** – Select the action that the escalation will trigger from the drop-down list.

- **Notify** – The specified user will be notified when the task is escalated. Enter the username in the text box. Press **Enter** to check whether or not the name is valid. You can also enter **$Manager of Approver** in the text box. The manager of the approver of the task will be notified when the task is escalated.
- **Re-assign to** – The task will be re-assigned to the specified users when the task is escalated. Enter the username in the text box. Press **Enter** to check whether or not the name is valid.

c. **E-mail Template** – Select an e-mail template from the drop-down list.

4. Click **Save** to save the configurations and return to the **Settings** interface, or click **Cancel** to return to the **Settings** interface without saving any changes.

Configuring the Timer Service

Use Timer Service Configuration Management to manually configure Timer Service setting. After saving the configurations for the Timer Service settings, they take effect immediately.

To access **Timer Service Configuration Management** settings, click **Timer Service Configuration Management** in the **System** group within the **Settings** interface.

In the **Timer Service Configuration Management** interface, configure the following settings:

1. **Site Collection Status Scan Job** – Select **Enable site collection status scan job** to enable this job. The site collection status scan job monitors the status of site collections, including inactivity, lease expiration, locking, and deletion. Configure the interval by which this job is performed by entering a number with **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit.
2. **Site Information Synchronization Job** – Select **Enable site information synchronization job** to enable this job. The site information synchronization job synchronizes the related site information. Configure the interval by which this job is performed by entering a number with **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit.
3. **Site Collection Information Synchronization Job** – Select **Enable site collection information synchronization job** to enable this job. The site collection information synchronization job synchronizes the related site collection information. Configure the interval by which this job is performed by entering a number with **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit.
4. **Deactivated Site Collection Contact Status Scan Job** – Select **Enable deactivated site collection contact status scan job** to enable this job. The site collection contact status scan job monitors the statuses of site collection contacts. Configure the interval by which this job is performed by entering a number with **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit.
5. **Recertification Scan Job** – Select **Enable recertification scan job** to enable this job. The recertification scan job checks the recertification profiles to see if it is time to run a recertification process. Configure the interval by which this job is performed by entering a number with **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit.
6. **Group Information Synchronization Job** – Select **Enable group information synchronization job** to enable this job. The group information synchronization job synchronizes the URL, quota, and

size of the sites for storing files of Governance Automation managed Office 365 groups. Configure the interval by which this job is performed by entering a number with **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit.

7. Click **Save** to save the configurations and return to the **Settings** interface, or click **Cancel** to return to the **Settings** interface without saving any configurations.

Configuring Report Export Locations

The Report Export Location is where you export Governance Automation Online reports.

To access **Report Export Location** settings, click **Report Export Location** in the **System** group within the **Settings** interface.

Searching Report Export Locations

You can search your desired report export locations by designated keywords. Enter the keyword in the **Search** text box and then click the search ( ) button. The **Location Name** and **Description** column support to search for export locations, and only the content in the column displayed in the current view can be searched.

Creating or Editing Report Export Locations

To create a new report export location, click **Create** on the ribbon. To modify a previously configured export location, select the export location, and click **Edit** on the ribbon.

In the interface for creating or editing a report export location, configure the following settings:

1. **Name and Description** – Enter a name for the new report export location. Enter an optional description for future reference.
2. **Microsoft Azure Storage Configuration** – Configure the connection to your Microsoft Azure Storage.
    - **Container name** – Enter the container name that you wish to access.
    - **Account name** – Enter the corresponding account name to access the container.
    - **Account key** – Enter the corresponding account key to access the container.

    Optionally, you can choose whether to Use https to access Microsoft Azure Storage.

    Click **Validation Test** to test the connection.
3. Click **Save** on the ribbon to save your configurations, or click **Cancel** to go back to the **Report Export Location** interface without saving any configuration.

Deleting Report Export Locations

To delete a report export location from Governance Automation Online, select an export location from the list of previously configured export locations, and then click **Delete** on the ribbon. A confirmation window appears asking if you are sure you want to proceed with the deletion. Click **OK** to delete the

selected export location, or click **Cancel** to return to the **Report Export Location** interface without deleting the selected export location.

Configuring Category Management

Use Category Management to manage categories, which are used to organize services, approval processes, policies, and questionnaires.

To access **Category Management** settings, click **Category Management** in the **System** group within the **Settings** interface.

Displaying and Searching Categories

To change the number of categories displayed, use the **Show rows** drop-down list in the upper right corner.

To search the displayed categories, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Categories

To create a new category, click **Create** on the ribbon. To modify a previously configured category, select the desired category, and click **Edit** on the ribbon.

In the **Create Category** interface or **Edit Category** interface, configure the following settings:

1. **Category Name** – Enter the name of the category that you are about to create.
2. **Category Name Mapping** – This allows the category to be displayed as different names in Governance Automation Online with different display languages. Enter the category names for different languages in the corresponding text boxes. If you do not wish to configure the category name mapping manually, Governance Automation Online automatically uses the category name specified in step 1 for the category names of all languages. The text boxes will be filled in with the name entered in **Category Name** when the cursor is moved away from the category name.
3. Click **Save** to save the configurations and return to the **Category Management** interface, or click **Cancel** to return to the **Category Management** interface without saving any configurations.

Deleting Categories

To delete a category, select a previously configured category, and then click **Delete** on the ribbon. A confirmation window appears asking if you are sure you want to proceed with the deletion. Click **OK** to delete the selected category, or click **Cancel** to return to the **Category Management** interface without deleting the selected category.

Configuring Recertification Profiles

Use Recertification Profile Management to manage recertification profiles. Recertification profiles enables you to apply different types of recertification process to site collection policies and Office 365 group policies.

***Note**: Permission recertification is not supported on SharePoint Online My Sites.

To access **Recertification Profile Management**, click **Recertification Profile Management** in the **System** group within the **Settings** interface.

Displaying and Searching Recertification Profiles

To change the number of recertification profiles displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the recertification profiles that are displayed, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Recertification Profiles

To create a new recertification profile, click **Add** on the ribbon. To modify a previously configured recertification profile, select the desired profile, and click **Edit** on the ribbon.

Complete the following steps:

1. **Recertification Scope** – Choose **Site collection** or **Office 365 group** as the recertification scope.
2. **Name and Description** – Enter a name and an optional description for the recertification profile.

   Category – Categories are used to organize recertification profiles. Select an existing category from the drop-down list or click **Create New** to create a new category.

3. **Permission Recertification** – If you chose **Site collection** as the recertification scope, permission recertification enables the periodic review of user and group permissions to site collection content. If you chose **Office 365 group** as the recertification scope, permission recertification enables the periodic review of the group permissions to the corresponding group team site. A permission recertification task will be generated according to the schedule. Approvers can then modify the permissions in Governance Automation Online and the permission changes will be updated to SharePoint Online.

   Select the **Permission recertification** checkbox and configure the following settings:

   a. **Specify a duration for the entire recertification process** (optional) – Allows you to define a duration for the entire recertification process. Enter a number in the text box and select **Day(s)** or **Week(s)** as the unit.

      You can select the **Enable reminder before the escalation** checkbox to remind the permission recertification task approver before the task expires. Select a reminder profile from the drop-down list or click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

   b. Configure the **Recurrence** of the permission search: **Daily**, **Weekly**, or **Monthly**.

c. Select an **Approval Process** from the drop-down list or click **Create New** to create a new one.

4. **Metadata Recertification** – If you chose **Site collection** as the recertification scope, you can enable metadata recertification. Metadata recertification enables the periodic review of site collection metadata. A metadata recertification task will be generated according to the schedule configured. Approvers can then modify the metadata values in Governance Automation Online and the metadata value changes will be updated to SharePoint Online.

   Select the **Metadata recertification** checkbox and configure the following settings:

   a. **Enable adding or deleting metadata during metadata recertification process** – Allows to add new metadata or delete metadata during the metadata recertification process.

   b. **Specify a duration for the entire recertification process** (optional) – Allows you to define a duration for the entire recertification process. Enter a number in the text box and select **Day(s)** or **Week(s)** as the unit.

      You can select the **Enable reminder before the escalation** checkbox to remind the permission recertification task approver before the task expires. Select a reminder profile from the drop-down list or click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

   c. Configure the **Recurrence** of the metadata search: **Daily**, **Weekly**, or **Monthly**.

   d. Select an **Approval Process** from the drop-down list or click **Create New** to create a new one.

5. **Ownership Recertification** – If you chose **Site collection** as the recertification scope you can enable ownership recertification. Ownership recertification enables the election process, which can be used to assign or re-assign site collection contacts on a periodic schedule.

   Select the **Ownership recertification** checkbox and configure the following settings:

   a. **Specify the users you want to exclude** (optional) – Enter the names of the users that will be excluded during the election process.

   b. **Notify the user when the election task is assigned** (optional) – Select the checkbox to send a notification e-mail to the user when the election task is assigned. Select an e-mail template that will be used to send the notification e-mail. By default, the **Built-in Election Task E-mail Template** is selected.

   c. **Notify the primary contact when the site collection is assigned** (optional) –

   d. **Notify the secondary contact when the site collection is assigned** (optional) –

   e. **Duration** – Define the duration for each election stage. Enter a number in the text box and select **Day(s)** or **Week(s)** as the unit.

You can **Remind the nominated user before each nomination task expires**. Select the checkbox and select a reminder profile from the drop-down list or click **Create New** to create a new one. AvePoint recommends that you select a reminder profile that has the **Built-in Task Reminder E-mail Template** selected. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

f. **Specify a duration for the entire recertification process** (optional) – Allows you to define a duration for the entire recertification process. Enter a number in the text box and select **Day(s)** or **Week(s)** as the unit.

   You can **Remind the nominated user before the entire recertification process expires**. Select the checkbox and select a reminder profile from the drop-down list or click **Create New** to create a new one. AvePoint recommends that you select a reminder profile that has the **Built-in Recertification Process Reminder E-mail Template** selected. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

g. Configure the **Recurrence** of the ownership search: **Daily**, **Weekly**, or **Monthly**.

h. Select an **Approval Process** from the drop-down list or click **Create New** to create a new one.

6. **Membership Recertification** – If you chose **Office 365 group** as the recertification scope, you can enable membership recertification. Membership recertification enables the periodic review of Office 365 group members and/or owners. A membership recertification task will be generated according to the schedule. Approvers can then modify the membership in Governance Automation Online and the membership changes will be updated to Office 365.

   Select the **Membership recertification** checkbox and configure the following settings:

   a. **Membership type** – Select the **Group owners** checkbox and/or the **Group members** checkbox to enable periodic review of group owners and/or members.

   b. **Specify a duration for the entire recertification process** (optional) – Allows you to define a duration for the entire recertification process. Enter a number in the text box and select **Day(s)** or **Week(s)** as the unit.

      You can select the **Enable reminder before the escalation** checkbox to remind the membership recertification task approver before the task expires. Select a reminder profile from the drop-down list or click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Creating or Editing Reminder Profiles.

   c. Configure the **Recurrence** of the membership search: **Daily**, **Weekly**, or **Monthly**.

   d. Select an **Approval Process** from the drop-down list or click **Create New** to create a new one.

7. **Administrator Contact** – Enter the name of the user or of the Azure Active Directory group that will become the administrator contact. If a recertification task encounters any errors, an error task will be generated and the error task will be assigned to this administrator contact.
8. Click **Save** to save your configurations on the profile or click **Cancel** to return to the **Recertification Profile Management** interface without saving any configurations.

Deleting Recertification Profiles

To delete a recertification profile, select a previously configured profile, and then click **Delete** on the ribbon. A confirmation window appears asking if you are sure you want to proceed with the deletion. Click **OK** to delete the selected profile, or click **Cancel** to return to the **Recertification Profile Management** interface without deleting the selected profile.

Managing the Election Process

Election Process Management is used to manage the site collection contact election process. For more information about site collection contact election process, refer to Electing Site Collection Contacts.

Election Process Management allows you to select and view stages of an election process and configure the number of nominees in the last three stages.

To access **Election Process Management**, click **Election Process Management** in the **System** group within the **Settings** interface.

In the **Election Process Management** window, select one or more of the following stages.

If a nominee of the last stage declines to be the primary site collection contact, or the nominee does not handle the election task when the duration is reached, the election task will be assigned to the nominee of the next stage. Once a nominee claims to become the primary site collection contact, the election process completes.

***Note**: The primary site collection contact must be selected, if you select the secondary site collection contact as the nominee.

- Primary Site Collection Contact – The election task will be assigned to the current primary site collection contact.
- Secondary Site Collection Contact – The election task will be assigned to the current secondary site collection contact.
- Primary Site Collection Administrator – The election task will be assigned to the current primary site collection administrator.
- Administrators within the Site Collection Administrators Group – The default number is **3**. You can enter a number between **1** and **10** in the text box. Governance Automation Online will randomly select the specific number of site collection administrators as the nominees.

- Users with certain permission – The default number is **3**. You can enter a number between **1** and **10** in the text box. Then, select **Full Control** or **Contribute** from the drop-down list. Governance Automation Online will randomly select the specific number of users who have the specified permission to the site collection as the nominees.
- Users with certain permission – The default number is **3**. You can enter a number between **1** and **10** in the text box. Then, select **Full Control** or **Contribute** from the drop-down list. Governance Automation Online will randomly select the specific number of users who have the specified permission to the site collection as the nominees.

When you have finished configuring the number of nominees, click **Save** on the ribbon to save your changes.

If a user declines to be the primary site collection contact in the previous election stages, but this user is also randomly selected as the nominee in any of the following election stages, the election task will not be assigned to this user and Governance Automation Online will randomly select another user to replace this user. If a user does not handle the election task in the previous election stages, but this user is also randomly selected as the nominee in any of the following election stages, the election task will be assigned to this user again.

Configuring E-mail Settings

E-mail Settings allows you to customize the settings used to send notification e-mails to business users.

To access **E-mail Settings**, click **E-mail Settings** in the **System** group within the **Settings** interface.

In the **E-mail Settings** interface, configure the following settings:

1. **Recipient Settings** – Choose to use the Office 365 e-mail address or use the custom e-mail mapping. Choose one of the following options:
    - **Use Office 365 e-mail address** – Choose this option to use the default Office 365 e-mail address. The e-mails will be sent to the recipients' Office 365 Outlook mailboxes.
    - **Use custom e-mail mapping** – Choose this option to send e-mails to recipients' custom e-mail addresses. The recipients' custom e-mail addresses will be retrieved according to the value of the specified Azure Active Directory property. Then, enter an Azure Active Directory property name in the text box.
2. **E-mail Settings** – Choose to use default e-mail settings or to use custom e-mail settings. Choose one of the following options:
    - **Use default e-mail settings** – Choose this option to use default e-mail settings. The e-mail will be sent from the default e-mail address.
    - **Use custom e-mail settings** – Choose this option to use custom e-mail settings. Then, configure the settings below:
        i. **E-mail server** – Enter the address of e-mail server.
        ii. **Port** – Enter the SMTP port.

iii. **E-mail address** – Enter the e-mail address for the e-mails sent from.

iv. **Username** – Enter the sender's username on the SMTP server.

v. **Password** – Enter the sender's password to log into the SMTP server.

vi. **Authentication** (Optional) – Select the **SSL authentication** or **Secure password authentication** according to your e-mail settings.

vii. **Validation Test** – Click **Validation Test** to test the information provided above.

3. **Branding Logo Settings** – Choose to use the default branding logo or to use a custom branding logo that will be displayed in the e-mail sent to business users. Choose one of the following options:

   - **Use the default branding logo** – Choose this option to display the default branding logo in the e-mail sent to business users.
   - **Use a custom branding logo** – Choose this option to display a custom branding logo in the e-mail sent to business users. Then, you must click **Browse** and upload an image. Note the following:
     - The uploaded image should be in one of the following file types: **.gif**, **.jpg**, **.jpeg**, or **.png**.
     - The maximum size of the image is 1 MB.
     - The recommended height of the image is 45 pixels, and the recommended width of the image is 420 pixels.

       ***Note:** If the uploaded image is greater than the recommended size, it will be automatically scaled to fit.

4. **Message Body Settings** – Choose to use the default message body or to hide references to AvePoint in the e-mail sent to business users. Choose from the following options:

   - **Use the default message body** – Choose this option to use the default message body in the e-mail sent to business users.
   - **Hide references to AvePoint** – Choose this option to hide references to AvePoint from the e-mail sent to business users.

Click **Save** to save the configurations and return to the **Settings** interface or click **Cancel** to return to the **Settings** interface without saving any configurations.

Business User Features Activation or Deactivation

This feature helps you define which section is visible to business users in the landing page.

To access **Business User Features Activation or Deactivation**, click **Business User Features Activation or Deactivation** in the **System** group within the **Settings** interface.

In the **Business User Features Activation or Deactivation** interface, select the sections that you wish the business users to view by selecting the corresponding checkboxes. For **Public Site Collection Directory**, you can also choose whether to allow business users to export the report. Click **Save** on the ribbon to save your configurations.

Configuring Governance Automation Online Terminology

Use Governance Automation Online Terminology Management to customize terminologies in your Governance Automation Online system. The terminologies displayed in Governance Automation Online interface, including role names, will be replaced with your desired values.

To access **Governance Automation Online Terminology Management**, click **Governance Automation Online Terminology Management** in the **System** group within the **Settings** interface.

Searching and Filtering Terminology Mappings

To change the number of rows displayed, use the **Show rows** drop-down list in the upper-right corner. To sort the terminology mappings, click the sort ( ) icon in the **Original Terminology** column or **the Current Terminology** column, then, select **Ascending** or **Descending**.

You can customize how terminology mappings are displayed in a number of different ways:

- **Search** – Allows you to filter terminology mappings displayed by keyword you designate. The **Original Terminology** column and the **Current Terminology** column support to search for the desired terminology mappings, and only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Allows you to manage which columns are displayed in the list so that only information you want to see is displayed. Click the manage columns ( ) icon, then, select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Allows you to filter which item in the list is displayed. Click the filter items ( ) icon in the **Language** column, then, select the checkbox next to the item name to have the item shown in the list.

Creating or Editing Terminology Mappings

To create a new terminology mapping, click **Create** on the ribbon. To modify a configured terminology mapping, select the terminology mapping, and click **Edit** on the ribbon.

Configure the following settings when creating or editing a terminology mapping:

1. **Language** – Select a language for the terminology mapping you are about to create.
2. **Terminology Mapping** – Enter the original terminology and the current terminology in the corresponding text boxes. The current terminology will be displayed in Governance Automation Online. Note that the original terminology is case-sensitive.

3. Click **Save** on the ribbon to save your configurations, or click **Cancel** on the ribbon to return to the **Governance Automation Online Terminology Management** window without saving any configurations.

***Note**: The current terminology you designate will take effect, after you log out and log into Governance Automation Online again.

Deleting Terminology Mappings

To delete terminology mappings, select one or more terminology mappings, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected terminology mappings, or click **Cancel** to return to the **Governance Automation Online Terminology Management** interface without deleting the selected terminology mappings.

Note the following:

- If you delete newly created terminology mappings, the terminologies displayed in your system will be reset to the original ones.
- The original terminologies will take effect, after you log out and log into Governance Automation Online again.

Configuring My Sites Request Initiation Setting

The My Sites Request Initiation Setting determines how requests can be initiated from the My Sites report.

To access **My Sites Request Initiation Setting**, click **My Sites Request Initiation Setting** in the **System** group within the **Settings** page. Then, choose one of the following options in the **My Sites Request Initiation Setting** window:

- **Display the service type filter** – When a business user starts a request in **My Sites**, the business user must select a service type first.
- **Hide the service type filter and select specific service types/services** – If you select this option, you must select one or more service types and select one or more services for each service type. When a business user starts a request in **My Sites**, the business user does not need to select a service type. The services you select here will be displayed to the business user if the following conditions are met:
    - The business user is assigned the permission to use the service.
    - The business user is assigned the permission to submit a request for the service.
    - The site collection selected by the business user is within the service scope.

Click **Save** on the ribbon to save your configurations, or click **Cancel** to close the **My Sites Request Initiation Setting** window without saving any configurations.

Configuring Settings in the SharePoint Group

The SharePoint group allows you to manage the settings related to SharePoint Online.

Configuring SharePoint Permission Levels

Permission levels allow you to assign a particular set of permissions to SharePoint Online users and security groups so that they can perform specific actions on your site.

To access **SharePoint Permission Level Management**, click **SharePoint Permission Level Management** in the **SharePoint** group within the **Settings** interface.

Displaying and Searching Permission Levels

To change the number of rows displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the displayed SharePoint permission level, enter the keyword in the **Search** textbox and click the search ( ) button.

Viewing Permission Levels

To view a permission level, click the permission level name under the **SharePoint Permission Level** column, then, the **View Details** window appears displaying the detailed permissions. You can also perform the following actions:

- **Back** – Click **Back** on the ribbon to return to the **SharePoint Permission Level Management** window.
- **Edit** – Click **Edit** on the ribbon to edit this permission level. Note that if the permission level is being used in any service, it cannot be edited.
- **Delete** – Click **Delete** on the ribbon to delete the permission level. A confirmation window appears asking you if you are sure to proceed the deletion. Click **OK** to delete the permission level, or click **Cancel** to return to the view details page without deleting the permission level.

Creating or Editing Permission Levels

To create a new permission level, click **Create** on the ribbon. To modify a previously configured permission level, select the desired permission level, and click **Edit** on the ribbon.

In the interface for creating or editing a SharePoint permission level, configure the following settings:

1. **Name and Description** – Enter a desired **Name** for the permission level. Then, enter an optional **Description** for the permission level for future reference.
2. **Permissions** – Add permissions to the permission level by selecting corresponding checkboxes.
3. Click **Save** to save the configurations and return to the **SharePoint Permission Level Management** interface, or click **Cancel** to return to the **SharePoint Permission Level Management** interface without saving any configurations.

Deleting Permission Levels

To delete a permission level from Governance Automation Online, select a previously configured permission level, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected permission level, or click **Cancel** to return to the **SharePoint Permission Level Management** interface without deleting the selected permission level.

Importing Existing Office 365 Objects

This feature allows you to manage existing SharePoint Online site collections/sites and Office 365 groups/users that were not created by Governance Automation Online. These site collections and sites are managed by configuring template files.

***Note**: SharePoint Online site collections and Communication Sites are both supported.

To access **Import Existing Office 365 Objects** settings, click **Import Existing Office 365 Objects** in the **SharePoint** group within the **Settings** interface.

Exporting a Template File

Export Mode allows you to generate a template file. The template file is configured for importing existing site collections, sites, groups, or users, so that they can be managed by Governance Automation Online.

To export a template file, complete the following steps:

1. Click **Export Mode** on the ribbon to access the export mode.
2. **Name and Description** – Enter a name for the export job. Enter an optional description for future reference.
3. **Object Type** –Select **Site Collection**, **Site**, **Office 365 User**, or **Office 365 Group**.
4. **Scope** – Expand the tree to select the node which you want to manage by Governance Automation Online.
    - If **Site Collection** is selected in the **Object Type** field, only SharePoint Online admin center can be selected from the tree.
    - If **Site** is selected in the **Object Type** field, SharePoint Sites groups, site collections, and sites can be selected from the tree. The selected SharePoint Sites group and site collections will not be included in the template file while the selected sites will be included in the template file.
    - If **Office 365 User** or **Office 365 Group** is selected in the **Object Type** field, select an Azure AD app profile that was created in AvePoint Online Services. The Azure AD app profile represents your Office 365 tenant.

5. **Export Location** – Choose to export the template file to a local path or an export location. If **Export to an export location** is selected, select an export location from the drop-down list or click **Add New Location** to create a new export location in the pop-up window.
6. Click **Save and Export** on the ribbon to export the template file.

Modifying the Exported Site Collection Template File

To modify an exported site collection template file, complete the following steps:

1. Navigate to the location where the exported site collection template file is saved.
2. Open the template file to view and configure the following settings for each entry:

   ***Note:** All information must be entered exactly, including spaces and capitalization.

   - **URL** – Displays the full URL of the site collection.
   - **Admin Center URL** – Displays the admin center URL of SharePoint Online site collections.
   - **Department** – Enter the department to which the site collection belongs. The department entered here must already be configured in **Settings** > **Department**.
   - **Policy Name** – Enter the name of the site collection policy that will be applied to the site collection.
   - **Primary Site Collection Contact** – Enter a username to assign a user to be the primary site collection contact.
   - **Secondary Site Collection Contact** – Enter a username to assign a user to be the secondary site collection contact.
   - **Metadata** – Enter the value for the metadata. Any metadata created in **Settings** > **Metadata** can be entered here. Note that if the type of the metadata is **Hyperlink**, the metadata value must be the desired text and the hyperlink address separated with a semicolon.
3. Save the template file after the configuration.

Modifying the Exported Site Template File

To modify an exported site template file, complete the following steps:

1. Navigate to the location where the exported template file is saved.
2. Open the template file to view and configure the following settings for each entry:

   ***Note:** All information must be entered exactly, including spaces and capitalization.

   - **URL** – Displays the full URL of the site.
   - **Site ID** – Displays the ID of the site.
   - **Site Collection URL** – Displays the full URL of the site collection to which the site belongs.

- **Site Collection ID** – Displays the ID of the site collection to which the site belongs.
- **Department** – Enter the department to which the site belongs. The department entered here must already be configured in **Settings** > **Department**.
- **Primary Site Contact** – Enter a username to assign a user to be the primary site contact.
- **Secondary Site Contact** – Enter a username to assign a user to be the secondary site contact.
- **Metadata** – Enter the value for the metadata. Any metadata created in **Settings** > **Metadata** can be entered here. Note that if the type of the metadata is **Hyperlink**, the metadata value must be the desired text and the hyperlink address separated by a semicolon.

3. Save the template file after the configuration.

Modifying the Exported User Template File

To modify an exported user template file, complete the following steps:

1. Navigate to the location where the exported template file is saved.
2. Open the template file to view and configure the following settings for each entry:

   ***Note:** The information you enter must be exactly correct, including spaces and capitalization.

   - **Display Name** – Displays the display name of the Office 365 user.
   - **Username** – Displays the username of the Office 365 user.
   - **User Policy** – Enter the name of the user policy that will be applied to the Office 365 user.
   - **Expiration Date** – Set the expiration date for the Office 365 user's contract by one of the following methods:
     - Enter a contract expiration date in the format of **YYYY/MM/DD**.
     - Enter a number as the contact term. The unit is day.
   - **Department** – Displays the department of the Office 365 user if the user's department has been configured in Office 365.
   - **Domain** – Displays the domain of the Office 365 user.
   - **Office** – Displays the office of the Office 365 user if the user's office has been configured in Office 365.

3. Save the template file after the configuration.

Modifying the Exported Group Template File

To modify an exported group template file, complete the following steps:

1. Navigate to the location where the exported template file is saved.
2. Open the template file to view and configure the following settings for each entry:

***Note:** The information you enter must be exactly correct, including spaces and capitalization.

- **Group Name** – Display the name of the Office 365 group.
- **Group ID** – Display the ID of the Office 365 group.
- **Group Policy** – Enter the name of the group policy that will be applied to the Office 365 group.
- **Expiration Date** – Set the expiration date for the Office 365 group's lease by one of the following methods:
  - Enter a lease expiration date in the format of **YYYY/MM/DD**.
  - Enter a number as the lease period. The unit is day.
- **Primary Group Contact** – Enter a username to assign a user to be the primary group contact.
- **Secondary Group Contact** – Enter a username to assign a user to be the secondary group contact.

3. Save the template file after the configuration.

Importing the Modified Template File

Import Mode allows you to import the modified template file and apply it for managing specific site collections, sites, users, or groups.

To import the modified template file, complete the following steps:

1. Click **Import Mode** on the ribbon to access the import mode.
2. **Name and Description** – Enter a name for the import job. Enter an optional description for future reference.
3. **Object Type** – Select **Site Collection**, **Site**, **Office 365 User**, or **Office 365 Group** according to the template file you are about to import.
4. **Import Location** – Click **Browse** to locate the modified template file.
5. Click **Save and Apply** on the ribbon to start the job for applying the configurations. You are brought to the **Job Status** tab. For more information, refer to Viewing Job Status.

Viewing Job Status

The **Job Status** tab allows you to view the status of the export/import job and the other information related to the jobs, including **Name**, **Description**, **Type**, **Object Type**, **Status**, **Modified By**, and **Last Modified Time**.

You can perform the following actions:

- Search – Filters displayed jobs by your entered keyword. You can search desired jobs by the following columns: **Name** and **Modified By**. Only the content in the column displayed in the current view can be searched.

- Show rows – Select the desired number from the **Show rows** drop-down list in the upper-right corner to change the number of jobs displayed per page.
- Sort – Click the sort ( ) button in the column **Name** and select **Ascending** or **Descending**, or click the sort ( ) button in the column **Last Modified Time**.
- Filter item ( ) – Filters which item in the list is displayed. Click the filter item ( ) in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- **Refresh** – Click **Refresh** on the ribbon to refresh the current interface.
- **Download** – Select an import job and click **Download** on the ribbon to download the import result file.
- **Delete** – Select one or more job and click **Delete** on the ribbon to delete the selected jobs.

If a root site collection failed to import due to disabled SharePoint Online Custom Script settings, note the following:

- Custom Script settings control whether SharePoint Online users can run custom script on personal sites and self-service created sites. For more information, refer to http://go.microsoft.com/fwlink/?LinkId=397546.
- Complete the following steps to enable Custom Script settings:
    i. Navigate to **SharePoint admin center** > **settings** > **Custom Script**.
    ii. Choose the **Allow users to run custom script on self-service created sites** option.
    iii. Click **OK** to save your change.

  ***Note**: Changes to Custom Script settings might take up to 24 hours to take effect. Re-import the failed site collection in 24 hours.

Managing App Branding

Use App Branding Management to manage the branding shown in the Governance Automation Online App and app part.

To access App Branding Management, click **App Branding Management** in the **SharePoint** group within **Settings**.

In the **App Branding Management** window, choose one of the following options:

- **Hide the branding** – No branding will be displayed on the Governance Automation Online App and app part.
- **Use the default branding** – The default branding provided by Governance Automation Online will be displayed on the Governance Automation Online App and app part.
- **Use a custom branding** – Displays your custom branding.
    i. Click **Browse**.
    ii. In the **Choose File to Upload** window, select the image of your branding, and then click **Open**.

    Note the following:

    The image of your branding should be one of the following formats: .gif, .jpg, .jpeg, or .png.

    The size of the image is not larger than 1 MB.

    The recommended pixels are 235x30. The height of the image is 30 pixels and the width of the image is 235 pixels.

Click **Save** on the ribbon to save your changes.

Managing the Site Information Card

Choose what information will be displayed on the Site Information Card app part that can be inserted on the top-level of a site collection or a site.

To access Site Information Card Management, click **Site Information Card Management** in the **SharePoint** group within **Settings**.

In the **Site Information Card Management** window, configure the following settings:

- **Site Collection Level** – Select one or more of the following fields that will be displayed on the Site Information Card app part of the site collection level:
    - **Basic Properties** – The **Basic Properties** tab will be displayed on the Site Information Card. The **Basic Properties** tab can contain the following properties. Choose one or more of them:

      Department

      Primary Site Collection Contact

      Secondary Site Collection Contact

      Primary Site Collection Administrator
    - **Metadata** – The **Metadata** tab will be displayed on the Site Information Card. Select one or more metadata from the drop-down list.

- **Policy Properties** – The **Policy Properties** tab will be displayed on the Site Information Card. The properties of the site collection policy applied to the site collection will be displayed on the tab.
- **Start a Request** – The **Start a Request** tab will be displayed on the Site Information Card. Filter the services that will be displayed on the **Start a Request** tab by selecting service categories and service names.

- **Site Level** – Select one or more of the following fields that will be displayed on the Site Information Card of the site level:
  - **Basic Properties** – The **Basic Properties** tab will be displayed on the Site Information Card. The **Basic Properties** tab can contain the following properties. Choose one or more of them:

    Department

    Primary Site Contact

    Secondary Site Contact
  - **Metadata** – The **Metadata** tab will be displayed on the Site Information Card. Select one or more metadata from the drop-down list.
  - **Policy Properties** – The **Policy Properties** tab will be displayed on the Site Information Card. The properties of the site collection policy applied to the site collection where the site resides will be displayed on the tab.
  - **Start a Request** – The **Start a Request** tab will be displayed on the Site Information Card. Filter the services that will be displayed on the **Start a Request** tab by selecting service categories and service names.

Click **Save** to save the configurations, or click **Cancel** to return to the **Settings** page without saving any changes.

Managing Site Governance Panel

Choose what information will be displayed on the Site Governance panel that can be added to communication sites.

To access Site Governance Panel Management, click **Site Governance Panel Management** in the **SharePoint** group within **Settings**.

In the **Site Governance Panel Management** window, configure the following settings:

- **Properties** – The **Properties** tab will be displayed on the Site Governance panel. The **Properties** tab contains **Basic properties** and **Policy properties**. Choose one or more of them:
  - **Basic properties** – The basic properties below will be displayed on the **Properties** tab. Choose one or more of them:

    Department

Primary Site Collection Contact

Secondary Site Collection Contact

Primary Site Collection Administrator

- **Policy properties** – The policy properties will be displayed on the **Properties** tab.

- **Metadata** – The **Metadata** tab will be displayed on the Site Governance panel. Select one or more metadata fields from the drop-down list.
- **Start a Request** – The **Start a Request** tab will be displayed on the Site Governance panel. Filter the services that will be displayed on the **Start a Request** tab by selecting service categories and service names.
- **Site Lifecycle Timeline** – The **Lifecycle Timeline** tab will be displayed on the Site Governance panel. The lifecycle timeline of the site collection will be displayed on the tab.

Click **Save** to save the configurations, or click **Cancel** to return to the **Settings** page without saving any changes.

Configuring Settings in the Request Management Group

The Request Management group allows you to configure the optional settings related to requests, including **Metadata**, **Execution Schedule**, and **Questionnaire Management**.

Configuring Metadata

In Governance Automation Online, you can create metadata that can be made available in services for users to select when submitting a request to create a new site collection or site. The metadata created by Governance Automation Online is stored in the property bag of the site collection/site and can be used to maintain information such as purpose of creation, geography, for compliance and records standards purposes, etc.

***Note: Publish to Directory** is a pre-defined metadata field which will be automatically added into the Create Site Collection service. You can set the metadata value to **Yes** or **No** for the site collection created by Governance Automation Online. All of the site collections with **Publish to Directory** metadata value **Yes** can be displayed in the Public Site Collection Directory. For information on Public Site Collection Directory, refer to Public Site Collection Directory.

To manage metadata created by Governance Automation Online, click **Metadata** in the **Request Management** group within **Settings**.

Searching and Filtering Metadata

To change the number of rows displayed, use the **Show rows** drop-down list in the upper-right corner. To sort the metadata, click the sort ( ) button in a column heading such as **Metadata Name**, **Default Value**, **Index Metadata**, **Last Modified Time**, and **Created By**, then select **Ascending** or **Descending**.

You can customize how the metadata are displayed in a number of different ways:

- **Search** – Allows you to filter metadata displayed by the keyword you designate. The Metadata Name column and the Created By column support to search for the desired metadata, and only the content in the column displayed in the current view can be searched.
- – You can manage which columns are displayed in the list so that only information you want to see is displayed. Click add column ( ) button, and then select the checkbox next to the column name to have that column shown in the list.
- – This allows you to filter which item in the list is displayed. Click the filter ( ) button of the column you want to filter, and then select the checkbox next to the item name to have that item shown in the list.

To view metadata details, click the metadata name.

Creating or Editing Metadata

To create new metadata, click **Create** on the ribbon. To modify previously configured metadata, select the metadata, and click **Edit** on the ribbon.

Configure the following settings when creating or editing metadata:

1. **Name and Type** – Enter a name for the new metadata into the **Metadata Name** text box. All metadata created by Governance Automation Online will have the prefix **GA_**. Then select the type of information you wish to store in this metadata field by clicking the corresponding option. Choose from **Single line of text**, **Multiple lines of text**, **Yes/No (check box)**, **Choice (menu to choose from)**, **Person or Group**, **Managed Metadata**, **Hyperlink**, or **User Profile Property**.

   ***Note**: If you select **Person or Group** or **User Profile Property** as the metadata type, you can select the **Allow a variable role reference to this metadata in the approval process** checkbox. Then, this metadata will be referred as a variable role that can be assigned as an approver in an approval process.

2. **Additional Column Settings** – Configure additional settings for the new metadata. Enter an optional description in the **Description** text box. For each type of metadata, select who assigns the metadata value. Choose between **Assign by Business User** and **Assign by IT Admin:**

   - **Assign by Business User** – Allows the business user to assign this metadata value when submitting requests via services. You can select the **Require Business User Input** checkbox to require the business user to assign the metadata value.
   - **Assign by IT Admin** – The **Default Value** you set will be assigned to requests via services. Select either **Show as Read-Only to Business User** or **Hide from Business User**.

   Then configure the following settings depending on your selected metadata type.

   - **Single line of text** – Enter the desired text into the **Default Value** text box. You can also validate the **Single line of text** value using a defined regular expression. Select the **Apply validation rule to metadata values on the request page** checkbox. Then, select a

validation rule from the drop-down list. For more information about how to create a text validation rule, refer to Configuring Text Validation Rules .

- **Multiple lines of text** – Enter the desired text in the **Default Value** text box. You may enter multiple lines of text by hitting the Enter key on your keyboard. You can also validate the **Multiple lines of text** value by a defined regular expression. Select the **Apply validation rule to metadata values on the request page** checkbox. Then, select a validation rule from the drop-down list. For more information about how to create a text validation rule, refer to Configuring Text Validation Rules .
- **Yes/No (checkbox)** – Choose whether or not to **Enable Terms and Conditions Agreement** by selecting the checkbox. If the option is enabled, enter the desired terms and conditions in the text box. Select **Yes** or **No** as the **Default Value** from the drop-down list.
- **Choice (menu to choose from)** – Enter the choices you wish to provide in the **Type each choice on a separate line** text box. Choose the type of selections to provide from the following: **Drop-down Menu**, **Radio Buttons** or **Checkboxes (allow multiple selections)**. Then, select a default value for this choice.
- **Person or Group** – Enter the usernames or group names in the **Default Value** field. For multiple entries, separate each entry with a semicolon.
- **Managed Metadata** – Configure the following settings for Managed Metadata.
    - **Multiple Value Field** – Select the **Allow multiple values** checkbox if you wish to create multiple terms for the site collection created by Governance Automation Online.
    - **Term Set Settings** – Select an admin center from the **Select admin center and term set** drop-down list to load the term sets where you can retrieve the terms. Expand the Managed Metadata Service tree to select the term set where to choose the term by clicking the term set name. The selected term set is highlighted in orange.
    - **Default Value** – Enter your desired terms as the default values in the text box or select a default value by selecting the select metadata ( ) button to access the **Select Default** interface. Expand the term set tree to select the desired term and click **Add** in the lower-left corner of the Select Default interface.
- **Hyperlink** – Enter the desired text in the **Text to display** text box and enter the address of the hyperlink in the **Address** text box.
- **User Profile Property**– Configure the following settings for User Profile Property metadata.
    i. **SharePoint Online admin center** – Select a SharePoint Online admin center from the drop-down list.
    ii. **Get value from user profile property – Select a property of the Office 365 user** from the drop-down list. The value of the selected property will be used as the metadata value.

iii. **Get user profile from Office 365 user** – Enter the username of an Office 365 user or enter the **$Requester** role in the text box to obtain user profile.

***Note**: Currently, User Profile Property metadata with the value of a variable role can only be added to Create Site Collection services and Create Site services.

3. **Display Metadata in Reports** – Choose whether or not to display the metadata in reports. If you select the **Display the metadata in reports** checkbox, select one or both of the following options:

   - **Display the metadata in Administration Reports**

     ***Note**: Administration Reports include Site Collection Report, Site Report, User Report, and Group Report.

   - **Display the metadata in Public Site Collection Directory**

4. Click **Save** to save the configurations and return to the **Metadata Management** interface, and click **Cancel** to return to the **Metadata Management** interface without saving any configurations.

   ***Note**: When you finish editing the metadata that is applied to existing services, click **Save and Update to All Applied Services** to save and update this metadata for the corresponding services.

Deleting Metadata

To delete a metadata, select a previously configured metadata, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected metadata, or click **Cancel** to return to the **Metadata Management** interface without deleting the selected property.

Configuring Execution Schedules

Use the Execution schedule feature to define when Governance Automation Online executes service requests.

To access **Execution Schedule** settings, in the **Settings** interface, click **Execution Schedule**.

Displaying and Searching Execution Schedules

To change the number of execution schedules displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the displayed execution schedules, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Execution Schedules

To create a new execution schedule, click **Create** on the ribbon. To modify a previously configured execution schedule, select the desired execution schedule, and click **Edit** on the ribbon.

On the interface for creating or editing an execution schedule, configure the following settings:

1. **Execution Schedule Name and Description** – Enter a desired **Name** for the execution schedule in the text box and enter an optional **Description** for the execution schedule for future reference.
2. **Define Execution Schedule** – Define an execution schedule for a service by selecting your desired days and hours. Then, click **Add to List** to add it to the execution schedule list below, or click **Clear Settings** to reset your execution schedule.
3. **Time Zone** – Select your time zone for the execution schedule.
4. Click **Save** to save the configurations and return to the **Execution Schedule** interface, or click **Cancel** to return to the **Execution Schedule** interface without saving any configurations.

Deleting Execution Schedules

To delete an execution schedule, select a previously configured execution schedule, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected execution schedule, or click **Cancel** to return to the **Execution Schedule** interface without deleting the selected execution schedule.

Configuring Questionnaires

Use Questionnaire Management to configure questionnaires to guide the requesters to appropriate services when starting a request. In a questionnaire, you can add your desired questions, define the order that the questions appear, customize the logical relationship for the questions, add the answer criterion, and select the services that will be visible to the requesters.

***Note**: The Questionnaire Management feature is not fully supported on Internet Explorer 8. To use this feature, AvePoint recommends that you use Google Chrome or Internet Explorer 9 or above to manage questionnaires.

To access **Questionnaire Management** settings, click **Questionnaire Management** in the **Request Management** group within **Settings**.

Displaying and Searching Questionnaires

To change the number of questionnaires displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the displayed questionnaire, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Questionnaires

To create a new questionnaire, click **Create** on the ribbon. To modify a previously configured questionnaire, select the desired questionnaire, and click **Edit** on the ribbon.

On the interface for creating or editing a questionnaire, configure the following settings:

1. **Name and Description** – Enter the name for the questionnaire that you are about to create. Enter an optional description for future reference.
2. **Language** – Choose the language for this questionnaire. When starting a request, the questionnaires can be filtered according to their languages.
3. **Questionnaire Category** – Categories are used to organize your questionnaires. Select an existing category from the drop-down list or create a new category for this questionnaire by clicking **Create New** then configuring the new category in the **Create Category** interface.
4. **Questionnaire Permissions** – Choose **Allow all users to use this questionnaire** to allow this questionnaire be viewed by any user, or specify the users or Office 365 groups that have permissions to access this questionnaire by choosing **Select users/groups to use this questionnaire** and entering the names of the users or groups in the text box. Press **Enter** to check whether or not the names are valid.
5. Click the arrow on the right-hand side to proceed to the next step.
6. **Questions** – Define the questions for this questionnaire.
    - To create a new question, click **Add Question** and then configure the following settings in the **Add Question** interface.
        i. **Question** – Enter your desired question and select the answer type, **Drop-down Menu**, **Radio Buttons**, or **Managed metadata**.

        ii. **Map to Metadata** – Choose whether to map the question to metadata on the service. If you select the **Map to metadata** checkbox, the answer to the question will be automatically set as the mapped metadata field value in the request form. If you select the checkbox, choose one of the following options:

            Save this question as new metadata – Choose this option to save the question entered above as new metadata. You must enter a metadata name in the text box. Then, enter a description for future reference.

            Select from existing metadata – Choose this option to map the question to existing metadata selected from the drop-down list.

        iii. **Answer Settings** – Define the answers for the question. Enter each answer on a separate line. You can also define a default answer for the question.

            ***Note**: If you map the question to existing metadata, this field is invisible.

        iv. Click **Save** to save this question.

- To edit a previously created question, click the edit ( ) button after the question name and then modify the settings in the **Edit Question** interface.
- To delete a previously created question, click the delete ( ) button after the question name.

7. Click the arrow on the right-hand side to proceed to the next step.
8. Follow the steps below to configure the logic diagram.
   a. Drag your desired question from the left pane to the Start point of the right pane.
   b. Drag another question under the arrow of one answer for the question above to determine the logical relationship.
   c. Repeat the step above to add multiple questions.

      ***Note**: You can add the same question to multiple logical flows on the right pane, but a question can only be added into a logical flow once.

   d. Drag your desired service to the end point of each logical flow
   e. If there are no services that fit the logical flow, click **Add End Points Automatically** to end all points with **No Service**. For the **No Service** end point, you are allowed to define a custom message that helps the requester find proper solutions if there is no service available to the requester.

      i. Click the edit ( ) button next to the **No Service** end point. The **Custom Message** window appears.
      ii. In the text box, enter the message that will be displayed to the requester.
      iii. Click **Save** on the ribbon to save your configuration.

      The previously created questions and the services in the left pane are supported to search. Enter the keyword of the question name or service name in the text box under **Questions** or **Services** and click the search ( ) button to search it.

      Click the remove ( ) button to remove a question from the logic diagram.

9. When you have finished configuring settings for this questionnaire, choose one of the following options:
   - Click the arrow on the left-hand side to go to previous steps to review and modify your configurations.
   - Click **Save As Draft** to save the questionnaire as a draft and return to the **Questionnaire Management** interface.
   - Click **Save and Activate** to save all of the configurations and activate this questionnaire.

- Click **Cancel** to return to the **Questionnaire Management** interface without saving any configurations.

Activating, Deactivating, Copying, and Deleting Questionnaires

To activate an inactive questionnaire, select the questionnaire, and then click **Edit** on the ribbon. Review the questionnaire settings, and then click **Save and Activate**.

To deactivate an active questionnaire, select the questionnaire, and then click **Deactivate** on the ribbon.

To duplicate an existing questionnaire to make minor changes in order to save as a new questionnaire, select a questionnaire and click **Copy** on the ribbon. Then, make the desired modifications.

To delete a questionnaire, select a previously configured questionnaire, and then click **Delete** on the ribbon. A confirmation window appears asking if you are sure you want to proceed with the deletion. Click **OK** to delete the selected questionnaire, or click **Cancel** to return to the **Questionnaire Management** interface without deleting the selected questionnaire.

Configuring Reminder Profiles for Upcoming Expiration

Use reminder profiles to send notification e-mails to task assignees before tasks expire.

To access **Reminder Profile for Upcoming Expiration** settings, click **Reminder Profile for Upcoming Expiration** in the **Request Management** group within **Settings**.

Displaying and Searching Reminder Profiles

To change the number of reminder profiles displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the displayed reminder profiles, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Reminder Profiles

To create a new reminder profile, click **Create** on the ribbon. To modify a previously configured reminder profile, select the profile, and click **Edit** on the ribbon.

On the interface for creating or editing a reminder profile, configure the following settings:

1. **Name and Description** – Enter a desired **Name** for the reminder profile in the text box and enter an optional **Description** for the reminder profile for future reference.
2. **Task Reminder Settings** – Configure the following task reminder settings:
    a. **E-mail template** – Select an e-mail template that will be used to send the notification e-mail.
    b. **Send the notification e-mail in advance by** – Enter a number in the text box and select **Day(s)**, **Week(s)**, or **Month(s)** as the unit.

c. **Enable recurrent reminder** – You can choose to enable recurrent reminder to re-send the notification e-mail in schedule. Select the checkbox and enter a number in the text box to define the schedule.

3. Click **Save** on the ribbon to save your configurations.

Deleting Reminder Profiles

To delete a reminder profile, select the profile, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected profile, or click **Cancel** to return to the **Reminder Profile for Upcoming Expiration** window without deleting the selected profile.

Configuring Site Collection Automated Locking Profiles

Use the site collection automated locking profiles to lock the site collection in “no access” status if the automated lifecycle tasks are not completed after a specified period.

To access the **Site Collection Automated Locking Profile Management** window, click **Site Collection Automated Locking Profile Management** in the **Request Management** group within **Settings**.

Displaying and Searching Site Collection Automated Locking Profiles

To change the number of site collection automated locking profiles displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the displayed site collection automated locking profiles, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Site Collection Automated Locking Profiles

To create a new site collection automated locking profile, click **Create** on the ribbon. To modify a previously configured site collection automated locking profile, select the desired site collection automated locking profile, and click **Edit** on the ribbon.

On the interface for creating or editing a site collection automated locking profile, configure the following settings:

1. **Name and Description** – Enter a name and an optional description for the site collection automated locking profile.
2. **Site Collection Automated Locking** – Configure the following settings for locking site collections.
   a. Choose one of the following locking types:
      - **Lock the site collection in "no access" status**
      - **Lock the site collection in "read-only" status**
   b. Define the condition to lock site collections. Enter a number in the text box and select **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit. If the automated lifecycle task is not

completed after the specified amount of time, the site collection will be locked in "no access" or "read-only" status.

You can also enable the following options:

- **Enable reminder before the site collection is locked** – Select the checkbox to enable reminder before the site collection is locked. Select a reminder profile from the drop-down list. You can also click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Configuring Reminder Profiles for Upcoming Expiration.
- **Notify the following people when the site collection is locked** – Select the checkbox to notify users or Office 365 groups when the site collection is locked. Enter the names of the users or Office 365 groups that will be notified about the site collection locking. You can also enter following roles: **$Primary Site Collection Contact**, **$Secondary Site Collection Contact**, and **$Primary Site Collection Administrator**.

  Then, select an e-mail template form the **E-mail template** drop-down list.

- **Start an additional site collection lifecycle action to escalate** – Select the checkbox to generate a site collection lifecycle action task after the site collection is locked at a certain time. Enter a number in the text box and select **Day(s)**, **Week(s)**, **Month(s)**, or **Year(s)** as the unit. Select **Delete Site Collection** or **Archive Site Collection** as the lifecycle action from the drop-down list. If you select either of the checkboxes, you can also configure the following settings:
  - **Use a unique approval process for this automated action** – Select a unique approval process instead of the default one for the lifecycle action task. Select an approval process from the drop-down list or click **Create New** to create a new approval process. If the configurations of the selected approval process do not meet your requirements, click **Create From This Existing Approval Process** to create a new one on the basis of the selected approval process.
  - **Enable reminder for the approvers about the site collection escalation before generating the lifecycle action task** – Select this checkbox to send notification e-mails to approvers about the site collection escalation before the lifecycle action task is generated. Select a reminder profile from the drop-down list. You can also click **Create New** to create a new one. For more information about configuring a reminder profile, refer to Configuring Reminder Profiles for Upcoming Expiration.

3. **Custom Action** – If you enabled reminder before the site collection is locked, the custom action is available. The custom action is defined via the methods that exist in a published Web Service. When the reminder for upcoming site collection locking is triggered for the first time, the custom action is executed. After the site collection is locked, the custom action ceases its execution.

   Select the **Enable custom action along with the upcoming site collection locking reminder** checkbox and complete the following steps:

   a. Enter the URL of your published Web Service in the **Web Service Address** text box.

b. Click **Retrieve** to retrieve the methods in the Web Service.

c. Select your desired method from drop-down list.

d. If there are parameters defined in the selected method, the parameters are displayed in a table. Enter the value for each parameter in the corresponding text box.

4. Click **Save** to save you configurations and return to the **Site Collection Automated Locking Profile Management** interface or click **Cancel** to return to the **Site Collection Automated Locking Profile Management** interface without saving any configurations.

Deleting Site Collection Automated Locking Profiles

To delete a site collection automated locking profile, select the profile, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected profile, or click **Cancel** to return to the **Site Collection Automated Locking Profile Management** window without deleting the selected profile.

Configuring Text Validation Rules

Configure text validation rules to set regular expressions. The rules can be applied to **Single line of text** or **Multiple lines of text** metadata. When end users enter values for these **Single line of text** or **Multiple lines of text** on the request page, the metadata values will be validated according to the regular expressions defined in the text validation rules.

To access the **Text Validation Rule Management** window, click **Text Validation Rule Management** in the **Request Management** group within **Settings**.

Displaying and Searching Text Validation Rules

To change the number of text validation rules displayed, use the **Show rows** drop-down list in the upper-right corner.

To search the displayed text validation rules, enter the keyword in the **Search** text box and click the search ( ) button.

Creating or Editing Text Validation Rules

To create a new text validation rule, click **Create** on the ribbon. To modify a previously configured text validation rule, select the desired rule, and click **Edit** on the ribbon.

In the interface for creating or editing a text validation rule, configure the following settings:

1. **Name and Description** – Enter a name and an optional description for the text validation rule.
2. **Rule Settings** – Configure the following rule settings:

   a. **Regular expression** – Enter a regular expression for this rule.

   ***Note**: The regular expression is validated according to the JavaScript language style here. A regular expression consists of the regular expression body and expression

options. In addition, the regular expression body must start with the character **/** and end with the character **/**.

For example, if you want to validate that the entered content matches three case-insensitive letters, the regular expression should be **/^[A-Z]{3}$/i**.

For more information about the regular expression, refer to the following articles:

http://msdn.microsoft.com/en-us/library/ie/h6e2eb7w(v=vs.94).aspx

https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Regular_Expressions?redirectlocale=en-US&redirectslug=JavaScript%2FGuide%2FRegular_Expressions

b. **Display message for invalid content** – Enter the message that will be displayed to the user if the entered content is invalid.

c. **Validation test** (optional) – Enter content in the text box and then click **Validation Test** to test the expected behavior of the entered regular expression.

3. Click **Save** to save the configurations and return to the **Text Validation Rule Management** interface, or click **Cancel** to return to the **Text Validation Rule Management** interface without saving any configurations.

Deleting Text Validation Rules

To delete a text validation rule, select a configured rule, and then click **Delete** on the ribbon. A confirmation window appears and asks if you are sure you want to proceed with the deletion. Click **OK** to delete the selected rule, or click **Cancel** to return to the **Text Validation Rule Management** window without deleting the selected rule.

Managing the Monitoring Reports

Monitoring Reports allows administrators to manage the settings and detailed information for all requests, tasks, and recertification reports created by and assigned to any user.

To access **Monitoring Reports**, go to the **Monitoring Reports** group in **Settings**.

All Requests

All Requests centralize all of the submitted service requests created by any users, providing you with one interface to process all of the requests.

To access **All Requests**, click **All Requests** in the **Monitoring Reports** group within **Settings**. Click **Back** to go back to the **Settings** interface.

You may change the number of requests displayed per page, as well the order they are displayed. To change the number of requests displayed per page, select the desired number from the **Show rows**

drop-down list in the upper-right corner. To sort the requests, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the requests are displayed in a number of different ways:

- Search – Filters displayed service requests by your entered keyword. You can search desired service requests by the following columns: **Service Request**, **Service** and **Assign To**. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter item ( ) – Filters which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

You can perform the following actions in **All Requests**:

- View Details – Click a request summary to see its configuration.
- **Cancel Request** – Select a request which you wish to cancel and click **Cancel Request** on the ribbon.
- **Delete** – Select the request that you wish to delete and click **Delete** on the ribbon.

All Tasks

All Tasks centralize all of the tasks assigned to any users, providing you with one interface to process all current tasks or review previous tasks.

To access **All Tasks**, click **All Tasks** in the **Monitoring Reports** group within **Settings**. To exit out of All Tasks, click **Back**.

You can change the number of tasks displayed per page, as well the order they are displayed in. To change the number of tasks displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the tasks, click the sort ( ) button in a column heading then select **Ascending** or **Descending**.

You can customize how the tasks are displayed in a number of different ways:

- Search – Filters displayed tasks by your entered keyword. You can search desired tasks by the following columns: **Title**, **Requester**, and **Assign To**. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.

- Filter items ( ) – Filters which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Approving or Rejecting Requests

You can approve or reject the following types of requests:

- Create Site Collection
- Create Site
- Create Library/List
- Create User
- Create Group
- Deploy Patterns
- Site Collection Lifecycle Management – Archive Site Collection
- Site Collection Lifecycle Management – Delete Site Collection
- Site Collection Lifecycle Management – Extend Site Collection Lease
- Site Collection Lifecycle Management – Change Site Collection Policy
- Site Collection Lifecycle Management – Change Site Collection Quota
- Site Collection Lifecycle Management – Unlock Site Collection
- Site Collection Lifecycle Management – Lock Site Collection
- Site Lifecycle Management – Archive Site
- Site Lifecycle Management – Delete Site
- User Lifecycle Management – Offboard Office 365 User
- User Lifecycle Management – Extend Office 365 User Contract
- User Lifecycle Management – Change Office 365 User Policy
- User Lifecycle Management – Unlock Office 365 User
- Group Lifecycle Management – Delete Office 365 Group
- Group Lifecycle Management – Extend Office 365 Group Lease
- Group Lifecycle Management – Change Office 365 Group Policy
- Group Lifecycle Management – Change Office 365 Group Team Site Quota
- Change Site Collection Contact or Administrator
- Change Site Collection Settings
- Change Site Contact

- Change Site Settings
- Change Library/List Settings
- Change User Properties
- Change Group Settings
- Content Move
- Change Permissions
- Grant Permissions
- Clone or Transfer User Permissions

1. Click a request summary to view more information about the request. The **View Details** window appears.
2. In the **View Details** window, you have the following options:
   - **Edit Request** – Click **Edit Request** on the ribbon to edit all of the settings of this request in the **Edit Request** window.

     ***Note**: This button is only visible to the approvers when **Allow approvers to edit this service request** is selected in the corresponding service.

   - **View Request History** – Click **View Request History** to view the versions of this request in the **View Request History** window.
3. Click **Approve** or **Reject** on the ribbon. Enter any comments you may have in the pop-up window.
4. Click **OK** to confirm or click **Cancel** to return to the **All Tasks** page without executing the task.

Reassigning Tasks

You can reassign a task to another approver if **Allow approvers to reassign tasks to others** is enabled in the approval process. All types of tasks, except for election tasks and error tasks, can be reassigned. To reassign a task, follow the steps below:

1. Select a task, and click **Reassign** on the ribbon.
2. In the pop-up window, enter the name of a user or group that will become the approver.
3. Click **OK** to confirm.

Managing Automatic Site Collection Lifecycle Management Tasks

When a site collection's inactivity threshold or lease period is exceeded, a Site Collection Lifecycle Management task is automatically generated and assigned to the approver. For the automatically generated tasks, besides the basic task information, you can view the **Lifecycle Action History** field to view the chosen lifecycle actions of the previous approval stages. Only the last approver's chosen lifecycle action will take effect. You can perform the following actions on the automatic Site Collection Lifecycle Management task. Note the following:

- These actions will be available only when the corresponding lifecycle actions are enabled in site collection policies and when the built-in Site Collection Lifecycle Management services are active.
- If **Yes/No (check box)** metadata with the **Enable Terms and Conditions Agreement** option enabled has been added to a built-in Site Collection Lifecycle Management service, you must choose **Yes** as the value for this metadata, when you manage the lifecycle of the site collection. Otherwise, the lifecycle action cannot be performed to the site collection.

Perform the following actions on the automatic Site Collection Lifecycle Management task:

- **Continue Access** – Select a task, and click **Continue Access** on the ribbon to execute the Extend Site Collection task. In the pop-up window, click **OK** to execute the task or **Cancel** to return to the **All Tasks** interface.
- **Archive** – Select a task, and click **Archive** on the ribbon to execute the site collection archival task. If metadata has been added to the Site Collection Lifecycle Management - Archive Service, the **Archive Site Collection** window will appear. In the pop-up window, you can enter comments for the site collection archival and modify the metadata values. Then, click **Submit** and a pop-up window appears asking you to confirm the site collection archival. Click **OK** to confirm the action, or click **Cancel** to return to the **All Tasks** interface.
- **Extend** – Select a task and click **Extend** on the ribbon to extend the lease for the site collection in this task. The **Extend Site Collection Lease Period** window appears. In the pop-up window, you can enter comments for the site collection lease extension. The lease extension period is displayed if the IT Admin has defined it; if the field is available to configure, define the amount of time to extend the lease period. Enter a number in the text box, then, select a time unit from the drop-down list.

  If metadata has been added to the Site Collection Lifecycle Management – Extend Service, you can modify the metadata values. Then click **Submit** and a pop-up window appears asking you to confirm the site collection lease extension. Click **OK** to confirm the action or **Cancel** to return to the **All Tasks** interface.

- **Delete** – Select a task, and click **Delete** on the ribbon to execute the Delete Entire Site Collection task. If metadata has been added to the Site Collection Lifecycle Management – Delete Service, the **Delete Site Collection** window will appear. In the pop-up window, you can enter comments for the site collection deletion, and modify the metadata values. Then, click **Submit** and a pop-up window appears asking you to confirm the site collection deletion. Click **OK** to execute the task, or click **Cancel** to return to the **All Tasks** interface.
- **Change Policy** – Select a task and click **Change Policy** on the ribbon to change the policy for the site collection in this task. The **Change Site Collection Policy** window appears. In the pop-up window, you can enter comments for the site collection policy change, and select a site collection policy that you want to apply to the site collection from the drop-down list. If metadata has been added to the Site Collection Lifecycle Management – Change Policy Service, you can modify the metadata values. Then, click **Submit** and a

pop-up window appears asking you to confirm the site collection policy change. Click **OK** to confirm the action or **Cancel** to return to the **All Tasks** interface.

Managing Automatic User Lifecycle Management Task

When the contract term of an Office 365 user has expired or the last contract extension has expired, a User Lifecycle Management task about user contract expiration is automatically generated and assigned to the approver. You can perform the following actions on the task:

- **Extend** – Select the task and click **Extend** on the ribbon. A pop-up window appears.
  i. The extended user contract term is displayed if your IT Admin has configured it. If allowed, you can define the extended user contract term.
  ii. Enter some comments for this task for further reference.
  iii. Click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface without executing the task.
- **Offboard** – Select the task and click **Extend** on the ribbon. A pop-up window appears. Choose one of the following options:
  - **Delete the Office 365 user**

    If you choose this option, you must change the administrator of this deleted user's OneDrive for Business. Enter a username in the text box and press **Enter** to check whether or not the name is valid.

    Then, enter some comments for this task for further reference, and click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface without executing the task.
  - **Block the Office 365 user**

    If you choose this option, you must assign a user who will receive a copy of e-mails sent to this blocked user. Enter a username in the text box and press **Enter** to check whether or not the name is valid.

    Then, enter some comments for this task for further reference, and click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface without executing the task.
  - **Reset the Office 365 user's password**

    If you choose this option, you must assign a user who will receive the new password. Enter a username in the text box and press **Enter** to check whether or not the name is valid. You may also click the browse ( ) button to search for users.

Then, enter some comments for this task for further reference, and click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface without executing the task.

Managing Automatic Group Lifecycle Management Tasks

When the lease of an Office 365 group has expired or the last lease extension has expired, a Group Lifecycle Management task about group lease expiration is automatically generated and assigned to the approver. You can perform the following actions on the task:

- **Delete** – Select the task and click **Delete** on the ribbon. In the pop-up window, enter some comments for this task for further reference, and click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface without executing the task.
- **Extend** – Select the task and click **Extend** on the ribbon. A pop-up window appears.
    i. The extended group lease period is displayed if your IT Admin has configured it. If allowed, you can define the extended group lease period.
    ii. Enter some comments for this task for further reference.
    iii. Click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface without executing the task.

Change and Clone or Transfer Permissions Tasks

You can perform the following actions on the tasks from Change Permissions and Clone or Transfer User Permissions services:

- View Task – Click a task title to see detailed information. In the **View Details** interface, you have the following options:
    - **Submit** – Click **Submit** on the ribbon to finish this task.
    - **Reject** – Click **Reject** on the ribbon to reject this task.
    - **Review the Report** – Review detailed report of this task. Choose one of the following options:

        View on screen – Open the report directly to view details on screen. If you view details of a Change Permissions task, refer to Reviewing Permissions.

        Download report – Download the report and then modify the data that you wish to change. In the pop-up window, click **Browse** to select the modified file to upload.
    - **Edit Request** (This button is only visible to the approvers when **Allow approvers to edit this service request** is selected in the corresponding service) – Click **Edit Request** on the ribbon to edit all of the settings of this request in the **Edit Request** interface.

    - **View Request History** – Click **View Request History** to view the versions of this request in the **View Request History** interface.

- **Submit** – Select a task, and click **Submit** on the ribbon to submit the task. Enter some comments for this task for further reference in the pop-up window. Click **OK** to finish this task or **Cancel** to return to the **All Tasks** interface.
- **Reject** – Select a task, and click **Reject** on the ribbon to reject the task. Enter some comments for this task for further reference in the pop-up window. Click **OK** to finish this task, or click **Cancel** to return to the **All Tasks** interface.

Reviewing Permissions

If you view details of a Change Permissions task, you can perform the following actions:

- Filter Records – Select **User Based** or **Object Based** from the drop-down list in the top left-hand corner. By default, **All Results** is selected.
- **Submit** – Click **Submit** on the ribbon to submit the task and apply all of your configurations to SharePoint.
- **Reset** – Click **Reset** on the ribbon to select **Reset My Changes** or **Reset All Changes**.
    - **Reset My Changes** – Your changes on the task will be cleared.
    - **Reset All Changes** – All users' changes on the task will be cleared.
- **Export Report** – Click **Export Report** on the ribbon to export the permission review report. In the **Export Report** window, choose to export the report to local machine or export the report to an export location, and select a report format (**CSV** or **XLS**). Then, click **Export to Datasheet** to export the report.
- **Edit User Permissions** – Select a user and click **Edit User Permissions**. In the **Edit Permissions** interface, modify the permission levels in the **Permissions** section. Then, click **Save** on the ribbon to save your changes and go back to the **View Details** page. The edited record is highlighted.
- **Remove User Permissions** – Select a user and click **Remove User Permissions**. A pop-up window appears which asks you to confirm your operation. Click **OK** to remove the user's permissions.
- **Delete User** – Select a user and click **Delete User**. A pop-up window appears which asks you to confirm your deletion. Click **OK** to delete the selected user.
- **Edit Group Permissions** – Select a group and click **Edit Group Permissions**. In the **Edit Permissions** interface, modify the permission levels in the **Permissions** section. Then, click **Save** to save your changes and go back to the **View Details** page. The edited record is highlighted.
- **Remove Group Permissions** – Select a group and click **Remove Group Permissions**. A pop-up window appears which asks you to confirm your operation. Click **OK** to remove the group's permissions and go back to the **View Details** page. The edited record is highlighted.

- **Delete User** – Click the display name of a group and you are brought to a new window. Select one or more group users and click **Delete User** on the ribbon. A pop-up window appears which asks you to confirm your deletion. Click **OK** to delete the selected users.
- **Remove User From Group** – Click the display name of a group and you are brought to a new window. Select one or more group users and click **Remove User From Group** on the ribbon. A pop-up window appears which asks you to confirm your operation. Click **OK** to remove the selected users from the group.
- **Change Group** – Click the display name of a group and you are brought to a new window. Select one or more group users and click **Change Group** on the ribbon.

  In the **Change Group** interface, select the group that you wish to change to and select the method for changing group, **Copy** or **Move**. Copy will copy the users to the new group. **Move** will remove the users from the previous group and then add the users to the new group. Click **Save** to save your changes and go back to the **View Details** page. The edited record is highlighted.

Managing Manual Archive Tasks

When there is site collection content that meets the Archiver rule, a manual archiver task will be generated. You can perform the following actions to the manual archive tasks:

- **View Task** – Click a task title to see detailed information. In the **View Details** window, you can perform the following actions:
  - **Submit** – Click **Submit** on the ribbon to submit the site collection content archival task. Enter comments in the pop-up window, then, click **OK** to submit the task or click **Cancel** to return to the **View Details** window without making any changes.
  - **Reassign** – Click **Reassign** on the ribbon to reassign the site collection content archival task. Enter the username of the user to whom you want to reassign the task in the pop-up window, then, click **OK** to reassign the task or click **Cancel** to return to the **View Details** window without making any changes.
  - **Review** – Click **Review** on the ribbon, and the **Review the Report** window appears. By default, all objects in the report will be archived.

    If you do not want to archive a specific object, select **Reject** from the drop-down list under the **Action** column of the object.

    If you do not want to archive some of these objects, select the objects and click **Reject** on the ribbon.

    When you finish, click **Finish** on the ribbon to confirm your action or click **Cancel** to return to the **View Details** window without making any changes.
- **Reassign** – Select a site collection content archival task and click **Reassign** on the ribbon to reassign the task. Enter the username of the user to whom you want to reassign the task in the pop-up window. Then, click **OK** to reassign the task or click **Cancel** to return to the **All Tasks** page without making any changes.

Election Tasks: Triggered from Site Collection Report

When an election process is started in a **Site Collection Report**, an election task is generated and assigned to the nominees.

You can perform the following actions on an election task:

- View Task – Click a task title to see the task details. In the **View Details** page, you have the following options:
    - **Claim** – Click **Claim** to become the primary site collection contact. In the pop-up window, define a user as the secondary site collection contact by entering a username in the text box. Then, click **OK** to save your configurations.

      Decline – Click **Decline** to decline to become the primary site collection contact. A pop-up window appears to ask for your confirmation. Click **OK** to confirm your action.
- **Claim** – Select a task and click **Claim** to become the primary site collection contact. In the pop-up window, define a user as the secondary site collection contact by entering a username in the text box. Then, click **OK** to save your configurations.
- **Decline** – Select a task and click **Decline** to decline to become the primary site collection contact. A pop-up window appears to ask for your confirmation. Click **OK** to confirm your action.

Election Tasks: Deactivated Contact Election for Site Collection

The deactivated contact election will be enabled on a site collection when a site collection policy with the **Automatically start the ownership election process if either of the site collection contact is deactivated** feature enabled is applied to the site collection. If the primary site collection contact is deactivated, refer to Election Tasks: Triggered from Site Collection Report. If the secondary site collection contact is deactivated, a deactivated contact election task will be generated and assigned to the primary site collection contact. The primary site collection contact can perform the following actions on the deactivated contact election task:

- **View Task** – Click a task title to see the task details. In the **View Details** page, click **Specify Secondary Contact** to directly define a user as the secondary site collection contact by entering their username in the text box. Then, click **OK** to save the configurations.
- **Specify Secondary Contact** – Select a task and click **Specify Secondary Contact** to directly define a user to be the secondary site collection contact. In the pop-up window, define a user as the secondary site collection contact by entering a username in the text box. Then, click **OK** to save the configurations.

Error Tasks

You can perform the following actions on the error tasks assigned to administrators:

- View Task – Click a task title to see detailed information. In the **View Details** interface, you have the following options:
    - **Retry** – Click **Retry** on the ribbon to re-run the failed section.
    - **Skip** – Click **Skip** to continue the workflow past the failed section.
    - **View Request History** – Click **View Request History** to view the versions of this request in the **View Request History** interface.
- **Retry** – For a task which contains failed section, click the select (☑) button before a task title to select it, and then click **Retry** on the ribbon to re-run the failed section.
- **Skip** – For a task which contains failed section, click the select (☑) button before a task title to select it, and then click **Skip** on the ribbon to continue the workflow past the failed section.

If an error task is generated due to disabled SharePoint Online Custom Script settings, enable Custom Script settings and then retry the error task. For more information about Custom Script settings and how to enable Custom Script settings, refer to Viewing Job Status.

All Recertification Reports

All Recertification Reports centralize all of the recertification tasks assigned to any users, providing you with one interface to process all recertification tasks.

To access **All Recertification Reports**, click **All Recertification Reports** in the **Monitoring Reports** group within **Settings**. To exit out of All Recertification Reports, click **Back**.

On the top of the **All Recertification Reports** interface, a message appears to remind you that Governance Automation Online will keep one year of historical information for the tasks. If you want to store the tasks older than one year, click the **select an export location** link in the message to store the tasks in an export location.

You can change the number of tasks displayed per page, as well the order they are displayed in. To change the number of tasks displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the tasks, click the sort (⇅) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the tasks are displayed in a number of different ways:

- Search – Filters displayed tasks by your entered keyword. You can search desired tasks by the following columns: **Request Summary**, **Requester**, and **Assign To**. Only the content in the column displayed in the current view can be searched.
- Manage columns (⊞) – Manages which columns are displayed in the list. Click the manage columns (⊞) button, then select the checkbox next to the column name to have that column shown in the list.

- Filter items ( ) – Filters which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Permission Recertification Tasks

When a recertification profile with permission recertification enabled is selected in a site collection policy and the site collection policy is applied to a Governance Automation Online managed site collection, a permission recertification task will be generated for the site collection. This task contains the searched permissions of users and groups for this site collection. Approvers can then modify the permissions in Governance Automation Online and the permission changes will be updated to SharePoint Online.

When a recertification profile with permission recertification enabled is selected in an Office 365 group policy and the Office 365 group policy is applied to a Governance Automation Online managed Office 365 group, a permission recertification task will be generated for the Office 365 group. This task contains the searched user permissions and SharePoint group permissions to the corresponding group team site. Approvers can then modify the permissions in Governance Automation Online and permission changes will be updated to Office 365.

You can perform the following actions on the permission recertification task:

- View Task – Click a request summary to see detailed information. In the task details page, you have the following options:
  - Filter Records – Select **User Based** or **Object Based** from the drop-down list in the top left-hand corner. By default, **All Results** is selected.
  - **Back** – Click **Back** on the ribbon to return to the **All Recertification Reports** page.
  - **Submit** – Click **Submit** on the ribbon to submit the changes and apply all of your configurations to SharePoint Online or to Office 365.
  - **Reassign** – Click **Reassign** on the ribbon to reassign the permission recertification task to another user.
  - **Reject** – Click **Reject** on the ribbon to finish the permission recertification task without making any changes.
  - **Reset** – Click **Reset** on the ribbon to select **Reset My Changes** or **Reset All Changes**.

    Reset My Changes – Your changes on the task will be cleared.

    Reset All Changes – All users' changes on the task will be cleared.
  - **Export Report** (for site collection permission recertification tasks only) – Click **Export Report** on the ribbon to export the permission recertification report. In the **Export Report** window, choose to export the report to local machine or export the report to an export location, and select a report format (**CSV** or **XLS**). Click **Export to Datasheet** to export the report.

- **View History** – Click **View History** to view the previous versions of the task.
- **Delete User** – Select a user and click **Delete User**. A pop-up window appears which asks you to confirm your deletion. Click **OK** to delete the selected user, or click **Cancel** to not make any changes.
- **Edit User Permissions** – Select a user and click **Edit User Permissions** on the ribbon. In the **Edit Permissions** interface, modify the permission levels in the **Permissions** section. Then, click **Save** on the ribbon to save your changes and go back to the **View Details** page. The edited record is highlighted.
- **Remove User Permissions** – Select a user and click **Remove User Permissions**. A pop-up window appears which asks you to confirm your operation. Click **OK** to remove the user's permissions, or click **Cancel** to not make any changes.
- **Edit Group Permissions** (for site collection permission recertification tasks only) – Select a group and click **Edit Group Permissions** on the ribbon. In the **Edit Permissions** interface, modify the permission levels in the **Permissions** section. Then, click **Save** to save your changes and go back to the **View Details** page. The edited record is highlighted.
- **Remove Group Permissions** (for site collection permission recertification tasks only) – Select a group and click **Remove Group Permissions**. A pop-up window appears which asks you to confirm your operation. Click **OK** to remove the group's permissions and go back to the **View Details** page. The edited record is highlighted.
- **Delete User** – Click the display name of a group and you are brought to a new window. Select one or more group users and click **Delete User** on the ribbon. A pop-up window appears which asks you to confirm your deletion. Click **OK** to delete the selected users, or click **Cancel** to not make any changes.
- **Remove User From Group** – Click the display name of a group and you are brought to a new window. Select one or more group users and click **Remove User From Group** on the ribbon. A pop-up window appears which asks you to confirm your operation. Click **OK** to remove the selected users from the group, or click **Cancel** to not make any changes.
- **Change Group** – Click the display name of a group and you are brought to a new window. Select one or more group users and click **Change Group** on the ribbon.

  In the **Change Group** interface, select the group that you wish to change to and select the method for changing group, **Copy** or **Move**. Copy will copy the users to the new group. **Move** will remove the users from the previous group and then add the users to the new group. Click **Save** to save your changes and go back to the **View Details** page. The edited record is highlighted.

- **Remove File Group** (for Office 365 group permission recertification tasks only) – If an Office 365 group team site has any file that is shared with other users via the **Get a link** function, the permission recertification task will contain a SharePoint group, which is used for sharing the file via a link. Users that only have the permission to view the file are placed to the group whose name

follows the format of **View File Group – [File Name]**. Users that have the permission to edit the file are placed to the group whose name follows the format of **Edit File Group – [File Name]**. You can select one of the groups and click **Remove File Group** on the ribbon. A pop-up window appears asking for your confirmation. If you click **OK**, the file is not shared with the group members any more, and the group is also removed from the permission recertification task.

- **Submit** – Select a task and click **Submit** on the ribbon to submit changes of the task. Enter comments for this task for further reference in the pop-up window. Click **OK** to finish this task or click **Cancel** to return to the **All Recertification Report** interface.
- **Reassign** – Select a task and click **Reassign** on the ribbon to reassign the permission recertification task to another user.
- **Reject** – Select a task and click **Reject** on the ribbon to finish the permission recertification task without making any changes.
- **Refresh** – Click **Refresh** on the ribbon to refresh the recertification task page.

Metadata Recertification Tasks

When a recertification profile with metadata recertification enabled is selected in a site collection policy and the site collection policy is applied to a Governance Automation Online managed site collection, a metadata recertification task will be generated. This task contains the searched metadata of this site collection. Approvers can then modify the metadata values in Governance Automation Online and the metadata value changes will be updated to SharePoint Online.

You can perform the following actions on the metadata recertification task:

- View Task – Click a request summary to see detailed information. In the task details page, you have the following options:
    - **Edit** – Select a metadata name and click **Edit** on the ribbon. In the **Edit** window, modify the metadata value, then click **Save** to save your changes.
    - **Add** – If you are allowed to add metadata to the site collection, click **Add** on the ribbon. The **Add Metadata** window appears. Select a metadata name and click **Add to List** to add the new metadata.
    - **Delete** – If you are allowed to delete metadata from the site collection, select a metadata name and click **Delete** on the ribbon.
    - **Submit** – Click **Submit** on the ribbon to submit the changes and apply all of your configurations to SharePoint Online.
    - **Reassign** – Click **Reassign** on the ribbon to reassign the metadata recertification task to another user.
    - **Reject** – Click **Reject** on the ribbon to finish the metadata recertification task without making any changes.
    - **Reset** – Click **Reset** on the ribbon to select **Reset My Changes** or **Reset All Changes**.

Reset My Changes – Your changes on the task will be cleared.

Reset All Changes – All users' changes on the task will be cleared.

- **View History** – Click **View History** on the ribbon to view the version history of the metadata recertification task.
- **Review All Metadata** – Click **Review All Metadata** on the ribbon. A pop-up window appears displaying all searched metadata. Review the metadata and modify the metadata value if necessary. Then, click **Save** to save all changes.

  ***Note**: If you have changed metadata values and you navigate to the **Review All Metadata** window again before you submit the task, the metadata that had value changes will be marked with the **Edited** label.

- **Submit** – Select a task and click **Submit** on the ribbon to submit changes of the task. Enter comments for this task for further reference in the pop-up window. Click **OK** to finish this task or click **Cancel** to return to the **All Recertification Reports** interface.
- **Reassign** – Select a task and click **Reassign** on the ribbon to reassign the task to another user.
- **Reject** – Select a task and click **Reject** on the ribbon to reject the metadata recertification task.
- **Refresh** – Click **Refresh** on the ribbon to refresh the recertification task page.

Ownership Recertification Tasks

When a recertification profile with ownership recertification enabled is selected in a site collection policy and the site collection policy is applied to a Governance Automation Online managed site collection, an ownership recertification task will be generated. This task is an election task. Approvers can claim or decline to become the primary site collection contact.

You can perform the following actions on the ownership recertification task:

- View Task – Click a request summary to see detailed information. In the task details page, you have the following options:
  - **Back** – Click **Back** to return to the **All Recertification Reports** page.
  - **Claim** – Click **Claim** to become the primary site collection contact. In the pop-up window, define a user as the secondary site collection contact by entering a username in the text box. Then, click **OK** to save your configurations.
  - **Decline** – Click **Decline** to decline to become the primary site collection contact. A pop-up window appears to ask for your confirmation. Click **OK** to confirm your action.
- **Claim** – Select a report and click **Claim** to become the primary site collection contact. In the pop-up window, define a user as the secondary site collection contact by entering a username in the text box. Then, click **OK** to save your configurations.

- **Decline** – Select a report and click **Decline** to decline to become the primary site collection contact. A pop-up window appears to ask for your confirmation. Click **OK** to confirm your action.
- **Refresh** – Click **Refresh** to refresh the recertification reports page.

Membership Recertification Tasks

When a recertification profile with membership recertification enabled is selected in an Office 365 group policy and the Office 365 group policy is applied to a Governance Automation Online managed Office 365 group, a membership recertification task will be generated. This task contains the searched members and/or owners of the Office 365 group. Approvers can add members and/or owners to the group, remove members and/or owners from the group, promote group members to group owners, or demote group owners to group members. The membership changes will be updated to Office 365.

You can perform the following actions on the membership recertification task:

- View Task – Click a request summary to see detailed information in the task details page. You have the following options:
    - **Back** – Click **Back** on the ribbon to return to the **All Recertification Reports** page.
    - **Submit** – Click **Submit** on the ribbon to submit the changes and apply all of your configurations to Office 365.
    - **Reassign** – Click **Reassign** on the ribbon to reassign the membership recertification task to another user.
    - **Reject** – Click **Reject** on the ribbon to finish the membership recertification task without making any changes.
    - **Reset** – Click **Reset** on the ribbon to select **Reset My Changes** or **Reset All Changes**.

        Reset My Changes – Your changes on the task will be cleared.

        Reset All Changes – All users' changes on the task will be cleared.
    - **View History** – Click **View History** on the ribbon to view the previous versions of the task.
    - **Add Member** – Click **Add Member** on the ribbon and the **Add Member** window appears. Enter the username in the text box. Press **Enter** to check whether or not the name is valid. Click **Add** to add the member to the group or click **Cancel** to not make any changes.
    - **Add Owner** – Click **Add Owner** on the ribbon and the **Add Owner** window appears. Enter the username in the text box. Press **Enter** to check whether or not the name is valid. Click **Add** to add the owner to the group or click **Cancel** to not make any changes.

- **Promote to Owner** – Select a group member and click **Promote to Owner** on the ribbon to promote the member to the group owner. The promoted users are highlighted.
- **Demote to Member** – Select a group owner and click **Demote to Member** on the ribbon to demote the owner to the group member. The demoted users are highlighted.
- **Remove from Group** – Select a group member or a group owner and click **Remove from Group** on the ribbon to remove the user from the group. The removed users are stroke through with a red line.

- **Submit** – Select a task and click **Submit** on the ribbon to submit changes of the task. Enter comments for this task for further reference in the pop-up window. Click **OK** to finish this task or click **Cancel** to return to the **All Recertification Report** interface.
- **Reassign** – Select a task and click **Reassign** on the ribbon to reassign the permission recertification task to another user.
- **Reject** – Select a task and click **Reject** on the ribbon to finish the permission recertification task without making any changes.
- **Back** – Click **Back** on the ribbon to return to the **Settings** page.
- **Refresh** – Click **Refresh** on the ribbon to refresh the recertification task page.

Managing the Audit Reports

To access **Audit Reports**, go to the **Audit Reports** group in **Settings**.

Audit Reports provide detailed information on all users, service request and approval process activities:

- **User Activity Report** – Provides detailed information on all actions performed by Governance Automation Online users, including administrators and business users. User Activity Report allows you to inspect the behaviors done by users when errors occur for furnishing useful information, or check the legality of user behaviors.
- **Service Request Report** – Provides detailed information for all of the submitted service requests. Service Request Report gives you overall usage information of service requests, which you can gather for IT chargeback and budgeting.
- **Approval Process Report** – Provides all of the processing tracks of the approval processes for the service request once they are approved. Approval Process Report allows you to view the detailed information of service requests for reviewing the performances, which can help you optimize your service request flow and make the processes more efficient.

User Activity Report

To access **User Activity Report**, click **User Activity Report** in the **Audit Reports** group. Click **Back** to close the **User Activity Report** interface.

Managing User Activity Reports

To change the number of reports displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the reports, click the sort ( ) button in the **Changed Time** column, then select **Ascending** or **Descending**.

On the top of the **User Activity Report** interface, a message appears to remind that Governance Automation Online will keep one year of historical information for this report. If you want to store the records older than one year, click the **select an export location** link in the message to store the records in an export location.

You can customize how the reports are displayed in a number of different ways:

- Search – Filters displayed reports by your entered keyword. You can search desired reports by the following columns: **User** and **Object Instance Name**. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter Item ( ) – Filter which item in the list is displayed. Click the filter item ( ) button in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating User Activity Reports

To filter and generate user activity reports, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **Object**, **Type**, **Action**, **Time Range** and **User**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting User Activity Reports

To export the currently displayed reports, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Service Request Report

To access **Service Request Report**, click **Service Request Report** in the **Audit Reports** group. Click **Back** to close the **Service Request Report** interface.

Managing Service Request Reports

To change the number of reports displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the reports, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the reports are displayed in a number of different ways:

- Search – Filters displayed reports by your entered keyword. You can filter desired reports by the following columns: **Service Name**, **Request Summary**, **Requester** and **Assign To**. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter Item ( ) – Filters which item in the list is displayed. Click the filter item ( ) button in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating Service Request Reports

To filter and generate service request reports, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **Service Type, Service Name, Requester**, **Assign To**, **Time Range**, and **Department**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting Service Request Reports

To export the currently displayed reports, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Approval Process Report

To access **Approval Process Report**, click **Approval Process Report** in the **Audit Reports** group. Click **Back** to close the **Approval Process Report** interface.

Managing Approval Process Reports

To change the number of reports displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the reports, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the reports are displayed in a number of different ways:

- Search – Filters displayed reports by your entered keyword. You can search desired reports by the following columns: **Request Summary** and **User**. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter Item ( ) – Filters which item in the list is displayed. Click the filter item ( ) in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating Approval Process Reports

To filter and generate approval process reports, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **Service Type**, **Request Summary**, **Status**, **Time Range, Department**, and **User**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting Approval Process Reports

To export the currently displayed reports, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Managing the Administration Reports

Administration Reports provide basic information on all site collections, sites, Office 365 users, and Office 365 groups managed by Governance Automation Online:

- Site Collection Report – Provides a list of site collections managed by Governance Automation Online and the corresponding information, including site collection URL, department, title, policy, site collection template, primary site collection administrator, primary site collection contact, secondary site collection contact, and so on. You can customize how the report displays the data by configurable criteria.
- Site Report – Provides a list of sites managed by Governance Automation Online and the corresponding information, including site URL, department, title, site template, primary site contact, and secondary site contact. You can customize how the report displays the data by configurable criteria.
- User Report – Provides a list of Office 365 users managed by Governance Automation Online and the corresponding information, including display name, username, roles, manager, location, user policy, user contract term expiration time, date created, status, and so on. You can customize how the report displays the data by configurable criteria.

- Group Report – Provides a list of Office 365 groups managed by Governance Automation Online and the corresponding information, including group name, group ID, group owners, group policy, privacy, member subscription, group lease expiration time, created time, status, and so on. You can customize how the report displays the data by configurable criteria.

Site Collection Report

To access **Site Collection Report**, click **Site Collection Report** in the **Administrator Reports** group. Click **Back** to close the **Site Collection Report** interface.

Managing Site Collection Report

To change the number of site collections displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the site collections, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the site collections are displayed in a number of different ways:

- Search – Filters displayed site collections by your entered keyword. You can search desired site collections by the following columns: **URL**, **Title**, **Description**, **Primary Site Collection Administrator**, **Additional Site Collection Administrators**, **Primary Site Contact**, **Secondary Site Collection Contact**, and metadata. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Filters which item in the list is displayed. Click the filter items ( ) button in the column heading you want to filter, then check the checkbox next to the item name to have that item shown in the list.

Filtering and Generating Site Collection Report

To filter and generate site collection report, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **URL**, **Site Template**, **Site Collection Size**, **Status**, **Department**, **Policy**, and **Primary Site Collection Contact**. **Filter by Expiration Date** is also supported. Set **Inactivity Threshold Date** and **Lease Period Expiration Date** to add more filter rules.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting Site Collection Report

To export the currently displayed site collections, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Applying a Site Collection Policy

In Site Collection Report, you can apply a site collection policy to site collections in bulk.

Complete the following steps to apply a site collection policy:

1. Select one or more site collections and click **Apply Policy** on the ribbon.

   ***Note**: The Apply Policy feature is only available to active and without ongoing process site collections.

2. In the **Apply Policy** window, configure the following settings:

   a. **Site Collection Policy** – Select a site collection policy from the drop-down list. This site collection policy will be applied to the selected site collections.

   b. **Export Location** – Choose one of the following locations to store the apply site collection policy result report.

      - **Export to an export location** – Select a previously configured export location from the drop-down list or click **Add New Location** to create a new one.
      - **Export to a folder in SharePoint Online** – Enter the URL of a folder in SharePoint Online.

3. Click **Submit** to save your configurations and go back to the **Site Collection Report** interface. Governance Automation Online will start to apply the site collection policy in the backend. You can click **Refresh** on the ribbon to view the site collection policy name. When the target policy name is displayed under the **Policy** column, the site collection policy is applied successfully.

4. Go to the export location and you can view the apply site collection policy result report, including the following information: **URL**, **Initial Policy**, **Target Policy**, **Result**, and **Comment**.

Electing Site Collection Contacts

The election process provides an automated nomination process to determine the primary site collection contact and the secondary site collection contact. The election tasks will be assigned to the nominated users, who in turn will decide if they want to be accountable for the site collection and become the primary site collection contact. The secondary site collection contact will be defined by the primary site collection contact during the election process. For more information about the election process, refer to Managing the Election Process.

Complete the following steps to start the election process:

1. Select one or more site collections and click **Elect Contact** on the ribbon.
2. In the **Elect Contact** window, configure the following settings:

   a. **Election Task Title** – Enter the title for the election task that will be generated during the election process.

   b. **Exclude Users** (optional) – Enter the names of the users that will be excluded during the election process.

c. **E-mail Settings** (optional) – Choose to enable the following notifications by selecting the corresponding checkboxes:

   - **Notify the user when the election task is assigned** – Select the checkbox to send a notification e-mail to the user when the election task is assigned to this user.
   - **Notify the primary contact when the site collection is assigned** – Select the checkbox to send a notification e-mail to the user when this user becomes the primary site collection contact.
   - **Notify the secondary contact when the site collection is assigned** – Select the checkbox to send a notification e-mail to the user when this user becomes the secondary site collection contact.

   Each notification has a default e-mail template. You can also select a custom e-mail template.

d. **Duration** – Set the duration for each election stage. If the nominee does not handle the election task during the duration, the election task will be assigned to the nominee of next election stage. Enter a number in the text box, then select **Day(s)** or **Week(s)** as the unit.

   You can also notify the nominee before the assigned time is reached. Select the **Remind the nominated user before each nomination task expires** checkbox and select a reminder profile from the drop-down list. You can also click **Create New** to create a reminder profile. For more information, refer to Creating or Editing Reminder Profiles.

3. Click **Submit** to start the election process or click **Cancel** to go back to the **Site Collection Report** interface without starting the election process.

Specifying Site Collection Contacts

In Site Collection Report, you can define the primary site collection contact and the secondary site collection contact.

Complete the following steps to define the site collection contacts:

1. Select one or more site collections and click **Specify Contact** on the ribbon.

   a. **Primary Site Collection Contact** – Enter the name of the user that will become the primary site collection contact of the selected site collections.

      You can also send an e-mail to notify the user when the site collection is assigned to this user. Select the **Notify the primary contact when the site collection is assigned** checkbox and select an e-mail template from the drop-down list.

   b. **Secondary Site Collection Contact** – Enter the name of the user that will become the secondary site collection contact of the selected site collections.

You can also send an e-mail to notify the user when the site collection is assigned to this user. Select the **Notify the secondary contact when the site collection is assigned** checkbox and select an e-mail template from the drop-down list.

2. Click **Submit** to save your configurations or click **Cancel** to go back to the **Site Collection Report** interface without saving any configurations.

Sending E-mails to Site Collection Contacts

In Site Collection Report, you can send e-mails to site collection contacts. Refer to the following instructions:

- **Mail All Contacts** – If you want to send e-mails to contacts of all of the site collections in the site collection report, click **Mail All Contacts** on the ribbon. The new e-mail application on your computer is opened. The e-mail addresses of all of the site collection contacts are automatically filled. Enter your desired e-mail subject and body. Then, send the e-mail.
- **Mail Contacts** – If you want to send e-mail to contacts of certain site collections or of all of the site collections, select one or more site collections and click **Mail Contacts** on the ribbon. Then, select **Mail Contacts of Selected Site Collections** or **Mail Contacts of All Site Collections** from the drop-down list. The e-mail application on your computer is opened. The e-mail addresses of site collection contacts are automatically filled. Enter your desired e-mail subject and body. Then, send the e-mail.

Note that if the **Site Collection Report** page does not response after you click **Mail All Contacts**, **Mail Contacts of Selected Site Collection**, or **Mail Contacts of All Site Collections**, complete the following steps to resolve the issue:

1. Navigate to **Control Panel** of your computer and click **Programs**. The **Programs** window appears.
2. In the **Programs** window, click **Default Programs**. The **Default Programs** window appears.
3. In the **Default Programs** window, click **Associate a file type or protocol with a program**. The **Set Associations** window appears.
4. In the **Set Associations** window, select **MAIL TO** under the **Name** column, then, click the **Change program…** option.
5. Choose your desired e-mail application.

Site Report

To access **Site Report**, click **Site Report** in the **Administration Reports** group. Click **Back** to close the **Site Report** interface.

Managing Site Report

To change the number of sites displayed per page, select the desired number from the **Show rows** drop-down list in the upper right-hand corner. To sort the sites, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the sites are displayed in a number of different ways:

- Search – Filters displayed sites by your entered keyword. You can search desired sites by the following columns: **URL** and **Title**. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ), then select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Filters which item in the list is displayed. Click the filter items ( ) button in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating Site Report

To filter and generate site report, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **URL, Site Template**, **Department**, and **Primary Site Contact**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting Site Report

To export the currently displayed sites, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

User Report

To access **User Report**, click **User Report** in the **Administration Reports** group. Click **Back** to close the **User Report** page.

Managing User Report

You can customize how the users are displayed in a number of different ways:

- Sort ( ) – To sort users, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ), then select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Filters which item in the list is displayed. Click the filter items ( ) button in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating User Report

To filter and generate user report, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **Display Name**, **Status**, **Department**, **Manager**, **User Contract Term Expiration Time**, and **Created Time**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting User Report

To export the currently displayed users, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Group Report

To access **Group Report**, click **Group Report** in the **Administration Reports** group. Click **Back** to close the **Group Report** page.

Managing Group Report

You can customize how the groups are displayed in a number of different ways:

- Sort ( ) – To sort groups, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ), then select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Filters which item in the list is displayed. Click the filter items ( ) button in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating Group Report

To filter and generate group report, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **Group Name**, **Status**, **Group Owners**, **Group Lease Expiration Time**, and **Created Time**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting Group Report

To export the currently displayed groups, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Applying a Group Policy

In Group Report, you can apply a group policy to Office 365 groups in bulk.

Complete the following steps to apply a group policy:

1. Select one or more groups and click **Apply Policy** on the ribbon.

   ***Note**: The Apply Policy feature is only available to active and without ongoing process groups.

2. In the **Apply Policy** window, configure the following settings:

   a. **Group Policy** – Select a group policy from the drop-down list. The group policy will be applied to the selected groups.

   b. **Export Location** – Select a previously configured export location from the drop-down list or click **Add New Location** to create a new one. This export location will be used to store the apply group result report.

3. Click **Submit** to save your configurations and go back to the **Group Report** interface. Governance Automation Online will start to apply the group policy in the backend. You can click **Refresh** on the ribbon to view the group policy name. When the target policy name is displayed under the **Policy** column, the group policy is applied successfully.

4. Go to the export location and you can view the apply group policy result report, including the following information: **Group Name**, **Group ID**, **Initial Policy**, **Target Policy**, **Result**, and **Comment**.

Managing Dashboard

Governance Automation Online Dashboard allows you to monitor your SharePoint Online site collections, Office 365 users, Governance Automation Online user activities, and Governance Automation Online tasks via bar charts, line charts, and pie charts.

To access **Dashboard**, click **Dashboard** in the **Dashboard** group in **Settings**.

Dashboard provides the following built-in charts:

- **Site Collection Status** – Displays the statuses of all Governance Automation Online managed site collections.
- **Service Types of Tasks** – Displays the service types of all Governance Automation Online tasks.
- **Task Status Distribution** – Displays the status distribution of all Governance Automation Online tasks.

Creating a Chart

To create a new chart, click **Create New Chart** on the ribbon and select **Bar Chart**, **Line Chart**, or **Pie Chart**.

Creating a Bar Chart or Line Chart

In the **Create Bar Chart** or **Create Line Chart** window, configure the following settings:

1. **Chart Title and Description** – Enter a title and an optional description for the chart.
2. **Data Source** – Select a data source for the chart: **Site Collection Report**, **User Activity Report**, or **User Report**.

   ***Note**: The retrieved user activity data is within the time range set in User Activity Report's advanced filter.

3. **Axis** – Define the horizontal axis and vertical axis for the chart.
   - **Horizontal Axis** – Select one type of data that is retrieved from the data source. This data will be used as the horizontal axis of the chart.
   - **Vertical Axis** – Select **Quantity** as the vertical axis of the chart.
4. **Legend** – Choose whether or not to display the legend on the chart. If you choose **Yes**, configure the following settings:
   a. **Legend source** – Select one type of data from the data source as the legend source.
   b. **Legend entries** – Select one or more data values as the legend entries.

      ***Note**: You can select five legend entries at most.

5. Click **Save** on the ribbon to create the chart.

Creating a Pie Chart

In the **Create Pie Chart** window, configure the following settings:

1. **Chart Title and Description** – Enter a title and an optional description for the chart.
2. **Data Source** – Select a data source for the chart: **Site Collection Report**, **User Activity Report**, **All Tasks**, or **User Report**.

   ***Note**: The retrieved user activity data is from within the time range set in User Activity Report's advanced filter.

3. **Statistic** – Select one type of data that is retrieved from the data source. Values of the selected data will become the statistic displayed on the pie chart.
4. Click **Save** on the ribbon to create the chart.

Editing a Chart

To edit a chart, click the edit ( ) button at the upper-right corner of the chart. For more information about editing settings of a chart, refer to Creating a Chart.

Refreshing Charts

To refresh a chart, click the refresh ( ) button at the upper-right corner of the chart.

To refresh all charts, click **Refresh** on the ribbon.

Generating a Chart

If one of the following circumstances is met, a chart will be displayed with a time interval:

- The data source of the chart is **All Tasks**.
- The type of the data displayed on the chart is Date and Time.

You can click the calendar ( ) button to change start time and end time of the time interval, and then click **Generate Report** to generate the report for the new time interval.

Deleting a Chart

To delete a chart, click the delete ( ) button at the upper-right corner of the chart. A confirmation window appears and asks if you want to proceed with the deletion. Click **OK** to delete the chart, or click **Cancel** to return to the **Dashboard** interface without deleting the chart.

Requests and To-Do Lists

Governance Automation Online administrators can create services which contain a set of configured settings for SharePoint Online operations that comply with your organization's rules and standards. These services are tailored to the needs of different departments and purposes within your organization. You will be able to submit requests for these services according to your SharePoint Online needs. Once you submit a service request, the approval process associated with each corresponding service will automatically notify the designated persons in your organization of your request. After all approvers of a service have approved the request, Governance Automation Online will perform the necessary operations to complete the service you have requested.

If you are a designated approver for any service, a task will appear in your **My Tasks** list whenever a request for the service is submitted and any/all previous approvers have approved the request. If you are a designated approver for a permission recertification process, a permission recertification report will appear in your **My Recertification Report** list according to the recertification schedule.

Requests

Refer to the following sections to start a request and managed the submitted/saved requests.

Starting a Request

Services that you can request are displayed in your service catalog. You can submit a request by selecting a service and entering the relevant information.

To access the **Start a Request** interface, click **Start a Request** in the Administrator landing page. To search service requests, enter the service name keyword in the provided text box in the upper-right corner. You can also filter service requests according to the language by clicking the language filter button on the ribbon. Then, select the checkboxes next to the language names to have the services of these languages shown.

In the **Start a Request** interface:

1. Select a service by clicking the service name.
2. Enter the necessary information as indicated in the service request.
3. When completing the configurations, choose one of the following options:
    - Click **Save As Draft** to save the request as a draft and leave the configured settings for later use.
    - Click **Save and Submit** to submit this request to the approvers.
    - Click **Cancel** to return to the **Start a Request** interface without saving any configurations.

My Requests

In **My Requests**, all of your previously created Governance Automation Online requests are displayed, including **Submitting and Submitted Requests** and **Saved Requests**.

To manage the requests, click **View My Requests** in the Administrator landing page.

Click the **Submitting and Submitted Requests** or **Saved Requests** tab in the **My Requests** page to access the corresponding request type.

Submitting and Submitted Requests

In **Submitting and Submitted Requests**, all of the requests that are pending on validation and/or successfully submitted by you are displayed here. You may change the number of submitting and/or submitted requests displayed per page, as well the order they are displayed in. To change the number of submitting and/or submitted requests displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the submitting and/or submitted requests, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the submitted requests are displayed in a number of different ways:

- Search – Filters displayed service requests by your entered keyword. You can search desired service requests using the following columns: Service Request, Service, and Assign To. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the managed columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Filters which item in the list is displayed. Click the filter items ( ) button of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list.

You can perform the following actions to submitting and/or submitted requests:

- View Details – Click a request summary of a submitted request to see detailed information. Close the interface to return to the **My Requests** interface.
- **Copy** – Duplicate the existing service request to make minor changes in order to submit as a new service request. Select a submitted request or a request whose status is **Did Not Pass Request Validation**. Click **Copy** on the ribbon, and make the desired modifications.

  When you have finished making changes, choose one of the following options:

  - Click **Save As Draft** to save the new service request as a draft.
  - Click **Save and Submit** to submit this request to the approvers.

    - Click **Cancel** to return to the **My Requests** interface without saving any configurations.

- **Cancel Request** – Select a submitted request that you wish to cancel and click **Cancel Request** on the ribbon.

Saved Requests

In **Saved Requests**, all of the requests saved by you without submitting are displayed here. You may change the number of saved requests displayed per page, as well the order they are displayed in. To change the number of saved requests displayed per page, select the desired number from the **Show rows** drop-down list in the upper right-hand corner. To sort the saved requests, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the saved requests are displayed in a number of different ways:

- Search – Filters displayed service requests by your entered keyword. You can search desired service requests using the following columns: Service Request and Service. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter items ( ) – Filters which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, and then select the checkbox next to the item name to have that item shown in the list.

You can perform the following actions in saved requests:

- View Details – Click a request summary to see detailed information.
- **Edit** – Select a saved request by clicking the select ( ) button before a service request summary, and click **Edit** on the ribbon to edit the settings of this request. When completing the configurations, click **Save** to save all of the settings, or click **Save and Submit** to submit this request to the approvers, or click **Cancel** to return to the **My Request** interface without saving any configurations.
- **Delete** – Select a saved request by clicking the select ( ) button before a service request summary, and click **Delete** on the ribbon. A pop-up window appears asking for your confirmation. Click **OK** to delete the selected request, or click **Cancel** to return to the My Request interface without deleting the selected request.
- **Copy** – Duplicate the existing service request to make minor changes in order to save as a new service request. Select a submitted request. Click **Copy** on the ribbon, and make the desired modifications.

  When you have finished making changes, choose one of the following options:

    - Click **Save As Draft** to save the new service request as a draft.
    - Click **Save and Submit** to submit this request to the approvers.

- Click **Cancel** to return to the **My Requests** interface without saving any configurations.

My To-Do List

When a service request is submitted and you are one of the approvers of this request, a task will be assigned to you. When you are the approver of a permission recertification process and the recertification schedule reaches, a permission recertification report will be assigned to you.

To view and manage your tasks and permission recertification reports, click **View My To-Do List** in the Administrator landing page.

My Tasks

In the **My Tasks** tab, all of the tasks assigned to you are displayed here. You may change the number of tasks displayed per page, as well the order they are displayed in. To change the number of tasks displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the tasks, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the tasks are displayed in a number of different ways:

- Search – Filters displayed Tasks by your entered keyword. You can search desired Tasks by the following columns: Title and Requester. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the managed columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter item ( ) – Allows you to filter which item in the list is displayed. Click the filter item ( ) button of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list.

For more information about each task type, refer to the instructions in All Tasks.

My Recertification Report

My Recertification Report is a report of recertification tasks that are assigned to you. In the **My Recertification Report** tab, all of the permission recertification tasks, metadata recertification tasks, ownership recertification tasks, and membership recertification tasks are displayed.

You may change the number of reports displayed per page, as well the order they are displayed in. To change the number of reports displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the reports, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the reports are displayed in a number of different ways:

- Search – Allows you to filter reports displayed by the keyword you designate. The **Request Summary** column supports being searched, and only the content in the column displayed in the current view can be searched.
- Manage Columns ( ) – You can manage which columns are displayed in the list so that only information you want to see is displayed. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter ( ) – This allows you to filter which item in the list is displayed. Click the filter ( ) button of the column you want to filter, and then select the checkbox next to the item name to have that item shown in the list.

For more information about dealing with recertification tasks, refer to Permission Recertification Tasks, Metadata Recertification Tasks, Ownership Recertification Tasks, and Membership Recertification Tasks.

Public Site Collection Directory

The Public Site Collection Directory allows business users to monitor business ownership and usage. Site collections with the **Publish to Directory** metadata value **Yes** are considered as published site collections. For more information, refer to Configuring Metadata.

To access the **Public Site Collection Directory**, click **Public Site Collection Directory** in the Administrator landing page.

Managing Public Site Collection Directory Reports

To change the number of the directory reports displayed per page, select the desired number from the **Show rows** drop-down list in the upper-right corner. To sort the directory reports, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the directory reports are displayed in a number of different ways:

- Search – Filters the displayed directory reports by your entered keyword. You can search desired reports by the following columns: **URL**, **Title**, **Description**, **Primary Site Collection Administrator**, **Additional Site Collection Administrators**, **Primary Site Collection Contact**, **Secondary Site Collection Contact**, and metadata. Only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – Manages which columns are displayed in the list. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.
- Filter item ( ) – Filters which item in the list is displayed. Click the filter item ( ) button in the column heading you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Filtering and Generating Public Site Collection Directory Reports

To filter and generate public site collection directory reports, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the directory report. You can set filters for **URL**, **Site Template, Site Collection Size**, **Status**, **Department**, **Policy**, and **Primary Site Collection Contact**. **Filter by Expiration Date** is also supported. Set **Inactivity Threshold Date** and **Lease Period Expiration Date** to add more filter rules.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting Public Site Collection Directory Reports

To export the currently displayed directory reports, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

My Sites

My Sites displays a list of site collections for which the login user is the primary site collection contact/secondary site collection contact/primary site collection administrator and a list of sites for which the login user is the primary site contact or secondary site contact.

To access **My Sites**, click **My Sites** in the **Home Page**.

Managing My Sites Reports

To change the number of reports displayed per page, select the desired number from the Show rows drop-down list in the upper right-hand corner. To sort the reports, click the sort ( ) button in a column heading, then select **Ascending** or **Descending**.

You can customize how the reports are displayed in a number of different ways:

- Search – Allow you to filter reports displayed by the keyword you designate. The **Title**, **URL**, **Primary Contact**, **Secondary Contact**, and **Primary Site Collection Administrator** columns support to search for the desired reports, and only the content in the column displayed in the current view can be searched.
- Manage columns ( ) – You can manage which columns are displayed in the list so that only information you want to see is displayed. Click the manage columns ( ) button, then select the checkbox next to the column name to have that column shown in the list.

Filtering and Generating My Sites Reports

To filter and generate reports, complete the following steps:

1. Click **Set Filter** on the ribbon to customize the report. You can set filters for **URL**, **Department**, **Policy**, and **Primary Contact**.
2. To set new filter rules, click **Reset** and the previous filter rules are cleared to the default ones.
3. Click **Generate Report** to retrieve data for your report. You can also click **Export to Datasheet** to export the report to a local path or an export location. For more information about exporting the report, refer to Exporting Reports.

Exporting My Sites Reports

To export the currently displayed reports, click **Export Report** on the ribbon. For instructions about exporting the report, refer to Exporting Reports.

Managing Lifecycle of My Sites

You can manage lifecycle of site collections displayed in **My Sites** report by performing the following actions. Note the following:

- These actions will be available only when the corresponding lifecycle actions are enabled in site collection policies and when the built-in Site Collection Lifecycle Management services are active.
- If **Yes/No (check box)** metadata with the **Enable Terms and Conditions Agreement** option enabled has been added to a built-in Site Collection Lifecycle Management service, you must choose **Yes** as the value for this metadata, when you manage the lifecycle of the site collection. Otherwise, the lifecycle action cannot be performed to the site collection.

Perform the following actions to manage the lifecycle of site collections:

- **Archive** – Select a site collection and click **Archive** on the ribbon to archive the site collection. If metadata has been added to the Site Collection Lifecycle Management - Archive Service, the **Archive Site Collection** window will appear. You can modify the metadata values. Then, click **Submit** and a pop-up window appears asking you to confirm the site collection archival. Click **OK** to archive the site collection, or click **Cancel** to not archive the site collection.
- **Delete** – Select a site collection and click **Delete** on the ribbon to delete this site collection. If metadata has been added to the Site Collection Lifecycle Management - Delete Service, the **Delete Site Collection** window will appear. You can modify the metadata values. Then, click **Submit** and a pop-up window appears asking you to confirm the site collection deletion. Click **OK** to delete the site collection, or click **Cancel** to not delete the site collection.
- **Lock** – Select a site collection and click **Lock** on the ribbon to lock the site collection.
  - If you are allowed to select the locking type, the **Lock Site Collection** window will appear. Choose one of the following locking types:

    Lock the site collection in "no access" status

    Lock the site collection in "read-only" status
  - If metadata has been added to the Site Collection Lifecycle Management - Lock Service, the **Lock Site Collection** window will appear. You can modify the metadata values.

  Then, click **Submit** and a pop-up window appears asking you to confirm the site collection locking. Click **OK** to lock the site collection, or click **Cancel** to not lock the site collection.
- **Unlock** – Select a locked site collection and click **Unlock** on the ribbon to unlock the site collection. If metadata has been added to the Site Collection Lifecycle Management - Unlock Service, the **Unlock Site Collection** window will appear. You can modify the

metadata values. Then, click **Submit** and a pop-up window appears asking you to confirm the site collection unlocking. Click **OK** to unlock the site collection, or click **Cancel** to not unlock the site collection.

- **Extend** – Select a site collection and click **Extend** on the ribbon to extend the site collection lease period. The **Extend Site Collection Lease Period** window appears.
    - The lease extension period is displayed if the IT Admin has defined it; if the field is available to configure, define the amount of time to extend the lease period. Enter a number in the text box, then, select a time unit from the drop-down list.
    - If metadata has been added to the Site Collection Lifecycle Management – Extend Service, you can modify the metadata values.

  Then, click **Submit** and a pop-up window appears asking you to confirm the site collection lease period extension. Click **OK** to extend the site collection lease period, or click **Cancel** to not extend the site collection lease period.

- **Change Policy** – Select a site collection and click **Change Policy** on the ribbon to change the site collection policy. The **Change Site Collection Policy** window appears.
    - Select a site collection policy that you want to apply to the site collection from the drop-down list.
    - If metadata has been added to the Site Collection Lifecycle Management – Change Policy Service, you can modify the metadata values.

  Then, click **Submit** and a pop-up window appears asking you to confirm the site collection policy change. Click **OK** to change the site collection policy, or click **Cancel** to not change the site collection policy.

- **Change Quota** – Select a site collection and click **Change Quota** on the ribbon to change the resources allocated to the site collection. The **Change Site Collection Quota** window appears.
    - Enter a number in the text box as the new storage quota size.
    - If metadata has been added to the Site Collection Lifecycle Management – Change Quota Service, you can modify the metadata values.

  Then, click **Submit** and a pop-up window appears asking you to confirm the site collection quota change. Click **OK** to change the site collection quota, or click **Cancel** to not change the site collection quota.

Starting a Request for a Site Collection

When viewing reports in My Sites, you can start a request for a specific site collection.

1. Select a site collection and click **Start a Request** on the ribbon. The **Start a Request** window appears.
2. You may need to select a service type from the drop-down list and click **OK**.

3. The service catalog appears displaying the selected type of services that meet all of the following conditions:
    - Services that you are assigned the permission to use.
    - Services that you are assigned the permission to submit requests for.
    - Services that contain the selected site collection in the service scope.

Exporting Reports

In Governance Automation Online, you are allowed to export the following reports:

- User Activity Report
- Service Request Report
- Approval Process Report
- Site Collection Report
- Site Report
- Public Site Collection Directory Report
- My Sites Report

In the **Export Report** window of each report, configure the following settings:

1. **Report Export Location** – Choose the location of the exported report.
    - **Export to a local path** – Export the report locally to your computer.
    - **Export to an export location** – Export the report to an export location on Microsoft Azure.
2. If you choose **Export to an export location**, select a location from the drop-down list, or click **Add New Location**. You will be redirected to the **New Report Export Location** interface.
3. **Report Format** – Select either **CSV** or **XLS** as the report format from the drop-down list.
4. Click **Export to Datasheet** to export the report.

Inviting Support

For help using Governance Automation Online, you can invite a member of AvePoint Support to access your Governance Automation Online environment to help troubleshoot. To do this, complete the following steps:

1. In Governance Automation Online, click the invite support ( ) button on the upper-right corner. A pop-up window appears.
2. In the **Invite Support** window, configure the following settings:
    a. **Services** – Select the service types related to your issue from the drop-down list.
    b. **Issue Type** – Choose the type of issue you are requesting support for.
        - **General guidance** – Get general help using Governance Automation Online.
        - **Troubleshoot an issue** – Invite AvePoint Support to help you troubleshoot a problem with Governance Automation Online.
    c. **Severity** – Define the severity of the issue by selecting a level on the scrollbar (1=Trivial, 5=Critical).
    d. **Details** – Enter detailed information about your issue in the textbox, such as how often the issue appears, what actions were taken prior to the error occurring, or what operation you require guidance for.

    If the issue is related to a particular service, enter the corresponding service name in the text box. To add multiple service names, separate the service names with semicolon.

    e. **Attachment** – If you have a file that will help explain or resolve your issue, click **Browse** and select your file.

    ***Note**: The maximum file size is 25 MB.

    f. **Contact Option** – Choose your preferred method of contact.
        - **Phone** –Enter your phone number in the textbox.
        - **E-mail** –Enter your e-mail address in the textbox.
3. Click **Submit** on the ribbon. A pop-up window appears to provide the following information:
    - An account for AvePoint Technical Support will be automatically created in AvePoint Online Services. This account has the Application Administrator permission for Governance Automation Online.
    - AvePoint Technical Support team will have access to your application logs.

    Click **I agree** to finish the invitation process.

***Note:** After AvePoint Technical Support completes troubleshooting, the account for the support will remain in the Account Manager. To remove the account, an AvePoint Online Services Service Administrator can delete the account by navigating to **AvePoint Online Services** > **User Management** > **User-based View**, selecting the checkbox next to the Support's user ID, and then clicking **Delete** on the ribbon.

Submitting Feedback

To report bugs, offer feature suggestions, or provide comments about your Governance Automation Online experience, refer to the following steps:

1. In Governance Automation Online, click the submit feedback ( ) button on the upper-right corner.

   If you would like to be contacted by an AvePoint representative after submitting feedback, select the **Would you like to be contacted by an AvePoint representative in regards to your issue?** checkbox at the top of the window.

2. Provide feedback in one or all of the three available feedback tabs: Bug Report, Interface Improvement, and Feature Suggestion. Refer to the appropriate section below for further details.

Bug Report

In the **Bug Report** tab, provide detailed information about the bug that you want to report:

1. **Service Types** – Select the types of services you were using when you found the bug/error. Select the checkboxes before the service types in the drop-down list.
2. **Bug Type** – Choose the type of the bug, **Logic** or **User Interface**.
3. **Severity** – Define the severity of the bug (1=Trivial, 5=Critical) by selecting a level on the scroll bar.
4. **Details** – Enter your own description to tell us the details of the bug (for example, how often the bug appears, what process the bug affects, and what actions were performed before the bug appears).
5. Click **Send Now** to submit your feedback.

Interface Improvement

In the **Interface Improvement** tab, you can provide feedback about your experience with the interface:

1. **Tree and Interface Performance** – Choose your evaluation for the performance of the data tree interface and SharePoint Online functions.
2. **How would you describe the DocAve Governance Automation Online Interface?** – Choose your evaluation of the DocAve Governance Automation Online interface.
3. **Additional Feedback** – Enter any additional feedback that you want to share with us in the provided text box.
4. Click **Send Now** to submit your feedback.

Feature Suggestion

In the **Feature Suggestion** tab, you can provide suggestions on any of our product features.

1. **Service Type** – Select the types of services that you would like to improve. Select the checkboxes before the service types in the drop-down list.
2. **Your Suggestion** – Enter your suggestion for the feature in the text box, providing as much detail as possible.
3. Click **Send Now** to submit your feedback.

Governance Automation Online Web API SDK

Create customizable, extendable, and programmable usage of Governance Automation Online functions by invoking the program interfaces provided by the Governance Automation Online Web API.

Getting Started

Refer to the sections below for important information on getting started with Governance Automation Online Web API.

Environment Requirements

For Governance Automation Online Web API SDK, the .NET Framework version must be v4.5 or later.

Help Page

Go to the Governance Automation Online Web API Help Page to view methods and examples for using the Governance Automation Online Web API.

Supported Features in Governance Automation Online Web API

The following features are supported by the Governance Automation Online Web API:

***Note**: All service types are supported.

- Get a list of activated services that the login user has the permission to use
- Get a service through a specific service ID
- Create a request that is dependent on a posted request model
- Get a request through a specific request ID
- Update a request
- Submit a request by request ID
- Cancel a request by request ID
- Get a list of requests that the login user has created
- View Site Collection Report – Get a list of all Governance Automation Online managed site collections
- View Site Report – Get a list of all Governance Automation Online managed sites

Implementing Governance Automation Online API

Refer to the following example to get a list of requests created by the login user through Governance Automation Online API.

Logging into Governance Automation Online

To log into Governance Automation Online, refer to the following example.

The `logOnurl` value is determined by the data center you selected when registering AvePoint Online Services.

- For US - East, use `https://eugaapi.avepointonlineservices.com/api/logon`.
- For EMEA - Ireland, use `https://negaapi.avepointonlineservices.com/api/logon`.
- For APAC - Singapore, use `https://apgaapi.avepointonlineservices.com/api/logon`.
- For APAC – Australia, use `https://asgaapi.avepointonlineservices.com/api/logon`.
- For USGov - Public Sector, use `https://gausgovapi.avepointonlineservices.com/api/logon`.
- For Japan West - Osaka, use `https://jpgaapi.avepointonlineservices.com/api/logon`

```
string logOnurl = " https://apgaapi.avepointonlineservices.com/api/logon";


var logonInfo = new

{

    userName = "someone@example.com",

    passWord = "12!@QW"

};


HttpWebRequest httpRequest = (HttpWebRequest)HttpWebRequest.Create(logOnurl);

httpRequest.ContentType = "application/json";

string reply = string.Empty;

ServicePointManager.ServerCertificateValidationCallback += ((sender, certificate,
chain, sslPolicyErrors) => true);

httpRequest.Method = "POST";
```

```
string content = JsonConvert.SerializeObject(logonInfo);

System.Text.UTF8Encoding encoding = new System.Text.UTF8Encoding();

byte[] data = encoding.GetBytes(content);

httpRequest.ContentLength = data.Length;

using (Stream requestStream = httpRequest.GetRequestStream())

{

    requestStream.Write(data, 0, data.Length);

}

HttpWebResponse response = (HttpWebResponse)httpRequest.GetResponse();

using (Stream responseStream = response.GetResponseStream())

{

    using (StreamReader responseReader = new StreamReader(responseStream,
Encoding.UTF8))

    {

        reply = responseReader.ReadToEnd();

    }

}

string token = JsonConvert.DeserializeObject(reply) as string;
```

Getting a List of Request Created by the Login User

Refer to the following example to get a list of requests created by the login user.

The `url` value is determined by the data center you selected when registering AvePoint Online Services.

- For US - East, use `https://eugaapi.avepointonlineservices.com/api/requests/get`.
- For EMEA - Ireland, use `https://negaapi.avepointonlineservices.com/api/requests/get`.
- For APAC - Singapore, use `https://apgaapi.avepointonlineservices.com/api/requests/get`.
- For APAC - Australia, use `https://asgaapi.avepointonlineservices.com/api/requests/get`.
- For USGov - Public Sector, use `https://gausgovapi.avepointonlineservices.com/api/requests/get`.

- For Japan West - Osaka, use `https://jpgaapi.avepointonlineservices.com/api/logon`

```
string url = " https://apgaapi.avepointonlineservices.com/api/requests/get";

HttpWebRequest httpRequest = (HttpWebRequest)HttpWebRequest.Create(url);

httpRequest.ContentType = "application/json";

string reply = string.Empty;

ServicePointManager.ServerCertificateValidationCallback += ((sender, certificate,
chain, sslPolicyErrors) => true);


httpRequest.Headers.Set("X_GovernanceAutomation_Access_Token", token);

httpRequest.Method = "GET";

HttpWebResponse response = (HttpWebResponse)httpRequest.GetResponse();

using (Stream responseStream = response.GetResponseStream())

{

    using (StreamReader responseReader = new StreamReader(responseStream,
Encoding.UTF8))

    {

        reply = responseReader.ReadToEnd();

    }

}

List<APIRequest> requests =
JsonConvert.DeserializeObject<IEnumerable<APIRequest>>(reply).ToList();
```

Appendix A: Using Custom Actions

To use the Custom Action feature in Governance Automation Online, there must be a published Web Service with defined methods. Refer to the following sections for detailed instructions:

1. Creating and Configuring a Web Service
2. Publishing a Web Service
3. Applying a Web Service to a Custom Action

Creating and Configuring a Web Service

To create and configure a Web Service, complete the following steps:

1. In Microsoft Visual Studio, navigate to **File** > **New** > **Project…**.
2. In the **New Project** window, navigate to **Templates** > **Visual C#** > **Web** on the left pane.
3. Select **.NET Framework 3.5** from the drop-down list on the top.
4. Select **ASP.NET Web Service Application** on the middle pane.

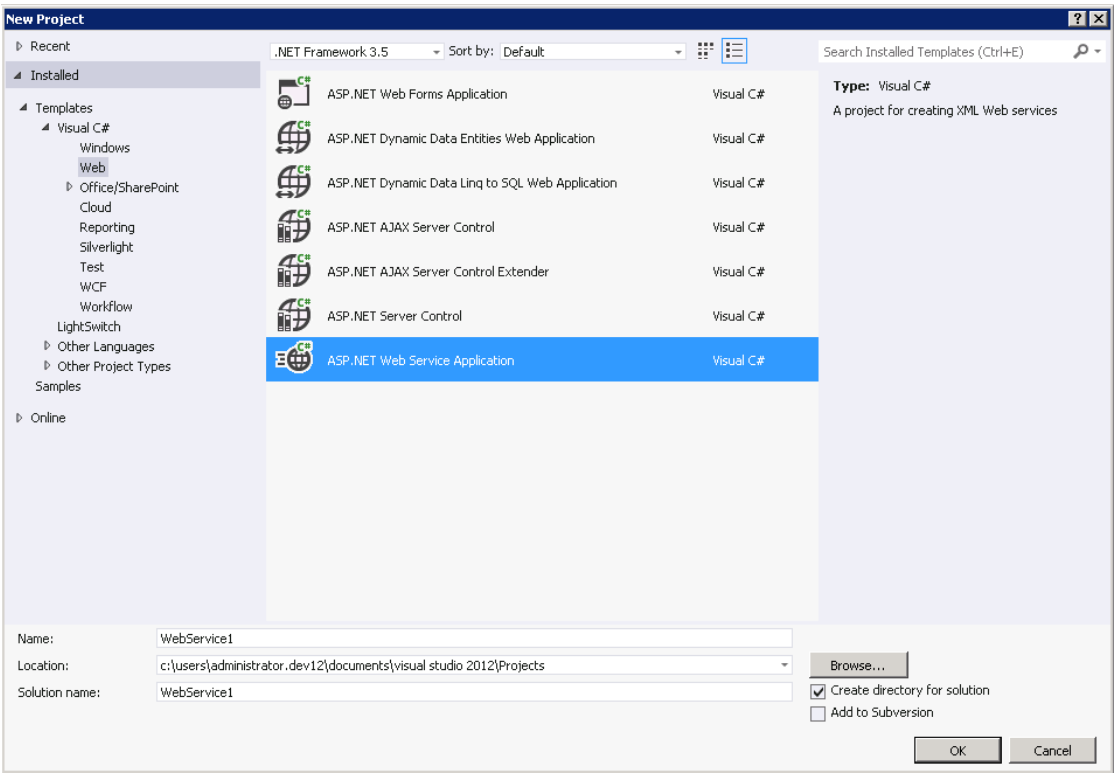

Figure 3: Creating a Web Service.

5. On the bottom, define the **Name**, **Location**, and **Solution name** for the Web Service.
6. Click **OK** to create the Web Service. The default Web Service **Service1.asmx.cs** appears.

7. In **Service1.asmx.cs**, define the method for your custom actions. The screenshot below shows the sample method.

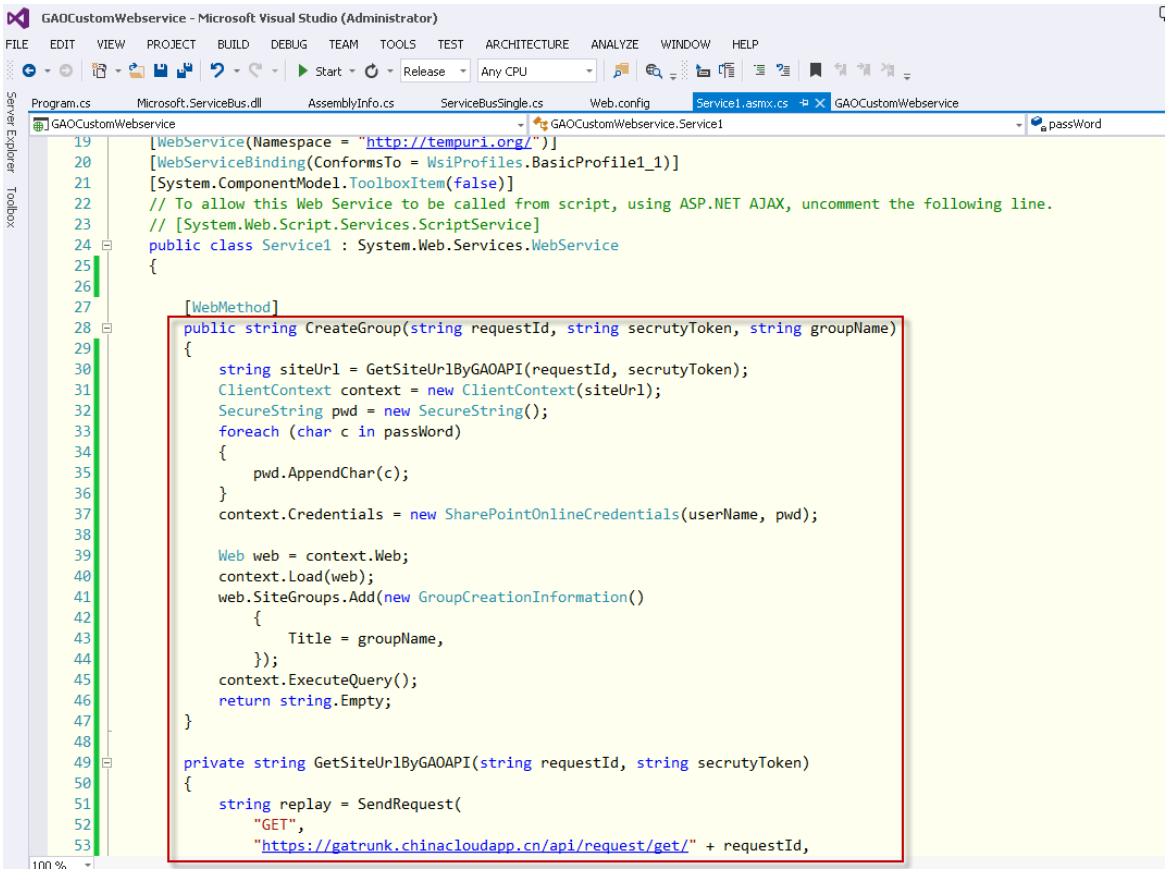

Figure 4: The sample method.

8. On the top of the method, add the **WebMethod** label.

9. On the right pane, click **Web.config**.

10. In **Web.config**, add the **<webServices>** node as the child node of the **<system.web>** node.
11. In the **<webServices>** node, add the access mode for the Web Service. The screenshot below shows an example.

```
<?xml version="1.0"?>
<configuration>
  <appSettings/>
  <connectionStrings/>
  <!--
    For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.

    The following attributes can be set on the <httpRuntime> tag.
      <system.Web>
        <httpRuntime targetFramework="4.5" />
      </system.Web>
  -->
  <system.web>
    <webServices>
      <protocols>
        <add name="HttpSoap"/>
        <add name="HttpPost"/>
        <add name="HttpGet"/>
        <add name="Documentation"/>
      </protocols>
    </webServices>
    <compilation debug="true" targetFramework="4.5"/>
    <authentication mode="Windows"/>
    <pages controlRenderingCompatibilityVersion="4.5" clientIDMode="AutoID"/>
  </system.web>
</configuration>
```

Figure 5: The sample access mode.

Publishing a Web Service

To publish a Web Service, complete the following steps:

1. In Microsoft Visual Studio, on the right pane, right-click the Web Service name and click **Publish…**.
2. In the **Publish Web** window, select **<New…>** from the **Select or import a publish profile** drop-down list.
3. In the **New Profile** window, enter a profile name and click **OK**.
4. In the **Connection** step, configure the following settings:
    a. **Publish method** – Select **File System** as the publish method.
    b. **Target location** – Select a directory as the location to store the published file.

5. Click **Next**.
6. In the **Settings** and **Preview** steps, keep the default configurations.
7. Click **Publish** to publish the Web Service file to the selected location.
8. Navigate to **Internet Information Services (IIS) Manager**.
9. Create an application pool for the Web Service.
    a. On the left pane, right-click the **Application Pools** node and click **Add Application Pool…**.
    b. In the **Add Application Pool** window, enter a name and select the **.NET Framework v4.0.30319** from the **.NET Framework version** drop-down list.
    c. Click **OK** to create the application pool.
10. Create a Web site to host the Web Service.
    a. On the left pane, right-click the **Sites** node and click **Add Web Site…**.
    b. In the **Add Web Site** window, configure the following settings:
        i. **Site Name** – Enter a name for the Web site.
        ii. **Application Pool** – Click **Select …** and select the application pool that is created in step 10 and step 11.
        iii. **Physical path** – Select the directory where the published Web Service file resides.
        iv. **Port** – Enter a port number for the Web site.

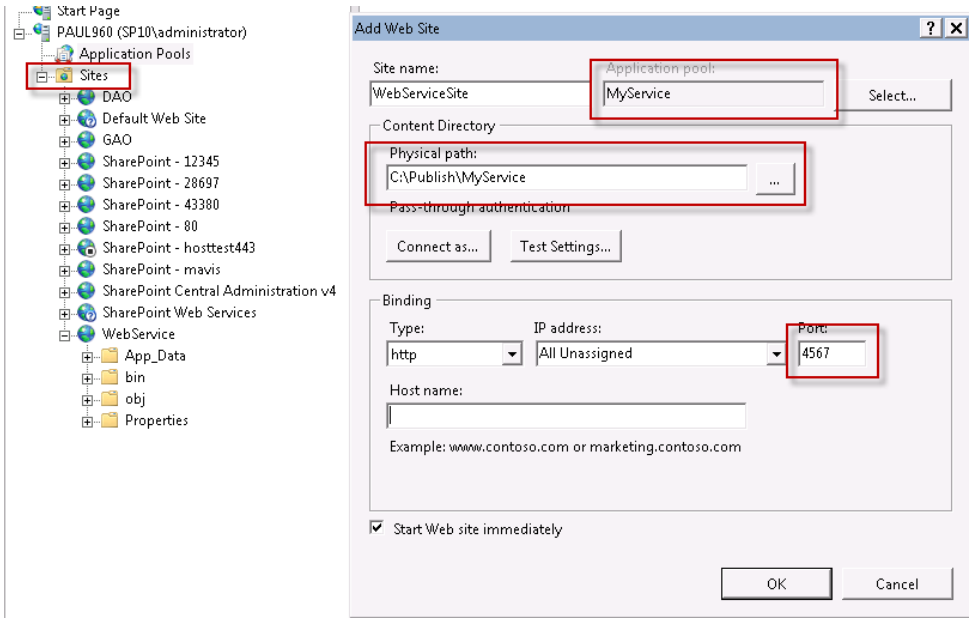

Figure 6: Creating a Web site.

v. Click **OK** to create the Web site.

Now you can access the Web Service by accessing the URL in the format of **[WebSiteAddress]+[ServiceName].asmx**.

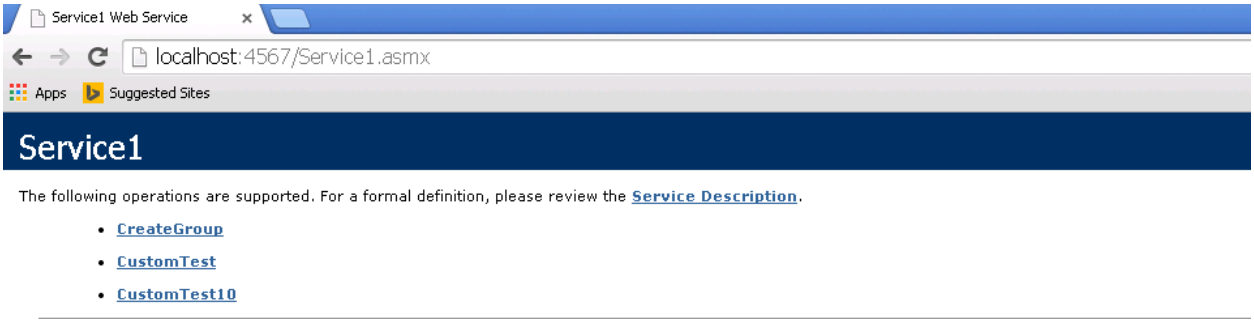

Figure 7: The sample Web Service.

Applying a Web Service to a Custom Action

To apply Web Service to a Governance Automation Online custom action, complete the following steps:

1. In the **Custom Action** section of a Governance Automation Online service, choose **Before approval**, **After approval**, or **After execution**.
2. In the **Web Service Address** text box, enter the URL of your published Web Service.
3. Select **Anonymous Access** or **Azure Active Directory Authentication** as the authentication type that will be used to access the Web service from the drop-down list. If you select **Azure Active Directory Authentication** as the authentication type, you must the Client ID of Azure Active Directory application in the text box.

   ***Note**: In order to use the Azure Active Directory account to access the Web service, you must configure your App service application first. Refer to the following Microsoft technical article to configure your App service application: https://azure.microsoft.com/en-us/documentation/articles/app-service-mobile-how-to-configure-active-directory-authentication/

4. Click **Retrieve** to retrieve the methods in the Web Service.
5. Select your desired method from the drop-down list. The parameters defined in the selected method are displayed in a table.
6. Choose one of the following options to define the parameter values:
   - Enter the value for a parameter in the text box.
   - Enter **$** and then select the custom metadata that is created in Governance Automation Online.

     When the custom metadata is applied to the service, the requester will define a value for the metadata. The defined metadata value will become the parameter value.

Governance Automation Online will send the parameter values to the Web Service and the parameter values will be used to execute the method in the Web Service.

The screenshot below details an example of a custom action:

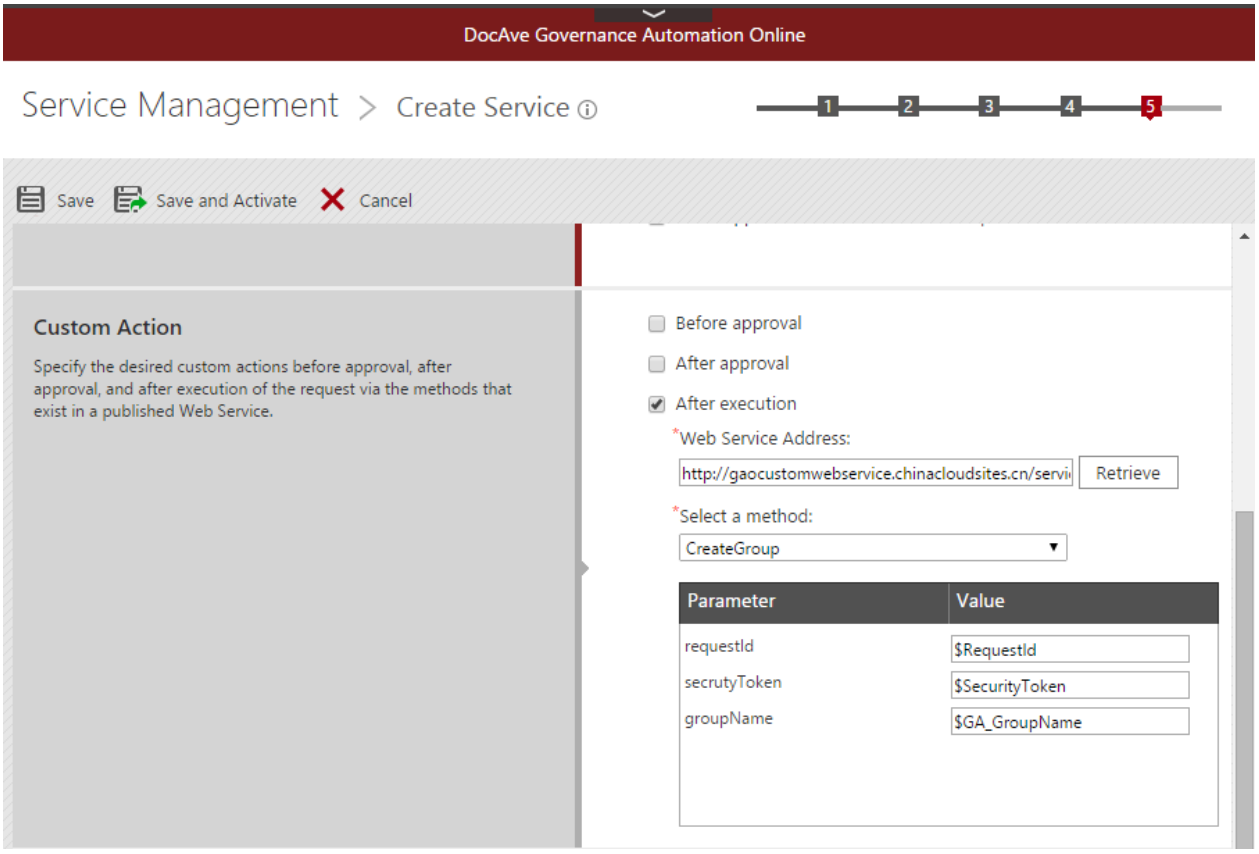

Figure 8: The sample custom action.

CreateGroup is selected as the method.

For the **groupName** parameter, the value of the **GA_GroupName** metadata is set to the parameter value.

In the sample request below, the requester enters **site1 group** as the value of the **GA_GroupName** metadata.

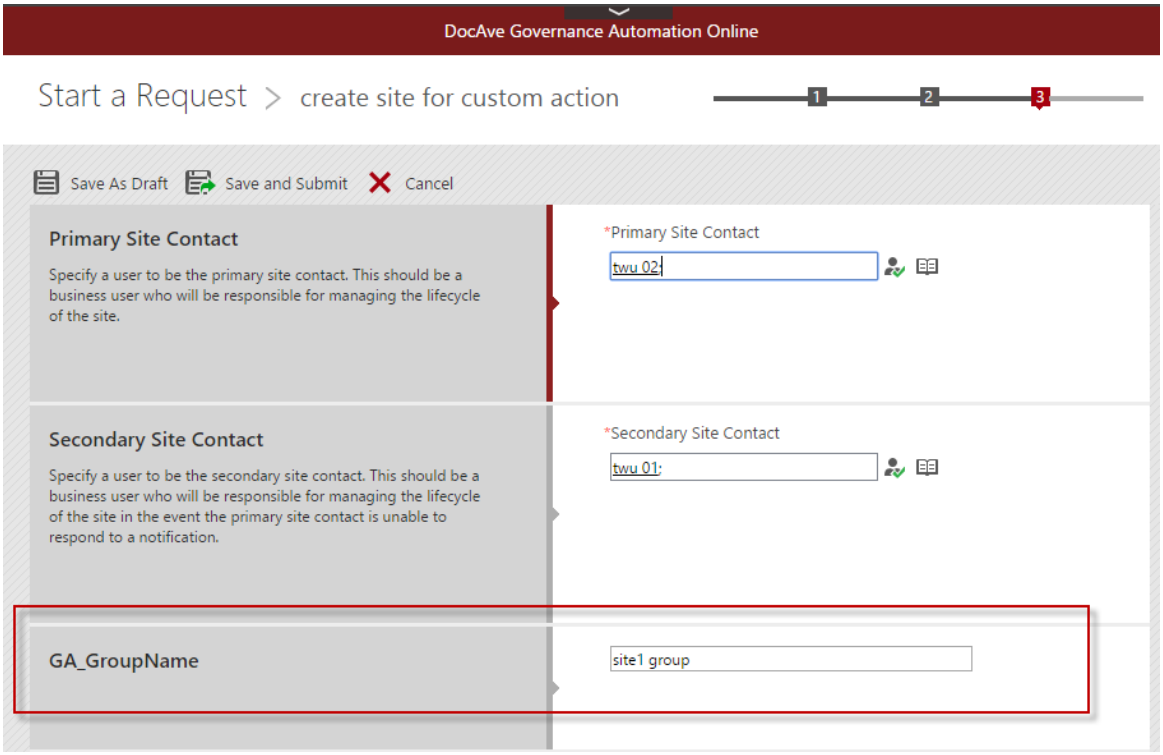

Figure 9: The sample request.

After the **CreateGroup** method in the Web Service is executed, **site1 group** is created in SharePoint Online.

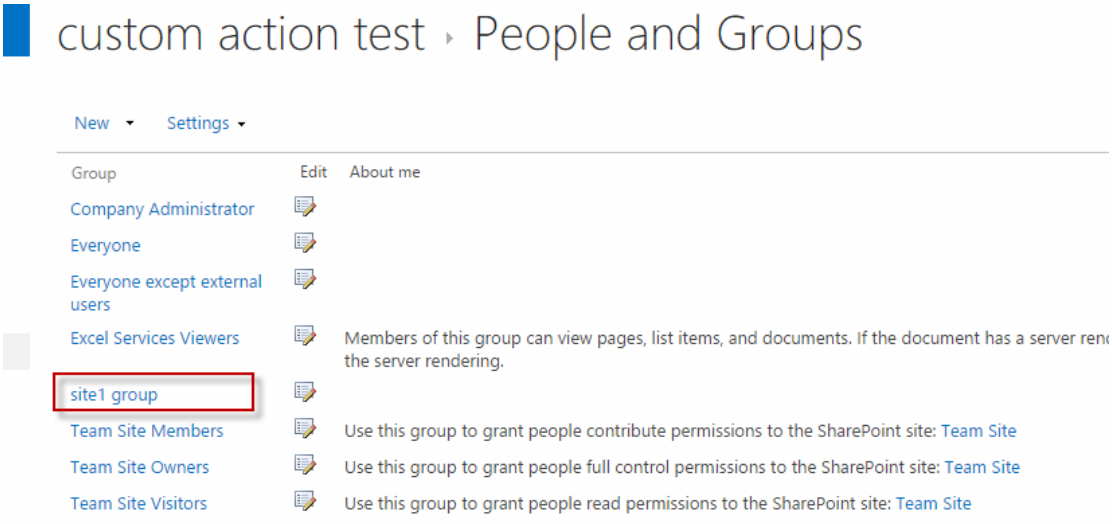

Figure 10: The created group in SharePoint Online.

Appendix B: Configuring a Filter Policy

This section describes how to configure filter policies in DocAve Online in order for Governance Automation Online to leverage DocAve Online Granular Backup and the Auditor feature in DocAve Online Report Center.

Configuring Filter Policy to Use DocAve Online Granular Backup

Log into DocAve Online and navigate to **Control Panel** > **Filter Policy** and click **Create** on the ribbon. Configure the filter policy as follows:

1. **Name** – Enter a name for this filter policy.
2. **Description** – Enter an optional description for future references.
3. Click **Add a Filter Level Group** to add a filter rule. The filter rule configuration filed appears.
    a. Select **Site Collection** from the first drop-down list.
    b. Click **Add a Criterion** and select **Custom Property**: **Text** from the second drop-down list. An additional text box will appear after the second drop-down list for you to enter the custom property text.
    c. In the new text box, enter **GA_PolicyForGranularBackup**
    d. In the **Condition** column, select **Equals** from the drop-down list.
    e. In the **Value** column, enter the exact name of the site collection policy for which you have Granular Backup enabled in the **DocAve Online Configurations** field.
4. When you have finished adding all of the site collection policies to the filter policy, click **OK** to save this filter policy.

Once the filter policy has been created, you must add it to a Granular Backup plan. For information on configuring Granular Backup plans, refer to the DocAve Granular Backup and Restore User Guide.

***Note**: You can add more than one Governance Automation Online site collection policy to each filter policy if you know that you would like to use the same Granular Backup plan for all site collections affected by those policies. Otherwise, create separate filter policies so that you can associate the different Governance Automation Online site collection policies to different Granular Backup plans.

Configuring Filter Policy to Use Audit Controller in DocAve Online Report Center

Log into DocAve Online and navigate to **Report Center** > **Settings** > **Audit Controller**. When creating a new Audit Controller plan or modifying an existing one, under **Apply Rule Settings**, configure the filter policy as follows:

1. Click **Add a Filter Level Group**.
2. In the **Rule** column, make sure that **Site Collection** is selected. All criteria within this group will only apply at the site collection level.
3. Click **Add a Criterion**.
4. For the first criterion, configure the following:
    a. In the **Rule** column, select **Custom Property: Text**
    b. In the text box that appears next to the drop-down list in the **Rule** column, enter **GA_PolicyForAuditing**
    c. In the **Condition** column, select **Equals**
    d. In the **Value** column, enter the exact name of the Governance Automation Online site collection policy for which you have Auditing enabled in the **DocAve Online Configurations** field.
5. Be sure all changes are saved.

For information on configuring the rest of Audit Controller plan in DocAve Online Report Center, refer to the DocAve Report Center User Guide.

***Note**: You can add more than one Governance Automation Online site collection policy to each filter policy if you know that you would like to use the same Audit Controller plan for all site collections affected by those policies. To do so, add a criterion for each policy. Otherwise, create separate Audit Controller plans.

Appendix C: Supported Features in Governance Automation and Governance Automation Online

The following tables compare the supported and unsupported features of Governance Automation 2 Service Pack 1 and Governance Automation Online Service Pack 9 Cumulative Update 6.

Approval Process

The table below lists the supported and unsupported features of Approval Process in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Approval Process Stages: Use approval stages	×	√	√	√	
Approval Process Stages: Use approval stages - Automatically approve the request if the requester and the approver are the same user	×	√	√	√	
Approval Process Stages: Auto-approve	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Approval Process Stages: Integrate with SharePoint Workflow	×	√	×	×	
Approval Process Stages: Integrate with K2 Workflow	×	√	√	×	
CC	×	√	√	√	
Approver(s): Assign To	×	√	√	√	
Approver(s): Order	×	√	√	√	
Approver(s): Allow approvers to reassign tasks to others	×	√	√	√	
E-mail Settings	×	√	√	√	
Duration and Escalation	×	√	√	√	
Duration and Escalation: Reminder	×	√	√	√	

Site Collection Policy

The table below lists the supported and unsupported features of Site Collection Policy in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Farm	×	√	√	×	
Content Database	×	√	×	×	
Content Database Policy	×	√	×	×	
Site Collection Quota Template	×	√	×	×	
Quota (Storage Quota & Server Storage Quota)	×	×	√	√	
SharePoint Designer Configuration	×	√	√	√	
Site Maximum Depth Limit	×	√	√	√	
Site Policy Bar	×	√	×	√	
Enable Policy Enforcer	√	√	√	√	
Enable Deployment Manager	√	√	√	√	
Enable Granular Backup	√	√	√	√	
Enabling Auditing	√	√	×	√	
Activate Connector Content Library Feature	√	√	×	×	DocAve Online does not support Connector.
Activate Connector Media Library Feature	√	√	×	×	DocAve Online does not support Connector.
Activate File Share Navigator Feature	√	√	×	×	DocAve Online does not support File Share Navigator.
Enable site collection content archival using DocAve Archiver	√	√	√	×	
Enable site collection content archival using AvePoint RevIM	√	√	√	×	
Enable Scheduled Storage Manager	√	√	×	×	DocAve Online does not support Scheduled Storage Manager.

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Enable Dead Account Cleaning	√	√	×	×	DocAve Online does not support this feature.
Enable Vault for Site Collection Content	√	√	√	×	Only supported for SharePoint 2010 on-premises.
Enable Usage Pattern Alerting	√	√	×	×	DocAve Usage Pattern Alerting is not applicable in SharePoint Online.
Enable archiving of entire site collection	√	√	√	√	
Enable deletion of entire site collection	×	√	√	√	
Enable extension of site collection lease	×	√	√	√	
Enable site collection policy change	×	√	√	√	
Enable site collection unlocking	×	√	√	√	
Enable site collection locking	×	√	√	√	
Enable site collection quota change	×	√	√	√	
Enable site collection inactivity threshold	×	√	√	√	
Enable site collection lease period	×	√	√	√	
Enable automated locking	×	√	√	√	
Enable site collection quota threshold	×	√	√	×	
Recertification Profile	√	√	√	√	

Office 365 Group Policy

The table below lists the supported and unsupported features of Office 365 Group Policy in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Azure Active Directory App Profile	×	√	√	√	
Group Team Site Quota	×	√	√	√	
Enable deletion of the Office 365 group	×	√	√	√	
Enable extension of the Office 365 group lease	×	√	√	√	
Enable Office 365 group policy change	×	√	√	√	
Enable Office 365 group team site quota change	×	√	√	√	
Enable Office 365 inactivity threshold	×	√	√	√	
Enable group inactivity threshold warning	×	√	√	√	
Enable automatic deletion of Office 365 group	×	√	√	√	
Enable Office 365 group lease management	×	√	√	√	
Enable group lease expiration warning	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Enable recertification	×	√	√	√	

Supported and Unsupported Services

The table below lists the current supported and unsupported service types in Governance Automation and Governance Automation Online.

√ indicates Supported.

× indicates Unsupported.

Service Type	Governance Automation	Governance Automation Online	Note
Create Site Collection	√	√	
Create Site	√	√	
Change Site Collection Contact or Administrator	√	√	Governance Automation Online only supports changing primary/secondary site collection contact and primary site collection administrator.
Change Site Collection Settings	√	√	
Change Site Contact	√	√	
Change Site Metadata	√	√	
Content Move	√	√	
Create Library/List	√	√	
Change Library/List Settings	√	√	
Site Collection Lifecycle Management	√	√	
Site Lifecycle Management	√	√	
Clone or Transfer User Permissions	√	√	
Grant Permissions	√	√	

Service Type	Governance Automation	Governance Automation Online	Note
Change Permissions	√	√	
Custom Service	√	√	
Manage Permissions	√	×	
Deploy Patterns	√	×	
Create Group	√	√	
Group Lifecycle Management	√	√	
Change Group Settings	√	√	

Common Service Features

The table below lists the supported and unsupported common service features in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Service Name and Description	×	√	√	√	
Language	×	√	√	√	
Service Category	×	√	√	√	
Department	×	√	√	√	
Service Permission	×	√	√	√	
Service Contact	×	√	√	√	
Administrator Contact	×	√	√	√	
Metadata	√	√	√	√	
Approval Process	×	√	√	√	
Approval Process: Allow all approvers to edit this service request	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Approval Process: Multiple approval process	√	√	√	√	
Custom Action	×	√	√	√	
Execution Schedule	×	√	√	√	
Schedule Date	×	√	√	×	

Create Site Collection Service

The table below lists the supported and unsupported features of Create Site Collection Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Dynamic Mode Service	×	√	√	×	
Web Applications and Managed Paths	√	√	√	×	
Show host header	×	√	×	×	
Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Site Collection Title Validation	×	√	√	×	
Policy	√	√	√	√	For details, refer to Site Collection Policy.

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Language	×	√	√	√	
Site Collection Template	×	√	√	√	
Experience Version	×	√	√	√	For SharePoint Online, only SharePoint 2013 is supported for this feature.
Time Zone	×	×	√	√	
Security Groups	×	√	√	√	Governance Automation Online Service Pack 7 does not support **Allow Business User to create Active Directory groups**.
Primary Site Collection Administrator	×	√	√	√	
Secondary Site Collection Administrator	×	√	×	×	SharePoint Online does not have this role.
Additional Site Collection Administrators	×	√	√	√	
Primary Site Collection Contact	×	√	√	√	
Primary Site Collection Contact: Notify the contact upon site collection creation	×	√	√	√	
Secondary Site Collection Contact	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Secondary Site Collection Contact: Notify the contact upon site collection creation	×	√	√	√	
DocAve Deployment Manager Plan	√	√	√	√	
Manage Site Collection Lifecycle: Enable site collection lease period	×	√	√	√	
Governance Automation App and App Parts	×	√	√	√	Governance Automation Online does not support the Site Directory app part.
Request Access via Governance Automation Grant Permissions Service	×	√	√	×	
Manually input URL	×	√	√	√	
Manually input URL: Construct URL	×	√	√	√	
Manually input URL: URL validation	×	√	√	√	
Automatically generate URL	×	√	√	√	

Create Site Service

The table below lists the supported and unsupported features of Create Site Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Dynamic Mode Service	×	√	√	×	
Farm/My Registered Sites Selection	√	√	√	×	
Manually input URL	×	√	√	√	
Enable security trimming in the tree of the request for this service	×	√	√	×	
Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Use site title in URL	×	√	√	√	
URL validation	×	√	√	√	
Site Title Validation	×	√	√	×	
Language	×	√	√	√	
Site Template	×	√	√	√	
Security Groups	×	√	√	√	
Navigation	×	√	√	√	
Navigation Inheritance	×	√	√	√	
Primary Site Contact	×	√	√	√	
Primary Site Contact: Notify the contact upon site creation	×	√	√	√	
Secondary Site Contact	×	√	√	√	
Secondary Site Contact: Notify the contact upon site creation	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
DocAve Deployment Manager Plan	√	√	√	√	
Governance Automation App and App Parts	×	√	√	√	Governance Automation Online does not support the Site Directory app part.
Inherit parent metadata	×	√	√	×	
Use unique metadata	×	√	√	√	
Copy metadata from its parent site	×	√	√	×	

Create Group Service

The table below lists the supported and unsupported features of Create Group Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
App Profile	×	√	√	√	
Privacy	×	√	√	√	
Subscribe Members	×	√	√	√	
Outside Senders	×	√	√	√	
Language	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Group Classification	×	√	√	√	
Primary Group Contact	×	√	√	√	
Secondary Group Contact	×	√	√	√	
Group Owner	×	√	√	√	
Group Member	×	√	√	√	
Enable hidden group membership to hide the members of the Office 365 group from users who are not members of the group	×	√	√	√	
Office 365 Group Policy	×	√	√	√	
Group Name/ID	×	√	√	√	
Construct group name	×	√	√	√	
Construct group ID	×	√	√	√	
Links in Request/Task Details Page: Planner	×	√	√	√	
Links in Request/Task Details Page: Sites	×	√	√	√	
Links in Request/Task Details Page: Files	×	√	√	√	
Links in Request/Task Details Page: Conversations	×	√	√	√	
Links in Request/Task Details Page: Notebook	×	√	√	√	

Group Lifecycle Management Service

The table below lists the supported and unsupported features of Group Lifecycle Management Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
App Profile	×	√	√	√	
Lifecycle Management Action: Delete Office 365 Group	×	√	√	√	
Lifecycle Management Action: Extend Office 365 Group Lease	×	√	√	√	
Lifecycle Management Action: Change Office 365 Group Policy	×	√	√	√	
Lifecycle Management Action: Change Office 365 Group Team Site Quota	×	√	√	×	
Office 365 Group Records Settings	×	√	√	×	

Change Group Settings Service

The table below lists the supported and unsupported features of Change Group Settings Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
App Profile	×	√	√	√	
Change Office 365 Group Name and Description	×	√	√	√	
Change Member Subscription Settings	×	√	√	√	
Change Outside Senders Settings	×	√	√	√	
Change Office 365 Group Classification	×	√	√	×	
Change Group Contacts	×	√	√	√	
Change Group Owner Settings	×	√	√	√	
Change Group Members	×	√	√	√	
Change Group Metadata	×	√	√	√	

Create Library/List Service

The table below lists the supported and unsupported features of Create Library/List Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Dynamic Mode Service	×	√	√	×	
Bulk Mode	×	√	√	×	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Enable security trimming in the tree of the request for this service	×	√	√	×	
Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Library/List Name Validation	×	√	√	×	
Navigation	×	√	√	√	
Type	×	√	√	√	
Library/List Template	×	√	√	√	
Document Version History/Item Version History	×	√	√	√	
Library or List Address: Construct URL	×	√	√	√	
Library or List Address: URL validation	×	√	√	√	

Site Collection Lifecycle Management Service

The table below lists the supported and unsupported features of Site Collection Lifecycle Management Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Extend Site Collection Lease	×	√	√	√	
Delete Site Collection	×	√	√	√	
Archive Site Collection	√	√	√	√	
Change Site Collection Policy	×	√	√	√	
Unlock Site Collection	×	√	√	√	
Lock Site Collection	×	√	√	√	
Change Site Collection Quota	×	√	√	√	
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	

Site Lifecycle Management Service

The table below lists the supported and unsupported features of Site Lifecycle Management Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Action Mode: Enable site deletion/archiving in bulk	×	√	√	×	
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Delete Site	×	√	√	√	
Archive Site	√	√	√	√	

Change Site Collection Contact or Administrator Service

The table below lists the supported and unsupported features of Change Site Collection Contact or Administrator Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope:	×	√	√	×	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Enable security trimming in the tree of the request for this service					
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Primary and secondary site collection contact	×	√	√	√	
Site collection administrators	×	√	√	√	Governance Automation Online only supports changing primary site collection administrator.
Primary My Site contact and primary My Site administrator	×	√	×	×	Limitation on SharePoint Online API.

Change Site Collection Settings Service

The table below lists the supported and unsupported features of Change Site Collection Settings Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Change Site Collection Settings: Title	×	√	√	√	
Title: Title validation	×	√	√	×	
Change Site Collection Settings: Description	×	√	√	√	
Change Site Collection Settings: Metadata	×	√	√	√	

Change Site Contact Service

The table below lists the supported and unsupported features of Change Site Contact Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	

Change Site Settings Service

The table below lists the supported and unsupported features of Change Site Settings Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Change Metadata: Enable inheriting metadata	×	√	√	×	
Change Metadata: Enable adding or deleting metadata	×	√	√	√	

Change Library/List Settings Service

The table below lists the supported and unsupported features of Change Library/List Settings Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Change Library/List Settings: Name	×	√	√	√	
Name:	×	√	√	×	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Name validation					
Change Library/List Settings: Description	×	√	√	√	
Change Library/List Settings: Navigation	×	√	√	√	
Change Library/List Settings: Versioning settings	×	√	√	√	

Content Move Service

The table below lists the supported and unsupported features of Content Move Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	×	√	
Specify a destination URL	√	√	√	×	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Select a destination scope	√	√	√	√	
Method: Copy/Move	√	√	√	√	
Source Documents/Items Deleted Method: Manually/Automatically	√	√	√	√	
Delete Checked Out Documents From Source	√	√	√	√	
Action: Attach/Merge	√	√	√	√	
Filter Policy	√	√	√	√	
Copy/Move configuration	√	√	√	√	
Copy/Move configuration: Keep look and feel	√	√	√	√	
Do not copy/move configuration	√	√	√	√	
Do not copy/move configuration: Copy/Move the item-dependent columns and content types to maintain item integrity	√	√	√	√	
Do not copy/move configuration: Do not copy/move the item-dependent columns or content types. Report the items if the corresponding column or content type	√	√	√	√	
Copy/Move security	√	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Copy/Move security: Exclude user/group without permission	√	√	√	×	DocAve Online does not support this feature.
Copy/Move content	√	√	√	√	
Copy/Move content: Include list attachment	√	√	√	√	
Include workflow definition	√	√	√	√	
Include workflow instance	√	√	×	×	DocAve Online does not support workflow instance.
Managed Metadata Service Setting	√	√	√	×	
Preserve the Null Column Values	√	√	√	√	
Data Compression	√	√	√	×	
Data Encryption	√	√	√	×	
Column Mapping	√	√	√	√	
Content Type Mapping	√	√	√	√	
User Mapping	√	√	√	√	
Domain Mapping	√	√	×	×	
Language Mapping	√	√	√	√	
Back Up Environment Before Running Plan	√	√	√	√	
Conflict Resolution	√	√	√	√	
Agent Group	√	√	√	×	

Change Permissions Service

The table below lists the supported and unsupported features of Change Permissions Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Enable security trimming in the tree of the request for this service	×	√	√	×	
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Allow any user/group	×	√	√	√	
Allow peers and direct or indirect reports	×	√	×	√	
Allow direct or indirect reports	×	√	×	√	
Task Notification for Requester	×	√	√	√	
Excluded Permissions	×	√	√	×	

Grant Permissions Service

The table below lists the supported and unsupported features of Grant Permissions Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Allow domain group permissions assignment only	×	√	√	×	
Allow permissions assignment to user/group	×	√	√	√	
Allow any user/group	×	√	√	√	
Allow peers and direct or indirect reports	×	√	×	√	
Allow direct or indirect reports	×	√	×	√	
Set requester as the default user	×	√	×	√	
Allow business users to add members to Active Directory groups	√	√	×	×	
Permission Duration: Permanent permissions	×	√	√	√	
Permission Duration:	√	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Temporary permissions					
Grant Permissions: Add users to a SharePoint group	×	√	√	√	
Grant Permissions: Grant users permission directly	×	√	√	√	
Grant Permissions: Permissions above the requester's own permissions cannot be granted to others	×	√	√	×	
Grant Permissions: Exclude specified permission levels from the request page	×	√	√	√	
Send welcome e-mail to the new users	√	√	√	√	

Clone or Transfer User Permissions Service

The table below lists the supported and unsupported features of Clone or Transfer User Permissions Service in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Scope: Use SharePoint context to automatically populate the service request scope	×	√	√	√	
Restrict Source User Selection: Allow any user/group	×	√	√	√	
Restrict Source User Selection: Allow peers and direct or indirect reports	×	√	×	√	
Restrict Source User Selection: Allow direct or indirect reports	×	√	×	√	
Restrict Target User Selection: Allow any user/group	×	√	√	√	
Restrict Target User Selection: Allow peers and direct or indirect reports	×	√	×	√	
Restrict Target User Selection: Allow direct or indirect reports	×	√	×	√	
Permission Option: Append	√	√	√	√	
Permission Option: Replace	√	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
User Alert Option	√	√	×	×	DocAve Online does not support this feature.
Change Metadata	√	√	×	×	DocAve Online does not support this feature.
Add target user to the same group in the destination	√	√	√	√	
Clone source user's group permissions to the target user directly	√	√	√	√	
Remove source user's explicit permission	√	√	√	√	
Remove source user from SharePoint groups	√	√	√	√	
Delete source user from site collection	√	√	√	√	

Monitoring and Reporting

The table below lists the supported and unsupported features of Monitoring and Reporting in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
All Requests	×	√	√	√	
All Tasks	×	√	√	√	
All Recertification Assignments	×	√	√	√	In Governance Automation Online, it is **All Recertification Reports**.
User Activity Report	×	√	√	√	
Service Request Report	×	√	√	√	
Approval Process Report	×	√	√	√	
Site Collection Report	×	√	√	√	
Site Collection Report: Apply Policy	×	√	√	√	
Site Collection Report: Elect Contact	×	√	√	√	
Site Collection Report: Specify Contact	×	√	√	√	
Site Report	×	√	√	√	
Content Database Report	×	√	×	×	
My Recertification Report	×	√	√	√	
Dashboard	×	√	√	√	

Settings and Other Options

The table below lists the supported and unsupported features of Settings and other options in Governance Automation and Governance Automation Online.

√ indicates Supported. (In the **Integration with DocAve 6/DocAve Online** column, √ indicates **Integrated**.)

× indicates Unsupported. (In the **Integration with DocAve 6/DocAve Online** column, × indicates **Not integrated**.)

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
User Profile Service	×	√	×	√	Do not need to configure User Profile Service in the interface. It is retrieved in the backend.
Department: Configure Departments	×	√	√	√	
Department: Use Property in User Profile Service	×	√	×	√	
Account Manager	√	√	√	√	
Report Export Location	×	√	√	√	
E-mail Templates	×	√	√	√	
Administrator Notification	×	√	√	√	
Metadata	×	√	√	√	Governance Automation Online does not support the following metadata types: **Date and Time Lookup**
SharePoint Permission Level Management	×	√	√	√	
Execution Schedule	×	√	√	√	
Category Management	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Timer Service Configuration Management: Site Collection Status Scan Job	×	√	√	√	Governance Automation Online only supports checking site collection lease expiration, inactivity, and deletion.
Timer Service Configuration Management: Tree Cache Synchronization Job	×	√	√	×	
Timer Service Configuration Management: Archive Site Collection Content Scan Job	√	√	√	√	
Timer Service Configuration Management: Site Information Synchronization Job	×	√	√	√	
Timer Service Configuration Management: Site Collection Information Synchronization Job	×	√	√	√	
Timer Service Configuration Management: User Profile Service Synchronization Job	×	√	√	×	The synchronization is achieved by AvePoint Online Services.
Timer Service Configuration Management:	√	√	×	×	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Temporary Permission Scan Job					
Timer Service Configuration Management: Content Database Information Synchronization Job	×	√	×	×	
Timer Service Configuration Management: SharePoint Workflow Integration Scan Job	×	√	×	×	
Timer Service Configuration Management: Task Reminder Scan Job	×	√	√	×	
Timer Service Configuration Management: Recertification Scan Job	×	√	√	√	
Questionnaire Management	×	√	√	√	
Export and Import Configuration Data	×	√	√	×	
Business User Features Activation or Deactivation	×	√	√	√	
Import Existing Site Collections and Sites	×	√	√	√	
System General Settings	×	√	√	×	
Request Access Settings	×	√	×	×	
SharePoint Workflow Integration Management	×	√	×	×	
Recertification Profile Management: Permission Recertification	√	√	√	√	Unsupported for SharePoint Online My Site

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Recertification Profile Management: Metadata Recertification	×	√	√	√	
Recertification Profile Management: Ownership Recertification	×	√	√	√	
Recertification Profile Management: Conditional Recertification	×	√	√	×	
Recertification Profile Management: Site Collection Automated Locking	×	√	√	×	
Recertification Profile Management: Administrator Contact	×	√	√	√	
Text Validation Rule Management	×	√	√	√	
Governance Automation Terminology Management	×	√	√	√	
Custom Filter on My Sites	×	√	√	×	
Active Directory Profile Management	√	√	×	×	
Site Information Card Management	×	×	√	√	
Public Site Collection Directory	×	√	√	√	
My Sites	×	√	×	√	
Configure Personal Settings: Time Zone	×	√	√	√	

Feature	Integration with DocAve 6/ DocAve Online	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Configure Personal Settings: Date Format	×	√	√	×	
Configure Personal Settings: Time Format	×	√	√	×	
Configure Personal Settings: Office 365 Account	×	√	√	×	
Language: English	×	√	√	√	
Language: Japanese	×	√	√	√	
Language: French	×	√	√	√	
Language: Germany	×	√	√	√	
Synchronize Authentication Method from DocAve	×	√	×	×	
Content Database Policy	×	√	×	×	
Governance Automation App	×	√	×	√	
Governance Automation App Parts	×	√	×	√	Governance Automation Online only supports the Site Information Card app part.

Web API

The table below lists the current supported and unsupported service types in Governance Automation Web API and Governance Automation Online Web API.

√ indicates Supported.

× indicates Unsupported.

Service Name	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Create Site Collection	√	√	√	
Create Site	√	√	√	
Change Site Collection Contact or Administrator	√	√	√	
Change Site Collection Settings	√	√	√	
Change Site Contact	√	√	√	
Change Site Metadata	√	√	√	
Content Move	√	√	√	
Content Migration	√	√	×	
Create Library/List	√	√	√	
Change Library/List Settings	√	√	√	
Create My Site	√	√	×	This service is unavailable in Governance Automation Online. In SharePoint Online, My Site is automatically created when the user logs into SharePoint Online.
Site Collection Lifecycle Management	√	√	√	

Service Name	Governance Automation (SharePoint on-premises)	Governance Automation (SharePoint Online)	Governance Automation Online	Note
Site Lifecycle Management	√	√	√	
Clone or Transfer User Permissions	√	√	√	
Grant Permissions	√	√	√	
Change Permissions	√	√	√	
Manage Permissions	√	√	×	
Deploy Patterns	√	√	×	
Create Group	×	√	√	
Group Lifecycle Management	×	√	√	
Change Group Settings	×	√	√	

Notices and Copyright Information

AvePoint, Inc.
525 Washington Blvd. Suite 1400
Jersey City, New Jersey 07310
USA