Chapter 7: Managing Groups, Contacts and Mail-Enabled Users

Gareth Gudger

In this chapter, we look at mail contacts, mail-enabled users and the various mail-enabled groups. You will learn about the following mail-enabled objects:

- Distribution Groups
- Dynamic Distribution Groups
- Mail-enabled Security Groups
- Mail Contacts
- Mail-Enabled Users (MEUs)

In addition, we discuss how to perform common administrative tasks through both the Exchange Admin Center (EAC) and the Exchange Management Shell (EMS).

Mail-Enabled Groups

The purpose of a mail-enabled group is to allow an organization to aggregate mail recipients into containers for easier addressing. For example, a distribution group may be named "All Employees" could contain all employees of the company. This distribution group may exist to send company-wide communications. The benefit of grouping these users is that the sender only has to specify a single address. Without groups a company of hundreds or thousands of recipients would have a very time consuming task getting this communication to its employees.

Mail-enabled groups can exist in three flavours. These are Distribution Groups, Dynamic Distribution Groups and Mail-Enabled Security Groups.

Distribution Groups are the most basic form of mail-enabled group. These groups cannot be used to assign security permissions to users. They are purely for aggregating users into a common container for addressing purposes. Membership is defined by either the Exchange administrator, a user designated as the owner, or, can be publicly open for anyone to join.

Dynamic Distribution Groups are similar to distribution groups in that they can only be used for mail purposes. Where they differ is that group membership is automated through OPATH filters. For example, a dynamic distribution group named "Corporate" could be configured to include only recipients within the organizational unit named "Corporate". Another example of an OPATH filter could be to include all recipients from a specific geography using the value from the state or province field. If a user were to be moved out of that OU, or as in the previous example if their state or province were changed, that user would no longer be a member of the group. Dynamic distribution groups are a great way to automate group membership.

Security Groups can be mail-enabled allowing a group to serve two functions. Not only can the group be used to assign permissions and rights to its members but it can also be used like a distribution group. For example, a mail-enabled security group named "Human Resources" could grant its members access to a network share, an HR database and be available in Exchange for addressing purposes. A mail-enabled security group is a great way to eliminate groups that contain identical membership. Unlike distribution groups membership cannot be open. Members can only be added or removed by an administrator or owner.

Real World: A mail enabled security group is a double-edged sword. While the group does allow for the elimination of separate distribution and security groups this combination also invites danger. The danger is the result of users being assigned to a mail-enabled security group for email purposes not realizing the user is receiving more security permissions than they were intended to have. In these cases, it might be best to keep mail operations strictly to distribution groups and security permissions strictly to security groups. Another possibility is to prefix each group type with a specific naming convention. For example, DG_<group name> for a distribution group and SG_<group name> for a mail-enabled security group.

The most common group seen in any Exchange environment is the distribution group. So, that is where we will start.

Distribution Groups

In this section, we will look at how to create a distribution group using both the EAC and EMS.

In this example, we are going to create a new group named Accounts Payable. This group will contain members of the accounting team. The email address for this group will be ap@space-corp.net.

To perform this task log into the Exchange Admin Center (EAC) and select **Recipients** on the left and **Groups** across the top. From here click the **New** button (represented by a plus sign) and select **Distribution Group**.

On the *New Group* window (Figure 7-1) type a **Display name** and **Alias** for the group. In our example, we have typed *Accounts Payable* for the display name and *AP* for the alias. The **Notes** field is a great way to tell others what this group is used for. Not only is this useful to other administrators but it is also displayed in the address book and contact card for other users to see.

Click **Browse** in the Organizational Unit section. This brings up the *Select an Organization Unit* dialog. From here you can select which OU you want the group to be created under.

The **Owners** box determines who can manage the group. By default, this is set to the account that is used to create the group. To add an owner, click the **Add** button and select them from the pop-up list. To remove an owner, select that individual and click the **Remove** button.

The checkbox **Add group owners as members** determines whether owners should also receive all communications sent to the group. There may be instances where the person managing the group, for example an Exchange administrator, does not need to receive communications sent to the group. Keeping this box checked means that group owners receive all email communications sent to the group.

The box directly below this checkbox allows us to set the initial list of group members. It is not required to set this now. This list can be left blank and be altered once the group is saved. To add members, click the **Add** button and select members for this group.

Note that other mail-enabled groups can be nested inside a distribution group. A good use case for nesting might be the result of nesting geographies. For example, a distribution list for New York Employees could be placed within a distribution list named North American Employees. The North American Employees distribution group could contain groups from many other geographies. Rather than add all employees individually from each geography it is easier to nest these groups into the North American Employees distribution group.

The next set of checkboxes determine how users can join the group.

Open allows anyone to join the group. A user can search for and join open groups using Outlook on the Web. This is managed through the **Options** screen under **General > Distribution Groups**.

Owner Approval allows a user to request access to a group. Similar to open groups users search for owner approval groups through Outlook on the Web. Users can then request access to the group which the owner either approves or declines.

Closed only permits administrators or group owners to add members to the group. Group owners can manage membership through Outlook on the Web.

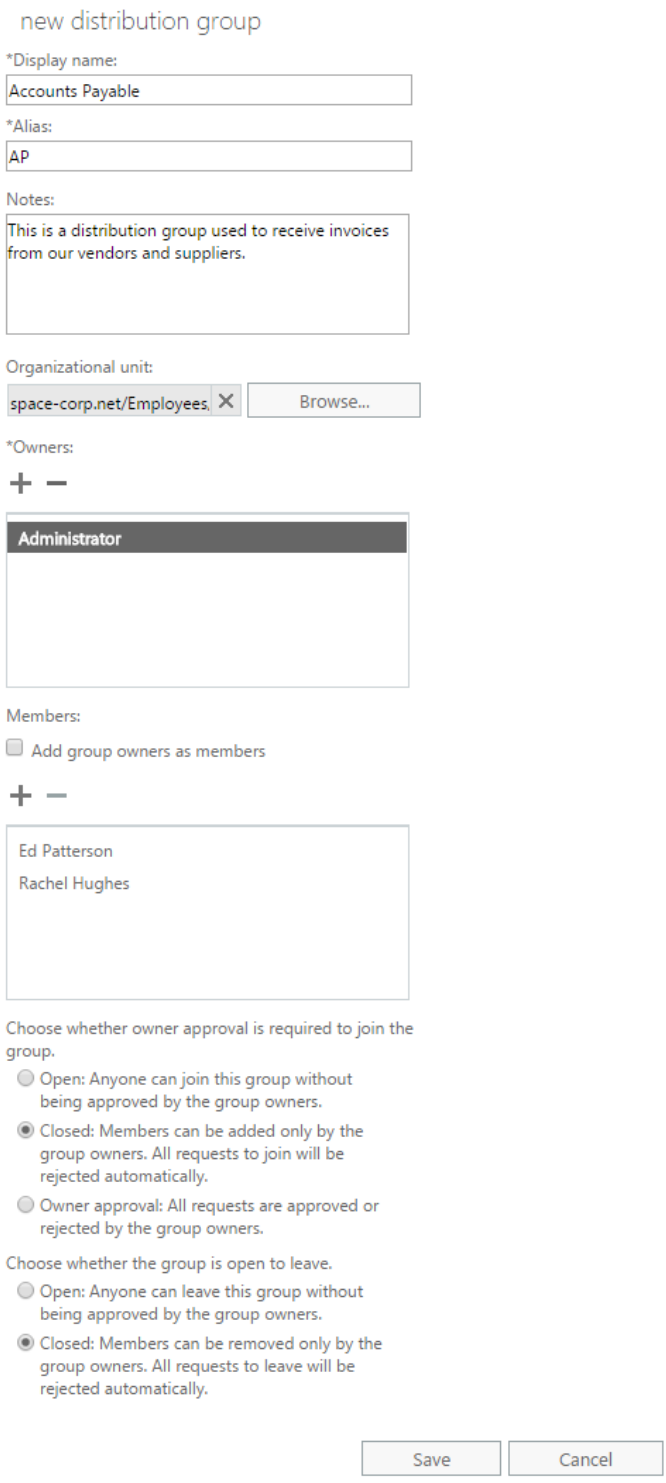

Figure 1: Creating a new distribution group

The next set of checkboxes determine how users can leave a group.

Open allows users to leave a group at any time. Users can manage their memberships through Outlook on the Web.

Closed blocks users from leaving a group. Only group owners or administrators can remove a user from a group.

Because our accounts payable group may receive sensitive financial information we will set the join type for the group as closed. It is also important that these invoices are processed in a timely manner so we want to make sure this group always has members of the accounting department. We will set the leave type as closed as well.

Click **Save** to create the group.

Let's explore how we would have completed the same task but using the Exchange Management Shell (EMS). To do this we will use the **New-DistributionGroup** cmdlet.

```
[PS] C:\> New-DistributionGroup -Name "Accounts Payable" -Alias "AP" -Notes "This is a distribution group used to receive invoices from our vendors and suppliers." -OrganizationalUnit "space-corp.net/Employees/Finance" -ManagedBy "Administrator" -Members "Rachel Hughes","Ed Patterson" -MemberJoinRestriction "Closed" -MemberDepartRestriction "Closed"
```

In this command:

-Name specifies the display name of the group.

-Alias specifies a unique mail nickname for the group and creates the initial email address.

-Notes specifies a description for the group. This is seen by both administrators and users alike.

-OrganizationalUnit specifies where in Active Directory the group should be created. In our example, we specified this as the Employees/Finance OU. This is an optional parameter.

-ManagedBy identifies the group owners. For multiple owners specify a comma separated list.

-Members identifies who will be a part of this group. This is a comma separated list.

-MemberJoinRestriction determines how users can join the group. Values include Open, Closed, or, ApprovalRequired

-MemberDepartRestriction determines how users can leave the group. Values include Open or Closed.

Additional New-DistributionGroup parameters not in our example include

-CopyOwnerToMember determines if owners should also receive all email communications sent to the group. There is no value for this parameter. Including it adds all owners as members.

-IgnoreNamingPolicy determines whether the group name is subject to the organization's group naming policy. Including this parameter allows this group to be created while ignoring the policy. We will discuss group naming policies in a later section.

-RequireSenderAuthenticationEnabled determines whether external senders can send to this distribution group. By default, this parameter is set to true and will block external senders from emailing this group. Configuring this parameter as false allows anonymous senders to email this group.

Note: For an extensive list of all available parameters for the **New-DistributionGroup** cmdlet check the following article https://technet.microsoft.com/en-us/library/aa998856(v=exchg.160).aspx

Security Groups

In this section, we will look at how to create a mail-enabled security group using both the EAC and EMS.

In this example, we are going to create a new security group named Human Resources. The plan is that this security group will provide its members access to a confidential network share, an HR database and to receive emails addressed to hr@space-corp.net.

To perform this task, select **Recipients** on the left and **Groups** across the top. From here click the **New** button and select **Security Group**.

On the *New Security Group* window (Figure 7-2) type a **Display name** and **Alias** for the group. In our example, we have typed *Human Resources* for the display name and *HR* for the alias. Similar to the distribution group the **Notes** field is a great way to tell others what this group is used for.

Click **Browse** in the Organizational Unit section. This brings up the *Select an Organization Unit* dialog. From here you can select which OU you want the group to be created under.

The **Owners** box determines who can manage the group. To add an owner, click the **Add** button. To remove an owner, select that individual and click the **Remove** button.

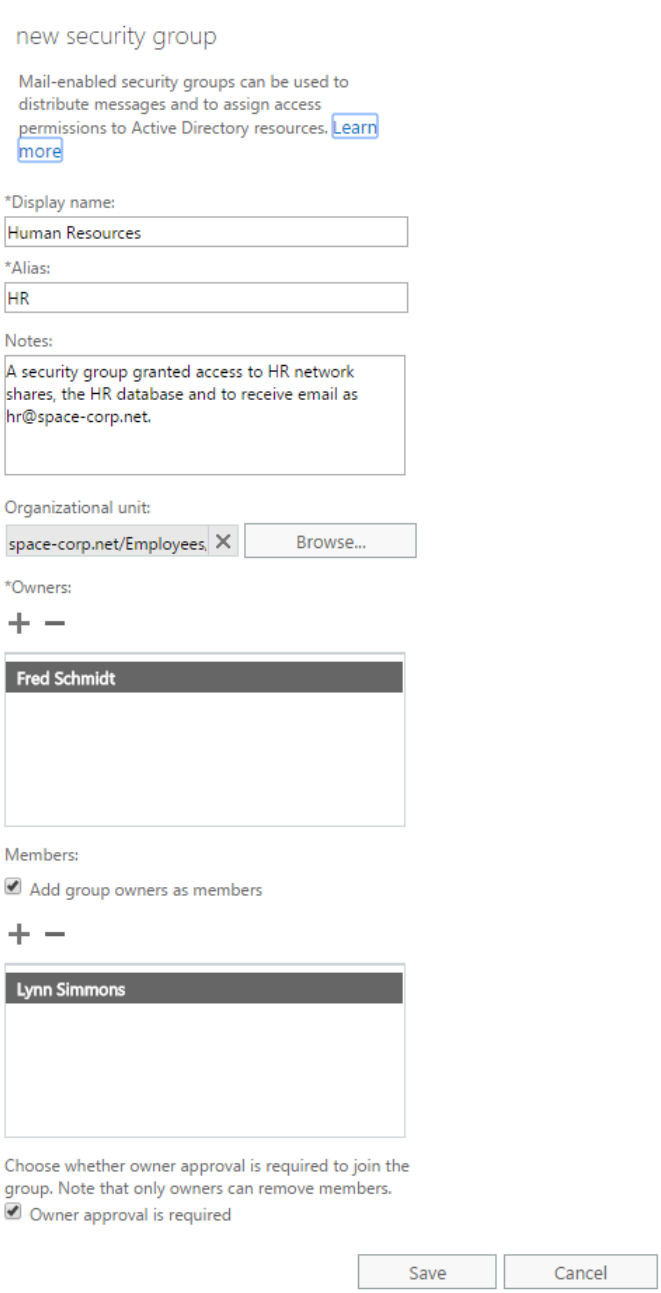

Figure 2: Creating a mail-enabled security group

The checkbox **Add group owners as members** determines whether owners should also receive all communications sent to the group.

The box directly below this checkbox allows us to set the initial list of group members. To add members, click the **Add** button and select the individuals or other mail-enabled groups to include. To remove members, select that entry from the list and click the **Remove** button.

Unlike a distribution group we only have a single option to manage group membership. This option is for owner approval to join the group. Toggle this box to govern whether users need approval to join the group. Click **Save**.

Like when we created a distribution group a security group is also created with the **New-DistributionGroup** cmdlet. The subtle difference is the addition of the **-Type** parameter. With this parameter, we specify that the group should be a security group. It is also worth noting that mail-enabled security groups are always created as universal groups. This is identified in the output of the command.

```
[PS] C:\> New-DistributionGroup -Name "Human Resources" -Alias "hr" -Notes "A security group
granting access to HR network shares, the HR database and to receive email as hr@space-corp.net." -
OrganizationalUnit "space-corp.net/Employees/Corporate" -ManagedBy "Fred Schmidt" -CopyOwnerToMember
-Members "Lynn Simmons" -MemberJoinRestriction "ApprovalRequired" -Type "Security"

Name                DisplayName         GroupType                PrimarySmtpAddress
----                -----------         ---------                ------------------
Human Resources     Human Resources     Universal, SecurityEnabled hr@space-corp.net
```

Mail-enabling an existing group

Mail-enabling a group is to take an existing group in Active Directory and enabling it for email purposes. A common use case is when you have an existing security group and need to enable that group for email.

To mail-enable an existing group that group must first be a universal group. We can check this setting through either Active Directory Users and Computers or through PowerShell.

To check through Active Directory Users and Computers edit the properties of the security group. Under the **Group Scope** the type should be set to **Universal**. In our example below (Figure 7-3) our security group is set to global. This is the default scope when a group is created. To switch the group to a universal group, toggle the radio button to **Universal** and click **Ok**.

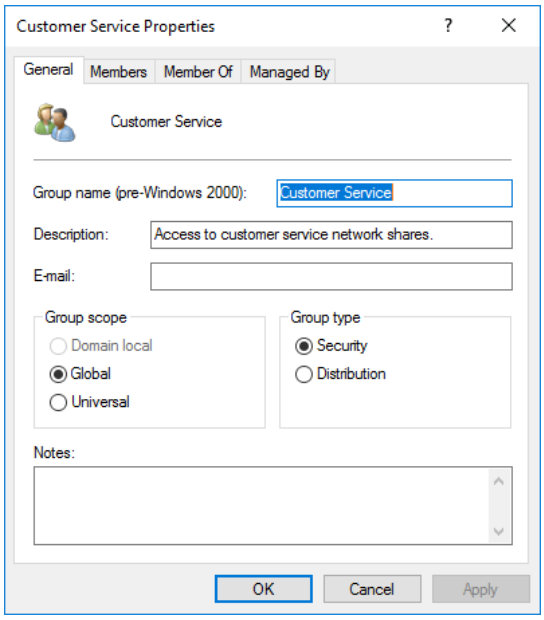

Figure 3:Setting an Active Directory group to Universal

To perform this same set of actions through PowerShell we can use the **Get-Group** and **Set-Group** cmdlets. Using our example of Customer Service, we can see that the group type is set to global.

```
[PS] C:\> Get-Group -Identity "Customer Service"

Name                DisplayName         SamAccountName           GroupType
----                -----------         --------------           ---------
Customer Service                        Customer Service         Global, SecurityEnabled
```

To change our group to universal, issue the **Set-Group** command with the **-Universal** parameter. This parameter does not have a value. This parameter will switch a domain local or global group to universal.

```
[PS] C:\> Set-Group -Identity "Customer Service" -Universal
```

If we rerun our get command, we will see the group type has switched to universal.

```
[PS] C:\> Get-Group -Identity "Customer Service"

Name                 DisplayName          SamAccountName               GroupType
----                 -----------          --------------               ---------
Customer Service                          Customer Service             Universal, SecurityEnabled
```

Now that our group is universal we can enable it for mail. This is not a task available through the EAC so let's explore this process through EMS. For this we will use the **Enable-DistributionGroup** cmdlet.

```
[PS] C:\> Enable-DistributionGroup -Identity "Customer Service"

Name                 DisplayName          GroupType                    PrimarySmtpAddress
----                 -----------          ---------                    ------------------
Customer Service     Customer Service     Universal, SecurityEnabled   CustomerService@space...
```

If we ever need to remove the mail attributes from a group but maintain the group and its members, you can run the **Disable-DistributionGroup** cmdlet. A common use case for this is when you need to turn a mail-enabled security group back into a regular security group.

```
[PS] C:\> Disable-DistributionGroup -Identity "Human Resources"

Confirm
Are you sure you want to perform this action?
Disabling distribution group "Human Resources" will remove the Exchange properties from the Windows
group object.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"): Y
```

Mail-enabled Non-Universal Groups

It is also possible that existing mail-enabled groups are not configured as universal. If you find these groups they may be a remnant from an older version of Exchange. Older versions of Exchange, such as Exchange 2003, allowed other group types to be mail-enabled. It is highly recommended to switch these to universal so these mail-enabled groups are available to the entire forest. This is especially important in multi-domain forests as the membership of domain local and global groups cannot be enumerated by other domains. Failure to enumerate membership will result in mail not being delivered. These legacy groups will show up in Exchange as mail non-universal groups.

To locate these groups, run the following **Get-DistributionGroup** cmdlet.

```
[PS] C:\> Get-DistributionGroup -RecipientTypeDetails MailNonUniversalGroup -ResultSize Unlimited
```

To convert all of these groups we can pipe the previous command into **Set-Group**.

```
[PS] C:\> Get-DistributionGroup -RecipientTypeDetails MailNonUniversalGroup -ResultSize Unlimited |
Set-Group -Universal
```

If you need to convert a single group, you can run the following command.

```
[PS] C:\> Set-Group -Identity "Name of Group" -Universal
```

If you receive any errors during this conversion it may be the result of group nesting. For example, a universal group cannot be a member of a global group. If this is the case, you will either need to convert the parent group first or remove the intended universal group from its membership.

Dynamic Distribution Groups

As mentioned at the beginning of this chapter a Dynamic Distribution Group (DDG) is a great way to create a group that automates its own membership. A great example of this may be an all-employee distribution group that is used to send company-wide announcements. Another example could be to create groups that define their membership by geography. In this section, we will explore creating DDGs for both of these scenarios.

To create a DDG select the **Recipients** on the left and **Groups** tab across the top. From here click the **New** button and select **Dynamic Distribution Group**.

On the *New Dynamic Distribution Group* window (Figure 7-4) type a **Display name** and **Alias** for the group. In our example, we have typed *All Employees* for the display name and *AllEmployees* for the alias. Enter the purpose of the group in the **Notes** field. Click **Browse** in the Organizational Unit section to select which OU you want the group to be created under. Click **Browse** in the Owners section to select an owner for the group. The Notes, Organizational Unit and Owner fields are all optional.

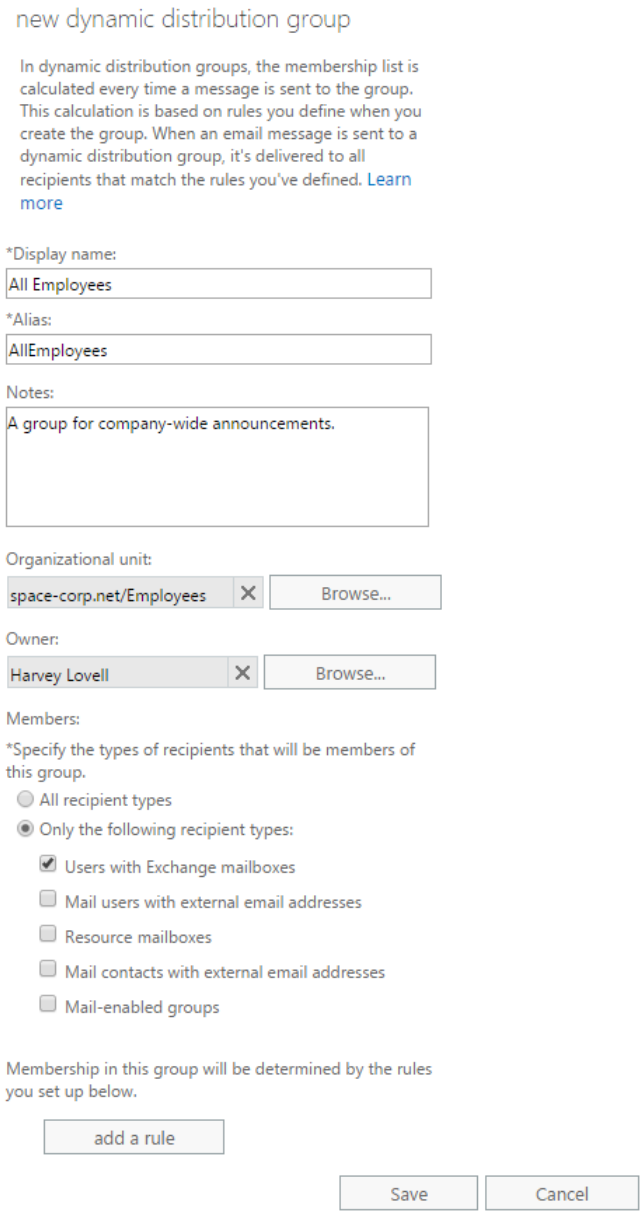

Figure 4: Creating a dynamic distribution group

Under **Members** we can narrow down who should be included in this group. By default, it is set to **All recipient types**. A dynamic distribution group can be narrowed down to specific recipient types. These include user mailboxes, mail users, resource mailboxes, mail contacts, and mail-enabled groups.

For our example, we only want our employees to receive these company-wide communications. We do not want external recipients such as mail contacts and mail users receiving these communications. Nor do we need our resource mailboxes or groups to receive these announcements. We will switch the checkbox to **Only the following recipient types** and select **Users with Exchange mailboxes**.

Membership can be further narrowed down by rules and filters. These can be configured in the section **Membership in this group will be determined by rules**. Using the drop down we can pick the various fields we want to filter on. For example, we can specify state or province with a value of Florida. With this rule set only objects with an Active Directory state or province attribute of Florida will be included in our group. In our example, we want all employees to be included in our group so we will not specify any rules.

Click **Save**.

To perform this task in EMS we utilize the **New-DynamicDistributionGroup** cmdlet. For example, to create a dynamic distribution group to include all mail-enabled objects with a state of province of Florida our command would look like this.

```
[PS] C:\> New-DynamicDistributionGroup -Name "All Florida Employees" -IncludedRecipients
"AllRecipients" -ConditionalStateOrProvince "Florida" -OrganizationalUnit "space-
corp.net/Employees/Florida Rocket Testing Site"
```

The **-IncludedRecipients** parameter can contain several conditions. These are *AllRecipients* (which includes all mail-enabled objects), *MailboxUsers*, *MailContacts, MailGroups, MailUsers & Resources*. In our example, we specified that we wanted to include all mail-enabled objects so we set the condition to *AllRecipients*. If we only wanted our group to include user mailboxes we could have set the condition to *MailboxUsers*.

We can also use a recipient filter to assign members to a dynamic distribution group. For example, to create a group that contains only members who have a title of *Research Assistant* we could use the following recipient filter.

```
[PS] C:\> New-DynamicDistributionGroup -Name "Research Assistants" -RecipientFilter {(RecipientType
-eq 'UserMailbox') -and (Title -like 'Research Assistant')} -OrganizationalUnit "space-
corp.net/Employees/R&D"
```

The entire recipient filter is enclosed in curly brackets. Each separate condition is identified in a curved bracket. In our example, we specify that the members must be both a user mailbox and have a title attribute of *Research Assistant*. Note that we use the **-and** operator to specify that the recipient must match both conditions.

To determine the accuracy of a recipient filter we can test it with the **Get-Recipient** cmdlet. In this command, we use the **-RecipientPreviewFilter** parameter followed by our recipient filter in curly braces.

```
[PS] C:\> Get-Recipient -RecipientPreviewFilter {(RecipientType -eq 'UserMailbox') -and (Title -like
'Research Assistant')} -ResultSize Unlimited

Name                                                  RecipientType
----                                                  -------------
Pam Kipling                                           UserMailbox
Alex Short                                            UserMailbox
Rachel Hughes                                         UserMailbox
```

If you expect this output to be rather large you can pipe these results to a CSV file. We use the **Select** statement to identify which column data we are interested in exporting. You can skip Select entirely from the pipe if you want to export all columns.

```
[PS] C:\> Get-Recipient -RecipientPreviewFilter {(RecipientType -eq 'UserMailbox') -and (Title -like
'Research Assistant')} -ResultSize Unlimited | Select Name, OrganizationalUnit, PrimarySMTPAddress,
RecipientType | Export-CSV C:\Users\Administrator\Desktop\DDGMembers.csv -NoTypeInformation
```

To test an existing group, we can run the following two commands. The first command stores our group data into a variable. The second command then parses that variable data into the Get-Recipient cmdlet.

```
[PS] C:\> $Members = Get-DynamicDistributionGroup "Research Assistants" -ResultSize Unlimited
[PS] C:\> Get-Recipient -RecipientPreviewFilter $Members.RecipientFilter

Name                                                  RecipientType
----                                                  -------------
Pam Kipling                                           UserMailbox
Alex Short                                            UserMailbox
Rachel Hughes                                         UserMailbox
```

Note: For an extensive list of all available parameters for the **New-DynamicDistributionGroup** cmdlet check the following article https://technet.microsoft.com/en-us/library/bb125127(v=exchg.160).aspx

Group naming policy

Naming policies are highly recommended in environments where users have been granted the ability to create and manage their own groups. A user can create and manage groups through their Outlook on the Web options screen (Figure 7-5). Note that a user must be assigned the *MyDistributionGroup* user right assignment before they can create and manage groups.

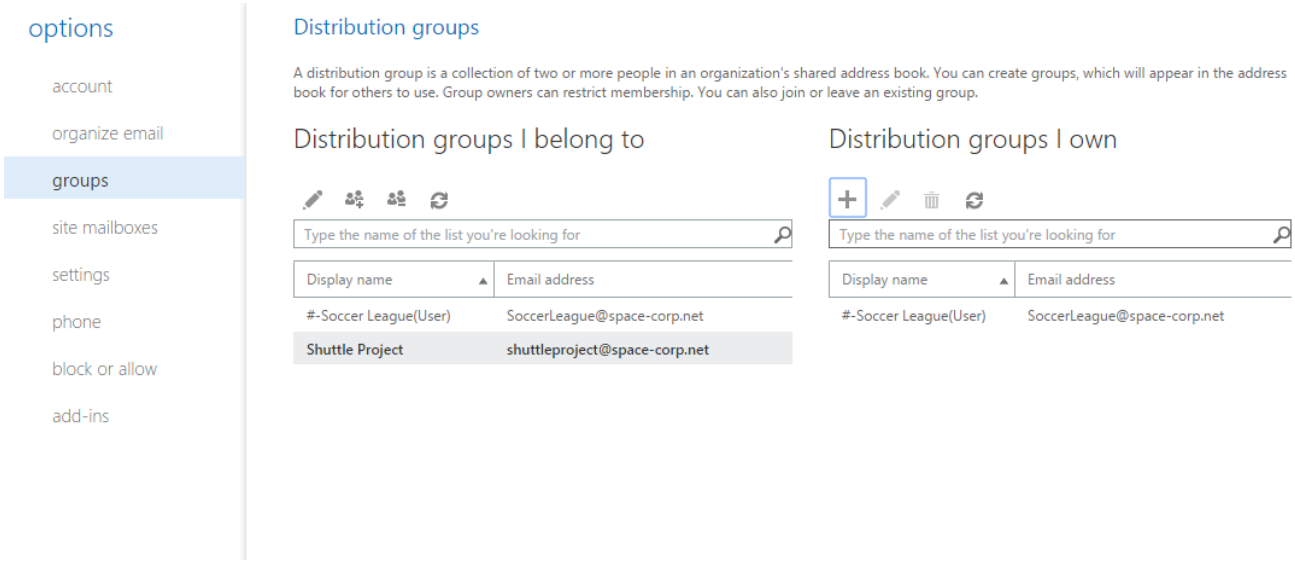

Figure 5: Allowing a user to create and manage their own distribution groups

A group naming policy governs the naming structure of user-created groups. For example, a group naming policy could prepend a special character to the beginning of the name so these groups always appear at the top of a global address list. Another possibility is that any user groups could be given a suffix of *"(User)"* to identify those groups as user created.

A group naming policy does not affect groups an administrator might create through the EAC. However, the policy does kick in for groups the administrator creates through EMS. To override this behaviour an administrator must use **-IgnoreNamingPolicy** parameter when creating or renaming a group via PowerShell.

To create a group naming policy, click the **Recipients** tab on the left and **Groups** tab across the top. Click the **More** button (represented by an ellipsis) and select **Configure group naming policy**. The group naming policy window will appear.

The **General** tab allows us to dictate if the group name should be prefixed or suffixed with certain text strings or attributes (Figure 7-6). Text is great when you need to add static words to each group. For example, we could prefix each group with a special character so it appears at the top of the global address list making it easier to find. Attributes allow us to create more dynamic prefixes or suffixes. For example, if we select attribute from either drop down we are given a list of all attributes we can use to populate the group name. Attributes include City, State, Country Code, Department and more than a dozen other custom attributes. Text strings and attributes can also be used in combination. For example, we could prepend the group with a hash tag and then follow that up with the department attribute. Any value in the department field of the group will be added to the group name. We can also add hyphens or underscores as text strings to make everything more readable. At the bottom of the general tab is a preview of what the group name will look like. In our example, we have used a hash tag and hyphen as a prefix and the text string of (User) as a suffix.

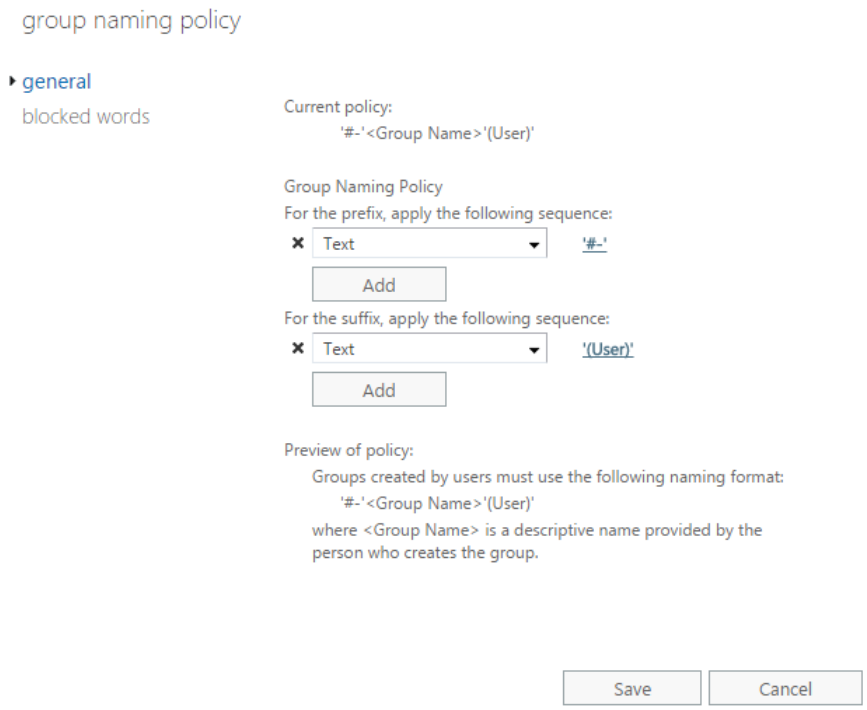

Figure 6: Creating a group naming policy

The **Blocked Words** tab is a list of words that cannot be used when creating a group. This helps prevent inappropriate group names entering the environment.

To create a group naming policy through EMS we must use the **Set-OrganizationConfig** cmdlet. Like figure 6-6 we prefix a hash tag and a hyphen as a text string. We then add (User) as a text-string suffix. <GroupName> identifies the placement of the user-created name. Anything before <GroupName> is considered a prefix. Anything after is considered a suffix. Attributes are entered as angle brackets. For example, to add the country code we would add <CountryCode> to our command. We have also identified blocked words with the **-DistributionGroupNameBlockedWordsList** parameter.

```
[PS] C:\> Set-OrganizationConfig -DistributionGroupNamingPolicy "#-<GroupName>(User)" -
DistributionGroupNameBlockedWordsList "Fantasy","Football","Chili","Cookoff"
```

To verify these settings have taken effect we use the **Get-OrganizationConfig** cmdlet.

```
[PS] C:\> Get-OrganizationConfig | Format-List DistributionGroup*

DistributionGroupDefaultOU            :
DistributionGroupNameBlockedWordsList : {Cookoff, Chili, Fantasy, Football}
DistributionGroupNamingPolicy         : #-<GroupName>(User)
```

Note: Group names have a maximum length of 64 characters. This includes all prefixes and suffixes defined in a group naming policy. Exchange only permits one naming policy.

Managing Group Properties

So far in this chapter we have discussed how to create the various types of mail-enabled groups. Let's now look at the managing some of the properties of a group. We will look at those first through the EAC.

To access the properties of a group, select the Recipients tab on the left and Groups sub tab across the top. From here you can either double click the group you want to edit, or, select the group and click the Edit button (represented by a pencil).

This will launch a dialog with several tabs. It is worth noting that the tabs will vary based on the type of group you are editing. For example, when editing a dynamic distribution group the membership approval tab will not be present. This is because membership is determined by a recipient filter and not the group owner.

The first tab is the **General** tab. The general tab allows us to change parameters such as the display name, alias, or, the description of the group. It also allows us to hide this group from address lists, including the global address list (GAL). Users will not be able to search for this group. The organization unit (OU) where the group is located is displayed as a non-editable field.

The **Ownership** tab allows to view and modify the current owner of the group. The group owner can add and remove members to the group. In addition, if the group is configured for owner approval the group owner receives all membership approval requests via email.

The **Membership** tab determines who is part of this group. This tab lists all current members and allows the administrator to add or remove members. Note that if this group is configured for open membership users will be able to add or remove themselves to the group through their Outlook on the Web options. For a dynamic distribution group this tab allows you to view and modify the recipient filter.

The **Membership Approval** tab determine how users are added or removed from a group. We covered this in a prior section but to summarize, open allows a user to join or leave a group without administrator or owner intervention. In contrast closed dictates that a user can only be added or removed by an administrator or group owner. The last option, Owner approval, requires that a user petition an owner to join the group. The owner receives an email notification that allows them to either accept or deny the request.

The **Delivery Management** tab determines who can send to the group.

By default, all groups are configured for internal senders only. This is governed by the checkbox **Only senders inside my organization**. This is great for distribution groups that should only be used for internal purposes. For example, you could have a distribution group named *All Employees* that is used for company-wide communications. On the flipside, you probably do not want an external sender using a distribution list that can send to everyone in the company.

If you need a distribution group for both internal and external use switch the checkbox to **Senders inside and outside of my organization**. A good use case for this type of group could be for the accounting department who need an email address for vendors to submit invoices. This list can then be configured with multiple members of the accounting team.

If you want to specify a list of allowed senders, you can use the box at the bottom of the tab. You can manage the list of allowed senders with the add or remove buttons. Only senders in this list will be able to send email to this group. Everyone else will be rejected. Using our *All Employees* group as an example we could use this feature to restrict senders to Space Corp's leadership and members of the human resources department.

The **Message Approval** tab (Figure 7-7) allows us to configure moderation on the group. Moderation is another great way to determine what can be sent to a group. A business use case for moderation is that you

do not need to restrict messages to a group of senders, more so you just need to govern the content that is being sent. Using our *All Employees* group as an example, Space Corp wants to allow anyone to send to the group. However, Space Corp wants to review and approve all messages destined to the group. Space Corp's goal is to prevent non-business related emails from being sent to the group's recipients.

By default, moderation is disabled. To enable moderation, select the checkbox **Messages sent to this group have to be approved by a moderator** (Figure 7-7). You will then need to add at least one moderator under the **Group moderators** list. You can do this with the add or remove buttons.

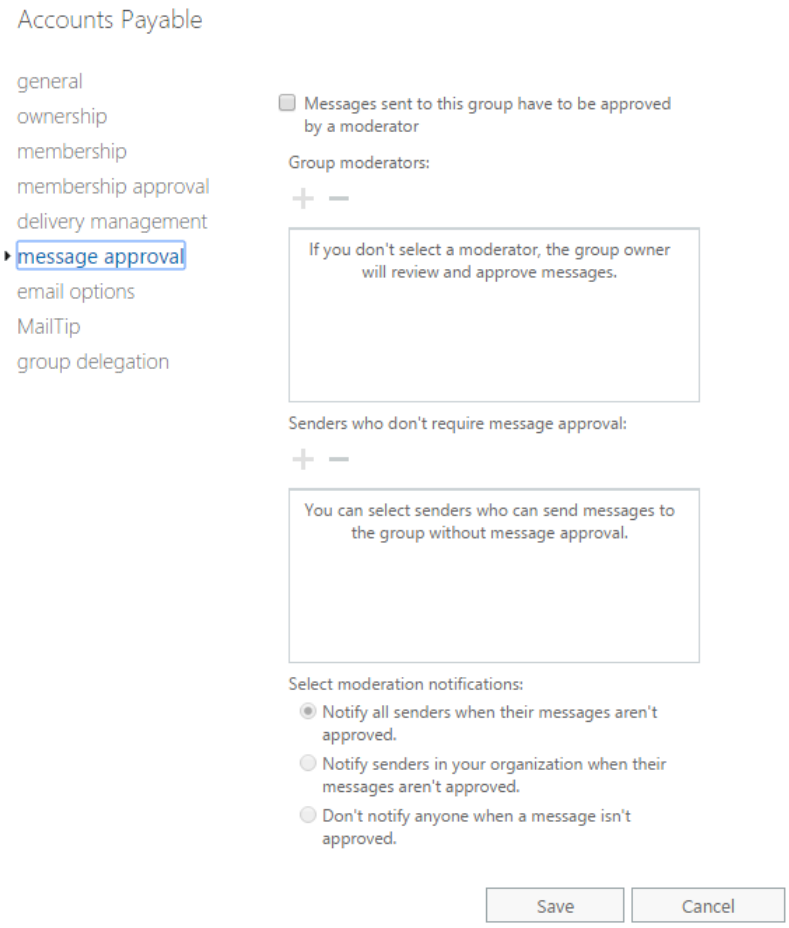

Figure 7: Configuring moderation for a distribution group

The drawback to moderation is that it does create a delay when sending to a group as each message requires the manual intervention of a moderator before it is delivered. **Senders who don't require message approval** is a great way to identify who can bypass moderation. Using the *All Employees* group as an example we could identify that the CEO of Space Corp, Harvey Lovell, should never be moderated. Harvey's messages will be received immediately without intervention whereas all other senders will continue to be moderated for approval.

Select moderation notifications determines whether or not the sender should be notified when their messages are rejected by a moderator. By default, all senders are notified when their messages are rejected. However, you can restrict this notification to just senders inside your organization, or, turn off rejection notices altogether. The absence of these notifications could cause an uptick in support calls.

Note: It is also possible to configure moderation with transport rules. For more information on transport rules refer to Chapter 5.

The **Email Options** tab lists all email addresses assigned to the group. By default, addresses populated here are assigned by an email address policy. Deselecting the checkbox **Automatically update email addresses**

based on the email address policy will block this group from retrieving its addresses from the email address policy. Keep in mind that any addresses already assigned by a policy will not be removed when this checkbox is unchecked.

The address highlighted in bold is the primary or reply address that recipients see when the group object sends them an email. The primary address is governed by the email address policy. To change the primary address, you will need to deselect the email address policy from managing this group, edit one of the secondary email addresses and check the box **Make this the reply address**. To manage the current list of email addresses, use the **Add**, **Edit** or **Remove** buttons.

The **MailTip** tab allows you to set custom notifications that alert senders when they add this mailbox as a recipient to an email message. This mail tip is shown above the recipient line. An example MailTip could be "All messages sent to this group are moderated."

The **Group Delegation** tab determines who can send as, or, send on behalf of the group. For example, a distribution group called *Customer Service* may be used to receive customer inquiries. These inquiries are then distributed to the individual mailboxes of the customer service team. The customer service team may wish to reply to these inquiries using the email address assigned to the customer service distribution group. Assigning the customer service representatives send as (or send on behalf) permissions allows them to send using this address. We covered delegation in greater detail in chapter 5. For more information check the section titled *Mailbox Delegation*.

Real World: A mail-enabled group is a great way to address multiple people at once. However, a common question is when should a shared mailbox be used over a distribution group.

A distribution group is a great form of one-way communication. Using our *All Employees* group as an example the use case for this group is for company-wide communications. This allows leadership to broadcast a message to all employees.

In contrast a shared mailbox is great for two-way communication or collaboration. For example, a shared mailbox could be used for a project. All conversations about the project are stored in the mailbox. The shared mailbox's calendar could be used to track project deadlines and milestones. Project team members can be added or removed to the mailbox as needed. The shared mailbox becomes particular useful as a historical record allowing any new team members to get up to speed regarding the project and decisions that have been made.

To take it one step further if SharePoint has been integrated a site mailbox could be used to add a document library to the mailbox. In Office 365 site mailboxes have given way to Office 365 groups which add even more functionality such as Planner. For more information on Office 365 groups check this article https://support.office.com/en-us/article/Learn-about-Office-365-groups-b565caa1-5c40-40ef-9915-60fdb2d97fa2

Let's look at performing some of these same tasks but with EMS. In this section, we also delve into some tasks that are not available via the EAC. To modify properties of a group we use either the **Set-DistributionGroup**, or, **Set-DynamicDistributionGroup** cmdlet depending on the group type.

In this example, we configure moderation for the *All Employees* dynamic distribution group. We specify a moderator, how rejection messages should be handled and which senders can bypass moderation. These parameters work for both Set-DynamicDistributionGroup and Set-DistributionGroup.

```
[PS] C:\> Set-DynamicDistributionGroup -Identity "All Employees" -ModerationEnable $true -
ModeratedBy "Rachel Hughes" -SendModerationNotifications Internal -
BypassModerationFromSendersOrMembers "Harvey Lovell"
```

In this command

-ModerationEnable either enables or disabled moderation with a true or false Boolean response.

-ModeratedBy identifies our moderators. You can specify multiple moderators with a comma separated list.

-SendModerationNotifications determines which senders will receive rejection notifications. Omitting this parameter keeps it at the default of *Always*. As its name implies *Always* will send a rejection notification to every sender. In our example, we specified *Internal*. *Internal* specifies that only internal senders will receive rejection notifications. The final setting is *Never*. *Never* instructs Exchange that no one should receive a rejection notification, regardless of whether they are internal or external.

-BypassModerationFromSendersOrMembers identifies a list of users who can send to the group without the need for moderation. In our example, we added Space Corp's CEO Harvey Lovell to this list.

An example of options not in the EAC include the maximum send and receive size of the group. For example, if we want to limit the maximum size of an email to a distribution group we can use the **-MaxReceiveSize** parameter. In the example below we set a max receive size of 1024 kilobytes. The unit of measure can include bytes, kilobytes, megabytes, gigabytes and terabytes.

```
[PS] C:\> Set-DistributionGroup -Identity "Accounts Payable" -MaxReceiveSize "1024 KB"
```

To manage distribution group membership, we use the **Get-DistributionGroupMember**, **Add-DistributionGroupMember** and **Remove-DistributionGroupMember** cmdlets. In this command, we retrieve members of the *Accounts Payable* group.

```
[PS] C:\> Get-DistributionGroupMember -Identity "Accounts Payable"

Name                                                    RecipientType
----                                                    -------------
Rachel Hughes                                           UserMailbox
Ed Patterson                                            UserMailbox
```

To add a member to the *Account Payable* group we can issue a command such as this.

```
[PS] C:\> Add-DistributionGroupMember -Identity "Accounts Payable" -Member "Sarah Gibbs"
```

Conversely to remove a member we simply switch the verb in the cmdlet to **Remove**. In this command, we take Sarah Gibbs back out of the Accounts Payable group.

```
[PS] C:\> Remove-DistributionGroupMember -Identity "Accounts Payable" -Member "Sarah Gibbs"
```

To manage membership for a dynamic distribution group we would use the **Set-DynamicDistributionGroup** cmdlet. For example:

```
[PS] C:\> Set-DynamicDistributionGroup -Identity "All Employees" -IncludedRecipients MailboxUsers -
ConditionalCompany "Space Corp"
```

Delete a group

In a prior section, we discussed how to mail-disable a group by removing its Exchange attributes. In this section, we will look at completely removing a group from both Exchange and Active Directory.

To delete a group, select the **Recipients** on the left and **Groups** tab across the top. Select the group you wish to delete. From the toolbar select the **Delete** button. Click **Yes** to confirm the deletion.

To delete a group from EMS we use the **Remove-DistributionGroup** cmdlet. For a dynamic distribution group, we use the cmdlet **Remove-DynamicDistributionGroup**. In the example below we remove a distribution group named "IT".

```
[PS] C:\> Remove-DistributionGroup -Identity "IT"
Confirm
Are you sure you want to perform this action?
Removing distribution group "IT" will remove the Active Directory group object.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"): Y
```

Mail-Enabled Contacts

Mail-enabled contacts are objects that contain information about people or entities external to your organization. A mail contact has an external email address and does not possess a mailbox in your organization.

A great example of this could be a supplier or vendor who needs to be frequently contacted by Space Corp employees. This supplier has their own email system which maintains its own mailboxes and email addresses. Email addresses for the supplier could be added as mail contacts. These mail contacts can then be added to the Global Address List so Space Corp employees can easily find them.

A second use case is for forwarding purposes. For example, if an employee needs their email forwarded from their mailbox to an external address, then a mail contact will need to be configured as the target.

One final use case is to allow external recipients to be added to a distribution group. External addresses cannot be added directly to a distribution group. They must be first created as a mail contact and that contact be added to the group.

In this section, we will look at how to create a mail-enabled contact using both the EAC and EMS.

In this example, we are going to create a contact for the research department at partner company Robotomics. This mail contact will be visible in the global address list for all Space Corp employees to see. Robotomics external email address for their research department is research@robotomics.com.

To perform this task, select **Recipients** on the left and **Contacts** across the top. From here click the **New** button and select **Mail Contact**.

On the *New Mail Contact* dialog (Figure 7-8) enter values for **Display name, Name, Alias** and **External Address**. First name, middle initial and last name are optional fields.

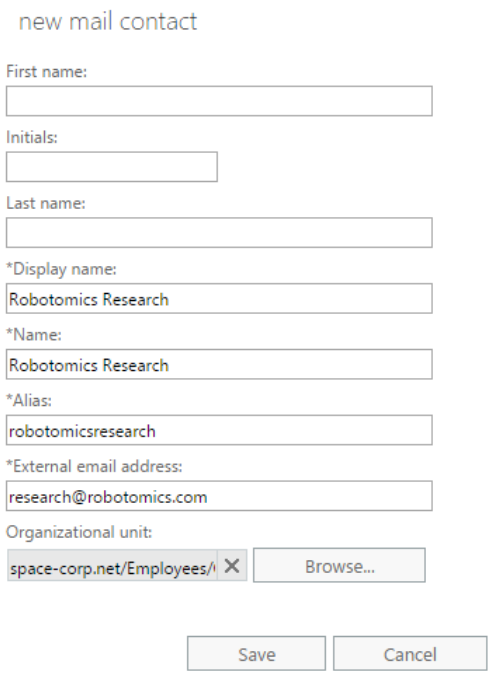

Figure 8: Creating a mail contact

Click **Browse** in the Organizational Unit section. This brings up the *Select an Organization Unit* dialog. From here you can select which OU you want the contact to be created under.

Click **Save**.

To create a contact in EMS we would use the **New-MailContact** cmdlet. Unlike the EAC not all the parameters are required. In EMS, we only need to specify the **-Name** and **-ExternalEmailAddress** parameters. The display name and alias fields will be generated from the name parameter.

```
[PS] C:\> New-MailContact -Name "Robotomics Research" -ExternalEmailAddress
"research@robotomics.com"
```

If we wanted to perfectly match our example from the EAC our command would look like this.

```
[PS] C:\> New-MailContact -Name "Robotomics Research" -DisplayName "Robotomics Research" -Alias
"robotomicsresearch" -ExternalEmailAddress "research@robotomics.com" -OrganizationalUnit "space-
corp.net/Employees/Contacts"
```

Note: For an extensive list of all available parameters for the **New-MailContact** cmdlet check the following article https://technet.microsoft.com/en-us/library/bb124519(v=exchg.160).aspx

It is also possible that contacts exist in Active Directory that are not mail-enabled. If you need to mail-enable an Active Directory contact you can use the **Enable-MailContact** cmdlet. This will assign mail attributes to the contact and allow it to be managed by Exchange.

In the following example we mail-enable an Active Directory contact named "Robotomics AP" and add an external email address.

```
[PS] C:\> Enable-MailContact -Identity "Robotomics AP" -ExternalEmailAddress
"accountspayable@robotomics.com"
```

If you ever need to reverse this action you can run the **Disable-MailContact** cmdlet.

```
[PS] C:\> Disable-MailContact -Identity "Robotomics AP"
```

To completely delete a mail contact and its Active Directory object you would run **Remove-MailContact** instead.

```
[PS] C:\> Remove-MailContact -Identity "Robotomics AP"
```

Mail-Enabled Users

Mail-enabled users take the mail contact one step farther. A mail-enabled user (or MEU) takes a user account in Active Directory and assigns it an external email address. A MEU does not have a mailbox. Like a mail contact the MEU will show in the global address list, can be used for forwarding and be added to a distribution group. The difference is that a MEU also provides the user with an Active Directory account that can be used to access internal resources such as network shares, printers or applications. Like any other AD account the MEU can be added to security groups and be granted security permissions.

A business case for a MEU could be contractor who needs access to internal resources but maintains their own external email address. In this instance an existing Active Directory account for the contractor could be mail-enabled to add their external address, or, if the contractor does not have an account a brand new mail-enabled user could be created in Exchange.

To create a mail-enabled user select **Recipients** on the left and **Contacts** across the top. From here click the **New** button and select **Mail User**.

On the *New Mail User* dialog (Figure 7-9) enter an **Alias**, pick the address type (in most cases this will be **SMTP**) and type the **External email address** for the user.

From here you can either mail-enable an existing user by selecting **Browse**. Or you can create a brand new Active Directory account by switching the toggle button over to **New User** and entering account details for **Display Name**, **Name**, **User logon name** and **Password**. First name, middle initial, last name and

organizational unit are optional fields but recommended. You can also select whether the user should change their password at next logon.

Click **Save**.

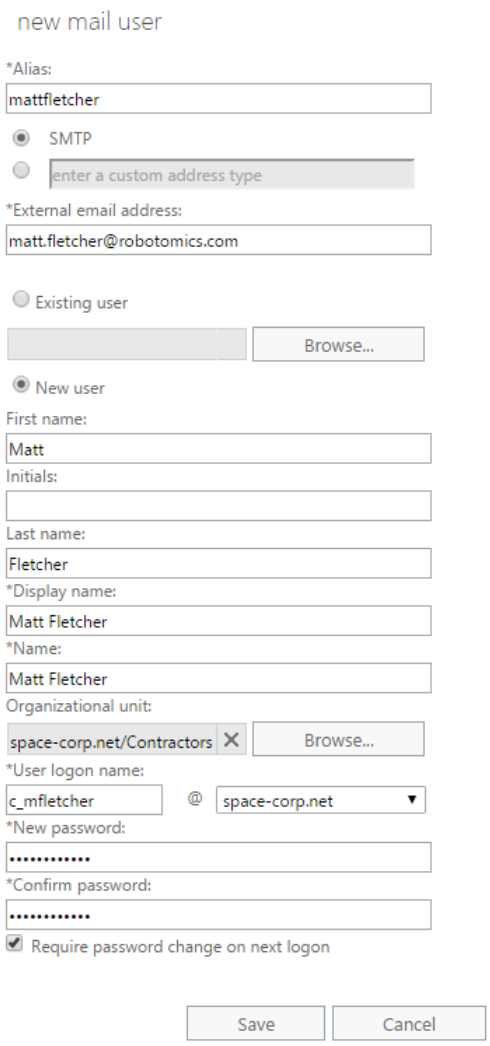

Figure 9: Creating a mail user

To create a new mail user from EMS we use the **New-MailUser** cmdlet. Using our example of Matt Fletcher from the EAC, let's see what that command would have looked like using EMS.

```
[PS] C:\> New-MailUser -Alias "mattfletcher" -ExternalEmailAddress
"SMTP:matt.fletcher@robotomics.com" -FirstName "Matt" -LastName "Fletcher" -DisplayName "Matt
Fletcher" -Name "Matt Fletcher" -OrganizationalUnit "space-corp.net/Contractors" -UserPrincipalName
"c_mfletcher@space-corp.net" -Password (ConvertTo-SecureString -String "Password123!" -AsPlainText -
Force) -ResetPasswordOnNextLogon $true

Name                                    RecipientType
----                                    -------------
Matt Fletcher                           MailUser
```

Like with mailbox creation in the previous chapter we specify the creation of an Active Directory account with the same parameters of **–UserPrincipleName** and **–Password**. Similarly, the **–ResetPasswordOnNextLogon** parameter dictates whether the user will need to reset their password the next time they log in.

> **Note:** For an extensive list of all available parameters for the **New-MailUser** cmdlet check the following article https://technet.microsoft.com/en-us/library/aa996335(v=exchg.160).aspx

To convert an existing Active Directory user into a mail-enabled user we use the **Enable-MailUser** cmdlet. In the following example, we add mail attributes and an external address to an Active Directory user with name Maureen Hurst.

```
[PS] C:\> Enable-MailUser -Identity "Maureen Hurst" -ExternalEmailAddress
"SMTP:maureen.hurst@robotomics.com"

Name                                    RecipientType
----                                    -------------
Maureen Hurst                           MailUser
```

If you ever need to reverse this action you can run the **Disable-MailUser** cmdlet.

```
[PS] C:\> Disable-MailUser -Identity "Maureen Hurst"
```

To completely delete a mail contact and its Active Directory object you would run **Remove-MailUser** instead.

```
[PS] C:\> Remove-MailUser -Identity "Maureen Hurst"
```

Office 365 Groups

Office 365 groups are a cloud-only collaboration option that includes a shared mailbox, a SharePoint document library, a OneNote notebook, and Microsoft Planner. In many ways, Office 365 Groups are the successor to the SharePoint site mailbox. Unfortunately, this feature rich collaboration is not available to on-premises users. Not even to those with a hybrid connection.

A small consolation does exist that allows on-prem users to send and receive email to and from the Office 365 group with the proper configuration and licensing. This is made available through a feature in Azure AD Connect called Group Writeback. Group Writeback creates a distribution group on-premises that represents the Office 365 group in the cloud. This makes the group available to the on-prem users for email purposes. This feature does require a subscription to Azure AD Premium.

Azure AD Connect and Office 365 Groups are outside the scope for this book.

For more information on Group Writeback check this article: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-feature-preview#group-writeback

For more information on Office 365 groups check this article: https://support.office.com/en-us/article/Learn-about-Office-365-groups-b565caa1-5c40-40ef-9915-60fdb2d97fa2?ui=en-US&rs=en-US&ad=US

Summary

In this chapter, we took a look at the various mail-enabled group. We also explored mail-enabled users and mail-enabled contacts. We discussed how to perform common administrative tasks through the Exchange Admin Center (EAC) and the Exchange Management Shell (EMS). Tasks that included the creation, deletion and management of these mail objects.

In the next chapter, we explore public folders including; architectural changes, managing the new architecture, and, the day to day administrative tasks surrounding public folders.