Configuring SecurityGateway to Filter Office365 Mail

Out of the box, Microsoft's Office 365 email security provides basic spam and malware filtering. If you want something more substantial that can be fine tuned to YOUR business, then SecurityGateway may be just what you need.

SecurityGateway incorporates multiple AV engines and proactive Outbreak Protection technology, combined with additional signature recognition and heuristic analysis, to detect viruses, spam, phishing, spyware and other types of unwanted and harmful email.

Outbound data leak prevention allows administrators the flexibility to customize and control the flow of outbound email - to prevent the sending of unauthorized content and attachments such as credit card numbers and banking information.

The new **Archive** feature ensures that you have a perfect copy of all emails if the email is accidentally or intentionally deleted.

Colour-coded and searchable logs make it quick and easy to understand the full end-to-end journey any inbound or outbound messages have taken.

SecurityGateway will hit the ground running with optimized default settings, however, you've also got granular control over every aspect of the security settings when it's needed.

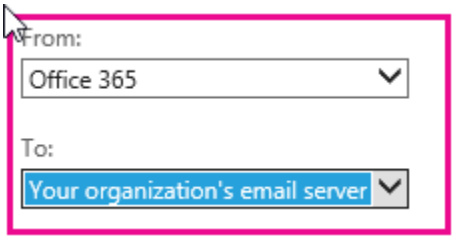
Overview of the steps

- **Part 1**: Configure mail to flow from Office 365 to SecurityGateway (Outgoing)
- **Part 2**: Configure mail to flow from SecurityGateway to Office 365 (Incoming)
- **Part 3**: Set up SecurityGateway
- **Part 4**: Change DNS Settings

PART 1: Setup **outgoing** email from Office 365 mailbox > SecurityGateway > Internet

1. Create connectors on Office 365 to relay to SecurityGateway

- Log in to the **Microsoft Office 365 admin center**.
- Click **Admin -> Admin Center -> Exchange -> Exchange Admin Center**
- Select **'mail flow'** -> **'accepted domains'**
- Edit your domain and switch your accepted domain type from 'Authoritative' to **'Internal Relay'** which is important until the account synchronization is done with SecurityGateway.
  *(You need to switch back to **Authoritative** once the all available accounts on Office 365 have been added into SecurityGateway.)*
- To create a connector, Select **'Mail Flow'** -> **'Connectors'**
- Click on the plus symbol **(+)** to add a new connector.
- If any connectors already exist for your organization, you can see them listed here.
- Under **'Select your mail flow scenario'**, select the following:
  - **From: Office 365**
  - **To: Your organization's email server**

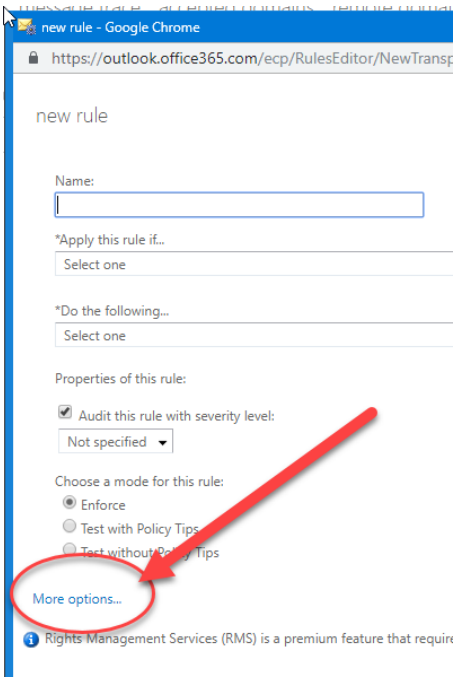


- Click **'Next'**
- Type a name and description for the new connector. ie *"SMTP- Outbound"*
- Check the options **'Turn it on'** and **'Retain internal Exchange email headers'**
- Click **'Next'**
- Select the first option **'Only when I have a transport rule set up that redirects messages to this connector'** and click **'Next'**
- In the **'Routing Method'** section, enable the option to **"Route email through these smart hosts"**
- Click the plus sign **(+)** and the **'add smart host'** dialogue box appears.

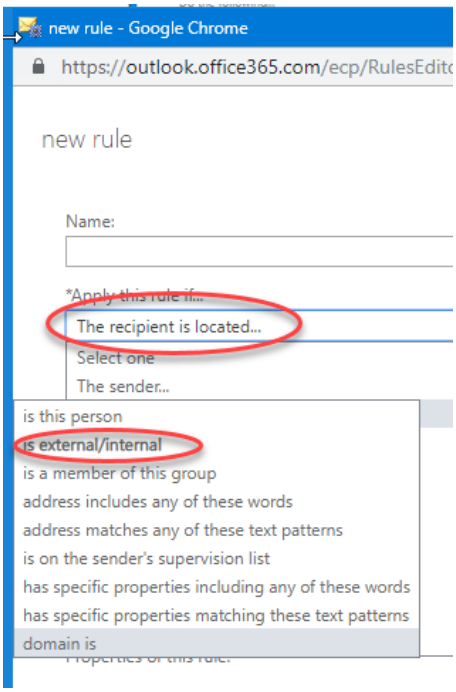
- Type the fully-qualified domain name (FQDN) of your SecurityGateway server. The FQDN is typically in the format of hostname.domain.com or the static IP.
- Click **'Save'**, and then click **'Next'**
- Choose if you want to have all emails use TLS when sending to SecurityGateway, and then click **'Next'**
- To validate the connector, type a recipient email address on a domain outside of your organization.
- Once the connector is successfully validated, click **'Save'**
- If the connector does not validate, double-click the message displayed to get more information and see About fixing connector validation errors for help resolving issues.

2. Create a rule to route all outgoing emails using the above connector

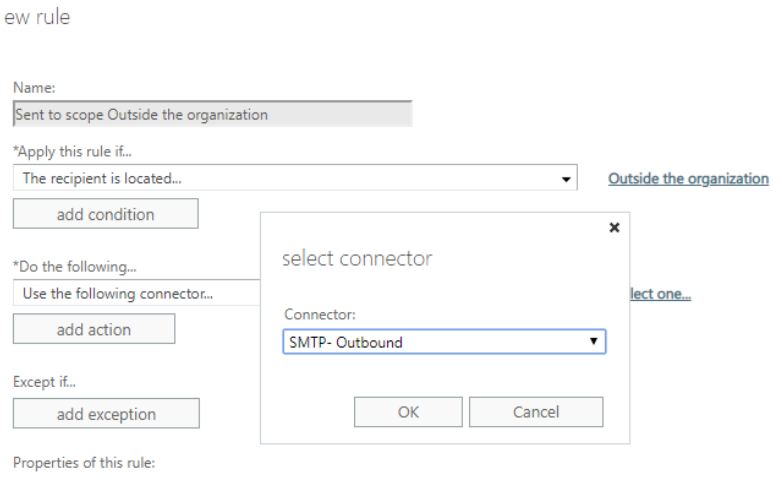
- Still in **Admin -> Admin Center -> Exchange -> Exchange Admin Center**
- Select **'Mail flow'** -> **'rules'**
- Click on the plus symbol **(+)** and select **'Create a new rule'**.
- Give an appropriate name to the rule
- Click the **"more options"** link



- Under the **'Apply this rule if'**, select **'the recipient'** -> **'is external/internal'** -> select **'outside the organization'** -> **OK**



- Under **'Do the following'** select **'Redirect the message to'** -> **'the following connector'**-> select the connector which you created in the above section -> **OK**



- **'Save'** the rule.

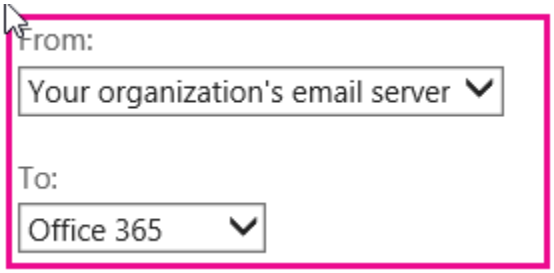
You now have all outgoing mail from Office 365 redirected to your SecurityGateway Email Firewall for filtering prior to delivery to the recipient address.

PART 2: Setup incoming email from the Internet > SecurityGateway > Office365 Mailbox

Create a new connector in Office365 to relay from SecurityGateway

1. Log in to the **Microsoft Office 365 admin center**.
2. Click **Admin** -> **Admin Center** -> **Exchange** -> **Exchange Admin Center**
3. To create a connector, Select **'Mail Flow'** --> **'Connectors'**
4. All currently existing connectors for your organization are displayed
5. Click on the plus symbol **(+)** to add a new connector.
6. Under **'Select your mail flow scenario',** select the following:

   From: Your organization's email server
   To: Office 365



7. Click **'Next'**
8. Type a name and description for the new connector.
9. Check **'Turn it on'** and **'Retain internal Exchange email headers'** click **'Next'**.
10. To identify your SecurityGateway server, either enter domain name by selecting the first option or if the SecurityGateway server has static IP (recommended) then add the IP by selecting the second option
11. Click **'Next'**
12. Confirm what you entered and **Save**

PART 3: Setup SecurityGateway

Domain Creation

- Log in with your Global Administrator account on SecurityGateway
- Click **SETUP/USERS →Accounts →Domains and Users**
- Under the Domain List, select **'New'**
- Enter the domain name. For example, wingate.ca -> **Save** and **Close**

User Verification Source

(This option is used to verify accounts on Office 365 during incoming and outgoing email transfer.)

Follow the steps below to allow SecurityGateway to utilize Office 365 as a user verification source.

Note: To allow SecurityGateway to access the Office 365 tenant, the Office 365 plan requires Exchange Online. Please make sure the Office 365 plan includes this feature.

SecurityGateway requires a service principal that has been granted permission to access the Office 365 tenant. This makes it possible for SecurityGateway to utilize Office 365 as a user verification source.

Office 365 utilizes Azure Active Directory as its directory service and a PowerShell module must be installed first. PowerShell 5.1 or higher is required on a 64-bit operating system in order to operate correctly. PowerShell 5.1 is the default build for Windows 10 and Windows Server 2016. Previous operating systems will need to install it from the Windows Management Framework.

Install and Configure Windows Management Framework (WMF) 5.1

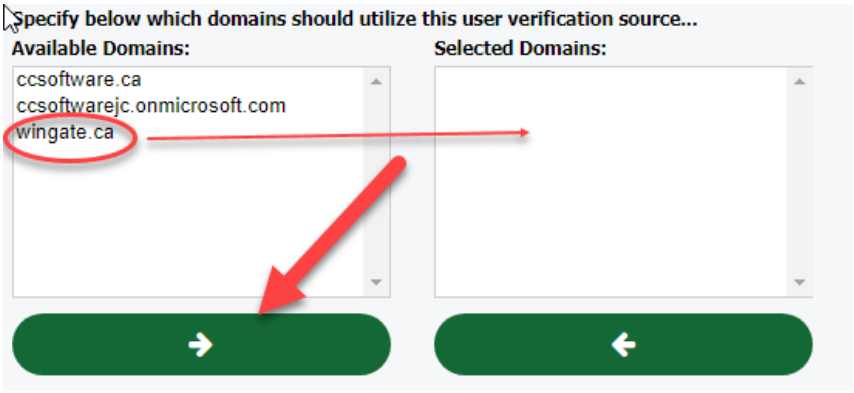
Connect to Office 365 PowerShell

When the PowerShell module has been installed, follow the steps below to create a service principle for SecurityGateway.

1. Open PowerShell
2. Use one of the following commands to connect to the AD Azure tenant.
    a. Office 365 Worldwide (+GCC)
        - **Connect-MsolService -AzureEnvironment AzureCloud**
    b. Office 365 Germany
        - **Connect-MsolService -AzureEnvironment AzureGermanyCloud**
    c. Azure China Cloud
        - **Connect-MsolService -AzureEnvironment AzureChinaCloud**
3. Enter the Office 365 administrator credentials when prompted.
4. (Optional) Enter the following command to review a list of existing service principals.
        - **Get-MsolServicePrincipal**
5. Enter the following to create a new service principal.
        - **$principal = New-MsolServicePrincipal -DisplayName 'SecurityGatewaySP' -ServicePrincipalNames @("SecurityGatewaySP") -Type Password -Value 'use_a_password_of_your_choice_here' -StartDate (Get-Date) -EndDate (Get-Date).AddYears(1)**
            - The service principal object will be created and stored in the $principal variable.
            - The service principal's password is valid for one year from its create date by default.
6. The Directory Readers role must be assigned for the service principal to be able to read information from the Azure AD tenant. Enter the following command to do this.
        - **Add-MsolRoleMember -RoleName "Directory Readers" -RoleMemberType ServicePrincipal -RoleMemberObjectId $principal.ObjectId**

7. Follow the remaining steps in SecurityGateway:
    1. Click **SETUP/USERS** -> **Accounts** -> **User Verification Sources**
    2. Under **'User Verification Sources'**, Select **'New'**
    3. Under the **'Properties',** select **'Type: Office 365'**
    4. Give a description
    5. Enter **Domain Name:.** For example: wingate.ca
    6. Select the **Cloud type** which you have selected in **Step-2**. Here it is Global

7. Enter **Service Principal name** and **password** which you entered in the powershell in **step-5**.
8. Under the **'Type'** section, select the name of your Office365 domain from available domains list and use the arrow **(→)** button to add in the selected domain.



9. Select **Save and Close**

8. Under the **User Verification Source** page, Select **Verify Users** to add your all users to SecurityGateway from Office 365.

Domain Mail Servers

These are the servers on which your users have their email accounts and where their messages are stored (in this case it is Office 365). When SecurityGateway receives a message for a verified user of one of your domains, it will attempt to deliver the message to the mail servers associated with that domain.

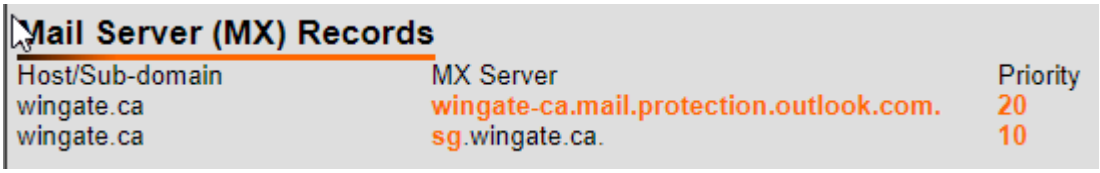
1. Click **SETUP/USERS** -> **Mail Configuration** -> **Domain Mail Servers**
2. Under Domain Mail Servers, select **'New'**
3. Insert all the same credentials and details you already added for **User Verification Source**

Now, let's do a test by sending a message from one of your Office365 accounts to any outside domain to test outbound email. The message must pass through SecurityGateway and the Call Forward Verification will automatically add the new account in SecurityGateway as the first user.

PART 4: Change DNS settings

• The final, and very important step in configuration!

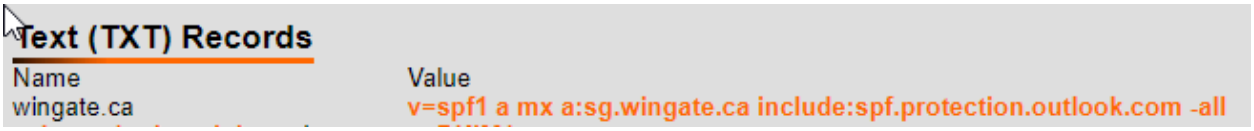
1. Add an 'A' record in your DNS settings to point to your SecurityGateway static IP address
2. In the MX record give the highest priority to your SecurityGateway then next to Ofice365 to direct emails first to your SecurityGateway. The lower number in the MX record is given the highest priority.



Mail Server (MX) Records

Host/Sub-domain	MX Server	Priority
wingate.ca	wingate-ca.mail.protection.outlook.com.	20
wingate.ca	sg.wingate.ca.	10

3. Create an SPF record for your Office 365 domain. An SPF record can be added to the TXT Records in DNS.



Text (TXT) Records

Name	Value
wingate.ca	v=spf1 a mx a:sg.wingate.ca include:spf.protection.outlook.com -all

• Validate your DNS settings and wait for the approval from your provider which can take up to 2 days.

If everything is set up correctly then you are ready to use SecurityGateway in front of Office 365 for both incoming and outgoing mail filtering. If you need any assistance configuring this, contact C&C Software and we'll be happy to assist you.

support@ccsoftware.ca