Connecting Microsoft365 with Cleanmail Sign+Encrypt

Prerequisites

1. Sign+Encrypt and Certificate retrieval is configured by Cleanmail, and you have the activation mail.
2. Domain Gateway is configured by Cleanmail, and you have the activation mail.
3. For Microsoft365 configuration, you have access to the Exchange Admin Center (“EAC”) on Microsoft365 for this tenant.
4. For log access, you have access to the Cleanmail quarantine for this customer (https://quar.cleanmail.ch/)
5. For DNS changes, you have direct access to the DNS administration for the customer domain, or you have the ability to order DNS changes.
6. You have access to a test mailbox in the customer domain.

Mailflow Incoming

1. Cleanmail configured the target server for the customer domain on Microsoft365 (<customer-domain-id>.protection.outlook.com).
2. Set the MX record for this domain according to the activation mail for the Domain Gateway (<customer-domain-shorthand>1/2.cleanmail.ch). For more information, see the Domain Gateway activation email.
3. Verify that messages from an external sender can be received in the test mailbox.
4. EAC / mail flow / accepted domains: Ensure that the domain is configured as “Authoritative”.
5. EAC / protection / connection filter: Ensure that the IP ranges of Cleanmail https://www.cleanmail.ch/cleanmail-ip-adressbereiche-und-firewall/ are in the “Default” connection filter in the “IP Allow” list.

Mailflow Outgoing

1. Set the SPF record for the customer domain according to https://www.cleanmail.ch/spf-eintrag/ (summary: add the “`include:_cmspf.cleanmail.ch`” directive).
2. Verify that messages can be sent from the text mailbox to an external recipient.

3. ~~EAC / mail flow / rules:~~ [1]

    a. ~~Create a new rule of type "modify messages".~~

    b. ~~Give it a descriptive name.~~

    c. ~~Select "Apply this rule if…" => "Outside the organization"~~

    d. ~~"Do the following…" => "Set the message header to this value…"~~

    e. ~~For message header, click on "Enter text…" and use the header provided in the activation mail ("X-Cleanmail-NNNNnn").~~

    f. ~~For "to the value", click on "Enter text…" and use the value provided in the activation mail ("<random string>").~~

    g. ~~De-select "Audit this rule with severity level…"~~

    h. ~~Click on "Save"~~

4. EAC / mail flow / connectors:

    a. Click the "+" icon to create a new connector

    b. Select From: "Office365", To: "Partner Organization", click "Next"

    c. Give the connector a meaningful name and description, select "Turn it on", click "Next"

    d. Select "Only when messages are sent to these domains", click the "+" icon and enter "*" for the domain name. Click "Next"

    e. Select "Route email through these smart hosts", click the "+" icon and enter "sign.cleanmail.ch" as the name of the smart host, click "Save", then "Next"

    f. Leave the defaults for "Always use Transport Layer Security (TLS).." page, click "Next"

    g. On the "Confirm your settings" page, click "Next"

    h. On the "Validate this connector" page, add one or more email addresses for testing by clicking the "+" icon. Note that you can not continue without a test, and that you must use an email address outside of the customer domain.

    i. The log entry for these validation emails will be available in the Cleanmail quarantine after a few minutes.

5. Test that you can send messages to external recipients. Depending on the settings for this customer, emails are automatically signed.

6. After you finished the test, and if this is a test-only mailbox, please notify support@cleanmail.ch to remove the account and certificate on Sign+Encrypt for this mailbox.

[1] Currently not in use

Note for combined use of Sign+Encrypt and Mail Archive

If the customer uses both Sign+Encrypt and the Mail Archive, it must be ensured that the mails to the journaling mailbox (<something>@journaling.cmarchive.ch) do *not* pass through the Sign+Encrypt smarthost. Such mails *must* be directly sent to the journaling destination. To do this, create an additional connector:

1. Send a test email from the customer domain on Microsoft365 to the journaling destination mailbox address. Note the Received: headers mentioning “seppmail”.
2. EAC / mail flow / connectors
    a. Click the “+” icon to add a new connector
    b. Select From: “Office365”, To “Partner Organization”, click “Next”
    c. Give the connector a meaningful name and description, select “Turn it on”, click “Next”
    d. Select “Only when messages are sent to these domains”, click the “+” icon and enter “journaling.cmarchiv.ch” for the domain name. Click “Next”
    e. Select “Use the MX records associated with partner’s domain”, click “Next”
    f. Leave the defaults for “Always use Transport Layer Security (TLS)..” page, click “Next”
    g. On the “Confirm your settings” page, click “Next”
    h. On the “Validate this connector” page, add the journaling destination mailbox address (<something>@journaling.cmarchive.ch) for testing by clicking the “+” icon. Note that you can not continue without a test, and that you must use an email address outside of the customer domain.
    i. The log entry for these validation emails will *not* be available in the Cleanmail quarantine or log files.
3. Send a test email from the customer domain on Microsoft365 to the journaling destination mailbox address and verify that there are no Received: headers mentioning “seppmail”.