Secure Delivery & Receipt in Mimecast

Last Modified on 23/01/2020 9:57 am GMT

Secure Delivery and Receipt policies allow you to control the TLS and encryption settings for emails sent and received with external email addresses by the Mimecast gateway. Some organisations dealing with sensitive data will require you to use these policies to communicate with them. This is common for Banks and other financial institutions.

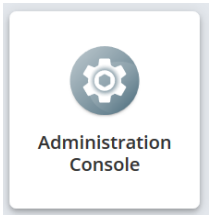
Secure Delivery defines the policy for outbound emails. Secure Receipt defines the policy for inbound emails.

These policies only control encryption on the connection. Once the email is received by the recipient, it does not prevent them keeping the email unencrypted.

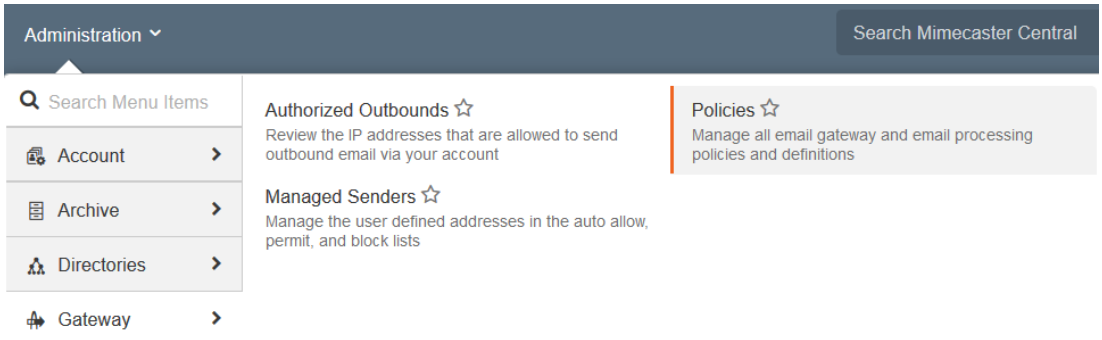
Delivery Definition

The Secure Delivery Definition defines the settings to use for the connection Mimecast makes with recipient servers.

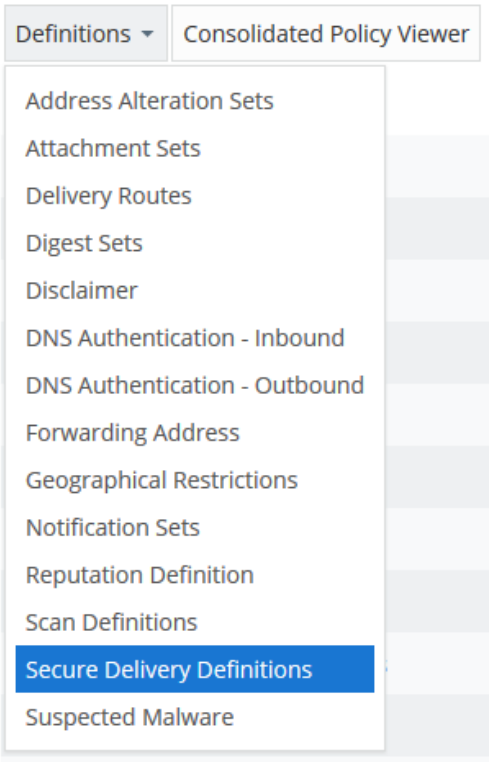
1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**



3. Go to **'Administration > Gateway > Policies'**

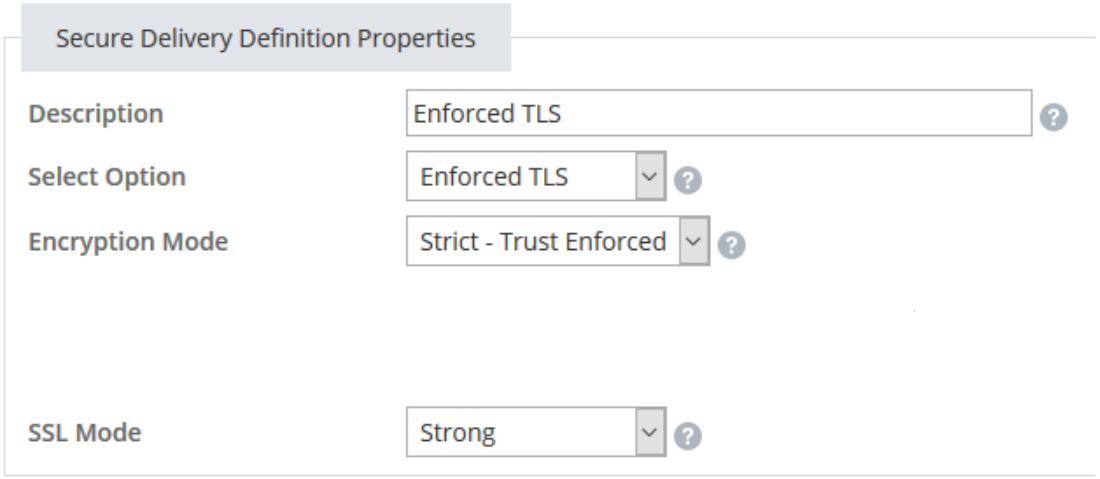


4. From the **Definitions** dropdown, select **Secure Delivery Definitions**



5. Select **Add Secure Delivery Definition**
6. Set the name (**Description**) for the Definition
7. Select the TLS setting (Option) to use:
    a. **Opportunistic TLS (Default)**: Mimecast will attempt to deliver the email using a encrypted TLS connection. It will failover to an unencrypted connection if it cannot establish the secure connection.
    b. **Enforced TLS**: Mimecast will attempt to deliver the email using a encrypted TLS connection. If the secure connection cannot be established, Mimecast will attempt to retry the secure connection periodically. The message will be dropped if it cannot be delivered after multiple retries.
    c. **No TLS**: Mimecast will not attempt to use an encrypted connection to the recipient server.
8. Set the Encryption Mode:
    a. **Strict**: Requires the recipient server to have a trusted public certificate when establishing a secure connection
    b. **Relaxed**: Allows the recipient server to use a valid certificate, even if it does not have a complete trust chain

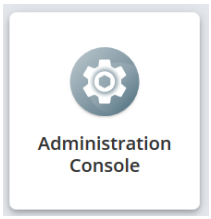
9. Set the SSL Mode
    a. You should generally use Strong or greater, however some older recipient mail servers may require a lower setting to be used.
10. Press **Save and Exit**



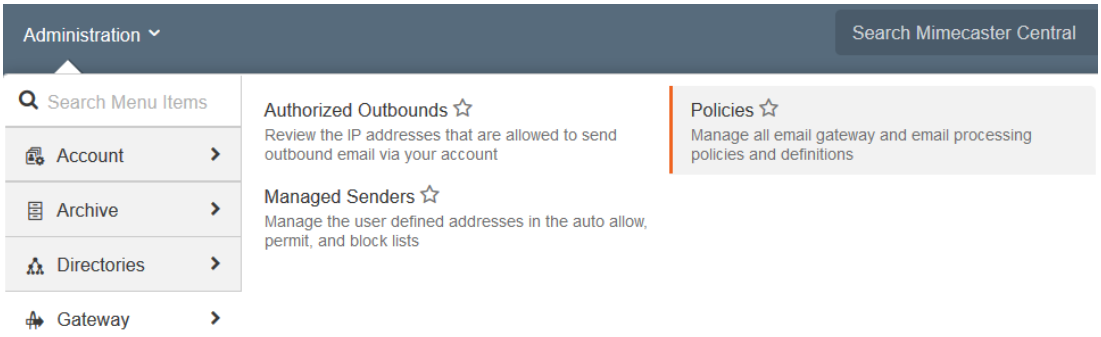
Delivery Policy

The Secure Delivery Policy determines when a Secure Delivery Definition should apply.

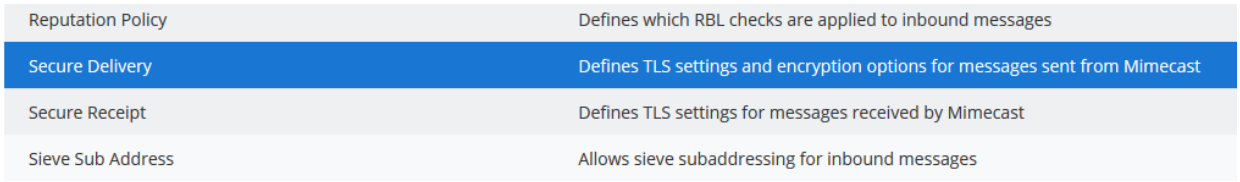
1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**



3. Go to **'Administration > Gateway > Policies'**

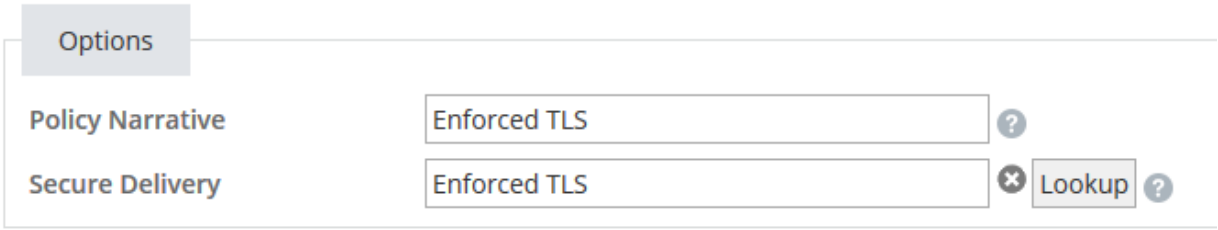


4. Select **Secure Delivery** from the policies list

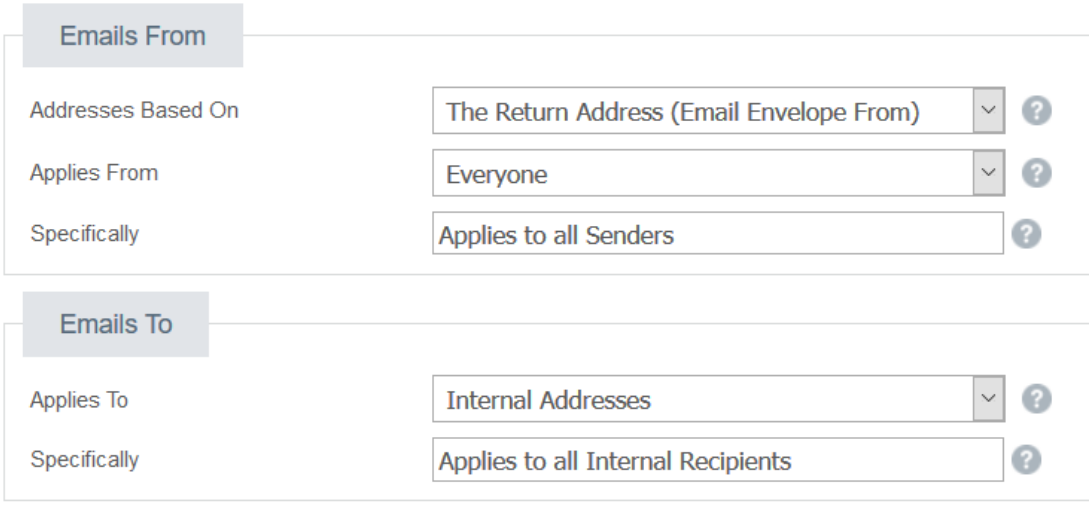


5. Select **New Policy**
6. Give the policy a name (**Policy Narrative**)
7. Set **Secure Delivery** to the Definition you created

Note: Use the Lookup button to browse your definitions, then use the**Select** option next to the definition to use.



8. Set the scope for the policy under **Emails From** and **Emails To**
9. Press **Save and Exit**

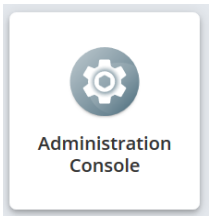


Only one Secure Delivery Policy will apply to an email. If you need to ensure a policy is picked, you should enable the **Policy Override** option within the policy.

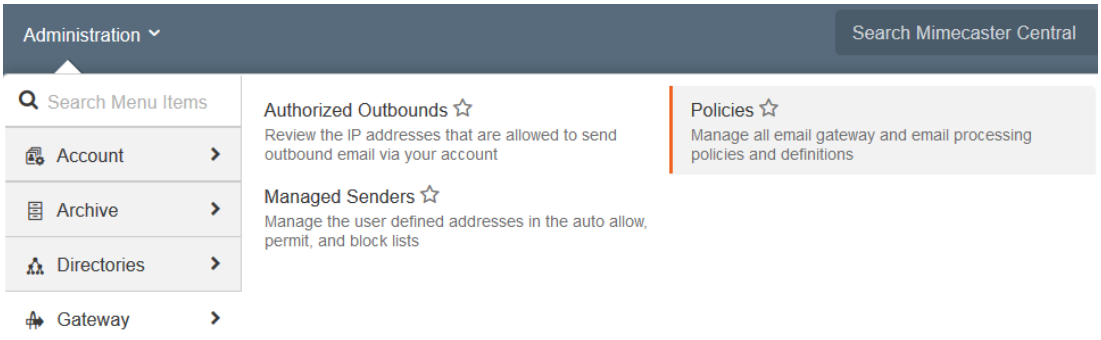
Receipt Policy

The Secure Receipt Policy determines which Secure Receipt option should apply. No definition is required for this policy, as these are pre-built by Mimecast.

1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**



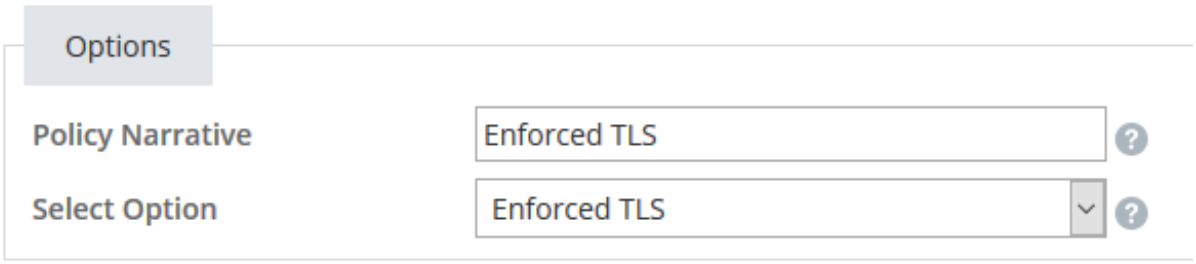
3. Go to **'Administration > Gateway > Policies'**



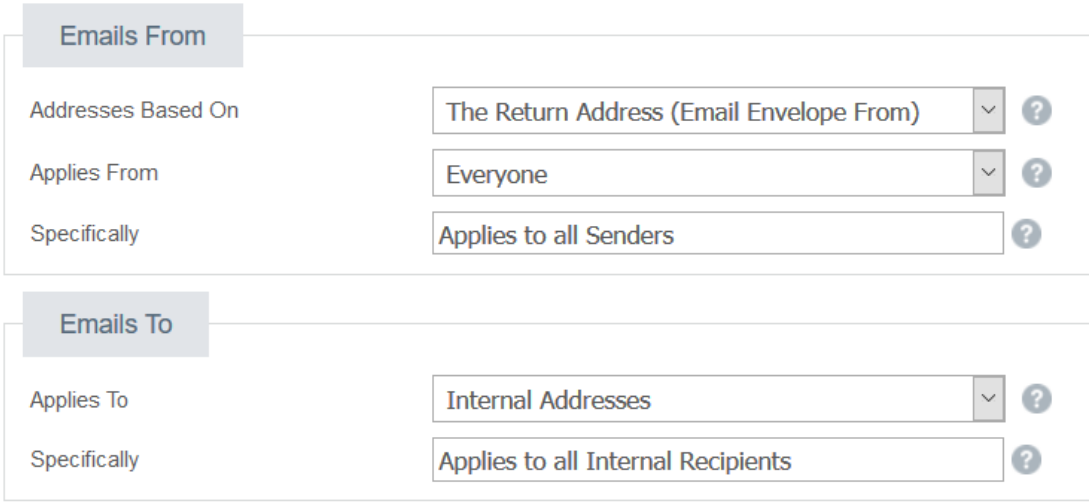
4. Select **Secure Receipt** from the policies list

Reputation Policy	Defines which RBL checks are applied to inbound messages
Secure Delivery	Defines TLS settings and encryption options for messages sent from Mimecast
Secure Receipt	Defines TLS settings for messages received by Mimecast
Sieve Sub Address	Allows sieve subaddressing for inbound messages

5. Select **New Policy**
6. Give the policy a name (**Policy Narrative**)
7. Set the Secure Receipt option to apply:
    a. **Opportunistic TLS (Default)**: Mimecast will attempt to receive the email using a encrypted TLS connection. It will failover to an unencrypted connection if it cannot establish the secure connection.
    b. **Enforced TLS**: Mimecast will attempt to receive the email using an encrypted TLS connection. The message will be dropped if the secure connection cannot be established.
    c. **TLS 1.2 or greater + NCSC**: Mimecast will attempt to receive the email using an encrypted TLS connection. The connection will need use TLS 1.2 or greater and conform to NCSC guidelines for securing email. The message will be dropped if the secure connection cannot be established.



8. Set the scope for the policy under **Emails From** and **Emails To**
9. Press **Save and Exit**



Only one Secure Receipt Policy will apply to an email. If you need to ensure a policy is picked, you should enable the **Policy Override** option within the policy.