

# DKIM configuration for Symantec cloud

Please follow the below three steps to configure DKIM for the office 365 cloud

- Add a selector to a domain
- Update the public DNS record
- Verify propagation and then enable DKIM for the domain

## **Step 1: Add a selector to a domain**

- On the **Outbound DKIM Signing Settings** page, locate the domain to which you want to add the selector. Enter the domain name in the Search box or scroll through the domains with the Previous Page/Next Page arrows.
- Click the domain name to select it. A new dialog box with the domain name at the top appears.
- Click **Add New**, and ensure that the radio button to the left of the new selector item is selected
- Enter a name for the selector (alphanumeric characters only). Symantec recommend usage of the date in the selector name to make it easier to rotate selectors in the future.
- Select a key length from the DKIM Key Length drop-down list. The longer the key, the more secure it is--select the longest key that your DNS provider supports.
- The two DNS TXT record fields are automatically populated. Click Save to save the values, but do not close the dialog. The dialog must stay open so that you can copy these values into your public DNS record in the next step.

## **Step 2: Update the public DNS record**

- With the domain name dialog box still open, navigate to the public DNS TXT record for the domain.
- Click the **Copy to Clipboard** icon to the right of the Host Name field. Follow your DNS provider's instructions to paste the value to the relevant field in your DNS record.
- Click the **Copy to Clipboard** icon to the right of the TXT value field. Follow your DNS provider's instructions to paste the value to the relevant field in your DNS record.
- Click Close to close the domain name dialog box.
- Note: It can take up to 72 hours for a DNS record change to propagate throughout the Internet. Propagation must be complete before DKIM can be enabled for this domain.

## **Step 3: Verify propagation and then enable DKIM for the domain**

- To be certain that the updated DNS record has propagated, on the main Outbound DKIM Signing Settings page, click the domain name. The domain name dialog box appears.
- Ensure that you have selected the appropriate selector. Then click Test to perform a DNS lookup to check whether the DNS TXT record matches the active selector in the portal.
- If the test succeeds, then close the domain name dialog box to return to the DKIM Signing Settings page. Use the slider in the DKIM Enable column to enable DKIM for that domain.

### **Note:**

Please refer to the below URL for further details

<https://support.symantec.com/us/en/article.tech249633.html>