[Now Available, Action Required] Secure Access SAML Authentication Certificate for Web Security and Zero Trust expiring 27th June 2024

Updated Certificate now available, action required.

You must renew the SWG SAML certificate before it expires on 27th June 2024.

The Secure Access SAML certificate used for user identification will expire on the 27th of June 2024 10:41:19 (UTC).

You must update your Identity provider (IdP) with the new Secure Access SAML certificate before 27th of June 2024 10:41:19 (UTC). **Updating this certificate is essential to avoid SAML user authentication failures and loss of internet access for these users, unless your IDP has already been configured to monitor the Umbrella SAML metadata URL provided below.**

Download the updated SAML Metadata:

https://api.sse.cisco.com/admin/v2/samlsp/certificates/Cisco_SSE_SP_Metadata.xml

Download the updated SAML Certificate:

https://api.sse.cisco.com/admin/v2/samlsp/certificates/Cisco_SP_Signing_Certificate_May2024.cer

The metadata has been updated and includes both the current and the new signing certificate. At expiry of the current certificate, the new certificate will be used for signing. **DO NOT** delete any current certificates. Secure Access continues signing with the old certificate until the time of expiry.

This is an annual task, and the Secure Access metadata URL remains constant from previous years. When the certificate is renewed, we will update the metadata without changing the URL. This approach will support those identity providers, like ADFS and Ping Identity, that can monitor the relying party metadata URL and automatically update when the relying party metadata is updated with a new certificate.

For more information on renewal options see, https://docs.sse.cisco.com/sse-user-guide/docs/saml-certificate-renewal-options

Note -

- Some Identity Providers do not perform validation of SAML request signatures and therefore do not require our new certificate. If in doubt, please contact your Identity Provider vendor for confirmation.

- If using the Secure Access SAML feature, Org-Specific EntityID feature, then you must not use URL-based metadata updates. Org-Specific Entity ID only applies if you have multiple Secure Access orgs linked to the same identity provider. In this scenario you should manually add the new certificate to each IDP configuration.

For more information, contact support.

Regards,

Secure Access Technical Support team.