**[Action Required] Secure Access SAML Authentication Certificate for Web Security and Zero Trust User Identity Expiring 27th of June 2024**

The Secure Access SAML certificate used for Web Security and Zero Trust Authentication will expire on the 27th of June 2024 10:41:19(UTC). This certificate will be renewed and made available on the 27th of May 2024. This will allow time from then until the 27th of June for you to update your identity provider (IdP) with the renewed Secure Access SAML certificate.

Updating the certificate is essential to avoid SAML user authentication failures and loss of internet access for those users.

This first communication is intended to make you aware of this upcoming event and provide time to plan and schedule the certificate update task with your Identity Provider.

Once the certificate is renewed and made available, a further confirmation update will be published.

This is an annual task; however, the Secure Access metadata URL will remain constant from previous years. This is why we recommend utilising the metadata URL to automatically acquire the renewed certificate, rather than using a manual import process. When the certificate is renewed, we will update the metadata without changing the metadata 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 you have any questions, do not hesitate to contact your support contact.