[Now Available, Action Required] Secure Access SAML Authentication Service Provider Certificate for VPNs with a configured VPN Profile expiring 13th September 2024

Updated Certificate now available, action required.

The Secure Access SAML certificate used for user identification will expire on the **13th of September 2024 19:24:58 (UTC)**. You must renew the VPN Service Provider SAML certificate before it expires on 13th September 2024.

If currently using SAML Request Validation within your IdP, you must download the new Service Provider certificate, update your IdP with this new certificate, and activate the certificate on the Cisco Secure Access dashboard within 24 hours before the current certificate expires. Failure to do this will result in SAML user authentication and connection failures.

For steps to renew, please see: https://docs.sse.cisco.com/sse-user-guide/docs/manage-certificate-rotation

Note -

- Some Identity Providers do not perform validation of SAML request signatures and therefore do not require our new certificate. However, we suggest activating new certificate to dismiss the expiry notifications. Please contact your Identity Provider vendor for confirmation.
- If you have multiple Secure Access orgs linked to the same identity provider, you should manually add the new certificate to each IdP configuration.

For more information, contact support.

Regards,

Secure Access Technical Support team.