Upgrade Expired Umbrella SWG SAML Certificate

Contents

Introduction

This document describes a call to action to upgrade the Cisco Umbrella Secure Web Gateway (SWG) SAML certificate that expired on 8/12/2023.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella SWG.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Action Required

Updated Umbrella SWG SAML Certificate are now available.

You must renew the SWG SAML certificate that expired on August 12, 2023.

The Umbrella SAML certificate used for Umbrella user identification expired on the 12th of August 2023 06:44:04 (UTC).

You must update your Identity provider (IdP) with the new Umbrella SAML certificate.**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 here:**

- Download the updated SAML
  Metadata: https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

- Download the updated SAML Certificate: https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Certificate_Jun2023.c

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

This is an annual task, and the Umbrella metadata URL remains constant from previous years. When the certificate is renewed, Cisco Umbrella updates the metadata without changing the URL. This approach supports 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 Umbrella Support articles.

Additional Information

- 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 Umbrella 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 Umbrella orgs linked to the same identity provider. In this scenario you must manually add the new certificate to each IDP configuration.

For more information, contact Umbrella Support.