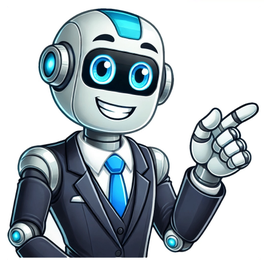
Continue



If you encounter any Security Assertion Markup Language (SAML) app error messages, here are sometroubleshooting steps to help you. Encode or decode SAML requests and responses To aid in troubleshooting, use the SAML encode/decode tool to process a SAML request and response in human readable form from the HTTP Archive Format (HAR) file. See . SAML App creation errors While creating a SAML app in the Admin console, you might see the following 400 error: 400 duplicate entity id You'll see this if you try to create an application with an already existing entity ID. To resolve the 400 duplicate entity id error: Use the already configured application or use a different entity ID. 500 errors for SAML app creation While creating a SAML app in the Admin console, you might see the following 500 errors: In the GoogleIdentity Provider detailssection, if you click the Download Certificate or Download Metadata button when the certificates service backend service is unavailable, a 500 error appears at the top of the screen. While loading the schemas in NameID Mapping or Attribute Mapping, if the schema service times out or displays a backend exception, a 500 error appears at the top of the screen. If the Service Provider Config service is unavailable a 500 error appears at the top of the screen when you click Finish. To resolve any 500 errors for SAML app creation: Wait for a whileand then try the flow again. If errors still occur, contactGoogle Cloud Support. SAML runtime errors The following error scenarios might occur when you tryout a SAML single sign-on (SSO) flow in identity provider(IdP) -initiated or service provider (SP)-initiated flows: 403 app_not_configured This error can occur in these scenarios: In an SP-initiated flow, the application corresponding to the entity ID mentioned in the request hasnot been created in the Admin console. In an SP-initiated flow, the entity ID provided in the SAMLRequest does not match any of the entity IDs of the currently installed apps. If someone tampers with the application ID (SP ID) mentioned in the IdP-initiated URL, then you will see an app_not_configured error. To resolve the 403 app_not_configured error: Ensure that the application corresponding to the entity ID mentioned in the requesthas been installed before you initiate the request. Ensure that the entity ID provided in the SAMLRequest is correct and matches with the one you specified during app creation. Ensure that the SP ID being passed in the request URL is the same as app-id app_not_enabled. 403 app_not_configured_for_user To resolve the 403 app_not_configured_for_user error: Verify that the value in the saml:Issuer tag in the SAMLRequest matches the Entity ID value configured in the SAML Service Provider Detailssection in the Admin console. This value is case-sensitive. 403 app_not_enabled_for_user To resolve the 403 app_not_enabled_for_usererror: Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In the app list, locate the SAML app generating the error. Click the app to open its Settings page. Click User access. Turn the app ON for everyone or for the users organization. 400 saml_invalid_user_id_mapping If an SP sends a NAMEID parameter in the SAMLRequest, then this parameter must be the same as that configured on the IdPside. Otherwise the SAMLRequest fails with this error. To resolvethe 400 saml_invalid_user_id_mapping error: Go to Basic Details and check the NAMEIDparameter. Ensure that the NAMEID parameter being passed in the SAMLRequest is the same as the one configured on the IdP side. 400 saml_invalid_sp_id This error occurs when the service provider ID in the URL of the IdP flow isincorrect, because of misconfiguration or tampering withthe URL. To resolve the 400 saml_invalid_sp_id error: Go to Basic Details and check theapp-id field. Ensure that the SP ID being passed in the request URL is the same as app-id. The SAML Response send back a status of DENIED for the following scenarios. You might see one of the following three related error messages. SP-initiated Flow Invalid request, ACS URL in request $parameter doesn't match configured ACS URL $parameter. In this case, the ACS URL specified in the SAMLRequest and the ACS URL configured in the Admin console for the corresponding application do not match. To resolve theACS URLin request $parameter doesn't match configured ACS URL $parameter error: Go to Service Provider Details. Check that the ACS URL is the same as in the SAMLRequest. Invalid idpid provided in the url The IdP ID (an obfuscated customer ID) provided in the URL has been tampered with and is incorrect. To resolve the invalid IdP ID in URL error: Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. Go to MenuSecurity > Authentication > SSO with SAML applications. Get the idpidstring from the end of the Entity ID URL. Ensure that the IdP ID in the Request URL is the same as the one inthe Entity ID URL. IdP-initiated Flow Invalid idpid provided in the request. The caller user has tampered with the IdP-initiated SSO URL and changed the IdP ID to another customer ID (obfuscated). To resolve the invalid IdP ID in request error: Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. Go to MenuSecurity > Authentication > SSO with SAML applications. Get the idpidstring from the end of the Entity ID URL. Ensure that the IdP ID in the Request URL is the same as the one in thethe Entity ID URL. 500 errors when testing a SAML SSO flow When your users are testing a SAML SSO flow in IdP-initiated or SP-initiated flows, they may encounter one of several 500 errors due to backend processes being unavailable. To resolve any 500 errors for testing a SAML SSO flow: Wait and then try the flow again. If this still doesnt work, contact Google Cloud Support. SAML app access error messages 1000 on access of SAML app page To resolve the SAML app page access error: Contact Google Cloud Support. 1000 on access of SAML app settings To resolve the SAML app settings access error: Contact Google Cloud Support. SAML app user schema deletion error message 400 This error occurs if you are trying to delete a custom schema that is associated as an attribute mapping for a SAML app that has already been deleted.If you have created the schema before this issue was fixed, this error can occur. To resolve the SAML apps user schema deletion error: Contact Google Cloud Support. (SSO) (SAML) XML Google SAML SSO Google Google Gmail Google Google Google SAML IdP (SSO) (Google) IdP (SSO) SAML (SSO) IdP PEM DER X.509 DSA RSA SAML SAML v2.0 (SSO) . (SAML) XML . ID Google SAML SSO . Google , Google Gmail . Google Google ID , , . ID Google SSO . SAML Google IdP SSO . IdP . SSO . SAML SSO . IdP . PEM DER X.509 . DSA RSA . SAML . SAML v2.0 . (SSO) (SAML) XML Google SSO SAML Google Google Gmail Google Google SSO Google SAML SSO IdP Google 1 IdP SSO 1 SAML SSO 2 IdP X.509 PEM DER DSA RSA SAML SAML v2.0 Se visualizzi messaggi di errore relativi a un'applicazione SAML (Security Assertion Markup Language), prova a eseguire i seguenti passaggi per la risoluzione dei problemi. Codificare o decodificare le richieste e le risposte SAML Per agevolare la risoluzione dei problemi, utilizza lo strumento di codifica/decodifica SAML per elaborare una richiesta e una risposta SAML in formato leggibile dal file HAR (HTTP Archive Format). Vedi . Errori durante la creazione di applicazioni SAML Durante la creazione di un'applicazione SAML nella Console di amministrazione, potresti vedere il seguente errore 400: 400 duplicate entity id (ID entit duplicato) Questo messaggio di errore viene visualizzato quando cerchi di creare un'applicazione con un ID entit gi esistente. Risoluzione dell'errore 400 relativo all'ID entit duplicato: Utilizza l'applicazione gi configurata o un ID entit diverso. Errori 500 per la creazione di applicazioni SAML Durante la creazione di un'applicazione SAML nella Console di amministrazione, potresti vedere i seguenti errori 500: Nella sezione Dettagli del provider di identit Google, se fai clic sul pulsante Download Certificate (Scarica certificato) o Download Metadata (Scarica metadati) quando il servizio di backend per i certificati non disponibile, verr visualizzato un errore 500 nella parte superiore dello schermo. Durante il caricamento degli schemi in NameID Mapping (Mappatura NameID) o Attribute Mapping (Mappatura attributo), in caso di timeout del servizio di schema o di visualizzazione di eccezioni del backend, verr visualizzato un errore 500 nella parte superiore dello schermo. Se il servizio Service Provider Config non disponibile, quando fai clic su Finish (Fine) viene visualizzato un errore 500 nella parte superiore dello schermo. Risoluzione di eventuali errori 500 relativi alla creazione di applicazioni SAML: Attendi prima di riprovare. Se si verificano ancora errori, contatta l'assistenza Google Cloud. Errori di runtime di SAML I seguenti scenari di errore possono verificarsi quando provi un flusso SSO (Single Sign-On) SAML nei flussi inizializzati dal provider di identit (IdP, Identity Provider) o dal provider di servizi (SP, Service Provider): 403 app_not_configured Questo errore pu verificarsi nei seguenti scenari: In un flusso inizializzato dal provider di servizi, l'applicazione corrispondente all'ID entit citato nella richiesta non stata creata nella Console di amministrazione. In un flusso inizializzato dal provider di servizi, l'ID fornito nella richiesta SAML (SAMLRequest) non corrisponde a nessuno degli ID entit delle applicazioni attualmente installate. Se qualcuno manomette l'ID applicazione (SP ID) citato nell'URL inizializzato dall'IdP, verr visualizzato un errore app_not_configured (app non configurata). Risoluzione dell'errore 403 "app_not_configured": Prima di inizializzare la richiesta, assicurati che l'applicazione corrispondente all'ID entit citato nella richiesta sia stata installata. Accertati che l'ID entit specificato in SAMLRequest sia corretto e che corrisponda a quello che hai specificato durante la creazione dell'applicazione. Accertati che l'ID SP indicato nell'URL della richiesta sia uguale all'app-id app_not_enabled. 403 app_not_configured_for_user Risoluzione dell'errore 403 "app_not_configured_for_user": Assicurati che il valore del tag saml:Issuer in SAMLRequest corrisponda al valore dell'ID entit configurato nella sezione Dettagli del fornitore di servizi SAML nella Console di amministrazione. Questo valore distingue tra maiuscole e minuscole. 403 app_not_enabled_for_user Risoluzione dell'errore 403 "app_not_enabled_for_user": Accedi a Console di amministrazione Google con un account amministratore.Se non utilizzi un account amministratore, non puoi accedere alla Console di amministrazione. Nell'elenco di app, trova l'app SAML che sta generando l'errore. Fai clic sull'app per aprire la pagina Impostazioni corrispondente. Fai clic su Accesso utenti. Attiva l'app per tutti o per l'organizzazione dell'utente. 400 saml_invalid_user_id_mapping Se un SP invia un parametro NAMEID in SAMLRequest, il parametro deve essere identico a quello configurato sul lato IdP. In caso contrario, SAMLRequest avr esito negativo e restituir questo errore. Risoluzione dell'errore 400 "saml_invalid_user_id_mapping": Vai a Dettagli di base e controlla il parametro NAMEID. Accertati che il parametro NAMEID indicato in SAMLRequest sia lo stesso che stato configurato sul lato IdP. 400 saml_invalid_sp_id Questo errore si verifica quando l'ID del fornitore di servizi nell'URL del flusso IdP non corretto, a causa di una configurazione errata o di manomissioni dell'URL. Risoluzione dell'errore 400 "saml_invalid_sp_id": Vai a Dettagli di base e controlla il campo app-id. Accertati che l'ID SP indicato nell'URL della richiesta sia uguale all'app-id. La risposta SAML restituisce lo stato DENIED per i seguenti scenari. Potresti visualizzare uno dei seguenti tre messaggi di errore correlati. SP-initiated Flow Invalid request, ACS URL in request $parameter doesn't match configured ACS URL $parameter (Richiesta non valida per il flusso inizializzato dall'SP; l'URL ACS nel $parameter della richiesta non corrisponde al $parameter URL ACS configurato). In questo caso, l'URL ACS specificato in SAMLRequest e l'URL ACS configurato nella Console di amministrazione per la relativa applicazione non corrispondono. Risoluzione dell'errore "ACS URL in request $parameter doesn't match configured ACS URL $parameter": Vai a Dettagli del fornitore di servizi. Verifica che l'URL ACS sia lo stesso di SAMLRequest. Invalid idpid provided in the url (ID IdP fornito nell'URL non valido) L'ID IdP (ID cliente offuscato) fornito nell'URL stato manomesso ed errato. Risoluzione dell'errore "invalid IdP ID in URL": Vai a SicurezzaConfigura il Single Sign-On (SSO) per le applicazioni SAML. Recupera la stringa idpiddalla parte finale dell'URL dell'ID entit. Accertati che l'ID IdP nell'URL della richiesta sia lo stesso che si trova nell'URL dell'ID entit. IdP-initiated Flow Invalid idpid provided in the request (Flusso inizializzato dall'IDP, ID IdP non valido fornito nella richiesta) L'utente chiamante ha manomesso l'URL SSO inizializzato dall'IdP e ha cambiato l'ID IdP in un altro ID cliente (offuscato). Risoluzione dell'errore "invalid IdP ID in request": Vai a SicurezzaConfigura il Single Sign-On (SSO) per le applicazioni SAML. Recupera la stringa idpiddalla parte finale dell'URL dell'ID entit. Accertati che l'ID IdP nell'URL della Richiesta sia uguale a quello contenuto nell'URL dell'ID entit. Errori 500 durante il test di un flusso SSO SAML Quando i tuoi utenti testano un flusso SSO SAML in flussi inizializzati dall'IdP o dall'SP, potrebbero riscontrare uno o pi errori 500 relativi alla mancata disponibilit dei processi backend. Risoluzione di eventuali errori 500 relativi al testing di un flusso SSO SAML: Attendi, quindi prova di nuovo il flusso. Se il problema persiste, contatta l'assistenza GoogleCloud. Messaggi di errore relativi all'accesso alle applicazioni SAML Errori 1000 relativi all'accesso alla pagina dell'applicazione SAML Risoluzione dell'errore di accesso alla pagina dell'applicazione SAML: Contatta l'assistenza Google Cloud. Errori 1000 relativi all'accesso alle impostazioni dell'applicazione SAML Risoluzione dell'errore di accesso alle impostazioni dell'applicazione SAML: Contatta l'assistenza Google Cloud. Messaggio di errore relativo all'eliminazione dello schema utente dell'applicazione SAML 400 Questo errore si verifica se tenti di eliminare uno schema personalizzato associato come mappatura di attributi per un'applicazione SAML che gi stata eliminata.L'errore pu verificarsi se lo schema stato creato prima della risoluzione del problema. Risoluzione dell'errore di eliminazione dello schema utente delle applicazioni SAML: Contatta l'assistenza Google Cloud. Single sign-on (SSO) letsusers sign in to all their enterprise cloud apps using their managed Google Account credentials. Google offers preintegrated SSO with over 200 popular cloud apps. Perform these steps to set up SAML-based SSO with a custom app that is not in the preintegrated catalog. Expandall|CollapseallStep 1: Add the custom SAML app Sign in with a superadministrator account to the GoogleAdminconsole.If you arent using a super administrator account, you cant complete these steps. Go to MenuApps > Web and mobile apps. Click Add AppAdd custom SAML app. Enter the app name and, optionally, upload an icon for your app. The app icon appears on the Web and mobile apps list, on the app settings page, and in the app launcher. If you don't upload an icon, an icon is created using the first two letters of the app name. Click Continue. On the Google Identity Provider details page, get the setup information needed by the service provider using one of these options: Download the IDP metadata. Copy the SSO URL and Entity ID and download the Certificate (or SHA-256 fingerprint, if needed). (Optional) To enter the information into the appropriate SSO configuration page, in a separate browser tab or window, sign in to your service provider and enter the information you copied in Step 5, then return to the Admin console. Click Continue. Contact your service provider for these field values. In the Service Provider Details window, enter: ACS URLThe service provider's Assertion Consumer Service URL receives the SAML response. It must start with https://. Entity IDThe globally unique name. Start URL(Optional) This sets the RelayState parameter in a SAML Request, which can be a URL to redirect to after authentication. (Optional) To indicate that your service provider requires the entire SAML authentication response to be signed, check the Signed response box. If this is unchecked (the default), only the assertion within the response is signed. (Optional) Set Name ID format and Name ID value for your custom SAML app. The default Name ID is the primary email. Tip: Check the setup articles in our SAML apps catalog for any Name ID mappings required for apps in the catalog. You can also create custom attributes, either in the Admin console or via Google Admin SDK APIs, and map to those. Click Continue. If needed, click Add mapping to map user attributes based on the service providers requirements. Note: You can define a maximum of 10,000 attributes over all apps. Because each app has one default attribute, the count includes the default attribute plus any custom attributes you add. For Google Directory attributes, click the Select field menu to choose a field name. Not all Google directory attributes are available in the drop-down list. If an attribute you want to map (for example, Manager's email) is not available, you can add that attribute as a custom attribute, which will make it available here for selection. For App attributes, enter the corresponding attribute for your custom SAML app. (Optional) To enter group names that are relevant for this app: For Group membership (optional), click Search for a group, enter one or more letters of the group name, and select the group name. Add additional groups as needed (maximum of 75 groups). For App attribute, enter the corresponding groups attribute name of the service provider. Regardless of how many group names you enter, the SAML response includes only groups that a user is a member of (directly or indirectly). For more information, go toAbout group membership mapping. Click Finish. Step 2: Turn on your SAML app Sign in with a superadministrator account to the GoogleAdminconsole.If you arent using a super administrator account, you cant complete these steps. Go to MenuApps > Web and mobile apps. Select your SAML app. To turn a service on or off for everyone in your organization, clickOn for everyone orOff for everyone, and then clickSave. (Optional) To turn a service on or offforan organizational unit: At the left, select the organizational unit. To change the Service status, selectOn orOff. Choose one: If the Service status is set toInheritedand you want to keep the updated setting, even if the parent setting changes, click Override. If the Service status is set toOverridden, either click Inherit to revert to the same setting as its parent, or clickSave to keep the new setting, even if the parent setting changes. Learn more about organizational structure. Ensure that the email addresses yourusers use to sign in to theSAML app match the email addresses theyuseto sign in to your Google domain. Changes can take up to 24 hours but typically happen more quickly.Learn moreStep 3: Verify that SSO is working with your custom app You can test for both identity provider-initiated (IdP) SSOand service provider-initiated (SP) SSO. IdP-initiated Sign in with a superadministrator account to the GoogleAdminconsole.If you arent using a super administrator account, you cant complete these steps. Go to MenuApps > Web and mobile apps. Select your custom SAML app. At the top left, click Test SAML login. Your app should open in a separate tab. If it doesnt, use the information in the resulting SAML app error messages to update your IdP and SP settings as needed, then retest SAML login. SP-initiated Open the SSO URL for your new SAML app.You should be automatically redirected to the Google sign-in page. Enter your username and password. After your sign-in credentials are authenticated, you'reredirected back to your new SAML app. Related topics With single sign-on (SSO), users can access many applications without having to enter their username and password for each application. Security Assertion Markup Language (SAML) is an XML standard that enables secure web domains to exchange user authentication and authorization data. The roles of service providers and identity providers Google offers a SAML-based SSO service that allows partner companies to authorize and authenticate hosted users who are trying to access secure content. Google acts as the online service provider and provides services, such as Google Calendar and Gmail. Google partners act as online identity providers and control usernames, passwords and other information used to identify, authenticate, and authorize users for web applications that Google hosts. Many open source and commercial identity providers can help you implement SSO with Google. SAML verification certificates To set up SSO with third-party IdPs where Google is the service provider, you need to upload one or more verification certificates. The certificate contains the public key which verifies sign-in from the IdP. If youre configuring the Third-party SSO profile for your organization, you upload one verification certificate. If youre creating a new SAML SSO profile, you can upload two certificates, giving you the option to rotate certificates. Youll usually get these certificates from your IdP. However, you can alsogenerate them yourself. Requirements The certificate must be a PEM or DER formatted X.509 certificate with an embedded public key. The public key must be generated with the DSA or RSA algorithms. The public key in the certificate must match the private key used to sign the SAML response. Related topic SAML v2.0 specifications (SSO) . (SAML) XML . Google (SSO) SAML . Google " Google" Gmail. Google Google. (SSO) Google. SAML (SSO) Google . . (SSO) . (SSO) SAML . (idP) . X.509 PEM DER . DSA RSA. SAML. SAML v2.0 You can set up SSO with Google as your service provider in a number of ways, depending on your organizations needs.Google Workspace supports both SAML-based and OIDC-based SSO. If your users use domain-specific service URLs to access Google services (for example, , you can also manage how these URLs work with SSO. If your organization needs conditional SSO redirection based on IP address, or SSO for super admins, you also have the option to configure the legacy SSO profile. Set up SSO with SAML Before you begin To set up a SAML SSO profile, youll need some basic configuration from your IdPs support team or documentation: Sign-in page URL This is also known as the SSO URL or SAML 2.0 Endpoint (HTTP). This is where users sign in to your IdP. Sign-out page URL Where the user lands after exiting the Google app or service. Change password URL The page where SSO users will go to change their password (instead of changing their password with Google). Certificate X.509 PEM certificate from your IdP. The certificate contains the public key which verifies sign-in from the IdP.Certificate requirements The certificate must be a PEM or DER formatted X.509 certificate with an embedded public key. The public key must be generated with the DSA or RSA algorithms. The public key in the certificate must match the private key used to sign the SAML response. Youll usually get these certificates from your IdP. However, you can also generate them yourself. Create a SAML SSO profile Follow these steps to create a third-party SSO profile. You can create up to 1000 profiles in your organization. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In Third-party SSO profiles, click Add SAML profile. Enter a name for the profile. (Optional) If you have an XML metadata file from your IdP, click upload XML file to provide IdP information, then continue with Step 8 Fill in the Sign-in page URL and other information obtained from your IdP. Enter a change password URL for your IdP. Users will go to this URL (rather than the Google change password page) to reset their passwords. Click Upload certificateto upload your certificate file. You can upload up to two certificates, giving you the optionto rotate certificates when necessary. Click Save. In the SP Details section, copy and save the Entity ID and ACS URL. Youll need these values to configure SSO with Google in your IdP admin control panel. (Optional)If your IdP supports encrypting assertions, you can generate and share a certificate with your IdP to enable encryption. Each SAML SSO profile can have up to 2 SP certificates. Click the SP Details section to enter edit mode. Under SP certificate, click Generate certificate. (The certificate will display after you save it.) Click Save. The certificate name, expiration date, and contents are displayed. Use the buttons above a certificate to either copy the certificate contents or download as a file, then share the certificate with your IdP. (Optional) If you need to rotate a certificate, return to SP Details and click Generate another certificate, then share the new certificate with your IdP. Once youre sure your IdP is using the new one, you can delete the original certificate. Configure your IdP To configure your IdP to use this SSO profile, enter the information from the Service Provider (SP) Details section of theprofile into the appropriate fields in your IdP SSO settings. Both the ACS URL and Entity ID are unique to this profile.Configure the legacy SSO profile The legacy SSO profile is supported for users who have not migrated to SSO profiles. It only supports usage with a single IdP. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In Third-party SSO profiles, click Add SAML profile. At the bottom of the IdP details page, click Go to legacy SSO profile settings. On the Legacy SSO profile page, check the Enable SSO with third-party identity provider box. Fill in the following information for your IdP: Enter the Sign-in page URL and Sign-out page URL for your IdP. Note: All URLs must be entered and must use HTTPS, for example . Click Upload certificate and locate and upload the X.509 certificate supplied by your IdP. For more information, see Certificate requirements. Choose whether to use a domain-specific issuer in the SAML request from Google. If you have multiple domains using SSO with your IdP, use a domain-specific issuer to identify the correct domain issuing the SAML request. Checked Google sends an issuer specific to your domain: google.com/a/example.com (where example.com is your primary Google Workspace domain name) Unchecked Google sends the standard issuer in the SAML request: google.com (Optional) To apply SSO to a set of users within specific IP address ranges, enter a network mask. For more information see Network mapping results. Note: you can also set up partial SSO by assigning the SSO profile to specific organizational units or groups. Enter a change password URL for your IdP. Users will go to this URL (rather than the Google change password page) to reset their passwords. Note: If you enter a URL here, users are directed to this page even if you dont enable SSO for your organization. Click Save. After saving, the legacy SSO profile is listed in the SSO profiles table. Configure your IdP To configure your IdP to use this SSO profile, enter the information from the Service Provider (SP) Details section of the profile into the appropriate fields in your IdP SSO settings. Both the ACS URL and Entity ID are unique to this profile. Format ACS URL domain.com}/acs Where {domain.com} is your organization's Workspace domain name Entity ID Either of the following: google.com google.com/a/customerprimarydomain (if you choose to use a domain-specific issuer when configuring the legacy profile). Disable the legacy SSO profile In the Third-party SSO profiles list, click Legacy SSO profile. In the Legacy SSO profile settings, uncheck Enable SSO with third-party identity provider. Confirm that you want to continue, then click Save. In the SSO profiles list, the Legacy SSO profile now shows as Disabled. Organizational units that have the Legacy SSO profile assigned will display an alert in the Assigned profile column. The top level organizational unit will display None in the Assigned profile column. In Manage SSO profile assignments, the Legacy SSO profile shows as inactive. Migratefrom legacy SAML to SSO profiles If your organization is using the legacy SSO profile, we recommend migrating to SSO profiles, which offer several advantages including OIDC support, more modern APIs, and greater flexibility in applying SSO settings to your user groups. Learn more. Set up SSO with OIDC Follow these steps to use OIDC-based SSO: Choose an OIDC optioneither create a custom OIDC profile, where you provide information for your OIDC partner, or use the pre-configured Microsoft Entra OIDC profile. Follow the steps in Decide which users should use SSO to assign the pre-configured OIDC profile to selected organizational units/groups. If you have users within an organizational unit (for example in a sub-organizational unit) who dont need SSO, you can also use assignments to turn SSO off for those users. Note: The Google Cloud Command Line Interface does not currently support reauthentication with OIDC. Before you begin To set up a custom OIDC profile, youll need some basic configuration from your IdPs support team or documentation: Issuer URL The complete URL of the IdP authorization server. An OAuth client, identified by its Client ID and authenticated by a Client secret. Change password URL The page where SSO users will go to change their password (instead of changing their password with Google). Also, Google needs your IdP to do this: The email claim from your IdP must match the users primary email address on the Google side. It must use the authorization code flow. Create a custom OIDC profile (beta) Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In Third-party SSO profiles, click Add OIDC profile. Name the OIDC profile. Enter OIDC details: Client ID, Issuer URL, Client secret. Click Save. On the OIDC SSO settings page for the new profile, copy the Redirect URI. Youll need to update your OAuth client on your IdP to respond to requests using this URI. To edit settings, hover over the OIDC Details, then click Edit . Use the Microsoft Entra OIDC profile Make sure youve configured the following prerequisites for OIDC in your organizations Microsoft Entra ID tenant: The Microsoft Entra ID tenant needs to be domain verified. End users must have Microsoft 365 licenses. The username (primary email) of the Google Workspace admin assigning the SSO profile must match the primary email address of your Azure ADtenant admin account. Decide which users should use SSO Turn SSO on for an organizational unit or group by assigning an SSO profile and its associated IdP. Or, turn SSO off by assigning None for the SSO profile. You can also apply a mixed SSO policy within an organizational unit or group, for example turning SSO on for the organizational unit as a whole, then turning it off for a sub-organizational unit. If you haven't created aSAMLor OIDC profile, do that before continuing. Or, you can assign the preconfigured OIDC profile. Click Manage SSO profile assignments. If this is your first time assigning the SSO profile, click Get started. Otherwise, click Manage assignments. On the left, select the organizational unit or group to which youre assigning the SSO profile. If the SSO profile assignment for an organizational unit or group differs from your domain-wide profile assignment, an override warning appears when you select that organizational unit or group. You cant assign the SSO profile on a per-user basis. The Users view lets you check the setting for a specific user. Choose an SSO profile assignment for the selected organizational unit or group: To exclude the organizational unit or group from SSO, choose None. Users in the organizational unit or group will sign in directly with Google. To assign another IdP to the organizational unit or group, choose Another SSO profile, then select the SSO profile from the dropdown list. (SAML SSO profiles only) After selecting a SAML profile, choose a sign-in option for users who go directly to a Google service without first signing in to the SSO profile's third-party IdP. You can prompt users for their Google username, then redirect them to the IdP, or require users to enter their Google username and password. Note: If you choose to require users to enter their Google username and password, the Change password URL setting for this SAML SSO profile (available at SSO Profile > IDP details) is ignored. This ensures that users are able to change theirGoogle passwords as needed. Click Save. (Optional) Assign SSO profiles to other organizational units or groups as needed. After you close the Manage SSO profile assignments card, youll see the updated assignments for organizational units and groups in the Manage SSO profile assignments section. Remove an SSO profile assignment Click a group or organizational unit name to open its profile assignment settings. Replace the existing assignment setting with the parent organization unit setting: For organizational unit assignmentsclick Inherit. For group assignmentsclick Unset. Note: Your top organizational unit is always present in the profile assignment list, even if the Profile is set to None. See also Google, Google Workspace, and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companieswith which they are associated. Si te aparece algn mensaje de error de las aplicaciones de lenguaje de marcado para confirmaciones de seguridad (SAML), aqu te mostramos algunos pasos para solucionar problemas que pueden ayudarte. Codificar o decodificar solicitudes y respuestas de SAML Utiliza la herramienta de codificacin y decodificacin de SAML para traducir las solicitudes y respuestas del archivo HAR (formato de archivo HTTP) a un formato legible; as te resultar ms fcil solucionar los problemas. Visita la pgina Errores al crear aplicacionesSAML Al crear una aplicacin SAML en la consola de administracin, podra aparecer este mensaje de error 400: 400 duplicate entity id (ID de entidad duplicado) Este mensaje aparece si intentas crear una aplicacin con un ID de entidad que ya existe. Para solucionar este error: Utiliza la aplicacin ya configurada o especifica un ID de entidad diferente. Errores 500 que se producen al crear aplicaciones SAML Al crear una aplicacin SAML en la consola de administracin, podran aparecer errores 500 en los siguientes casos: En la seccin Detalles de proveedor de identidades de Google, si haces clic en el botn Descargar certificado o Descargar metadatos cuando el servicio de backend de certificados no est disponible, aparece un mensaje de error 500 en la parte superior de la pantalla. Al cargar los esquemas en Mapeo de ID de nombre o en Mapeo de atributo, si se agota el tiempo de espera del servicio de esquemas o se muestra una excepcin de backend, aparece un mensaje de error 500 en la parte superior de la pantalla. Si el servicio Service Provider Config no est disponible, aparece un mensaje de error 500 en la parte superior de la pantalla al hacer clic en Finalizar. Para solucionar estos errores: Espera un rato y vuelve a intentarlo. Si los mensajes de error siguen apareciendo, ponte en contacto con el equipo de asistencia de Google Cloud. Errores del entorno de ejecucin de SAML Cuando pruebas el inicio de sesin nico (SSO) de SAML en flujos iniciados por el proveedor de identidades (IdP) o por el proveedor de servicios (SP), pueden aparecer los siguientes mensajes de error: 403 app_not_configured (Aplicacin no configurada) Este error se puede producir en estos casos: En un flujo iniciado por el SP, la aplicacin correspondiente al ID de entidad mencionado en la solicitud no se ha creado en la consola de administracin. En un flujo iniciado por el SP, el ID de entidad proporcionado en la solicitud SAMLRequest no coincide con ninguno de los ID de entidad de las aplicaciones instaladas actualmente. Si alguien manipula el ID de aplicacin (ID de SP) que figura en la URL iniciada por el IdP, aparece el mensaje de error app_not_configured. Para solucionar este error: Antes de iniciar la solicitud, comprueba que se ha instalado la aplicacin correspondiente al ID de entidad que figura en ella. Asegrate de que el ID de entidad que se proporciona en la solicitud SAMLRequestes correcto y coincide con el que especificaste al crear la aplicacin. Asegrate de que el ID de SP que se incluye en la URL de la solicitud coincide con el de app-id app_not_enabled. 403 app_not_configured_for_user (Aplicacin no configurada en cuentas de usuarios) Para solucionar este error: Comprueba que el valor de la etiqueta saml:Issuer de la solicitud SAMLRequest coincide con el de ID de entidad configurado en la seccin Datos del proveedor de servicios de SAML de la consola de administracin. En cuanto a este valor, el sistema distingue entre mayscula y minscula. 403 app_not_enabled_for_user Para solucionar este error: Inicia sesin con una cuenta de administrador en consola de administracin de Google.Si no usas una cuenta de administrador, no podrs acceder a la consola de administracin. En la lista de aplicaciones, localiza la aplicacin SAML que genera el error. Haz clic en la aplicacin para abrir la pgina de configuracin. Haz clic en Acceso de usuarios. Activa la aplicacin para todos o para la organizacin del usuario. 400 saml_invalid_user_id_mapping (Asignacin de ID de usuario no vlida en SAML) Si un proveedor de servicios enva un parmetro NAMEID en la solicitud SAMLRequest, dicho parmetro debe ser idntico al configurado en el proveedor de identidades. De lo contrario, se producir un error en la solicitud SAMLRequest y aparecer este mensaje de error. Para solucionarlo: Ve a Informacin bsica y comprueba el parmetro NAMEID. Asegrate de que el parmetro NAMEID que figura en la solicitud SAMLRequest es idntico al configurado en el proveedor de identidades. 400 saml_invalid_sp_id (ID de SP no vlido en SAML) Este mensaje de error aparece cuando el ID de SP incluido en la URL del flujo del IdP es incorrecto debido a un error de configuracin o a una manipulacin de la URL. Para solucionar este error: Ve a Informacin bsica y comprueba el campo app-id. Asegrate de que el ID de SP que se incluye en la URL de la solicitud coincide con el de app-id. La respuesta de SAML devuelve el estado DENIED (Denegado) en las siguientes situaciones. Es posible que aparezca uno de estos tres mensajes de error relacionados. SP-initiated Flow Invalid request, ACS URL in request $parameter doesn't match configured ACS URL $parameter (Solicitud no vlida en el flujo iniciado por el SP; la URL ACS del valor $parameter de la solicitud no coincide con la del valor $parameter configurado) En este caso, la URL ACS especificada en la solicitud SAMLRequest y la URL ACS configurada en la consola de administracin para la aplicacin correspondiente no coinciden. Para solucionar este error: Ve a Datos del proveedor de servicios. Comprueba que la URL ACS coincida con la de la solicitud SAMLRequest. Invalid idpid provided in the url (El ID de IdP proporcionado en la URL no es vlido) El ID del proveedor de identidades (ID de cliente ofuscado) proporcionado en la URL se ha manipulado y no es correcto. Para solucionar este error: Ve a SeguridadConfigurar el inicio de sesin nico (SSO) en aplicaciones SAML. Consulta la cadena idpid que se encuentra al final de la URL del ID de entidad. Asegrate de que el ID del proveedor de identidades que aparece en la URL de la solicitud coincide con el de la URL del ID de entidad. IdP-initiated Flow Invalid idpid provided in the request (El ID de IdP proporcionado en la solicitud del flujo iniciado por el IdP no es vlido) El usuario que realiza la llamada ha manipulado la URL de SSO iniciada por el IdP y ha cambiado el ID de IdP por otro ID de cliente (ofuscado). Para solucionar este error: Ve a SeguridadConfigurar el inicio de sesin nico (SSO) en aplicaciones SAML. Consulta la cadena idpid que se encuentra al final de la URL del ID de entidad. Asegrate de que el ID del proveedor de identidades que aparece en la URL de la solicitud coincide con el de la URL del ID de entidad. Errores 500 que se producen al probar un flujo de SSO de SAML Cuando tus usuarios prueban el SSO de SAML en flujos iniciados por el IdP o por el SP, puede aparecer alguno de los diferentes errores 500 que se producen cuando los procesos de backend no estn disponibles. Para solucionar estos errores: Espera y vuelve a probar el flujo. Si el problema no se soluciona, ponte en contacto con el equipo de asistencia de Google Cloud. Mensajes de error de acceso a aplicaciones SAML Error 1000 al acceder a la pgina de una aplicacin SAML Para solucionar este error: Ponte en contacto con el equipo de asistencia de Google Cloud. Error 1000 al acceder a la configuracin de una aplicacin SAML Para solucionar este error: Ponte en contacto con el equipo de asistencia de Google Cloud. Error al eliminar el esquema de usuarios de una aplicacin SAML 400 Este error se produce al intentar eliminar un esquema personalizado que est asociado como un mapeo de atributos de una aplicacin SAML que ya se ha eliminado.Si has creado el esquema antes de solucionar este problema, se puede producir este error. Para solucionarlo: Ponte en contacto con el equipo de asistencia de Google Cloud.

Saml 2.0 standard. Saml2 certificate. Saml certificate. Saml 2.0 request example. Saml certificate requirements.