AMEX GBT
Select

Single Sign-On access setup guide

GBT Digital Products: Amex GBT Account and Amex GBT Mobile App

AMERICAN EXPRESS GLOBAL BUSINESS TRAVEL

AMEX GBT
Select

Contents

AMEX GBT
Select

Introduction

Simplify the way your employees access digital travel products and services by setting up Single Sign-On (SSO) to American Express Global Business Travel (GBT) digital channels: GBT Account, GBT Mobile, WhatsApp, Microsoft Teams, Zoom and Slack.

This document describes the SSO solution available to you and high-level steps for set up. Please review the guide end to end.

Checklist:
☐ Have a technical resource fill out the SSO integration questionnaire of this document along with your certificate/metadata file. Return it to your GBT Deployment manager.
☐ Review client requirements on page 7.

What role do you play in the overall process?

GBT will assign a Deployment Manager to manage your setup. You will require a technical resource assigned on your side to support the implementation. GBT technical resources cannot configure SSO for clients or provide training on how to do so. At a high level, here is what will be needed:

1. Assign a technical resource at your company that will be setting up the SSO at your company and provide them with this document.

2. Read this guide.

3. Please have **a technical resource return completed questionnaire on next page along with your certificate/metadata file to GBT Deployment manager a minimum of 30 days prior to desired launch date.** GBT will assign a resource to complete set up in our systems and share the meta data file within 30 days.

Please refer to Technical Details and Set Up Values section of this document for more detail around data points required for IdP SAML setup.

4. Once the questionnaire and the certificate/metadata file are provided back to the GBT Deployment Manager, the GBT SSO configuration can start. GBT will provide the client specific values and the metadata file for setup completion on your side within 2-4 weeks of receiving the completed questionnaire.

5. If you have any questions, please ensure you have reviewed this guide fully. If you still have questions, please email your assigned GBT Deployment Manager.

6. If a technical call is needed with the GBT Okta tech team, please provide your technical resource's availability. The GBT Deployment Manager will coordinate the meeting between your technical resource and the GBT Okta tech team.

7. Once your technical resource completes the setup on your side, you can start testing.

Generally, SSO setup can be completed within 30 days from when you submit back the filled questionnaire and certificate submission. However, this is a guideline as timing will vary based on demand, your technical resource's bandwidth, and testing.

AMEX GBT
Select

SSO Integration Questionnaire for Client Partner

Client Partner Name (Customer Name)	
Client Partner Technical Contact	Email: Time zone:
GBT Relationship Manager	Email: Time zone:
User Identity Attribute used for SSO logins: • Email Address (Recommended for non-Flex HR Feed clients) • Employee Number (Recommended for Flex HR Feed clients) • Network ID • Badge Number • Alternate Employee ID	
Supported SSO Protocols for IDP (Inbound SSO): SAML2 is standard offered. If you require OIDC, a consultation will be required.	SAML 2.
Selected SSO Authentication Setup at launch: • **SSO Only*** – authorized users can only be authenticated via SSO by your IDP solution • **SSO & Login –** authorized users can be authenticated via SSO or via login with email and GBT password * GBT Deployment and Support teams will need to access to your site during implementation for testing. If you select this option, it will be executed on after GBT testing completion and prior to launch. Post launch, this means GBT employees cannot access your site for training or technical support unless you provide select GBT employees with access to your network.	
SAML details for set-up	
SAML - IdP Issuer URI Issuer URI of the Identity Provider. This value is usually the SAML Metadata EntityID of the IdP EntityDescriptor.	
SAML - IdP Single Sign-On URL The binding-specific IdP Authentication Request Protocol endpoint that receives SAML Authn Request messages from Okta.	

SAML - SSO IdP Signature Certificate or IDP Metadata Please attach the SSO (PEM or DER encoded) public key certificate or SSO IDP Metadata XML file.	
OIDC details for set-up	
OIDC - Client ID: Client ID	
OIDC - Client Secret: Client Secret. [Send this in separate email.]	
OIDC - Issuer: The identifier of the OpenID Connect provider	
OIDC - Authorization endpoint: The URL of the Identity Provider's OAuth 2.0 authorization endpoint	
OIDC -Token endpoint: The URL of the Identity Provider's token endpoint for obtaining access and ID tokens	
OIDC - JWKS endpoint: The URL of the Identity Provider's JSON Web Key Set document. This document contains signing keys that are used to validate the signatures from the provider	
OIDC - User info endpoint (optional): The endpoint for getting identity information about the user.	
SSO Logout URL This is the URL travelers will be taken to upon logout from Global Portal. If none supplied, users will be taken to login page of access.amexgbt.com	
Special Notes: Any other special notes	

AMEX GBT
Select

Supported Configuration & Availability

Supported Configuration & Coverage

GBT supports standard IdP initiated SAML 2.0 configuration. If OIDC configuration is required, it can also be supported as a non-standard request and must be flagged to your Deployment Manager prior to the implementation.

SSO is available to the following GBT Digital channels:

1. GBT Account full experience and base experience that supports access to the following:

    a) Insights (via GBT Account platform)
    b) Premier Insights (via GBT Account platform)
    c) One DDS Invoices (via GBT Account platform)
    d) Expert Care (coming soon via GBT Account platform)
    e) Expert Auditor (coming via GBT Account platform)

2. Amex GBT Mobile app
3. WhatsApp
4. Microsoft Teams
5. Zoom
6. Slack

Please note that SSO can only be configured to work with one Identity and Access Management (IAM) connection per client. If a given client uses more than one IAM (e.g., for certain countries, channels, or subsidiaries), users that do not connect through the primary one may encounter issues. In this situation, please contact your GBT account team for consultation.

The metadata file that will be provided during deployment will cover all GBT Digital Channels above.

Supported SSO Authentication Setup Options

We support two SSO setups for you to choose from when completing the Setup Questionnaire:

1. **SSO Only*** – authorized users can only be authenticated via SSO by your IDP solution, or
2. **SSO & Login** – authorized users can be authenticated via SSO or via login with email and GBT password.

* GBT Deployment and Support teams will need to access to your site during implementation for testing. If you select this option, it will be executed on after GBT testing completion and prior to launch. Post launch, this means GBT employees cannot access your site for live training or technical support unless you provide select GBT employees with access to your network. If live training on your site or GBT technical support is required post launch of first country, you may consider launching with SSO & Login or providing GBT employees you need support from access to your network.

Supported Testing

The GBT setup is on the GBT production environment only. Testing can be done from your test environment if desired and will require submission of questionnaires for both testing and production environment to set up both.

Client Requirements

It is essential to plan for the following for a successful set up:

1. Secure a technical resource to support the implementation. GBT technical resources cannot configure client IdP configuration or provide training on how to do so.
2. Technical resource to test all GBT Channels to ensure users can access services in those channels should they choose to.
3. On launch date, ensure your IT resource is scheduled to release the SSO URL to GBT, to the required users.

Technical details including setup values

The following values will be required to set up the IdP initiated SAML SSO:

- IdP Signature Certificate: To be provided in a Privacy Enhanced Mail (.pem extension) format (.cer is also acceptable).
- User Attribute: The unique user identifier. Email Address is recommended. Employee Unique ID (customer unique value listed) is also supported. This value is determined with your Deployment Manager.
- IdP issuer URI: The SAML issuer also known as Federation URI or Entity.
- IdP Single Sign-on URL: Binding-specific IdP Authentication Request Protocol endpoint that receives SAML AuthnRequest messages from Okta.
- Destination: The value of the destination in the SAML Authentication Request (optional).
- Logout/Timeout URL: The URL to direct a user when they log out of GBT Account (if no value is provided the default is the GBT Account login page). Not applicable for mobile app setup.

Data points required for IdP SAML setup on next page.

ATTRIBUTES	OKTA VALUE	COMMENTS
IdP Initiated interface	IdP	Only IdP initiated supported. No GBT metadata/certificate file is needed with IdP configuration
SAML Version / Protocol	SAML 2.0	Only 2.0 supported
SAML Issuer/ Federation URI / Entity	e.g. urm:federation:mycorp	Client defined value
SAML NameID / User Attribute	xxxx	xxxx reflects the unique user value used in the authentication request to GBT
SignatureMethod (Algorithm)	http://www.w3.org/2000/09/xmldsig#rsa-sha1 or http://www.w3.org/2000/09/xmldsig#rsa-sha256	
Entity / Entity ID	https://access.amexgbt.com	Unique identifier
Certificate	RSA certificate in PEM or CRT format	Provided by the client
Service Name	AMEX GBT	Exact value to be used
Service Type	Prod	Default is prod and testing is done in the GBT prod environment only
POST URL / Request/ Response Binding / Reply URL	https://access.amexgbt.com/sso/saml2/xxxxxxxxxxxxxxxxxxx	GBT OKTA team provides value after you submit the questionnaire
Destination URL	https://access.amexgbt.com/sso/saml2/xxxxxxxxxxxxxxxxxxx	GBT OKTA team provides value after you submit the questionnaire
Recipient URL	https://access.amexgbt.com/sso/saml2/xxxxxxxxxxxxxxxxxxx	GBT OKTA team provides value after you submit the questionnaire
Audience URL	https://www.okta.com/saml2/service-provider/xxxxxxxxxxxxxxxxxxx	GBT OKTA team provides value after you submit the questionnaire
Transport Protocol	HTTPS	
Send RelayState (CSP to SP)	N/A to GBT SAML SSO IDP	
Variable RelayState	N/A to GBT SAML SSO IDP	
RelayState Parameter	N/A to GBT SAML SSO IDP	
RelayState Value	N/A to GBT SAML SSO IDP	
Signed Responses	TRUE	
Signed Assertions	FALSE	
Signed Responses and Signed Assertions	FALSE	

The metadata file that will be provided to you during deployment will cover all GBT Digital channels: GBT Account, GBT Mobile App, WhatsApp, Microsoft Teams, Slack & Zoom.

Federation

AMEX GBT
Select

QUESTIONS	ANSWERS
Can the application support artifact binding per the SAML 2.0 binding specification? What alternatives does the application offer to secure communication?	No; SAML Assertion with algorithm AES256-CBC
What is the maximum token validity period time that is accepted by the application?	2 minutes
Does the application support the one-use property for the assertion?	Yes
Does the application expose a web-based metadata endpoint for IdP consumption? How does the application provide metadata?	No; will be shared via email
Does the application support signed assertions using RSA keys of at least 2048 bits or ECC keys of at least 256 bits in length?	Yes
Can the application generate digital signatures using SHA-2 hash functions that produce digests of at least 256 bits in length?	Yes; SHA-256 RSA
Does the application support HTTP communications over TLS? Which Version of TLS?	Yes; TLS1.2
Do TLS communications use x509 certificates?	Yes
Are the certificates signed by a Certificate Authority using RSA signing keys at least 4096 bits or ECC signing keys at least 512 bits in length?	RSA 2048 bits
Are the certificates signed using a SHA-2 hash function that produces a digest of at least 256 bits in length?	Yes, SHA-256
Do the certificates contain an RSA public key at least 2048 bits or an ECC key at least 256 bits in length?	RSA 2048
Do TLS communications support perfect forward secrecy via ephemeral session key exchange?	Yes
Do TLS communications support strong cipher suites (such as an IANA recommended cipher suite)?	Yes
Does the application support XML decryption of the assertion?	Yes
Does the application support metadata endpoint monitoring with automated configuration updates?	No; configuration updates are manual currently
Does the application support the use of multiple IdP certificates at any given time?	Yes, if necessary

AMEX GBT
Select

Access Management

QUESTIONS	ANSWERS
Does the application currently implement or support Dynamic Session Management (Claims Based Authorization)?	No, only authentication
Does the application implement or support On Demand Provisioning using SAML Assertion?	Yes
Does the application currently implement or support Automated Access Removal after a period of inactivity?	No
Does the application currently implement or support SCIM based automated provisioning and de-provisioning?	No
If SCIM support is not available, Is SCIM based automated provisioning and de-provisioning on your IT Roadmap?	No
If SCIM support is not available on the roadmap, is there an alternate provisioning/de-provisioning API available?	Yes, HR Feed via EFG and Web Services
Can this API be available to be published?	Yes
Can this API be SAML secured?	No
Does this API support establishment of all roles, including privileged roles (such as access administration, etc.)?	Yes, following GBT role definition
Does the application provide a user interface?	No
Does the application provide alternate access mechanisms that do not require authentications with an IdP (for example, direct access break glass accounts for restoration of service)?	No

General Implementation

QUESTIONS	ANSWERS
Is any component of the application hosted on public cloud infrastructure, such as AWS, Azure?	Okta Public Cloud
Where is the application IdP (relying party STS) hosted (public cloud, on-prem, other)?	Okta Public Cloud
What devices can be used to access the application?	iOS, Android, PC, MAC
Does the application provide non-web-based access points (DB, OS)?	No
What channels can be used to access application (Internet, Internet with IP restriction, leased lines, VPN, other)?	Internet, Internet with IP Restriction

AMEX GBT
Select

Testing

Testing environment

The GBT setup is on the GBT production environment only. Testing can be done from your test environment if desired and will require submission of questionnaires for both testing and production environment to set up both.

Recommended testing scope

We recommend testing with all unique configuration scenarios for your company setup to avoid issues post launch and all channels your travelers will be accessing.

1. GBT Account – from https://access.amexgbt.com/ and using SSO link created during this set for access from your intranet (where applicable)
2. Amex GBT Mobile app - from Android and Apple device at a minimum. If your company's configurations vary by device type, we also recommend testing those: Company owned, Bring Your Own device and personal mobile phone.
3. WhatsApp
4. Microsoft Teams
5. Zoom
6. Slack

Please note that while your company may not promote use of all the above products, **we highly recommend testing GBT Account and AMEX GBT Mobile app at a minimum**. GBT Account is the gateway access to Travel Program solutions including reporting and trip invoices so some of your team members will need access at some point. Our AMEX GBT Mobile app is also available for download on personal devices so it's best to test to avoid access issues should your team members download the app.

Common errors & Troubleshooting tips

1. We were unable to sign you in. Please try again.

   User being sent in the SSO request does not match a user in GBT systems. Either the user does not exist, or the unique user value sent doesn't match what is associated to the user.

   - Verify the user data sent.
   - Compare the data within GBT systems.
   - Ensure certificate sent to GBT matched what is being sent in SSO request.

2. 404 Error

Setup on client side is likely missing values or was configured with the incorrect data values.

- Verify all configuration values are correct.

3. 400 Error

SSO message is not correctly formatted on client site.

- Verify that request is being sent as IdP initiated.
- Ensure full Post URL matches exactly what was provided by GBT.
- Values are case sensitive, so ensure values like service name are typed exactly as shown in above data points chart.

4. Redirected to Okta login page.

User does not exist or match.

- Check to see that the user is loaded in Okta.
- Validate that user ID value in SSO request matches the user data in Okta.
- Do not login or register (via the Get Started link).

What happens if I still get errors?

Provide details to your GBT Deployment Manager on all steps including user email, browser, URL from client intranet, mobile device, mobile app version, timestamp, and screenshots of error showing URLs where applicable.

AMEX GBT
Select

FAQs

1. What happens when my certificate expires?

You are responsible for contacting your GBT Account Manager at least 30 days prior to certificate expiry to ensure your certificate is changed on time.

2. Can I stagger SSO launch by country?

GBT supports a single global authentication set up across all our GBT Digital Channels that applies to all authorized users across all countries. Users are authorized once their profiles are in our systems.

If you decide to control access at a country level in your company configuration, you will need to ensure it's updated as you roll out future countries or if you have employees that need access to Travel Program solutions including GBT reporting products and One DDS trip invoices outside of these countries.

3. How about if I want to change my GBT Digital Access Set up post launch?

Yes, you can request a change to the authentication access set up at any time. Please contact your account manager to submit a maintenance case.

4. Can I set up SSO to a single GBT Digital Channel/ product instead of all at once?

GBT supports a single global authentication set up across all our GBT Digital Channels that applies to all authorized users across all countries. Users are authorized once their profiles are in our systems. GBT does not support varying login experiences by channel. Please refer to Support Configuration section of this guide for details on products included.

5. I'm setting up SSO to GBT account online and have users that need access to my site but don't have access to our intranet. How can they access my GBT Account site?

All users that you authorize via SSO will have access to your site. Users can access GBT account via your SSO link or by going to access.amexgbt.com. After they enter their email address, authorized users will be redirected to login with their corporate credentials via IDP discovery. No additional setup is required.

Version History

A list of changes to the document:

VERSION	PUBLISH DATE	SUMMARY OF CHANGES
1.0	16 July 2021	• Initial document
2.0	2 February 2022	• Included Apple IPA and Android APK • Provided more guidance in testing section for Mobile • Clarification regarding IAM solution and metadata file
3.0	27 May 2022	• Mobile SSO primarily available for non-MDM use cases • Clarification on there being no country-level SSO setup
4.0	3 June 2022	• Integrated questionnaire
5.0	10 June 2022	• Eliminated optional MDM config
6.0	14 June 2022	• Embedded SSO Questionnaire
7.0	5 December 2022	• Updated all aspects of doc to support single SSO config across all GBT Digital Channels
7.1	28 November 2023	• Rebrand
7.2	22 April 2026	• Footer updated