Microsoft Entra authentication and authorization error codes

Article • 02/03/2025

Looking for info about the AADSTS error codes that are returned from the Microsoft Entra security token service (STS)? Read this document to find AADSTS error descriptions, fixes, and some suggested workarounds.

> **Note**
>
> This information is preliminary and subject to change. Have a question or can't find what you're looking for? Create a GitHub issue or see Support and help options for developers to learn about other ways you can get help and support.
>
> This documentation is provided for developer and admin guidance, but should never be used by the client itself. Error codes are subject to change at any time in order to provide more granular error messages that are intended to help the developer while building their application. Apps that take a dependency on text or error code numbers will be broken over time.

Lookup current error code information

Error codes and messages are subject to change. For the most current info, take a look at the https://login.microsoftonline.com/error page to find AADSTS error descriptions, fixes, and some suggested workarounds.

For example, if you received the error code "AADSTS50058" then do a search in https://login.microsoftonline.com/error for "50058". You can also link directly to a specific error by adding the error code number to the URL: https://login.microsoftonline.com/error?code=50058 .

Handling error codes in your application

The OAuth2.0 spec provides guidance on how to handle errors during authentication using the `error` portion of the error response.

Here's a sample error response:

JSON

```json
{
  "error": "invalid_scope",
  "error_description": "AADSTS70011: The provided value for the input parameter 'scope' isn't valid. The scope https://example.contoso.com/activity.read isn't valid.\r\nTrace ID: 0000aaaa-11bb-cccc-dd22-eeeeee333333\r\nCorrelation ID: aaaa0000-bb11-2222-33cc-444444dddddd\r\nTimestamp: 2016-01-09 02:02:12Z",
  "error_codes": [
    70011
  ],
  "timestamp": "2016-01-09 02:02:12Z",
  "trace_id": "0000aaaa-11bb-cccc-dd22-eeeeee333333",
  "correlation_id": "aaaa0000-bb11-2222-33cc-444444dddddd",
  "error_uri":"https://login.microsoftonline.com/error?code=70011"
}
```

Expand table

Parameter	Description
`error`	An error code string that can be used to classify types of errors that occur, and should be used to react to errors.
`error_description`	A specific error message that can help a developer identify the root cause of an authentication error. Never use this field to react to an error in your code.
`error_codes`	A list of STS-specific error codes that can help in diagnostics.
`timestamp`	This returns the time at which the error occurred.
`trace_id`	A unique identifier for the request that can help in diagnostics.
`correlation_id`	A unique identifier for the request that can help in diagnostics across components.
`error_uri`	A link to the error lookup page with additional information about the error. This is for developer usage only, don't present it to users. Only present when the error lookup system has additional information about the error - not all error have additional information provided.

The `error` field has several possible values - review the protocol documentation links and OAuth 2.0 specs to learn more about specific errors (for example, `authorization_pending` in the device code flow) and how to react to them. Some common ones are listed here:

Expand table

Error Code	Description	Client Action
`invalid_request`	Protocol error, such as a missing required parameter.	Fix and resubmit the request.

Error Code	Description	Client Action
`invalid_grant`	Some of the authentication material (auth code, refresh token, access token, PKCE challenge) was invalid, unparseable, missing, or otherwise unusable	Try a new request to the `/authorize` endpoint to get a new authorization code. Consider reviewing and validating that app's use of the protocols.
`unauthorized_client`	The authenticated client isn't authorized to use this authorization grant type.	This usually occurs when the client application isn't registered in Microsoft Entra ID or isn't added to the user's Microsoft Entra tenant. The application can prompt the user with instruction for installing the application and adding it to Microsoft Entra ID.
`invalid_client`	Client authentication failed.	The client credentials aren't valid. To fix, the Application Administrator updates the credentials.
`unsupported_grant_type`	The authorization server doesn't support the authorization grant type.	Change the grant type in the request. This type of error should occur only during development and be detected during initial testing.
`invalid_resource`	The target resource is invalid because it doesn't exist, Microsoft Entra ID can't find it, or it's not correctly configured.	This indicates the resource, if it exists, hasn't been configured in the tenant. The application can prompt the user with instruction for installing the application and adding it to Microsoft Entra ID. During development, this usually indicates an incorrectly set up test tenant or a typo in the name of the scope being requested.
`interaction_required`	The request requires user interaction. For example, another authentication step is required.	Retry the request with the same resource, interactively, so that the user can complete any challenges required.
`temporarily_unavailable`	The server is temporarily too busy to handle the request.	Retry the request. The client application might explain to the user that its response is delayed because of a temporary condition.

AADSTS error codes

Expand table

Error	Description
AADSTS16000	InteractionRequired - User account '{EmailHidden}' from identity provider '{idp}' doesn't exist in tenant '{tenant}' and can't access the application '{appid}'({appName}) in that tenant. This account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Microsoft Entra user account. This error is fairly common when you try to sign

Error	Description
	in to Microsoft Entra admin center by using personal Microsoft Account and no directory associated with it.
AADSTS16001	UserAccountSelectionInvalid - You see this error if the user selects on a tile that the session select logic has rejected. When triggered, this error allows the user to recover by picking from an updated list of tiles/sessions, or by choosing another account. This error can occur because of a code defect or race condition.
AADSTS16002	AppSessionSelectionInvalid - The app-specified SID requirement wasn't met.
AADSTS160021	AppSessionSelectionInvalidSessionNotExist - Application requested a user session that doesn't exist. This issue can be resolved by creating new Azure account.
AADSTS16003	SsoUserAccountNotFoundInResourceTenant - Indicates that the user hasn't been explicitly added to the tenant.
AADSTS17003	CredentialKeyProvisioningFailed - Microsoft Entra ID can't provision the user key.
AADSTS20001	WsFedSignInResponseError - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.
AADSTS20012	WsFedMessageInvalid - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.
AADSTS20033	FedMetadataInvalidTenantName - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.
AADSTS230109	CachedCredentialNonGWAuthNRequestsNotSupported - Backup Auth Service only allows AuthN requests from Microsoft Entra Gateway. This error is returned when traffic targets the backup auth service directly instead of going through the reverse proxy.
AADSTS28002	Provided value for the input parameter scope '{scope}' isn't valid when requesting an access token. Specify a valid scope.
AADSTS28003	Provided value for the input parameter scope can't be empty when requesting an access token using the provided authorization code. Specify a valid scope.
AADSTS399284	InboundIdTokenIssuerInvalid - The inbound ID token received in the federation has an invalid issuer. Either it is empty, or it does not match the realm identifier.
AADSTS40008	OAuth2IdPUnretryableServerError - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.
AADSTS40009	OAuth2IdPRefreshTokenRedemptionUserError - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.
AADSTS40010	OAuth2IdPRetryableServerError - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.
AADSTS40015	OAuth2IdPAuthCodeRedemptionUserError - There's an issue with your federated Identity Provider. Contact your IDP to resolve this issue.

Error	Description
AADSTS50000	TokenIssuanceError - There's an issue with the sign-in service. Open a support ticket to resolve this issue.
AADSTS50001	InvalidResource - The resource is disabled or doesn't exist. Check your app's code to ensure that you have specified the exact resource URL for the resource you're trying to access.
AADSTS50002	NotAllowedTenant - Sign-in failed because of a restricted proxy access on the tenant. If it's your own tenant policy, you can change your restricted tenant settings to fix this issue.
AADSTS500011	InvalidResourceServicePrincipalNotFound - The resource principal named {name} wasn't found in the tenant named {tenant}. This can happen if the application hasn't been installed by the administrator of the tenant or consented to by any user in the tenant. You might have sent your authentication request to the wrong tenant. If you expect the app to be installed, you might need to provide administrator permissions to add it. Check with the developers of the resource and application to understand what the right setup for your tenant is.
AADSTS500014	InvalidResourceServicePrincipalDisabled - The service principal for resource '{identifier}' is disabled. This indicates that a subscription within the tenant has lapsed, or that an administrator for this tenant has disabled the application's service principal, preventing tokens from being issued for it. For more information, see Disable user sign-in for application.
AADSTS500021	Access to '{tenant}' tenant is denied. AADSTS500021 indicates that the tenant restriction feature is configured and that the user is trying to access a tenant that isn't in the list of allowed tenants specified in the header `Restrict-Access-To-Tenant`. For more information, see Use tenant restrictions to manage access to SaaS cloud applications.
AADSTS500022	Access to '{tenant}' tenant is denied. AADSTS500022 indicates that the tenant restriction feature is configured and that the user is trying to access a tenant that isn't in the list of allowed tenants specified in the header `Restrict-Access-To-Tenant`. For more information, see Use tenant restrictions to manage access to SaaS cloud applications.
AADSTS50003	MissingSigningKey - Sign-in failed because of a missing signing key or certificate. This might be because there was no signing key configured in the app. To learn more, see the troubleshooting article for error AADSTS50003. If you still see issues, contact the app owner or an app admin.
AADSTS50005	DevicePolicyError - User tried to sign in to a device from a platform not currently supported through Conditional Access policy.
AADSTS50006	InvalidSignature - Signature verification failed because of an invalid signature.
AADSTS50007	PartnerEncryptionCertificateMissing - The partner encryption certificate wasn't found for this app. Open a support ticket with Microsoft to get this fixed.
AADSTS50008	InvalidSamlToken - SAML assertion is missing or misconfigured in the token. Contact your federation provider.
AADSTS5000224	NotAllowedTenantBlockedTenantFraud - We are sorry, this resource is not available. If you are seeing this message by mistake, please contact Microsoft support.

Error	Description
AADSTS5000819	InvalidSamlTokenEmailMissingOrInvalid - SAML Assertion is invalid. Email address claim is missing or doesn't match domain from an external realm.
AADSTS50010	AudienceUriValidationFailed - Audience URI validation for the app failed since no token audiences were configured.
AADSTS50011	InvalidReplyTo - The reply address is missing, misconfigured, or doesn't match reply addresses configured for the app. As a resolution ensures to add this missing reply address to the Microsoft Entra application or have someone with the permissions to manage your application in Microsoft Entra IF do this for you. To learn more, see the troubleshooting article for error AADSTS50011.
AADSTS50012	AuthenticationFailed - Authentication failed for one of the following reasons: • The subject name of the signing certificate isn't authorized • A matching trusted authority policy wasn't found for the authorized subject name • The certificate chain isn't valid • The signing certificate isn't valid • Policy isn't configured on the tenant • Thumbprint of the signing certificate isn't authorized • Client assertion contains an invalid signature
AADSTS50013	InvalidAssertion - Assertion is invalid because of various reasons - The token issuer doesn't match the API version within its valid time range -expired -malformed - Refresh token in the assertion isn't a primary refresh token. Contact the app developer.
AADSTS500133	Assertion isn't within its valid time range. Ensure that the access token isn't expired before using it for user assertion, or request a new token. Current time: {curTime}, expiry time of assertion {expTime}. Assertion is invalid because of various reasons: • The token issuer doesn't match the API version within its valid time range • Expired • Malformed • Refresh token in the assertion isn't a primary refresh token
AADSTS50014	GuestUserInPendingState - The user account doesn’t exist in the directory. An application likely chose the wrong tenant to sign into, and the currently logged in user was prevented from doing so since they didn't exist in your tenant. If this user should be able to sign in, add them as a guest. For further information, please visit add B2B users.
AADSTS50015	ViralUserLegalAgeConsentRequiredState - The user requires legal age group consent.
AADSTS50017	CertificateValidationFailed - Certification validation failed, reasons for the following reasons: • Cannot find issuing certificate in trusted certificates list • Unable to find expected CrlSegment • Cannot find issuing certificate in trusted certificates list • Delta CRL distribution point is configured without a corresponding CRL distribution point • Unable to retrieve valid CRL segments because of a timeout issue • Unable to download CRL

Error	Description
	Contact the tenant admin.
AADSTS500141	The user's redemption is complete but the request was not initiated by the target application.
AADSTS5001256	Failed to complete authentication with external provider due to invalid id_token. Failure details: {details}
AADSTS50020	UserUnauthorized - Users are unauthorized to call this endpoint. User account '{email}' from identity provider '{idp}' does not exist in tenant '{tenant}' and cannot access the application '{appid}'({appName}) in that tenant. This account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Microsoft Entra user account. If this user should be a member of the tenant, they should be invited via the B2B system. For additional information, visit AADSTS50020.
AADSTS500207	The account type can't be used for the resource you're trying to access.
AADSTS500208	The domain is not a valid login domain for the account type - This situation occurs when the user's account does not match the expected account type for the given tenant. For instance, if the tenant is configured to allow only work or school accounts, and the user tries to sign in with a personal Microsoft account, they will receive this error.
AADSTS500212	NotAllowedByOutboundPolicyTenant - The user's administrator has set an outbound access policy that doesn't allow access to the resource tenant.
AADSTS500213	NotAllowedByInboundPolicyTenant - The resource tenant's cross-tenant access policy doesn't allow this user to access this tenant.
AADSTS50027	InvalidJwtToken - Invalid JWT token because of the following reasons: • doesn't contain nonce claim, sub claim • subject identifier mismatch • duplicate claim in idToken claims • unexpected issuer • unexpected audience • not within its valid time range • token format isn't proper • External ID token from issuer failed signature verification.
AADSTS50029	Invalid URI - domain name contains invalid characters. Contact the tenant admin.
AADSTS50032	WeakRsaKey - Indicates the erroneous user attempt to use a weak RSA key.
AADSTS50033	RetryableError - Indicates a transient error not related to the database operations.
AADSTS50034	UserAccountNotFound - To sign into this application, the account must be added to the directory. This error can occur because the user mis-typed their username, or isn't in the tenant. An application might have chosen the wrong tenant to sign into, and the currently logged in user was prevented from doing so since they did not exist in your tenant. If this user should be able to log in, add them as a guest. See docs here: Add B2B users.

Error	Description
AADSTS50042	UnableToGeneratePairwiseIdentifierWithMissingSalt - The salt required to generate a pairwise identifier is missing in principle. Contact the tenant admin.
AADSTS50043	UnableToGeneratePairwiseIdentifierWithMultipleSalts
AADSTS50048	SubjectMismatchesIssuer - Subject mismatches Issuer claim in the client assertion. Contact the tenant admin.
AADSTS50049	NoSuchInstanceForDiscovery - Unknown or invalid instance.
AADSTS50050	MalformedDiscoveryRequest - The request is malformed.
AADSTS50053	This error can result from two different reasons: • IdsLocked - The account is locked because the user tried to sign in too many times with an incorrect user ID or password. The user is blocked due to repeated sign-in attempts. See Remediate risks and unblock users. • Or, sign-in was blocked because it came from an IP address with malicious activity. To determine which failure reason caused this error, sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator. Navigate to your Microsoft Entra tenant and then **Monitoring & health** -> **Sign-in logs**. Find the failed user sign-in with **Sign-in error code** 50053 and check the **Failure reason**.
AADSTS50055	InvalidPasswordExpiredPassword - The password is expired. The user's password is expired, and therefore their login or session was ended. They will be offered the opportunity to reset it, or can ask an admin to reset it via Reset a user's password using Microsoft Entra ID.
AADSTS50056	Invalid or null password: password doesn't exist in the directory for this user. The user should be asked to enter their password again.
AADSTS50057	UserDisabled - The user account is disabled. The user object in Active Directory backing this account has been disabled. An admin can re-enable this account through PowerShell
AADSTS50058	UserInformationNotProvided - Session information isn't sufficient for single-sign-on. This means that a user isn't signed in. This is a common error that's expected when a user is unauthenticated and hasn't yet signed in. If this error is encountered in an SSO context where the user has previously signed in, this means that the SSO session was either not found or invalid. This error might be returned to the application if prompt=none is specified.
AADSTS50059	MissingTenantRealmAndNoUserInformationProvided - Tenant-identifying information wasn't found in either the request or implied by any provided credentials. The user can contact the tenant admin to help resolve the issue.
AADSTS50061	SignoutInvalidRequest - Unable to complete sign out. The request was invalid.
AADSTS50064	CredentialAuthenticationError - Credential validation on username or password has failed.

Error	Description
AADSTS50068	SignoutInitiatorNotParticipant - Sign out has failed. The app that initiated sign out isn't a participant in the current session.
AADSTS50070	SignoutUnknownSessionIdentifier - Sign out has failed. The sign out request specified a name identifier that didn't match the existing session(s).
AADSTS50071	SignoutMessageExpired - The logout request has expired.
AADSTS50072	UserStrongAuthEnrollmentRequiredInterrupt - User needs to enroll for second factor authentication (interactive).
AADSTS50074	UserStrongAuthClientAuthNRequiredInterrupt - Strong authentication is required and the user did not pass the MFA challenge.
AADSTS50076	UserStrongAuthClientAuthNRequired - Due to a configuration change made by the admin such as a Conditional Access policy, per-user enforcement, or because you moved to a new location, the user must use multifactor authentication to access the resource. Retry with a new authorize request for the resource.
AADSTS50078	UserStrongAuthExpired- Presented multifactor authentication has expired due to policies configured by your administrator. You must refresh your multifactor authentication to access '{resource}'.
AADSTS50079	UserStrongAuthEnrollmentRequired - Due to a configuration change made by the admin such as a Conditional Access policy, per-user enforcement, or because the user moved to a new location, the user is required to use multifactor authentication. Either a managed user needs to register security info to complete multifactor authentication, or a federated user needs to get the multifactor claim from the federated identity provider.
AADSTS50085	Refresh token needs social IDP login. Have user try signing-in again with username -password
AADSTS50086	SasNonRetryableError
AADSTS50087	SasRetryableError - A transient error has occurred during strong authentication. Please try again.
AADSTS50088	Limit on telecom MFA calls reached. Please try again in a few minutes.
AADSTS50089	Authentication failed due to flow token expired. Expected - auth codes, refresh tokens, and sessions expire over time or are revoked by the user or an admin. The app will request a new login from the user.
AADSTS50097	DeviceAuthenticationRequired - Device authentication is required.
AADSTS50099	PKeyAuthInvalidJwtUnauthorized - The JWT signature is invalid.
AADSTS50105	EntitlementGrantsNotFound - The signed in user isn't assigned to a role for the signed in app. Assign the user to the app. To learn more, see the troubleshooting article for error AADSTS50105.

Error	Description
AADSTS50107	InvalidRealmUri - The requested federation realm object doesn't exist. Contact the tenant admin.
AADSTS50120	ThresholdJwtInvalidJwtFormat - Issue with JWT header. Contact the tenant admin.
AADSTS50124	ClaimsTransformationInvalidInputParameter - Claims Transformation contains invalid input parameter. Contact the tenant admin to update the policy.
AADSTS501241	Mandatory Input '{paramName}' missing from transformation ID '{transformId}'. This error is returned while Microsoft Entra ID is trying to build a SAML response to the application. NameID claim or NameIdentifier is mandatory in SAML response and if Microsoft Entra ID failed to get source attribute for NameID claim, it returns this error. As a resolution, ensure that you add claim rules. To add claim rules, sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator, and then browse to **Identity** > **Applications** > **Enterprise applications**. Select your application, select **Single Sign-On** and then in **User Attributes & Claims** enter the Unique User Identifier (Name ID).
AADSTS50125	PasswordResetRegistrationRequiredInterrupt - Sign-in was interrupted because of a password reset or password registration entry.
AADSTS50126	InvalidUserNameOrPassword - Error validating credentials due to invalid username or password. The user didn't enter the right credentials. Expect to see some number of these errors in your logs due to users making mistakes.
AADSTS50127	BrokerAppNotInstalled - User needs to install a broker app to gain access to this content.
AADSTS50128	Invalid domain name - No tenant-identifying information found in either the request or implied by any provided credentials.
AADSTS50129	DeviceIsNotWorkplaceJoined - Workplace join is required to register the device.
AADSTS50131	ConditionalAccessFailed - Indicates various Conditional Access errors such as bad Windows device state, request blocked due to suspicious activity, access policy, or security policy decisions.
AADSTS50132	SsoArtifactInvalidOrExpired - The session isn't valid due to password expiration or recent password change.
AADSTS50133	SsoArtifactRevoked - The session isn't valid due to password expiration or recent password change.
AADSTS50134	DeviceFlowAuthorizeWrongDatacenter - Wrong data center. To authorize a request that was initiated by an app in the OAuth 2.0 device flow, the authorizing party must be in the same data center where the original request resides.
AADSTS50135	PasswordChangeCompromisedPassword - Password change is required due to account risk.
AADSTS50136	RedirectMsaSessionToApp - Single MSA session detected.

Error	Description
AADSTS50139	SessionMissingMsaOAuth2RefreshToken - The session is invalid due to a missing external refresh token.
AADSTS50140	KmsiInterrupt - This error occurred due to "Keep me signed in" interrupt when the user was signing-in. This is an expected part of the sign in flow, where a user is asked if they want to remain signed into their current browser to make further logins easier. For more information, see The new Microsoft Entra sign-in and “Keep me signed in” experiences rolling out now!. You can open a support ticket with Correlation ID, Request ID, and Error code to get more details.
AADSTS50143	Session mismatch - Session is invalid because user tenant doesn't match the domain hint due to different resource. Open a support ticket with Correlation ID, Request ID, and Error code to get more details.
AADSTS50144	InvalidPasswordExpiredOnPremPassword - User's Active Directory password has expired. Generate a new password for the user or have the user use the self-service reset tool to reset their password.
AADSTS50146	MissingCustomSigningKey - This app is required to be configured with an app-specific signing key. It's either not configured with one, or the key has expired or isn't yet valid. Please contact the owner of the application.
AADSTS501461	AcceptMappedClaims is only supported for a token audience matching the application GUID or an audience within the tenant's verified domains. Either change the resource identifier, or use an application-specific signing key.
AADSTS50147	MissingCodeChallenge - The size of the code challenge parameter isn't valid.
AADSTS501481	The Code_Verifier doesn't match the code_challenge supplied in the authorization request.
AADSTS501491	InvalidCodeChallengeMethodInvalidSize - Invalid size of Code_Challenge parameter.
AADSTS50155	DeviceAuthenticationFailed - Device authentication failed for this user.
AADSTS50158	ExternalSecurityChallenge - External security challenge was not satisfied.
AADSTS50161	InvalidExternalSecurityChallengeConfiguration - Claims sent by external provider isn't enough or Missing claim requested to external provider.
AADSTS50166	ExternalClaimsProviderThrottled - Failed to send the request to the claims provider.
AADSTS50168	ChromeBrowserSsoInterruptRequired - The client is capable of obtaining an SSO token through the Windows 10 Accounts extension, but the token was not found in the request or the supplied token was expired.
AADSTS50169	InvalidRequestBadRealm - The realm isn't a configured realm of the current service namespace.
AADSTS50170	MissingExternalClaimsProviderMapping - The external controls mapping is missing.

Error	Description
AADSTS50173	FreshTokenNeeded - The provided grant has expired due to it being revoked, and a fresh auth token is needed. Either an admin or a user revoked the tokens for this user, causing subsequent token refreshes to fail and require reauthentication. Have the user sign in again.
AADSTS50177	ExternalChallengeNotSupportedForPassthroughUsers - External challenge isn't supported for passthrough users.
AADSTS50178	SessionControlNotSupportedForPassthroughUsers - Session control isn't supported for passthrough users.
AADSTS50180	WindowsIntegratedAuthMissing - Integrated Windows authentication is needed. Enable the tenant for Seamless SSO.
AADSTS50187	DeviceInformationNotProvided - The service failed to perform device authentication.
AADSTS50192	Invalid Request - RawCredentialExpectedNotFound - No Credential was included in the sign-in request. Example: user is performing certificate-based authentication (CBA) and no certificate is sent (or Proxy removes) the user's certificate in the sign-in request.
AADSTS50194	Application '{appId}'({appName}) isn't configured as a multitenant application. Usage of the /common endpoint isn't supported for such applications created after '{time}'. Use a tenant-specific endpoint or configure the application to be multitenant.
AADSTS50196	LoopDetected - A client loop has been detected. Check the app’s logic to ensure that token caching is implemented, and that error conditions are handled correctly. The app has made too many of the same request in too short a period, indicating that it is in a faulty state or is abusively requesting tokens.
AADSTS50197	ConflictingIdentities - The user could not be found. Try signing in again.
AADSTS50199	CmsiInterrupt - For security reasons, user confirmation is required for this request. Interrupt is shown for all scheme redirects in mobile browsers. No action required. The user was asked to confirm that this app is the application they intended to sign into. This is a security feature that helps prevent spoofing attacks. This occurs because a system webview has been used to request a token for a native application. To avoid this prompt, the redirect URI should be part of the following safe list: http:// https:// chrome-extension:// (desktop Chrome browser only)
AADSTS51000	RequiredFeatureNotEnabled - The feature is disabled.
AADSTS51001	DomainHintMustbePresent - Domain hint must be present with on-premises security identifier or on-premises UPN.
AADSTS1000104	XCB2BResourceCloudNotAllowedOnIdentityTenant - Resource cloud {resourceCloud} isn't allowed on identity tenant {identityTenant}. {resourceCloud} - cloud instance which owns the resource. {identityTenant} - is the tenant where signing-in identity is originated from.

Error	Description
AADSTS51004	UserAccountNotInDirectory - The user account doesn’t exist in the directory. An application likely chose the wrong tenant to sign into, and the currently logged in user was prevented from doing so since they did not exist in your tenant. If this user should be able to log in, add them as a guest. For further information, please visit add B2B users.
AADSTS51005	TemporaryRedirect - Equivalent to HTTP status 307, which indicates that the requested information is located at the URI specified in the location header. When you receive this status, follow the location header associated with the response. When the original request method was POST, the redirected request will also use the POST method.
AADSTS51006	ForceReauthDueToInsufficientAuth - Integrated Windows authentication is needed. User logged in using a session token that is missing the integrated Windows authentication claim. Request the user to log in again.
AADSTS52004	DelegationDoesNotExistForLinkedIn - The user has not provided consent for access to LinkedIn resources.
AADSTS53000	DeviceNotCompliant - Conditional Access policy requires a compliant device, and the device isn't compliant. The user must enroll their device with an approved MDM provider like Intune. For additional information, please visit Conditional Access device remediation.
AADSTS53001	DeviceNotDomainJoined - Conditional Access policy requires a domain joined device, and the device isn't domain joined. Have the user use a domain joined device.
AADSTS53002	ApplicationUsedIsNotAnApprovedApp - The app used isn't an approved app for Conditional Access. User needs to use one of the apps from the list of approved apps to use in order to get access.
AADSTS53003	BlockedByConditionalAccess - Access has been blocked by Conditional Access policies. The access policy does not allow token issuance. If this is unexpected, see the Conditional Access policy that applied to this request or contact your administrator. For additional information, please visit troubleshooting sign-in with Conditional Access.
AADSTS530035	BlockedBySecurityDefaults - Access has been blocked by security defaults. This is due to the request using legacy auth or being deemed unsafe by security defaults policies. For additional information, please visit enforced security policies.
AADSTS53004	ProofUpBlockedDueToRisk - User needs to complete the multifactor authentication registration process before accessing this content. User should register for multifactor authentication.
AADSTS53010	ProofUpBlockedDueToSecurityInfoAcr - Cannot configure multifactor authentication methods because the organization requires this information to be set from specific locations or devices.
AADSTS53011	User blocked due to risk on home tenant.
AADSTS530034	DelegatedAdminBlockedDueToSuspiciousActivity - A delegated administrator was blocked from accessing the tenant due to account risk in their home tenant.
AADSTS54000	MinorUserBlockedLegalAgeGroupRule

Error	Description
AADSTS54005	OAuth2 Authorization code was already redeemed, please retry with a new valid code or use an existing refresh token.
AADSTS65001	DelegationDoesNotExist - The user or administrator hasn't consented to use the application with ID X. Send an interactive authorization request for this user and resource.
AADSTS65002	Consent between first party application '{applicationId}' and first party resource '{resourceId}' must be configured via preauthorization - applications owned and operated by Microsoft must get approval from the API owner before requesting tokens for that API. A developer in your tenant might be attempting to reuse an App ID owned by Microsoft. This error prevents them from impersonating a Microsoft application to call other APIs. They must move to another app ID they register.
AADSTS65004	UserDeclinedConsent - User declined to consent to access the app. Have the user retry the sign-in and consent to the app
AADSTS65005	MisconfiguredApplication - The app required resource access list doesn't contain apps discoverable by the resource, or the client app has requested access to resource, which wasn't specified in its required resource access list or Graph service returned bad request or resource not found. If the app supports SAML, you might have configured the app with the wrong Identifier (Entity). To learn more, see the troubleshooting article for error AADSTS650056.
AADSTS650052	The app needs access to a service `(\"{name}\")` that your organization `\"{organization}\"` hasn't subscribed to or enabled. Contact your IT Admin to review the configuration of your service subscriptions.
AADSTS650054	The application asked for permissions to access a resource that has been removed or is no longer available. Make sure that all resources the app is calling are present in the tenant you're operating in.
AADSTS650056	Misconfigured application. This could be due to one of the following: the client has not listed any permissions for '{name}' in the requested permissions in the client's application registration. Or, the admin has not consented in the tenant. Or, check the application identifier in the request to ensure it matches the configured client application identifier. Or, check the certificate in the request to ensure it's valid. Please contact your admin to fix the configuration or consent on behalf of the tenant. Client app ID: {ID}. Please contact your admin to fix the configuration or consent on behalf of the tenant.
AADSTS650057	Invalid resource. The client has requested access to a resource which isn't listed in the requested permissions in the client's application registration. Client app ID: {appId} ({appName}). Resource value from request: {resource}. Resource app ID: {resourceAppId}. List of valid resources from app registration: {regList}.
AADSTS67003	ActorNotValidServiceIdentity

Error	Description
AADSTS70000	InvalidGrant - Authentication failed. The refresh token isn't valid. Error might be due to the following reasons: • Token binding header is empty • Token binding hash does not match
AADSTS70001	UnauthorizedClient - The application is disabled. To learn more, see the troubleshooting article for error AADSTS70001.
AADSTS700011	UnauthorizedClientAppNotFoundInOrgIdTenant - Application with identifier {appIdentifier} was not found in the directory. A client application requested a token from your tenant, but the client app doesn't exist in your tenant, so the call failed.
AADSTS70002	InvalidClient - Error validating the credentials. The specified client_secret does not match the expected value for this client. Correct the client_secret and try again. For more info, see Use the authorization code to request an access token.
AADSTS700025	InvalidClientPublicClientWithCredential - Client is public so neither 'client_assertion' nor 'client_secret' should be presented.
AADSTS700027	Client assertion failed signature validation. Developer error - the app is attempting to sign in without the necessary or correct authentication parameters.
AADSTS70003	UnsupportedGrantType - The app returned an unsupported grant type.
AADSTS700030	Invalid certificate - subject name in certificate isn't authorized. SubjectNames/SubjectAlternativeNames (up to 10) in token certificate are: {certificateSubjects}.
AADSTS70004	InvalidRedirectUri - The app returned an invalid redirect URI. The redirect address specified by the client does not match any configured addresses or any addresses on the OIDC approve list.
AADSTS70005	UnsupportedResponseType - The app returned an unsupported response type due to the following reasons: • response type 'token' isn't enabled for the app • response type 'id_token' requires the 'OpenID' scope -contains an unsupported OAuth parameter value in the encoded wctx
AADSTS700054	Response_type 'id_token' isn't enabled for the application. The application requested an ID token from the authorization endpoint, but did not have ID token implicit grant enabled. Sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator and then browse to **Identity** > **Applications** > **App registrations**. Select your application and then select **Authentication**. Under **Implicit grant and hybrid flows**, make sure **ID tokens'** is selected.
AADSTS70007	UnsupportedResponseMode - The app returned an unsupported value of `response_mode` when requesting a token.

Error	Description
AADSTS70008	ExpiredOrRevokedGrant - The refresh token has expired due to inactivity. The token was issued on XXX and was inactive for a certain amount of time.
AADSTS700082	ExpiredOrRevokedGrantInactiveToken - The refresh token has expired due to inactivity. The token was issued on {issueDate} and was inactive for {time}. Expected part of the token lifecycle - the user went an extended period of time without using the application, so the token was expired when the app attempted to refresh it.
AADSTS700084	The refresh token was issued to a single page app (SPA), and therefore has a fixed, limited lifetime of {time}, which can't be extended. It is now expired and a new sign in request must be sent by the SPA to the sign in page. The token was issued on {issueDate}.
AADSTS70011	InvalidScope - The scope requested by the app is invalid.
AADSTS70012	MsaServerError - A server error occurred while authenticating an MSA (consumer) user. Try again. If it continues to fail, open a support ticket
AADSTS70016	AuthorizationPending - OAuth 2.0 device flow error. Authorization is pending. The device will retry polling the request.
AADSTS70018	BadVerificationCode - Invalid verification code due to User typing in wrong user code for device code flow. Authorization isn't approved.
AADSTS70019	CodeExpired - Verification code expired. Have the user retry the sign-in.
AADSTS70043	BadTokenDueToSignInFrequency - The refresh token has expired or is invalid due to sign-in frequency checks by Conditional Access. The token was issued on {issueDate} and the maximum allowed lifetime for this request is {time}.
AADSTS75001	BindingSerializationError - An error occurred during SAML message binding.
AADSTS75003	UnsupportedBindingError - The app returned an error related to unsupported binding (SAML protocol response can't be sent via bindings other than HTTP POST).
AADSTS75005	Saml2MessageInvalid - Microsoft Entra doesn’t support the SAML request sent by the app for SSO. To learn more, see the troubleshooting article for error AADSTS75005.
AADSTS7500514	A supported type of SAML response was not found. The supported response types are 'Response' (in XML namespace 'urn:oasis:names:tc:SAML:2.0:protocol') or 'Assertion' (in XML namespace 'urn:oasis:names:tc:SAML:2.0:assertion'). Application error - the developer will handle this error.
AADSTS750054	SAMLRequest or SAMLResponse must be present as query string parameters in HTTP request for SAML Redirect binding. To learn more, see the troubleshooting article for error AADSTS750054.
AADSTS75008	RequestDeniedError - The request from the app was denied since the SAML request had an unexpected destination.

Error	Description
AADSTS75011	NoMatchedAuthnContextInOutputClaims - The authentication method by which the user authenticated with the service doesn't match requested authentication method. To learn more, see the troubleshooting article for error AADSTS75011.
AADSTS75016	Saml2AuthenticationRequestInvalidNameIDPolicy - SAML2 Authentication Request has invalid NameIdPolicy.
AADSTS76021	ApplicationRequiresSignedRequests - The request sent by client is not signed while the application requires signed requests
AADSTS76026	RequestIssueTimeExpired - IssueTime in an SAML2 Authentication Request is expired.
AADSTS80001	OnPremiseStoreIsNotAvailable - The Authentication Agent is unable to connect to Active Directory. Make sure that agent servers are members of the same AD forest as the users whose passwords need to be validated and they are able to connect to Active Directory.
AADSTS80002	OnPremisePasswordValidatorRequestTimedout - Password validation request timed out. Make sure that Active Directory is available and responding to requests from the agents.
AADSTS80005	OnPremisePasswordValidatorUnpredictableWebException - An unknown error occurred while processing the response from the Authentication Agent. Retry the request. If it continues to fail, open a support ticket to get more details on the error.
AADSTS80007	OnPremisePasswordValidatorErrorOccurredOnPrem - The Authentication Agent is unable to validate user's password. Check the agent logs for more info and verify that Active Directory is operating as expected.
AADSTS80010	OnPremisePasswordValidationEncryptionException - The Authentication Agent is unable to decrypt password.
AADSTS80012	OnPremisePasswordValidationAccountLogonInvalidHours - The users attempted to log on outside of the allowed hours (this is specified in AD).
AADSTS80013	OnPremisePasswordValidationTimeSkew - The authentication attempt couldn't be completed due to time skew between the machine running the authentication agent and AD. Fix time sync issues.
AADSTS80014	OnPremisePasswordValidationAuthenticationAgentTimeout - Validation request responded after maximum elapsed time exceeded. Open a support ticket with the error code, correlation ID, and timestamp to get more details on this error.
AADSTS81004	DesktopSsoIdentityInTicketIsNotAuthenticated - Kerberos authentication attempt failed.
AADSTS81005	DesktopSsoAuthenticationPackageNotSupported - The authentication package isn't supported.
AADSTS81006	DesktopSsoNoAuthorizationHeader - No authorization header was found.
AADSTS81007	DesktopSsoTenantIsNotOptIn - The tenant isn't enabled for Seamless SSO.

Error	Description
AADSTS81009	DesktopSsoAuthorizationHeaderValueWithBadFormat - Unable to validate user's Kerberos ticket.
AADSTS81010	DesktopSsoAuthTokenInvalid - Seamless SSO failed because the user's Kerberos ticket has expired or is invalid.
AADSTS81011	DesktopSsoLookupUserBySidFailed - Unable to find user object based on information in the user's Kerberos ticket.
AADSTS81012	DesktopSsoMismatchBetweenTokenUpnAndChosenUpn - The user trying to sign in to Microsoft Entra ID is different from the user signed into the device.
AADSTS90002	InvalidTenantName - The tenant name wasn't found in the data store. Check to make sure you have the correct tenant ID. The application developer will receive this error if their app attempts to sign into a tenant that we cannot find. Often, this is because a cross-cloud app was used against the wrong cloud, or the developer attempted to sign in to a tenant derived from an email address, but the domain isn't registered.
AADSTS90004	InvalidRequestFormat - The request isn't properly formatted.
AADSTS90005	InvalidRequestWithMultipleRequirements - Unable to complete the request. The request isn't valid because the identifier and login hint can't be used together.
AADSTS90006	ExternalServerRetryableError - The service is temporarily unavailable.
AADSTS90007	InvalidSessionId - Bad request. The passed session ID can't be parsed.
AADSTS90008	TokenForItselfRequiresGraphPermission - The user or administrator hasn't consented to use the application. At the minimum, the application requires access to Microsoft Entra ID by specifying the sign-in and read user profile permission.
AADSTS90009	TokenForItselfMissingIdenticalAppIdentifier - The application is requesting a token for itself. This scenario is supported only if the resource that's specified is using the GUID-based application ID.
AADSTS90010	NotSupported - Unable to create the algorithm.
AADSTS9001023	The grant type isn't supported over the /common or /consumers endpoints. Please use the /organizations or tenant-specific endpoint.
AADSTS90012	RequestTimeout - The requested has timed out.
AADSTS90013	InvalidUserInput - The input from the user isn't valid.
AADSTS90014	MissingRequiredField - This error code might appear in various cases when an expected field isn't present in the credential.
AADSTS900144	The request body must contain the following parameter: '{name}'. Developer error - the app is attempting to sign in without the necessary or correct authentication parameters.

Error	Description
AADSTS90015	QueryStringTooLong - The query string is too long.
AADSTS90016	MissingRequiredClaim - The access token isn't valid. The required claim is missing.
AADSTS90019	MissingTenantRealm - Microsoft Entra ID was unable to determine the tenant identifier from the request.
AADSTS90020	The SAML 1.1 Assertion is missing ImmutableID of the user. Developer error - the app is attempting to sign in without the necessary or correct authentication parameters.
AADSTS90022	AuthenticatedInvalidPrincipalNameFormat - The principal name format isn't valid, or doesn't meet the expected `name[/host][@realm]` format. The principal name is required, host, and realm are optional and can be set to null.
AADSTS90023	InvalidRequest - The authentication service request isn't valid.
AADSTS900236	InvalidRequestSamlPropertyUnsupported- The SAML authentication request property '{propertyName}' isn't supported and must not be set.
AADSTS9002313	InvalidRequest - Request is malformed or invalid. - The issue arises because there was something wrong with the request to a certain endpoint. The suggestion to this issue is to get a fiddler trace of the error occurring and looking to see if the request is properly formatted or not.
AADSTS9002332	Application '{principalId}'({principalName}) is configured for use by Microsoft Entra users only. Please do not use the /consumers endpoint to serve this request.
AADSTS90024	RequestBudgetExceededError - A transient error has occurred. Try again.
AADSTS90027	We are unable to issue tokens from this API version on the MSA tenant. Please contact the application vendor as they need to use version 2.0 of the protocol to support this.
AADSTS90033	MsodsServiceUnavailable - The Microsoft Online Directory Service (MSODS) isn't available.
AADSTS90036	MsodsServiceUnretryableFailure - An unexpected, non-retryable error from the WCF service hosted by MSODS has occurred. Open a support ticket to get more details on the error.
AADSTS90038	NationalCloudTenantRedirection - The specified tenant 'Y' belongs to the National Cloud 'X'. Current cloud instance 'Z' does not federate with X. A cloud redirect error is returned.
AADSTS900384	JWT token failed signature validation. Actual message content is runtime specific, there are a variety of causes for this error. Please see the returned exception message for details.
AADSTS90043	NationalCloudAuthCodeRedirection - The feature is disabled.
AADSTS900432	Confidential Client isn't supported in Cross Cloud request.
AADSTS90051	InvalidNationalCloudId - The national cloud identifier contains an invalid cloud identifier.
AADSTS90055	TenantThrottlingError - There are too many incoming requests. This exception is thrown for blocked tenants.

Error	Description
AADSTS90056	BadResourceRequest - To redeem the code for an access token, the app should send a POST request to the `/token` endpoint. Also, prior to this, you should provide an authorization code and send it in the POST request to the `/token` endpoint. Refer to this article for an overview of OAuth 2.0 authorization code flow. Direct the user to the `/authorize` endpoint, which will return an authorization_code. By posting a request to the `/token` endpoint, the user gets the access token. Check **App registrations** > **Endpoints** to confirm that the two endpoints were configured correctly.
AADSTS900561	BadResourceRequestInvalidRequest - The endpoint only accepts {valid_verbs} requests. Received a {invalid_verb} request. {valid_verbs} represents a list of HTTP verbs supported by the endpoint (for example, POST), {invalid_verb} is an HTTP verb used in the current request (for example, GET). This can be due to developer error, or due to users pressing the back button in their browser, triggering a bad request. It can be ignored.
AADSTS90072	PassThroughUserMfaError - The external account that the user signs in with doesn't exist on the tenant that they signed into; so the user can't satisfy the MFA requirements for the tenant. This error also might occur if the users are synced, but there is a mismatch in the ImmutableID (sourceAnchor) attribute between Active Directory and Microsoft Entra ID. The account must be added as an external user in the tenant first. Sign out and sign in with a different Microsoft Entra user account. For more information, please visit configuring external identities.
AADSTS90081	OrgIdWsFederationMessageInvalid - An error occurred when the service tried to process a WS-Federation message. The message isn't valid.
AADSTS90082	OrgIdWsFederationNotSupported - The selected authentication policy for the request isn't currently supported.
AADSTS90084	OrgIdWsFederationGuestNotAllowed - Guest accounts aren't allowed for this site.
AADSTS90085	OrgIdWsFederationSltRedemptionFailed - The service is unable to issue a token because the company object hasn't been provisioned yet.
AADSTS90086	OrgIdWsTrustDaTokenExpired - The user DA token is expired.
AADSTS90087	OrgIdWsFederationMessageCreationFromUriFailed - An error occurred while creating the WS-Federation message from the URI.
AADSTS90090	GraphRetryableError - The service is temporarily unavailable.
AADSTS90091	GraphServiceUnreachable
AADSTS90092	GraphNonRetryableError
AADSTS90093	GraphUserUnauthorized - Graph returned with a forbidden error code for the request.
AADSTS90094	AdminConsentRequired - Administrator consent is required.
AADSTS900382	Confidential Client isn't supported in Cross Cloud request.

Error	Description
AADSTS90095	AdminConsentRequiredRequestAccess- In the Admin Consent Workflow experience, an interrupt that appears when the user is told they need to ask the admin for consent.
AADSTS90099	The application '{appId}' ({appName}) has not been authorized in the tenant '{tenant}'. Applications must be authorized to access the external tenant before partner delegated administrators can use them. Provide pre-consent or execute the appropriate Partner Center API to authorize the application.
AADSTS900971	No reply address provided.
AADSTS90100	InvalidRequestParameter - The parameter is empty or not valid.
AADSTS901002	AADSTS901002: The 'resource' request parameter isn't supported.
AADSTS90101	InvalidEmailAddress - The supplied data isn't a valid email address. The email address must be in the format `someone@example.com`.
AADSTS90102	InvalidUriParameter - The value must be a valid absolute URI.
AADSTS90107	InvalidXml - The request isn't valid. Make sure your data doesn't have invalid characters.
AADSTS90112	Application identifier is expected to be a GUID.
AADSTS90114	InvalidExpiryDate - The bulk token expiration timestamp will cause an expired token to be issued.
AADSTS90117	InvalidRequestInput
AADSTS90119	InvalidUserCode - The user code is null or empty.
AADSTS90120	InvalidDeviceFlowRequest - The request was already authorized or declined.
AADSTS90121	InvalidEmptyRequest - Invalid empty request.
AADSTS90123	IdentityProviderAccessDenied - The token can't be issued because the identity or claim issuance provider denied the request.
AADSTS90124	V1ResourceV2GlobalEndpointNotSupported - The resource isn't supported over the `/common` or `/consumers` endpoints. Use the `/organizations` or tenant-specific endpoint instead.
AADSTS90125	DebugModeEnrollTenantNotFound - The user isn't in the system. Make sure you entered the user name correctly.
AADSTS90126	DebugModeEnrollTenantNotInferred - The user type isn't supported on this endpoint. The system can't infer the user's tenant from the user name.
AADSTS90130	NonConvergedAppV2GlobalEndpointNotSupported - The application isn't supported over the `/common` or `/consumers` endpoints. Use the `/organizations` or tenant-specific endpoint instead.
AADSTS120000	PasswordChangeIncorrectCurrentPassword

Error	Description
AADSTS120002	PasswordChangeInvalidNewPasswordWeak
AADSTS120003	PasswordChangeInvalidNewPasswordContainsMemberName
AADSTS120004	PasswordChangeOnPremComplexity
AADSTS120005	PasswordChangeOnPremSuccessCloudFail
AADSTS120008	PasswordChangeAsyncJobStateTerminated - A non-retryable error has occurred.
AADSTS120011	PasswordChangeAsyncUpnInferenceFailed
AADSTS120012	PasswordChangeNeedsToHappenOnPrem
AADSTS120013	PasswordChangeOnPremisesConnectivityFailure
AADSTS120014	PasswordChangeOnPremUserAccountLockedOutOrDisabled
AADSTS120015	PasswordChangeADAdminActionRequired
AADSTS120016	PasswordChangeUserNotFoundBySspr
AADSTS120018	PasswordChangePasswordDoesnotComplyFuzzyPolicy
AADSTS120020	PasswordChangeFailure
AADSTS120021	PartnerServiceSsprInternalServiceError
AADSTS130004	NgcKeyNotFound - The user principal doesn't have the NGC ID key configured.
AADSTS130005	NgcInvalidSignature - NGC key signature verified failed.
AADSTS130006	NgcTransportKeyNotFound - The NGC transport key isn't configured on the device.
AADSTS130007	NgcDeviceIsDisabled - The device is disabled.
AADSTS130008	NgcDeviceIsNotFound - The device referenced by the NGC key wasn't found.
AADSTS135010	KeyNotFound
AADSTS135011	Device used during the authentication is disabled.
AADSTS140000	InvalidRequestNonce - Request nonce isn't provided.
AADSTS140001	InvalidSessionKey - The session key isn't valid.
AADSTS165004	Actual message content is runtime specific. Please see returned exception message for details.
AADSTS165900	InvalidApiRequest - Invalid request.
AADSTS220450	UnsupportedAndroidWebViewVersion - The Chrome WebView version isn't supported.

Error	Description
AADSTS220501	InvalidCrlDownload
AADSTS221000	DeviceOnlyTokensNotSupportedByResource - The resource isn't configured to accept device-only tokens.
AADSTS240001	BulkAADJTokenUnauthorized - The user isn't authorized to register devices in Microsoft Entra ID.
AADSTS240002	RequiredClaimIsMissing - The id_token can't be used as `urn:ietf:params:oauth:grant-type:jwt-bearer` grant.
AADSTS501621	ClaimsTransformationTimeoutRegularExpressionTimeout - Regular expression replacement for claims transformation has timed out. This indicates a too complex regular expression may have been configured for this application. A retry of the request may succeed. Otherwise, please contact your admin to fix the configuration.
AADSTS530032	BlockedByConditionalAccessOnSecurityPolicy - The tenant admin has configured a security policy that blocks this request. Check the security policies that are defined on the tenant level to determine if your request meets the policy requirements.
AADSTS700016	UnauthorizedClient_DoesNotMatchRequest - The application wasn't found in the directory/tenant. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You might have misconfigured the identifier value for the application or sent your authentication request to the wrong tenant.
AADSTS700020	InteractionRequired - The access grant requires interaction.
AADSTS700022	InvalidMultipleResourcesScope - The provided value for the input parameter scope isn't valid because it contains more than one resource.
AADSTS700023	InvalidResourcelessScope - The provided value for the input parameter scope isn't valid when requesting an access token.
AADSTS7000215	Invalid client secret is provided. Developer error - the app is attempting to sign in without the necessary or correct authentication parameters.
AADSTS7000218	The request body must contain the following parameter: 'client_assertion' or 'client_secret'.
AADSTS7000222	InvalidClientSecretExpiredKeysProvided - The provided client secret keys are expired. Create new keys for your app, or consider using certificate credentials for added security: https://aka.ms/certCreds
AADSTS700229	ForbiddenTokenType- Only app-only tokens can be used as Federated Identity Credentials for Microsoft Entra issuer. Use an app-only access token (generated during a client credentials flow) instead of a user-delegated access token (representing a request coming from a user context).
AADSTS700005	InvalidGrantRedeemAgainstWrongTenant - Provided Authorization Code is intended to use against other tenant, thus rejected. OAuth2 Authorization Code must be redeemed against

Error	Description
	same tenant it was acquired for (/common or /{tenant-ID} as appropriate)
AADSTS1000000	UserNotBoundError - The Bind API requires the Microsoft Entra user to also authenticate with an external IDP, which hasn't happened yet.
AADSTS1000002	BindCompleteInterruptError - The bind completed successfully, but the user must be informed.
AADSTS100007	Microsoft Entra Regional ONLY supports auth either for MSIs OR for requests from MSAL using SN+I for 1P apps or 3P apps in Microsoft infrastructure tenants.
AADSTS1000031	Application {appDisplayName} can't be accessed at this time. Contact your administrator.
AADSTS7000112	UnauthorizedClientApplicationDisabled - The application is disabled.
AADSTS7000114	Application 'appIdentifier' isn't allowed to make application on-behalf-of calls.
AADSTS7500529	The value ‘SAMLId-Guid’ isn't a valid SAML ID - Microsoft Entra ID uses this attribute to populate the InResponseTo attribute of the returned response. ID must not begin with a number, so a common strategy is to prepend a string like "ID" to the string representation of a GUID. For example, id6c1c178c166d486687be4aaf5e482730 is a valid ID.
AADSTS9002341	V2Error: `invalid_grant` - The user is required to permit single sign-On (SSO). This error occurs when the user has not granted the necessary permissions for the application to perform SSO. The user should be redirected to the consent screen to grant the necessary permissions. Refer to this announcement for more information."
AADSTS901011	NoEmailAddressCollectedFromExternalOidcIDP - No email address was obtained from the external OpenID Connect (OIDC) identity provider. This usually happens when the user selects **Hide my email** upon signing up.
AADSTS901012	EmailAddressCollectedFromExternalOidcIDPNotVerified - No verified email address was obtained from the identity provider. The email address is not verified in the ID token from the external OIDC identity provider.
AADSTS901014	NoExternalIdentifierCollectedFromExternalOidcIDP - The external identifier does not exist in the ID token from the external OIDC identity provider.

Next steps

- Have a question or can't find what you're looking for? Create a GitHub issue or see Support and help options for developers to learn about other ways you can get help and support.

Feedback

Was this page helpful? 👍 Yes 👎 No

Provide product feedback