MICROSOFT ENTRA ACCESS

Resolve AADSTS500021 for NCREIF Access

A precise IT runbook for member organizations whose Microsoft Entra tenant restriction policy is blocking access to the NCREIF application.

ISSUE COVERED

AADSTS500021 | Access to the NCREIF tenant is denied

Primary cause: legacy / proxy-based Microsoft Entra Tenant Restrictions v1 allowlist

Version 2.0 | October 2026
For member organization IT and security teams

START HERE

What this error actually tells us

The observed sign-in error is AADSTS500021. Microsoft documents this code as a Tenant Restrictions decision: the requested tenant is not in the allowlist carried in the legacy Restrict-Access-To-Tenants header.

Primary diagnosis	Treat Tenant Restrictions v1 / legacy proxy header injection as the first remediation path for this exact error. Do not begin by changing TLS policy, Azure Front Door, DNS, WAF, or the NCREIF application.

Why this matters

1	**User starts NCREIF sign-in**	Browser reaches Microsoft authentication
2	**Member security policy adds tenant restriction signal**	Often on a firewall, proxy, or secure web gateway
3	**Microsoft Entra evaluates the target tenant**	NCREIF is not present in the allowed tenant list
4	**AADSTS500021 is returned**	The application does not receive a successful authenticated session

If your organization says it uses Tenant Restrictions v2	First verify that no network device is still injecting the legacy Restrict-Access-To-Tenants header. Microsoft migration guidance says to remove that v1 header after moving to v2. A stale v1 header can continue to produce this exact failure.

MINIMUM INPUT

What member IT actually needs from NCREIF

For this error, the member organization does not need a long list of application and network details. Start with the tenant identifier required by the policy.

NCREIF Microsoft Entra Tenant ID	13894ea7-d291-4721-aa62-03f17ef77db1 Required for the tenant allowlist / partner organization.
Application name	NCREIF_DataConnect_App Reference only.
Application / Client ID	cd4b20cd-ab76-47fd-be66-4657b73f6809 Only needed if the member organization applies application-level scoping.

Not required for the v1 tenant allowlist Application URL is not used in Restrict-Access-To-Tenants. A verified domain can identify a tenant, but it is unnecessary when the Tenant ID is available. The tenant display name is descriptive only.

Information the member organization provides from its own tenant

Member organization Tenant ID	Used as the value of Restrict-Access-Context in Tenant Restrictions v1 and as the tenant identifier for v2 signaling.
Affected user / test group	Use a limited test scope where the proxy or policy platform supports staged rollout.
Policy owner	Network / security administrator for v1; Entra security administrator for v2 partner policy changes.

Important Do not place the NCREIF application Client ID into Restrict-Access-To-Tenants. That header accepts tenant identifiers, not application IDs.

PRIMARY REMEDIATION

Tenant Restrictions v1 - update the proxy allowlist

Use this procedure when a proxy, firewall, secure web gateway, or other egress control inserts Microsoft Entra tenant restriction headers. This is the primary path for AADSTS500021.

1	**Find the header injection policy**	Locate the rule that modifies authentication traffic sent to login.microsoftonline.com, login.microsoft.com, and login.windows.net. Common enforcement points include Palo Alto, Cisco, Zscaler, Fortinet, Netskope, or a dedicated proxy.
2	**Add the NCREIF Tenant ID**	Append the NCREIF Tenant ID to the existing comma-separated Restrict-Access-To-Tenants value. Preserve every tenant that is already approved. Do not add spaces between entries.
3	**Keep the member context unchanged**	Restrict-Access-Context should contain the member organization's own Tenant ID. Do not replace it with the NCREIF Tenant ID.
4	**Respect Microsoft endpoint exclusions**	Do not include device.login.microsoftonline.com or enterpriseregistration.windows.net in TLS break-and-inspect / header injection. Microsoft warns this can interfere with device registration and device-based Conditional Access.
5	**Apply and retest**	Start a new InPrivate session and sign in to the NCREIF application. If AADSTS500021 disappears, the tenant restriction issue is resolved. If a different error appears, stop changing this allowlist and troubleshoot the new error separately.

Configuration pattern

Preserve the existing list	Restrict-Access-To-Tenants: existing-tenant,[NCREIF-TENANT-ID],other-approved-tenant Restrict-Access-Context: [MEMBER-ORGANIZATION-TENANT-ID]

IF YOUR ORGANIZATION USES V2

Tenant Restrictions v2 - check migration state first

First check If users still receive AADSTS500021, inspect the proxy/firewall for the legacy v1 Restrict-Access-To-Tenants header. Microsoft instructs organizations to remove that header when migrating the proxy from v1 to v2.

If the legacy v1 header is no longer present

1	**Open Cross-tenant access settings**	Microsoft Entra admin center > Entra ID > External Identities > Cross-tenant access settings > Organizational settings.
2	**Add NCREIF as a partner organization**	Use the NCREIF Tenant ID (preferred). A verified domain also works, but is not required if the Tenant ID is known.
3	**Open the Tenant restrictions column**	Select the organization-specific tenant restriction settings instead of weakening the global default.
4	**Customize only what is required**	Allow the required external users/groups and external applications. If the policy is application-scoped, the NCREIF application Client ID is required to target the application precisely.
5	**Confirm v2 signaling**	For proxy-based v2 enforcement, the signal is sec-Restrict-Tenant-Access-Policy: <MemberTenantID>:<PolicyGUID>. NCREIF is allowed in the Entra cloud policy - not by putting the NCREIF Tenant ID into this v2 header.

Admin permissions Microsoft documents Security Administrator as the baseline role for tenant restriction configuration. Partner-specific settings can also be configured by an appropriately authorized Conditional Access Administrator.

ONLY AFTER AADSTS500021 IS GONE

Secondary access checks

Do not mix these controls into the first remediation step. Tenant restrictions, B2B cross-tenant access, Conditional Access, and application authorization are separate controls. Use the new error or sign-in log result to decide which one to investigate next.

Outbound B2B collaboration

Check only if your organization has customized outbound B2B access.

Microsoft Entra allows B2B collaboration by default. If your organization changed the default or created a partner-specific block, review:

Entra ID > External Identities > Cross-tenant access settings > Organizational settings > NCREIF > Outbound access.

If application-level scoping is used, the NCREIF Client ID may be required.

Conditional Access

A successful tenant restriction change can expose a separate Conditional Access requirement such as MFA, device compliance, sign-in risk, or location policy.

Use the Entra sign-in log to identify the specific Conditional Access policy and result. Do not relax organization-wide CA rules solely because the original tenant restriction was fixed.

Application / guest authorization

If the authentication proceeds but the application denies access, NCREIF may need to validate guest onboarding, enterprise application assignment, or NCREIF-side authorization. Member IT should provide the new error evidence rather than repeatedly changing its own tenant restriction policy.

Device state: Unregistered

The original screenshot shows an unregistered device state. That is not the cause of AADSTS500021. It becomes relevant only if a later Conditional Access policy requires a compliant or Microsoft Entra hybrid joined device.

Rule of thumb Once AADSTS500021 disappears, consider the v1 allowlist issue closed. If the sign-in still fails, use the new AADSTS code, Conditional Access result, or application response as the next source of truth.

VALIDATE AND CLOSE

Proof of resolution and escalation package

1	**Start a clean session**	Use Edge or Chrome InPrivate to avoid cached Microsoft sign-in state.
2	**Sign in to NCREIF**	Use the affected member account from the normal corporate network and device.
3	**Confirm AADSTS500021 is gone**	If the same code remains, re-check the v1 allowlist/header path. If the code changes, move to the new error.
4	**Validate application access**	Confirm the user reaches the NCREIF application and the intended function.
5	**Capture evidence if anything still fails**	Record Request ID, Correlation ID, UTC timestamp, exact error code/message, user UPN, and the policy path used (v1 or v2).

Useful Microsoft evidence sources

Tenant Restrictions v1 report	Entra ID > Overview > Tenant restrictions. Filter by time, user, application, client, status, and target tenant ID.
Microsoft Entra sign-in logs	Use Request ID / Correlation ID / timestamp to locate the failed sign-in and identify the next policy decision.

What not to change for AADSTS500021

Do not change Azure Front Door TLS policy, Front Door IP ranges, DNS records, WAF rules, or the NCREIF application URL to resolve this code. Those items may matter for other connectivity incidents, but they are not the control producing this Entra tenant restriction error.

Microsoft references

Authentication error codes
https://learn.microsoft.com/en-us/entra/identity-platform/reference-error-codes
Tenant Restrictions v1
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/tenant-restrictions
Tenant Restrictions v2
https://learn.microsoft.com/en-us/entra/external-id/tenant-restrictions-v2
Cross-tenant access settings
https://learn.microsoft.com/en-us/entra/external-id/cross-tenant-access-settings-b2b-collaboration

Guest Invitation being rejected by SPAN policies

Create recipient-side exception for application.ncreif.org

1	**Go to Microsoft Defender Portal**	Use Edge or Chrome InPrivate to avoid cached Microsoft sign-in state.
2	**Email & collaboration → Policies & rules → Threat policies → Anti-spam → Inbound anti-spam policy**	Add under Allowed domains **application.ncreif.org**
3	**Microsoft supports custom inbound anti-spam policies scoped to particular recipients, groups, or domains.**	Create a dedicated custom inbound anti-spam policy rather than relaxing the default policy for everyone
4	**Validate e-mail**	Confirm the e-mail invitation reaches guest user.
5	**Capture evidence if anything still fails**	

Microsoft references

Configure anti-spam policies for cloud mailboxes

https://learn.microsoft.com/en-us/defender-office-365/anti-spam-policies-configure

Email nondelivery reports and SMTP errors in Exchange Online

https://learn.microsoft.com/en-us/troubleshoot/exchange/email-delivery/ndr/non-delivery-reports-in-exchange-online

Guest Invitation being rejected by SPAN policies

Configure SPF, DKIM and DMARC of subdomain

1	**Go to your DNS provider**	
2	**Create a TXT Record for SPF**	Host: application Type: TXT Value: v=spf1 include:spf.protection.outlook.com -all
3	**Create the first CNAME Record for DKIM**	selector1._domainkey.application.ncreif.org CNAME selector1-application-ncreif-org._domainkey.ncreifapp.onmicrosoft.com
4	**Create the second CNAME Record fo DKIM**	selector2._domainkey.application.ncreif.org CNAME selector2-application-ncreif-org._domainkey.ncreifapp.onmicrosoft.com
5	**Create the TXT Record for DMARC**	Host: _dmarc.application Type: TXT Value: v=DMARC1; p=none; rua=mailto:dmarc@ncreif.org; fo=1

Microsoft references

https://learn.microsoft.com/en-us/entra/external-id/invitation-email-elements#dns-configuration-spf-dkim-dmarc

https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about
https://learn.microsoft.com/en-us/defender-office-365/email-authentication-spf-configure#scenario-microsoft-365-email-only

https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure#syntax-for-dkim-cname-records

https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dmarc-configure#syntax-for-dmarc-txt-records