Microsoft Ignite

Nov 19–22, 2024

Register now ›

✕

Learn

Discover ⌄   Product documentation ⌄   Development languages ⌄   Topics ⌄   🔍   Sign in

Microsoft Entra   Microsoft Entra ID   External ID   Global Secure Access   ID Governance   Permissions Management   More ⌄   Admin center

Learn / Microsoft Entra / Microsoft Entra ID / Monitoring and health /

⊕   ✎   ⋮

Microsoft Entra audit log categories and activities

Article • 10/05/2024 • 25 contributors

⌂ Feedback

In this article

Microsoft Entra (AAD) Management UX
Access reviews
Account provisioning
Application proxy

Show 24 more

Microsoft Entra audit logs collect all traceable activities within your Microsoft Entra tenant. Audit logs can be used to determine who made a change to service, user, group, or other item.

This article provides a comprehensive list of the audit categories and their related activities. To jump to a specific audit category, use the "In this article" section.

Audit log activities and categories change periodically. The tables are updated regularly, but might not be in sync with what is available in Microsoft Entra ID. Provide us with feedback if you think there's a missing audit category or activity.

1. Sign in to the Microsoft Entra admin center ⧉ as at least a Reports Reader.
2. Browse to **Identity** > **Monitoring & health** > **Audit logs**.
3. Adjust the filters accordingly.
4. To view the details, select a row from the resulting table.

Microsoft Entra (AAD) Management UX

Microsoft Graph PowerShell cmdlets

SLA performance for Microsoft Entra ID

FAQs

> Microsoft Graph APIs

🔖 **Download PDF**

⌞⌝ **Expand table**

Audit Category	Activity
AdministrativeUnit	Bulk add members to administrative unit - finished (bulk)
AdministrativeUnit	Bulk remove members to administrative unit - finished (bulk)
AdministrativeUnit	started (bulk)
DeviceManagement	Bulk add authentication devices - finished (bulk)
DeviceManagement	Download devices - finished (bulk)
DeviceManagement	started (bulk)
DirectoryManagement	Bulk download hardware tokens - finished (bulk)
DirectoryManagement	Download registration and reset events - finished (bulk)
DirectoryManagement	Download role assignments - finished (bulk)
DirectoryManagement	Download service principals - finished (bulk)
DirectoryManagement	Download user registration details - finished (bulk)
DirectoryManagement	Download users - finished (bulk)
DirectoryManagement	Export summary data - finished (bulk)
DirectoryManagement	Export summary data new - finished (bulk)
DirectoryManagement	started (bulk)
GroupManagement	Bulk import group members - finished (bulk)
GroupManagement	Bulk remove group members - finished (bulk)
GroupManagement	Download group members - finished (bulk)
GroupManagement	Download groups - finished (bulk)
GroupManagement	started (bulk)
Policy	Add blocked user
Policy	Add bypass user
Policy	Clear block on user
Policy	Remove bypassed user
Policy	Update Sign-In Risk Policy
Policy	Update User Risk and MFA Registration Policy
UserManagement	Bulk create users - finished (bulk)
UserManagement	Bulk delete users - finished (bulk)
UserManagement	Bulk invite users - finished (bulk)
UserManagement	Bulk restore deleted users - finished (bulk)

UserManagement	Download users - finished (bulk)
UserManagement	started (bulk)

Access reviews

With Microsoft Entra ID Governance access reviews, you can ensure users have the appropriate access. Access review audit logs can tell you who initiated or ended an access review. These logs can also tell you if any access review settings were changed.

⌞⌝ Expand table

Audit Category	Activity
DirectoryManagement	Create program
DirectoryManagement	Link program control
DirectoryManagement	Unlink program control
DirectoryManagement	Update program
Policy	Access review ended
Policy	Apply decision
Policy	Approve decision
Policy	Bulk Approve decisions
Policy	Bulk Deny decisions
Policy	Bulk Reset decisions
Policy	Bulk mark decisions as don't know
Policy	Cancel request
Policy	Create access review
Policy	Create request
Policy	Delete access review
Policy	Delete approvals
Policy	Deny decision
Policy	Don't know decision
Policy	Request expired
Policy	Reset decision
Policy	Update access review
Policy	Update partner directory settings
Policy	Update request

UserManagement	Apply review
UserManagement	Approve all requests in business flow
UserManagement	Auto review
UserManagement	Auto apply review
UserManagement	Create business flow
UserManagement	Create governance policy template
UserManagement	Delete access review
UserManagement	Delete business flow
UserManagement	Delete governance policy template
UserManagement	Deny all decisions
UserManagement	Deny all requests in business flow
UserManagement	Request approved
UserManagement	Request denied
UserManagement	Update business flow
UserManagement	Update governance policy template

Account provisioning

Configuration changes for application provisioning, HR provisioning, cross-tenant synchronization, and Microsoft Entra Connect cloud sync, are found in this log. The provisioning service only has one audit category in the logs. For actions that the provisioning service performs such as creating users, updating users, and deleting users we recommend using the provisioning logs. For monitoring changes to your provisioning configuration, we recommend using the audit logs.

⌗ Expand table

Audit Category	Activity	Description
ProvisioningManagement	Add provisioning configuration	A new provisioning configuration has been created.
ProvisioningManagement	Delete provisioning configuration	The provisioning configuration has been deleted.
ProvisioningManagement	Disable/pause provisioning configuration	The provisioning job has been disabled / paused.
ProvisioningManagement	Enable/restart provisioning configuration	The provisioning job as been restarted.
ProvisioningManagement	Enable/start provisioning	The provisioning job has been started.

	configuration	
ProvisioningManagement	Export	The provisioning job has exported a change to the target system (ex: create a user).
ProvisioningManagement	Import	The provisioning job imported the object from the source system (ex: import the user properties in Entra before provisioning the account into Salesforce).
ProvisioningManagement	Other	
ProvisioningManagement	Process escrow	The provisioning service was unable to export a change to the target application and is retrying the operation.
ProvisioningManagement	Quarantine	The provisioning job is executing at a reduced frequency due to issues such as a lack of connectivity to the target application. Learn more
ProvisioningManagement	Synchronization rule action	The provisioning service evaluated the object and did not export a change to the target system. This even is most often emitted when a user is skipped due to being out of scope for provisioning.
ProvisioningManagement	Update attribute mappings or scope	The attribute mappings or scoping rules for the provisioning job have been updated.
ProvisioningManagement	Update provisioning setting or credentials	The settings on your provisioning job (ex: notification email change, sync all vs. sync assigned users and groups, accidental deletions prevention) have been updated. The credentials for your provisioning job (ex: add a new bearer token) have been updated.
ProvisioningManagement	User Provisioning	The schema for the provisioning job has been restored to the default.

Application proxy

If you're utilizing Application Proxy to provide your users with remote access to internal apps, the Application Proxy audit logs can help you keep track of changes to available applications or Connector groups.

⌞⌝ **Expand table**

Audit Category	Activity
Application Management	Add application
Application Management	Delete application
Application Management	Update application
Authentication	Add a group to feature rollout
Authentication	Create rollout policy for feature
Authentication	Delete rollout policy of feature
Authentication	Remove a group from feature rollout

Authentication	Remove user from feature rollout
Authentication	Update rollout policy of feature
Authorization	User authorization for application access
DirectoryManagement	Disable Desktop Sso
DirectoryManagement	Disable Desktop Sso for a specific domain
DirectoryManagement	Disable application proxy
DirectoryManagement	Disable passthrough authentication
DirectoryManagement	Enable Desktop Sso
DirectoryManagement	Enable Desktop Sso for a specific domain
DirectoryManagement	Enable application proxy
DirectoryManagement	Enable passthrough authentication
ResourceManagement	Add connector Group
ResourceManagement	Add a Connector to Connector Group
ResourceManagement	Add application SSL certificate
ResourceManagement	Delete Connector Group
ResourceManagement	Delete SSL binding
ResourceManagement	Register connector
ResourceManagement	Update Connector Group

Authentication Methods

The Audit logs for Authentication Methods can be used to make sure that your users have registered their mobile device properly to enable multifactor authentication.

⌞⌝ Expand table

Audit Category	Activity
ApplicationManagement	Assign Hardware Oath Token
ApplicationManagement	Authentication Methods Policy Reset
ApplicationManagement	Authentication Methods Policy Update
ApplicationManagement	Authentication Strength Combination Configuration Create
ApplicationManagement	Authentication Strength Combination Configuration Delete
ApplicationManagement	Authentication Strength Combination Configuration Update
ApplicationManagement	Authentication Strength Policy Create
ApplicationManagement	Authentication Strength Policy Delete

ApplicationManagement	Authentication Strength Policy Update
ApplicationManagement	Bulk upload Hardware Oath Token
ApplicationManagement	Create Hardware Oath Token
ApplicationManagement	Delete Hardware Oath Token
ApplicationManagement	MFA Service Policy Update
ApplicationManagement	PATCH UserAuthMethod.PatchSignInPreferencesAsync
ApplicationManagement	PATCH UserAuthMethod.ResetQRPinAsync
ApplicationManagement	PATCH UserAuthMethod.UpdateQRPinAsync
ApplicationManagement	POST UserAuthMethod.SecurityInfoRegistrationCallback
ApplicationManagement	POST UserAuthMethod.SoftwareOathProofupRegistration
ApplicationManagement	Update Hardware Oath Token
DirectoryManagement	DELETE Subscription.DeleteProviders
DirectoryManagement	DELETE Tenant.DeleteAgentStatuses
DirectoryManagement	DELETE Tenant.DeleteCaches
DirectoryManagement	DELETE Tenant.DeleteGreetings
DirectoryManagement	PATCH Tenant.Patch
DirectoryManagement	PATCH Tenant.PatchCaches
DirectoryManagement	POST SoundFile.Post
DirectoryManagement	POST Subscription.CreateProvider
DirectoryManagement	POST Subscription.CreateSubscription
DirectoryManagement	POST Tenant.CreateBlockedUser
DirectoryManagement	POST Tenant.CreateBypassedUser
DirectoryManagement	POST Tenant.CreateCacheConfig
DirectoryManagement	POST Tenant.CreateGreeting
DirectoryManagement	POST Tenant.CreateTenant
DirectoryManagement	POST Tenant.GenerateNewActivationCredentials
DirectoryManagement	POST Tenant.RemoveBlockedUser
DirectoryManagement	POST Tenant.RemoveBypassedUser
UserManagement	Admin deleted security info
UserManagement	Admin registered security info
UserManagement	Admin started password reset
UserManagement	Admin updated security info

UserManagement	Get passkey creation options
UserManagement	Restore multifactor authentication on all remembered devices
UserManagement	Update per-user multifactor authentication state
UserManagement	User canceled security info registration
UserManagement	User changed default security info
UserManagement	User deleted security info
UserManagement	User registered all required security info
UserManagement	User registered security info
UserManagement	User reviewed security info
UserManagement	User started password change
UserManagement	user started password reset
UserManagement	User started security info registration
UserManagement	User updated security info

Microsoft Entra (Azure AD) Recommendations

Microsoft Entra Recommendations monitors your Microsoft Entra tenant and provides personalized insights and actionable guidance to implement best practices for Microsoft Entra features and optimize your tenant configurations. These logs provide a history of the changes made to the status of a recommendation.

⟦ ⟧ **Expand table**

Audit Category	Activity
DirectoryManagement	Dismiss recommendation
DirectoryManagement	Mark recommendation as complete
DirectoryManagement	Postpone recommendation

Microsoft Entra (Azure MFA) multifactor authentication

The Microsoft Entra multifactor authentication audit logs can help you track trends in suspicious activity or when fraud was reported. Use the Microsoft Entra sign-in logs ⧉ to see each time a user signs in when MFA is required.

⟦ ⟧ **Expand table**

Audit Category	Activity
DirectoryManagement	DeleteDataFromBackend
DirectoryManagement	DeleteDataFromCosmosDb
DirectoryManagement	ExportDataFromBackend
DirectoryManagement	ExportDataFromCosmosDb
UserManagement	Fraud reported - no action taken
UserManagement	Fraud reported - user is blocked for MFA
UserManagement	Suspicious activity reported
UserManagement	User registered security info

Azure RBAC (Elevated Access)

⌟⌞ Expand table

Audit Category	Activity
AzureRBACRoleManagementElevateAccess	The role assignment of User Access Administrator has been removed from the user
AzureRBACRoleManagementElevateAccess	User has elevated their access to User Access Administrator for their Azure Resources

B2B Auth

⌟⌞ Expand table

Audit Category	Activity
UserManagement	Redeem extern user invite

B2C

This set of audit logs is related to B2C. Due to the number of connected resources and potential external accounts, this service has a large set of categories and activities. Audit categories include ApplicationManagement, Authentication, Authorization, DirectoryManagement, IdentityProtection, KeyManagement, PolicyManagement, and ResourceManagement. Logs related to one-time passwords are found in the Other category.

⌟⌞ Expand table

Audit Category	Activity
Authentication	A self-service sign-up request was completed

Authentication	An API was called as part of a user flow
Authentication	Delete all available strong authentication devices
Authentication	Evaluate Conditional Access policies
Authentication	Exchange token
Authentication	Federate with an identity provider
Authentication	Get available strong authentication devices
Authentication	Issue a SAML assertion to the application
Authentication	Issue an access token to the application
Authentication	Issue an authorization code to the application
Authentication	Issue an id_token to the application
Authentication	Make phone call to verify phone number
Authentication	Register TOTP secret
Authentication	Remediate user
Authentication	Send SMS to verify phone number
Authentication	Send verification email
Authentication	Validate Client Credentials
Authentication	Validate local account credentials
Authentication	Validate user authentication
Authentication	Verify email address
Authentication	verify one time password
Authentication	Verify phone number
Authorization	Add v2 application permissions
Authorization	Check whether the resource name is available
Authorization	Create API connector
Authorization	Create Identity Provider
Authorization	Create authenticationEventListener
Authorization	Create authenticationEventsFlow
Authorization	Create custom identity provider
Authorization	Create custom policy
Authorization	Create customAuthenticationExtension
Authorization	Create or update a B2C directory resource
Authorization	Create or update a B2C directory tenant and resource

Authorization	Create or update a CIAM directory tenant and resource
Authorization	Create or update a Guest Usages resource
Authorization	Create or update localized resource
Authorization	Create policy key
Authorization	Create starter pack
Authorization	Create user attribute
Authorization	Create user flow
Authorization	Create v2 application
Authorization	Delete API connector
Authorization	Delete B2C Tenant where the caller is an administrator
Authorization	Delete B2C directory resource
Authorization	Delete CIAM directory resource
Authorization	Delete Guest Usages resource
Authorization	Delete Identity Provider
Authorization	Delete authenticationEventlistener
Authorization	Delete authenticationEventsFlow
Authorization	Delete custom policy
Authorization	Delete customAuthenticationExtension
Authorization	Delete localized resource
Authorization	Delete policy key
Authorization	Delete user attribute
Authorization	Delete user flow
Authorization	Delete v2 application
Authorization	Delete v2 application permission grant
Authorization	Generate key
Authorization	Get API connector
Authorization	Get API connectors
Authorization	Get B2C Tenants where the caller is an administrator
Authorization	Get B2C directory resource
Authorization	Get B2C directory resources in a resource group
Authorization	Get B2C directory resources in a subscription
Authorization	Get CIAM directory resource

Authorization	Get CIAM directory resources in a resource group
Authorization	Get CIAM directory resources in a subscription
Authorization	Get Guest Usages resources
Authorization	Get Guest Usages resources in a subscription
Authorization	Get Identity Provider
Authorization	Get Identity Providers
Authorization	Get OnAttributeCollectionStartCustomExtension
Authorization	Get OnAttributeCollectionSubmitCustomExtension
Authorization	Get OnPageRenderStartCustomExtension
Authorization	Get active key metadata from policy key
Authorization	Get age gating configuration
Authorization	Get authentication flows policy
Authorization	Get authenticationEventListener
Authorization	Get authenticationEventsFlow
Authorization	Get authenticationEventsFlows
Authorization	Get available output claims
Authorization	Get configured custom identity providers
Authorization	Get configured identity providers
Authorization	Get configured local identity providers
Authorization	Get custom domains
Authorization	Get custom identity provider
Authorization	Get custom policies
Authorization	Get custom policy
Authorization	Get custom policy metadata
Authorization	Get customAuthenticationExtension
Authorization	Get customAuthenticationExtensions
Authorization	Get identity provider types
Authorization	Get list of tenants
Authorization	Get localized resource
Authorization	Get operation status for an async operation
Authorization	Get operations of Microsoft.AzureActiveDirectory resource provider
Authorization	Get policy key

Authorization	Get policy keys
Authorization	Get resource properties of a tenant
Authorization	Get supported cultures
Authorization	Get supported identity providers
Authorization	Get supported page contracts
Authorization	Get tenant details
Authorization	Get tenant domains
Authorization	Get the authenticationEventsPolicy
Authorization	Get user attribute
Authorization	Get user attributes
Authorization	Get user flow
Authorization	Get user flows
Authorization	Get v1 and v2 applications
Authorization	Get v1 applications
Authorization	Get v2 application
Authorization	Initialize tenant
Authorization	Move resources
Authorization	Restore policy key
Authorization	Retrieve v2 application permissions grants
Authorization	Retrieve v2 application service principals
Authorization	Update API connector
Authorization	Update Identity Provider
Authorization	Update OnAttributeCollectionStartCustomExtension
Authorization	Update OnAttributeCollectionSubmitCustomExtension
Authorization	Update OnPageRenderStartCustomExtension
Authorization	Update a B2C directory resource
Authorization	Update a CIAM directory resource
Authorization	Update a Guest Usages resource
Authorization	Update age gating configuration
Authorization	Update authentication flows policy
Authorization	Update authenticationEventListener
Authorization	Update authenticationEventsFlow

Authorization	Update authenticationEventsPolicy
Authorization	Update custom identity provider
Authorization	Update custom policy
Authorization	Update customAuthenticationExtension
Authorization	Update identity provider
Authorization	Update local identity provider
Authorization	Update policy key
Authorization	Update subscription status
Authorization	Update tenant metadata
Authorization	Update user attribute
Authorization	Update user flow
Authorization	Upload certificate to policy key
Authorization	Upload key to policy key
Authorization	Upload secret into policy key
Authorization	Validate customExtension authenticationConfiguration
Authorization	Validate move resources
Authorization	Verify if tenant is B2C
Device	Delete pre-created device
Device	Pre-create device
Device	Recover device local administrator password
Device	Register device
Device	Unregister device
Device	Update device local administrator password
Directory Management	Get age gating configuration
Directory Management	Get list of tenants
Directory Management	Get resources properties of a tenant
Directory Management	Get tenant details
Directory Management	Get tenant domains
Directory Management	Initialize tenant
Directory Management	Update age gating configuration
Directory Management	Update tenant metadata
Directory Management	Verify if tenant is B2C

IdentityProtection	Evaluate Conditional Access policies
IdentityProtection	Remediate user
KeyManagement	Add BitLocker key
KeyManagement	Create policy key
KeyManagement	Delete BitLocker key
KeyManagement	Delete policy key
KeyManagement	Get active key metadata from policy key
KeyManagement	Get policy key
KeyManagement	Get policy keys
KeyManagement	Read BitLocker key
KeyManagement	Restore policy key
KeyManagement	Update policy key
KeyManagement	Upload key to policy key
KeyManagement	Upload secret into policy key
Other	Generate one time password
Other	Verify one time password
PolicyManagement	Create authenticationEventListener
PolicyManagement	Create authenticationEventsFlow
PolicyManagement	Create customAuthenticationExtension
PolicyManagement	Delete authenticationEventListener
PolicyManagement	Delete authenticationEventsFlow
PolicyManagement	Delete customAuthenticationExtension
PolicyManagement	Get OnAttributeCollectionStartCustomExtension
PolicyManagement	Get OnAttributeCollectionSubmitCustomExtension
PolicyManagement	Get OnPageRenderStartCustomExtension
PolicyManagement	Get authenticationEventListener
PolicyManagement	Get authenticationEventListeners
PolicyManagement	Get authenticationEventsFlow
PolicyManagement	Get authenticationEventsFlows
PolicyManagement	Get customAuthenticationExtension
PolicyManagement	Get customAuthenticationExtensions
PolicyManagement	Get the authenticationEventsPolicy

PolicyManagement	Update OnAttributeCollectionStartCustomExtension
PolicyManagement	Update OnAttributeCollectionSubmitCustomExtension
PolicyManagement	Update OnPageRenderStartCustomExtension
PolicyManagement	Update authenticationEventListener
PolicyManagement	Update authenticationEventsFlow
PolicyManagement	Update authenticationEventsPolicy
PolicyManagement	Update customAuthenticationExtension
PolicyManagement	Validate customExtension authenticationConfiguration
ResourceManagement	Check whether the resource name is available
ResourceManagement	Create API connector
ResourceManagement	Create Identity Provider
ResourceManagement	Create custom identity provider
ResourceManagement	Create custom policy
ResourceManagement	Create or update a B2C directory resource
ResourceManagement	Create or update a B2C directory tenant and resource
ResourceManagement	Create or update a CIAM directory tenant and resource
ResourceManagement	Create or update a Guest Usages resource
ResourceManagement	Create or update a localized resource
ResourceManagement	Create policy key
ResourceManagement	Create user attribute
ResourceManagement	Create user flow
ResourceManagement	Delete API connector
ResourceManagement	Delete B2C Tenant where the caller is an administrator
ResourceManagement	Delete B2C directory resource
ResourceManagement	Delete CIAM directory resource
ResourceManagement	Delete Guest Usages resource
ResourceManagement	Delete Identity Provider
ResourceManagement	Delete custom policy
ResourceManagement	Delete localized resource
ResourceManagement	Delete policy key
ResourceManagement	Delete user attribute
ResourceManagement	Delete user flow

ResourceManagement	Generate key
ResourceManagement	Get API connector
ResourceManagement	Get API connectors
ResourceManagement	Get B2C Tenant where the caller is an administrator
ResourceManagement	Get B2C directory resource
ResourceManagement	Get B2C directory resources in a resource group
ResourceManagement	Get B2C directory resources in a subscription
ResourceManagement	Get CIAM directory resource
ResourceManagement	Get CIAM directory resources in a resource group
ResourceManagement	Get CIAM directory resources in a subscription
ResourceManagement	Get Guest Usages resource
ResourceManagement	Get Guest Usages directory resources in a resource group
ResourceManagement	Get Guest Usages directory resources in a subscription
ResourceManagement	Get Identity Provider
ResourceManagement	Get Identity Providers
ResourceManagement	Get active key metadata from policy key
ResourceManagement	Get authentication flows policy
ResourceManagement	Get available output claims
ResourceManagement	Get configured custom identity providers
ResourceManagement	Get configured identity providers
ResourceManagement	Get configured local identity providers
ResourceManagement	Get custom identity provider
ResourceManagement	Get custom policies
ResourceManagement	Get custom policy
ResourceManagement	Get custom policy metadata
ResourceManagement	Get identity provider
ResourceManagement	Get identity provider types
ResourceManagement	Get identity providers
ResourceManagement	Get localized resource
ResourceManagement	Get operation status of an async operation
ResourceManagement	Get operations of Microsoft.AzureActiveDirectory resource provider
ResourceManagement	Get policy key

ResourceManagement	Get policy keys
ResourceManagement	Get supported cultures
ResourceManagement	Get supported identity providers
ResourceManagement	Get supported page contracts
ResourceManagement	Get user attribute
ResourceManagement	Get user attributes
ResourceManagement	Get user flow
ResourceManagement	Get user flows
ResourceManagement	Move resources
ResourceManagement	Update API connector
ResourceManagement	Identity Provider
ResourceManagement	Update B2C directory resource
ResourceManagement	Update CIAM directory resource
ResourceManagement	Update Guest Usages resource
ResourceManagement	Update authentication flows policy
ResourceManagement	Update custom identity provider
ResourceManagement	Update custom policy
ResourceManagement	Update identity provider
ResourceManagement	Update local identity provider
ResourceManagement	Update policy key
ResourceManagement	Update subscription status
ResourceManagement	Update user attribute
ResourceManagement	Update user flow
ResourceManagement	Update certificate to policy key
ResourceManagement	Update secret into policy key
ResourceManagement	Validate move resources
UserManagement	Add Windows Hello for Business credential
UserManagement	Add passwordless phone sign-in credential
UserManagement	Delete Windows Hello for Business credential
UserManagement	Delete passwordless phone sign-in credential

Conditional Access

Use these logs to see when changes were made to your Conditional Access policies.

⌞⌝ Expand table

Audit Category	Activity
Policy	Add AuthenticationContextClassReference
Policy	Add Conditional Access policy
Policy	Add named location
Policy	Delete AuthenticationContextClassReference
Policy	Delete Conditional Access policy
Policy	Delete named location
Policy	Update AuthenticationContextClassReference
Policy	Update Conditional Access policy
Policy	Update continuous access evaluation
Policy	Update named location
Policy	Update security defaults

Core Directory

Logs captured in the Core Directory service cover a wide variety of scenarios. Changes to service principals and applications, updates to company settings, and many other directory related details are captured here. Because so many logs are included in this service, utilize the filter options and date ranges to narrow down the results.

⌞⌝ Expand table

Audit Category	Activity
AdministrativeUnit	Add administrative unit
AdministrativeUnit	Add member to administrative unit
AdministrativeUnit	Add member to restricted management administrative unit
AdministrativeUnit	Delete administrative unit
AdministrativeUnit	Hard Delete administrative unit
AdministrativeUnit	Remove member from administrative unit
AdministrativeUnit	Remove member from restricted management administrative unit
AdministrativeUnit	Restore administrative unit
AdministrativeUnit	Update administrative unit

Agreement	Add agreement
Agreement	Delete agreement
Agreement	Hard delete agreement
Agreement	Update agreement
ApplicationManagement	Add app role assignment to service principal
ApplicationManagement	Add application
ApplicationManagement	Add delegated permission grant
ApplicationManagement	Add owner to application
ApplicationManagement	Add owner to service principal
ApplicationManagement	Add policy to application
ApplicationManagement	Add policy to service principal
ApplicationManagement	Add service principal
ApplicationManagement	Add service principal credentials
ApplicationManagement	Cancel application update with safe rollout
ApplicationManagement	Complete application update after safe rollout
ApplicationManagement	Consent to application
ApplicationManagement	Delete application
ApplicationManagement	Hard Delete application
ApplicationManagement	Hard delete service principal
ApplicationManagement	Remove app role assignment from service principal
ApplicationManagement	Remove delegated permission grant
ApplicationManagement	Remove owner from application
ApplicationManagement	Remove owner from service principal
ApplicationManagement	Remove policy from application
ApplicationManagement	Remove policy from service principal
ApplicationManagement	Remove service principal
ApplicationManagement	Remove service principal credentials
ApplicationManagement	Restore application
ApplicationManagement	Restore service principal
ApplicationManagement	Restore consent
ApplicationManagement	Set verified publisher
ApplicationManagement	Unset verified publisher

ApplicationManagement	Update application
ApplicationManagement	Update application with safe rollout
ApplicationManagement	Update application - Certificates and secrets management
ApplicationManagement	Update external secrets
ApplicationManagement	Update service principal
Authentication	Test audit log
AuthorizationPolicy	Update authorization policy
CertBasedConfiguration	Add CertBasedAuthConfiguration
CertBasedConfiguration	Hard delete CertificationBasedAuthConfiguration
CertificateAuthorityEntity	Create CertificateAuthorityEntity
CertificateAuthorityEntity	Delete CertificateAuthorityEntity
CertificateAuthorityEntity	Hard Delete CertificateAuthorityEntity
CertificateAuthorityEntity	Restore CertificateAuthorityEntity
CertificateAuthorityEntity	Update CertificateAuthorityEntity
CertificateBasedAuthConfiguration	Add CertificateBasedAuthConfiguration
CertificateBasedAuthConfiguration	Delete CertificateBasedAuthConfiguration
CertificateBasedAuthConfiguration	Update CertificateBasedAuthConfiguration
CompanyBranding	Create Branding Theme
CompanyBranding	Delete Branding Theme
CompanyBranding	Hard Delete Branding Theme
CompanyBranding	Update Branding Theme
CompanyBrandingLocale	Create Branding Theme Localization
CompanyBrandingLocale	Delete Branding Theme Localization
CompanyBrandingLocale	Hard Delete Branding Theme Localization
CompanyBrandingLocale	Update Branding Theme Localization
Contact	Add contact
Contact	Delete contact
Contact	Update contact
CrossTenantAccessSettings	Add a domain-based partner to cross-tenant access setting
CrossTenantAccessSettings	Add a partner to cross-tenant access setting
CrossTenantAccessSettings	Delete a domain-based partner to cross-tenant access setting
CrossTenantAccessSettings	Delete partner specific cross-tenant access setting

CrossTenantAccessSettings	Migrated partner cross-tenant access settings to the scalable model
CrossTenantAccessSettings	Reset the cross-tenant access default setting
CrossTenantAccessSettings	Update a domain-based partner to cross-tenant access setting
CrossTenantAccessSettings	Update a partner cross-tenant access setting
CrossTenantAccessSettings	Update the company default cross-tenant access setting
CrossTenantIdentitySyncSettings	Create a partner cross-tenant identity sync setting
CrossTenantIdentitySyncSettings	Delete a partner cross-tenant identity sync setting
CrossTenantIdentitySyncSettings	Update a partner cross-tenant identity sync setting
DelegatedAdminServiceProviderConstraints	Adding allowed assignable roles
DelegatedAdminServiceProviderConstraints	Updating allowed assignable roles
Device	Add device
Device	Add registered owner to device
Device	Add registered users to device
Device	Delete device
Device	Device no longer compliant
Device	Device no longer managed
Device	Hard Delete device
Device	Remove registered owner from device
Device	Remove registered users from device
Device	Restore device
Device	Update device
DeviceConfiguration	Add device configuration
DeviceConfiguration	Delete device configuration
DeviceConfiguration	Update device configuration
DeviceTemplate	Add device from DeviceTemplate
DeviceTemplate	Add DeviceTemplate
DeviceTemplate	Add owner to DeviceTemplate
DeviceTemplate	Delete DeviceTemplate
DirectoryManagement	Add partner to company
DirectoryManagement	Add sharedEmailDomainInvitation
DirectoryManagement	Add unverified domain

DirectoryManagement	Add verified domain
DirectoryManagement	Create Company
DirectoryManagement	Create company settings
DirectoryManagement	Delete company allowed data location
DirectoryManagement	Delete company settings
DirectoryManagement	Delete subscription
DirectoryManagement	Deleting Source Tenant subscriptions
DirectoryManagement	Demote partner
DirectoryManagement	Directory deleted
DirectoryManagement	Directory deleted permanently
DirectoryManagement	Directory scheduled for deletion (Lifecycle)
DirectoryManagement	Directory scheduled for deletion (UserRequest)
DirectoryManagement	Get cross-cloud verification code for domain
DirectoryManagement	Hard Delete Domain
DirectoryManagement	Promote company to partner
DirectoryManagement	Promote sub domain to root domain
DirectoryManagement	Remove partner from company
DirectoryManagement	Remove unverified domain
DirectoryManagement	Remove verified domain
DirectoryManagement	Schedule Add sharedEmailDomain
DirectoryManagement	Schedule Remove sharedEmailDomain
DirectoryManagement	Set Company Information
DirectoryManagement	Set DirSync feature
DirectoryManagement	Set DirSyncEnabled flag
DirectoryManagement	Set Partnership
DirectoryManagement	Set accidental deletion threshold
DirectoryManagement	Set company allowed data location
DirectoryManagement	Set company multinational feature enabled
DirectoryManagement	Set directory feature on tenant
DirectoryManagement	Set domain authentication
DirectoryManagement	Set federation settings on domain
DirectoryManagement	Set password policy

DirectoryManagement	Soft Delete Domain
DirectoryManagement	Suspending Source Tenant Subscriptions
DirectoryManagement	Update Domain
DirectoryManagement	Update company
DirectoryManagement	Update company settings
DirectoryManagement	Update domain
DirectoryManagement	Update sharedEmailDomain
DirectoryManagement	Update sharedEmailDomainInvitation
DirectoryManagement	Verify domain
DirectoryManagement	Verify email verified domain
GroupManagement	Add app role assignment to group
GroupManagement	Add group
GroupManagement	Add member to group
GroupManagement	Add owner to group
GroupManagement	Assign label to group
GroupManagement	Create group settings
GroupManagement	Delete group
GroupManagement	Delete group settings
GroupManagement	Finish applying group based license to user
GroupManagement	Grant contextual consent to application
GroupManagement	Hard Delete group
GroupManagement	Remove app role assignment from group
GroupManagement	Remove eligible member from group
GroupManagement	Remove eligible owner from group
GroupManagement	Remove label from group
GroupManagement	Remove member from group
GroupManagement	Remove owner from group
GroupManagement	Restore group
GroupManagement	Set group license
GroupManagement	Set group to be managed by user
GroupManagement	Start applying group based license to users
GroupManagement	Trigger group license recalculation

GroupManagement	Update group
GroupManagement	Update group settings
KerberosDomain	Add kerberos domain
KerberosDomain	Delete kerberos domain
KerberosDomain	Restore kerberos domain
KerberosDomain	Update kerberos domain
Label	Add label
Label	Delete label
Label	Update label
MicrosoftSupportAccessManagement	Access approved
MicrosoftSupportAccessManagement	Access removed
MicrosoftSupportAccessManagement	Request approved
MicrosoftSupportAccessManagement	Request canceled
MicrosoftSupportAccessManagement	Request created
MicrosoftSupportAccessManagement	Request rejected
MultiTenantOrg	Create a MultiTenantOrg
MultiTenantOrg	Hard Delete MultiTenantOrg
MultiTenantOrg	Update a MultiTenantOrg
MultiTenantOrgIdentitySyncPolicyUpdate	Reset a multi tenant org identity sync policy template
MultiTenantOrgIdentitySyncPolicyUpdate	Update a multi tenant org identity sync policy template
MultiTenantOrgPartnerConfigurationTemplate	Reset a multi tenant org partner configuration template
MultiTenantOrgPartnerConfigurationTemplate	Update a multi tenant org partner configuration template
MultiTenantOrgTenant	Add MultiTenantOrg tenant
MultiTenantOrgTenant	Delete MultiTenantOrg tenant
MultiTenantOrgTenant	Hard Delete MultiTenantOrg tenant
MultiTenantOrgTenant	Tenant joining MultiTenantOrg tenant
MultiTenantOrgTenant	Update MultiTenantOrg tenant
OrganizationalUnitContainer	Create OrganizationalUnit
OrganizationalUnitContainer	Delete OrganizationalUnit
OrganizationalUnitContainer	Update OrganizationalUnit
PendingExternalUserProfile	Create PendingExternalUserProfile
PendingExternalUserProfile	Delete PendingExternalUserProfile

PendingExternalUserProfile	Hard Delete PendingExternalUserProfile
PermissionGrantPolicy	Add permission grant policy
PermissionGrantPolicy	Delete permission grant policy
PermissionGrantPolicy	Update permission grant policy
Policy	Add owner to policy
Policy	Add policy
Policy	Delete policy
Policy	Hard Delete policy
Policy	Remove owner from policy
Policy	Remove policy credentials
Policy	Restore policy
Policy	Update policy
PublicKeyInfrastructure	Create PublicKeyInfrastructure
PublicKeyInfrastructure	Delete PublicKeyInfrastructure
PublicKeyInfrastructure	Hard Delete PublicKeyInfrastructure
PublicKeyInfrastructure	Initiate PublicKeyInfrastructure
PublicKeyInfrastructure	Restore PublicKeyInfrastructure
PublicKeyInfrastructure	Update PublicKeyInfrastructure
RoleManagement	Add EligibleRoleAssignment to RoleDefinition
RoleManagement	Add eligible member to role
RoleManagement	Add member to role
RoleManagement	Add member to role scoped over Restricted Management Administrative Unit
RoleManagement	Add role assignment to role definition
RoleManagement	Add role definition
RoleManagement	Add role from template
RoleManagement	Add scoped member to role
RoleManagement	Delete role definition
RoleManagement	Remove EligibleRoleAssignment from RoleDefinition
RoleManagement	Remove eligible member from role
RoleManagement	Remove member from role
RoleManagement	Remove member from role scoped over Restricted Management Administrative Unit

RoleManagement	Remove role assignment from role definition
RoleManagement	Remove scoped member from role
RoleManagement	Update role
RoleManagement	Update role definition
UserManagement	Add app role assignment to group
UserManagement	Add user
UserManagement	Add user sponsor
UserManagement	Change user license
UserManagement	Change user password
UserManagement	Convert federated user to managed
UserManagement	Create application password for user
UserManagement	Delete application password for user
UserManagement	Delete user
UserManagement	Disable Strong Authentication
UserManagement	Disable account
UserManagement	Enable Strong Authentication
UserManagement	Enable account
UserManagement	Hard Delete user
UserManagement	Remove OrganizationalUnit assigned to a user
UserManagement	Remove app role assignment from user
UserManagement	Remove user sponsor
UserManagement	Reset password
UserManagement	Restore user
UserManagement	Set force change user password
UserManagement	Set user manager
UserManagement	Takeover user cloned
UserManagement	Update OrganizationalUnit assigned to a user
UserManagement	Update StsRefreshTokenValidFrom Timestamp
UserManagement	Update external secrets
UserManagement	Update user

Device Registration Service

If you need to manage Microsoft Entra ID and Microsoft Entra hybrid joined devices, use the logs captured in the Device Registration Service to review changes to devices.

⛶ **Expand table**

Audit Category	Activity
Device	Delete pre-created device
Device	Pre-create device
Device	Recover device local administrator password
Device	Register device
Device	Unregister device
Device	Update local administrator password
KeyManagement	Add BitLocker key
KeyManagement	Delete BitLocker key
KeyManagement	Read BitLocker key
Policy	Set device registration policies
UserManagement	Add Passkey (device-bound)
UserManagement	Add Windows Hello for Business credential
UserManagement	Add passwordless phone sign-in credential
UserManagement	Add platform credential
UserManagement	Delete Passkey (device-bound)
UserManagement	Delete Windows Hello for Business credential
UserManagement	Delete passwordless phone sign-in credential
UserManagement	Delete platform credential

Entitlement Management

Use these logs to monitor changes to Entitlement Management settings. Entitlement Management can be used to streamline how you assign members of Microsoft Entra security groups, grant licenses for Microsoft 365, or provide access to applications. Access reviews and Lifecycle workflows have separate logs.

⛶ **Expand table**

Audit Category	Activity
EntitlementManagement	Add Entitlement Management role assignment
EntitlementManagement	Administrator directly assigns user to access package

EntitlementManagement	Administrator directly removes user access package assignment
EntitlementManagement	Approval stage completed for access package assignment request
EntitlementManagement	Approve access package assignment request
EntitlementManagement	Assign user as external sponsor
EntitlementManagement	Assign user as internal sponsor
EntitlementManagement	Auto approve access package assignment request
EntitlementManagement	Cancel access package assignment request
EntitlementManagement	Create access package
EntitlementManagement	Create access package assignment policy
EntitlementManagement	Create access package assignment user update request
EntitlementManagement	Create access package catalog
EntitlementManagement	Create connected organization
EntitlementManagement	Create custom extension
EntitlementManagement	Create incompatible access package
EntitlementManagement	Create incompatible group
EntitlementManagement	Create resource environment
EntitlementManagement	Create resource remove request
EntitlementManagement	Create resource request
EntitlementManagement	Delete access package
EntitlementManagement	Delete access package assignment policy
EntitlementManagement	Delete access package assignment request
EntitlementManagement	Delete access package assignment policy for a deleted user
EntitlementManagement	Delete access package catalog
EntitlementManagement	Delete connected organization
EntitlementManagement	Delete custom extension
EntitlementManagement	Delete incompatible access package
EntitlementManagement	Delete incompatible group
EntitlementManagement	Deny access package assignment request
EntitlementManagement	Entitlement Management creates access package assignment request for user
EntitlementManagement	Entitlement Management removes access package assignment request for user
EntitlementManagement	Execute custom extension
EntitlementManagement	Extend access package assignment

EntitlementManagement	Failed access package assignment request
EntitlementManagement	Fulfill access package assignment request
EntitlementManagement	Fulfill access package resource assignment
EntitlementManagement	Partially fulfill access package assignment request
EntitlementManagement	Ready to fulfill access package assignment request
EntitlementManagement	Remove Entitlement Management role assignment
EntitlementManagement	Remove access package resource assignment
EntitlementManagement	Remove user as external sponsor
EntitlementManagement	Remove user as internal sponsor
EntitlementManagement	Schedule a future access package assignment
EntitlementManagement	Update access package
EntitlementManagement	Update access package assignment policy
EntitlementManagement	Update access package assignment request
EntitlementManagement	Update access package catalog
EntitlementManagement	Update access package catalog resource
EntitlementManagement	Update connected organization
EntitlementManagement	Update custom extension
EntitlementManagement	Update request answers by approver
EntitlementManagement	Update tenant setting
EntitlementManagement	User requests access package assignment
EntitlementManagement	User requests an access package assignment on behalf of service principal
EntitlementManagement	User requests to extend access package assignment
EntitlementManagement	User requests to remove access package assignment

Global Secure Access

If you're using Microsoft Entra Internet Access or Microsoft Entra Private Access to acquire and secure network traffic to your corporate resources, these logs can help identify when changes were made to your network policies. These logs capture changes to traffic forwarding policies and remote networks, such as branch office locations. For more information, see What is Global Secure Access.

⌧ **Expand table**

Audit Category	Activity
ApplicationManagement	Create Certificate

ApplicationManagement	Delete Certificate
ApplicationManagement	Update Certificate
ObjectManagement	Offboarding Process Started
ObjectManagement	Onboarding Process Started
ObjectManagement	Update Adaptive Access Policy
ObjectManagement	Update Enriched Audit Logs Settings
ObjectManagement	Update Forwarding Options Policy
PolicyManagement	Create Filtering Policy
PolicyManagement	Create Filtering Policy Profile
PolicyManagement	Create Remote Network
PolicyManagement	Create Security Provider Policy
PolicyManagement	Delete Filtering Policy
PolicyManagement	Delete Filtering Policy Profile
PolicyManagement	Delete Forwarding Policy
PolicyManagement	Delete Private Access Policy
PolicyManagement	Delete Remote Network
PolicyManagement	Delete Security Provider Policy
PolicyManagement	Update Filtering Policy
PolicyManagement	Update Filtering Policy Profile
PolicyManagement	Update Filtering Profile
PolicyManagement	Update Forwarding Options Policy
PolicyManagement	Update Forwarding Policy
PolicyManagement	Update Forwarding Profile
PolicyManagement	Update Forwarding Rule
PolicyManagement	Update Private Access Policy
PolicyManagement	Update Remote Network
PolicyManagement	Update Security Provider Policy
ResourceManagement	Create Registration of Security Provider

Hybrid Authentication

⌞⌝ Expand table

Audit Category	Activity
Authentication	Add user to feature rollout
Authentication	Remove user from feature rollout

Microsoft Entra ID Protection (Identity Protection)

⟦ ⟧ **Expand table**

Audit Category	Activity
IdentityProtection	Update IdentityProtectionPolicy
IdentityProtection	Update NotificationSettings
Other	ConfirmAccountCompromised
Other	ConfirmAccountSafe
Other	ConfirmCompromised
Other	ConfirmSafe
Other	DismissRisk
Other	DismissUser
Other	confirmServicePrincipalCompromised
Other	DismissServicePrincipal

Invited users

Use the Invited users logs to help you manage the status of users who were invited to collaborate as guests in your tenant. These logs can help troubleshoot issues with invitations sent to external users.

⟦ ⟧ **Expand table**

Audit Category	Activity
UserManagement	Delete external user
UserManagement	Email not sent, user unsubscribed
UserManagement	Invitation Email
UserManagement	Invite external user
UserManagement	Invite external user with reset invitation status
UserManagement	Invite internal user to B2B collaboration
UserManagement	Redeem external user invite

Lifecycle Workflows

Lifecycle Workflows(preview) are a great way to automate identity related processes for joiners, movers, and leavers so you don't have to. For more information, see Lifecycle Workflows audits.

⬚ Expand table

Audit Category	Activity
Other	Create custom task extension
Other	Delete custom task extension
Other	Update custom task extension
TaskManagement	Add task to workflow
TaskManagement	Disable task
TaskManagement	Enable task
TaskManagement	Remove task from workflow
TaskManagement	Update task
WorkflowManagement	Add execution conditions
WorkflowManagement	Add workflow version
WorkflowManagement	Create workflow
WorkflowManagement	Delete workflow
WorkflowManagement	Disable workflow
WorkflowManagement	Disable workflow schedule
WorkflowManagement	Enable workflow
WorkflowManagement	Enable workflow schedule
WorkflowManagement	Hard delete workflow
WorkflowManagement	On-demand workflow execution completed
WorkflowManagement	Restore workflow
WorkflowManagement	Schedule workflow execution completed
WorkflowManagement	Schedule workflow execution started
WorkflowManagement	Set workflow for on-demand execution
WorkflowManagement	Update execution conditions
WorkflowManagement	Update tenant settings
WorkflowManagement	Update workflow

Microsoft Identity Manager (MIM) Service

If you're using MIM to automate identity and group provisioning based on business policy and workflow, these audit logs can help track when change were made to groups and members through the MIM service.

⟦ ⟧ Expand table

Audit Category	Activity
GroupManagement	Add group
GroupManagement	Add member to group
GroupManagement	Add owner to group
GroupManagement	Delete group
GroupManagement	Remove member from group
GroupManagement	Remove owner from group
GroupManagement	Update group
UserManagement	User Password Registration
UserManagement	User Password Reset

Mobility Management

⟦ ⟧ Expand table

Audit Category	Activity
Authentication	User confirmed unusual sign-in event as legitimate
Authentication	User reported unusual sign-in event as not legitimate
UserManagement	User changed default security info
UserManagement	User deleted security info
UserManagement	User registered security info
UserManagement	User started security info registration

MyAccess

⟦ ⟧ Expand table

Audit Category	Activity
ApplicationManagement	Create application collection

MyApps

Use the MyApps audit logs to identify when an application was added to a collection for your
MyApp portal.

⊡ Expand table

Audit Category	Activity
ApplicationManagement	Create application collection
ApplicationManagement	Delete application collection
ApplicationManagement	Update application collection
ApplicationManagement	Update application collection order
ApplicationManagement	Update preview settings

Privileged Identity Management (PIM)

Many of the activities captured in the PIM audit logs are similar, so take note of details like *renew*,
timebound, and *permanent*. PIM activities can generate many logs in a 24 hour period, so utilize the
filters to narrow things down. For more information on the audit capabilities within the PIM service,
see View audit history for Microsoft Entra roles in PIM.

⊡ Expand table

Audit Category	Activity
ApplicationManagement	Add member to role approval requested (PIM activation)
ApplicationManagement	Add member to role in PIM completed (timebound)
ApplicationManagement	Add member to role in PIM requested (timebound)
ApplicationManagement	Approve request - direct role assignment
ApplicationManagement	PIM activation request expired
ApplicationManagement	PIM policy removed
ApplicationManagement	Remove member from role in PIM completed (timebound)
ApplicationManagement	Remove request
ApplicationManagement	Role definition created
ApplicationManagement	Update role setting in PIM
GroupManagement	Add eligible member to role in PIM canceled (renew)
GroupManagement	Add eligible member to role in PIM canceled (timebound)
GroupManagement	Add eligible member to role in PIM completed (permanent)
GroupManagement	Add eligible member to role in PIM completed (timebound)

GroupManagement	Add eligible member to role in PIM requested (permanent)
GroupManagement	Add eligible member to role in PIM requested (renew)
GroupManagement	Add eligible member to role in PIM requested (timebound)
GroupManagement	Add member to role approval requested (PIM activation)
GroupManagement	Add member to role canceled (PIM activation)
GroupManagement	Add member to role completed (PIM activation)
GroupManagement	Add member to role in PIM canceled (permanent)
GroupManagement	Add member to role in PIM canceled (renew)
GroupManagement	Add member to role in PIM canceled (timebound)
GroupManagement	Add member to role in PIM completed (permanent)
GroupManagement	Add member to role in PIM completed (timebound)
GroupManagement	Add member to role in PIM requested (permanent)
GroupManagement	Add member to role in PIM requested (renew)
GroupManagement	Add member to role in PIM requested (timebound)
GroupManagement	Add member to role request approved (PIM activation)
GroupManagement	Add member to role request denied (PIM activation)
GroupManagement	Add member to role requested (PIM activation)
GroupManagement	Cancel request
GroupManagement	Cancel request for role removal
GroupManagement	Cancel request for role update
GroupManagement	Offboarded resource from PIM
GroupManagement	Onboarded resource to PIM
GroupManagement	PIM activation request expired
GroupManagement	PIM policy removed
GroupManagement	Process request
GroupManagement	Process role removal request
GroupManagement	Remove eligible member from role in PIM completed (permanent)
GroupManagement	Remove eligible member from role in PIM completed (timebound)
GroupManagement	Remove eligible member from role in PIM requested (permanent)
GroupManagement	Remove eligible member from role in PIM requested (timebound)
GroupManagement	Remove member from role (PIM activation expired)
GroupManagement	Remove member from role completed (PIM deactivate)

GroupManagement	Remove member from role in PIM completed (permanent)
GroupManagement	Remove member from role in PIM completed (timebound)
GroupManagement	Remove member from role in PIM requested (permanent)
GroupManagement	Remove member from role in PIM requested (timebound)
GroupManagement	Remove member from role requested (PIM deactivate)
GroupManagement	Remove permanent direct role assignment
GroupManagement	Remove permanent eligible role assignment
GroupManagement	Remove request
GroupManagement	Resource updated
GroupManagement	Restore eligible member from role in PIM completed
GroupManagement	Restore member from role
GroupManagement	Restore member from role in PIM completed
GroupManagement	Restore permanent direct role assignment
GroupManagement	Update eligible member in PIM canceled (extend)
GroupManagement	Update eligible member in PIM requested (extend)
GroupManagement	Update member in PIM approved by admin (extend/renew)
GroupManagement	Update member in PIM canceled (extend)
GroupManagement	Update member in PIM denied by admin (extend/renew)
GroupManagement	Update member in PIM requested (extend)
GroupManagement	Update role setting in PIM
ResourceManagement	Add eligible member to role in PIM canceled (permanent)
ResourceManagement	Add eligible member to role in PIM canceled (renew)
ResourceManagement	Add eligible member to role in PIM canceled (timebound)
ResourceManagement	Add eligible member to role in PIM completed (permanent)
ResourceManagement	Add eligible member to role in PIM completed (timebound)
ResourceManagement	Add eligible member to role in PIM requested (permanent)
ResourceManagement	Add eligible member to role in PIM requested (renew)
ResourceManagement	Add eligible member to role in PIM requested (timebound)
ResourceManagement	Add member to role approval requested (PIM activation)
ResourceManagement	Add member to role canceled (PIM activation)
ResourceManagement	Add member to role completed (PIM activation)
ResourceManagement	Add member to role in PIM canceled (renew)

ResourceManagement	Add member to role in PIM canceled (timebound)
ResourceManagement	Add member to role in PIM completed (permanent)
ResourceManagement	Add member to role in PIM completed (timebound)
ResourceManagement	Add member to role in PIM requested (permanent)
ResourceManagement	Add member to role in PIM requested (renew)
ResourceManagement	Add member to role in PIM requested (timebound)
ResourceManagement	Add member to role outside of PIM (permanent)
ResourceManagement	Add member to role request approved (PIM activation)
ResourceManagement	Add member to role request denied (PIM activation)
ResourceManagement	Add member to role requested (PIM activation)
ResourceManagement	Cancel request
ResourceManagement	Cancel request for role removal
ResourceManagement	Cancel request for role update
ResourceManagement	Deactivate PIM alert
ResourceManagement	Disable PIM alert
ResourceManagement	Enable PIM alert
ResourceManagement	Offboarded resource from PIM
ResourceManagement	Onboarded resource from PIM
ResourceManagement	PIM activation request expired
ResourceManagement	PIM policy removed
ResourceManagement	Process request
ResourceManagement	Process role removal request
ResourceManagement	Process role update request
ResourceManagement	Remove eligible member from role in PIM completed (permanent)
ResourceManagement	Remove eligible member from role in PIM completed (timebound)
ResourceManagement	Remove eligible member from role in PIM requested (permanent)
ResourceManagement	Remove eligible member from role in PIM requested (timebound)
ResourceManagement	Remove member from role (PIM activation expired)
ResourceManagement	Remove member from role completed (PIM deactivate)
ResourceManagement	Remove member from role in PIM completed (permanent)
ResourceManagement	Remove member from role in PIM completed (timebound)
ResourceManagement	Remove member from role in PIM requested (permanent)

ResourceManagement	Remove member from role in PIM requested (timebound)
ResourceManagement	Remove member from role requested (PIM deactivate)
ResourceManagement	Remove permanent direct role assignment
ResourceManagement	Remove permanent eligible role assignment
ResourceManagement	Remove request
ResourceManagement	Resolve PIM alert
ResourceManagement	Resource updated
ResourceManagement	Restore eligible member from role in PIM completed
ResourceManagement	Restore member from role
ResourceManagement	Restore member from role in PIM completed
ResourceManagement	Restore permanent direct role assignment
ResourceManagement	Restore permanent eligible role assignment
ResourceManagement	Tenant offboarded from PIM
ResourceManagement	Triggered PIM alert
ResourceManagement	Update eligible member in PIM canceled (extend)
ResourceManagement	Update eligible member in PIM requested (extend)
ResourceManagement	Update member in PIM approved by admin (extend/renew)
ResourceManagement	Update member in PIM canceled (extend)
ResourceManagement	Update member in PIM denied by admin (extend/renew)
ResourceManagement	Update member in PIM requested (extend)
ResourceManagement	Update role setting in PIM
RoleManagement	Add eligible member to role in PIM canceled (permanent)
RoleManagement	Add eligible member to role in PIM canceled (renew)
RoleManagement	Add eligible member to role in PIM canceled (timebound)
RoleManagement	Add eligible member to role in PIM completed (permanent)
RoleManagement	Add eligible member to role in PIM completed (timebound)
RoleManagement	Add eligible member to role in PIM requested (permanent)
RoleManagement	Add eligible member to role in PIM requested (renew)
RoleManagement	Add eligible member to role in PIM requested (timebound)
RoleManagement	Add member to role approval requested (PIM activation)
RoleManagement	Add member to role canceled (PIM activation)
RoleManagement	Add member to role completed (PIM activation)

RoleManagement	Add member to role in PIM canceled (renew)
RoleManagement	Add member to role in PIM canceled (timebound)
RoleManagement	Add member to role in PIM completed (permanent)
RoleManagement	Add member to role in PIM completed (timebound)
RoleManagement	Add member to role in PIM requested (permanent)
RoleManagement	Add member to role in PIM requested (renew)
RoleManagement	Add member to role in PIM requested (timebound)
RoleManagement	Add member to role outside of PIM (permanent)
RoleManagement	Add member to role request approved (PIM activation)
RoleManagement	Add member to role request denied (PIM activation)
RoleManagement	Add member to role requested (PIM activation)
RoleManagement	Cancel request for role removal
RoleManagement	Cancel request for role update
RoleManagement	Deactivate PIM alert
RoleManagement	Disable PIM alert
RoleManagement	Enable PIM alert
RoleManagement	Offboarded resource from PIM
RoleManagement	Onboarded resource from PIM
RoleManagement	PIM activation request expired
RoleManagement	PIM policy removed
RoleManagement	Process request
RoleManagement	Process role removal request
RoleManagement	Process role update request
RoleManagement	Refresh PIM alert
RoleManagement	Remove eligible member from role in PIM completed (permanent)
RoleManagement	Remove eligible member from role in PIM completed (timebound)
RoleManagement	Remove eligible member from role in PIM requested (permanent)
RoleManagement	Remove eligible member from role in PIM requested (timebound)
RoleManagement	Remove member from role (PIM activation expired)
RoleManagement	Remove member from role completed (PIM deactivate)
RoleManagement	Remove member from role in PIM completed (permanent)
RoleManagement	Remove member from role in PIM completed (timebound)

RoleManagement	Remove member from role in PIM requested (permanent)
RoleManagement	Remove member from role in PIM requested (timebound)
RoleManagement	Remove member from role requested (PIM deactivate)
RoleManagement	Remove permanent direct role assignment
RoleManagement	Remove permanent eligible role assignment
RoleManagement	Remove request
RoleManagement	Resolve PIM alert
RoleManagement	Restore eligible member from role in PIM completed
RoleManagement	Restore member from role
RoleManagement	Restore member from role in PIM completed
RoleManagement	Restore permanent direct role assignment
RoleManagement	Restore permanent eligible role assignment
RoleManagement	Tenant offboarded from PIM
RoleManagement	Triggered PIM alert
RoleManagement	Update PIM alert setting
RoleManagement	Update eligible member in PIM canceled (extend)
RoleManagement	Update eligible member in PIM requested (extend)
RoleManagement	Update member in PIM approved by admin (extend/renew)
RoleManagement	Update member in PIM canceled (extend)
RoleManagement	Update member in PIM denied by admin (extend/renew)
RoleManagement	Update member in PIM requested (extend)
RoleManagement	Update role setting in PIM

Self-service group management

Users in your tenant can manage many aspects of their group memberships on their own. Use the Self-service group management logs to help troubleshoot issues with these scenarios.

Many of the activities in this group are associated with background processes related to a user's activity. For example, you might see multiple `Features_GetFeaturesAsync` instances in your logs when a user accesses the MyApps or MyGroups portal. This activity doesn't indicate if the user made any changes. Other activities such as `GroupsODataV4_Get` often occur in groups for similar user actions.

⌄⌄ **Expand table**

Audit Category	Activity

GroupManagement	ApprovalNotification_Create
GroupManagement	Approval_Act
GroupManagement	Approval_Get
GroupManagement	Approval_GetAll
GroupManagement	Approvals_Post
GroupManagement	Approve a pending request to join a group
GroupManagement	Cancel a pending request to join a group
GroupManagement	Create lifecycle management policy
GroupManagement	Delete a pending request to join a group
GroupManagement	Delete lifecycle management policy
GroupManagement	Device_Create
GroupManagement	Device_Delete
GroupManagement	Device_Get
GroupManagement	Device_GetAll
GroupManagement	Features_GetFeaturesAsync
GroupManagement	Features_IsFeatureEnabledAsync
GroupManagement	Features_UpdateFeaturesAsync
GroupManagement	GroupLifecyclePolicies_Get
GroupManagement	GroupLifecyclePolicies_addGroup
GroupManagement	GroupLifecyclePolicies_removeGroup
GroupManagement	Group_AddMember
GroupManagement	Group_AddOwner
GroupManagement	Group_BatchValidateDynamicMembership
GroupManagement	Group_Create
GroupManagement	Group_Delete
GroupManagement	Group_Get
GroupManagement	Group_GetAll
GroupManagement	Group_GetDynamicGroupProperties
GroupManagement	Group_GetDynamicMembershipDeviceAttributes
GroupManagement	Group_GetDynamicMembershipOperators
GroupManagement	Group_GetDynamicMembershipUserBaseAttributes
GroupManagement	Group_GetExpiryNotificationDate

GroupManagement	Group_GetMembers
GroupManagement	Group_GetOwners
GroupManagement	Group_RemoveMember
GroupManagement	Group_RemoveOwner
GroupManagement	Group_Restore
GroupManagement	Group_Update
GroupManagement	Group_ValidateDynamicMembership
GroupManagement	GroupsODataV4_Get
GroupManagement	GroupsODataV4_GetgroupLifecyclePolicies
GroupManagement	GroupsODataV4_evaluateDynamicMembership
GroupManagement	Groups_CreateLink
GroupManagement	Groups_Get
GroupManagement	LcmPolicy_Get
GroupManagement	LcmPolicy_RenewGroup
GroupManagement	Reject a pending request to join a group
GroupManagement	Renew group
GroupManagement	Request to join a group
GroupManagement	set dynamic group properties
GroupManagement	Settings_GetSettingsAsync
GroupManagement	Update lifecycle management policy
GroupManagement	User_Create
GroupManagement	User_Delete
GroupManagement	User_Get
GroupManagement	User_GetAll
GroupManagement	User_GetMemberOf
GroupManagement	User_GetOwnedObjects
Other	ApprovalNotification_Create
UserManagement	Updated ConvergedUXV2 feature value
UserManagement	Updated MyApps feature value
UserManagement	Update MyStaff feature value
UserManagement	Updated SSPRConvergence feature value
UserManagement	Updated SignInReports feature value

Self-service password management

The Self-service password management logs provide insight into changes made to passwords by users and admins or when users register for self-service password reset.

⟦ ⟧ Expand table

Audit Category	Activity
DirectoryManagement	Disable password writeback for directory
DirectoryManagement	Enable password writeback for directory
UserManagement	Blocked from self-service password reset
UserManagement	Change password (self-service)
UserManagement	Reset password (by admin)
UserManagement	Reset password (self-service)
UserManagement	Security info saved for self-service password reset
UserManagement	Self-service password reset flow activity progress
UserManagement	Unlock user account (self-service)

Terms of use

⟦ ⟧ Expand table

Audit Category	Activity
Policy	Accept Terms Of Use
Policy	Create Terms Of Use
Policy	Decline Terms Of Use
Policy	Delete Consent
Policy	Delete Terms Of Use
Policy	Edit Terms Of Use
Policy	Publish Terms Of Use

Verified ID

⟦ ⟧ Expand table

Audit Category	Activity
ResourceManagement	Create authority

ResourceManagement	Create authorization policy
ResourceManagement	Create contract
ResourceManagement	Create issuance policy
ResourceManagement	Delete issuance policy
ResourceManagement	Process POST /authorities/:issuerId/didInfo/signingKeys/rotate request
ResourceManagement	Process POST /authorities/:issuerId/didInfo/signingKeys/synchronizeWithDidDocument request
ResourceManagement	Revoke credential
ResourceManagement	Rotate signing key
ResourceManagement	Tenant onboarding
ResourceManagement	Tenant opt-out
ResourceManagement	Update MyAccount settings
ResourceManagement	Update authority
ResourceManagement	Update contract
ResourceManagement	Update issuance policy
ResourceManagement	Update linked domains

Next steps

- Microsoft Entra monitoring and health overview.
- Audit logs report
- Programmatic access to Microsoft Entra reports

Feedback

Was this page helpful? 👍 Yes   👎 No

Provide product feedback ⧉