

libro de Azure AD

Daniel Wood

Administrador de programa

Seguridad de identidad Azure AD

18 de febrero de 2021

Serie de videos sobre Solorigate

La importancia de usar el libro de Azure AD para ayudar a ver patrones de ataques comunes

- 01.** Cómo tener acceso al libro de Azure AD
- 02.** Parte 1: Aplicación, credenciales de servicio y métodos de autenticación modificados
- 03.** Parte 2: Configuración de federación modificada
- 04.** Parte 3: Nuevos permisos concedidos a las entidades de seguridad
- 05.** Parte 4: Información general de los cambios realizados a las suscripciones a las entidades de seguridad

01.

Inicia sesión en el **portal de Azure**.

02.

Ve a **Azure Active Directory > Supervisión > Libros**

03.

En la sección de Solucionador de problemas, abre el **Informe de operaciones confidenciales**

01.

Aplicación y credenciales de
entidad de seguridad/
métodos de autenticación
modificados

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
 - Sign-ins
 - Audit logs
 - Provisioning logs (Preview)
 - Logs
 - Diagnostic settings
- Workbooks
- Usage & insights
- Troubleshooting + Support
 - Virtual assistant (Preview)
 - New support request

Workbooks

Edit

Modified Application and Service Principal Credentials/Authentication Methods

Applications and service principals can have multiple authentication methods that are simultaneously valid. It's important to monitor updates to your service principal authentication methods in case bad actors are adding new rogue credentials to allow themselves to authenticate as that service principal.

TimeRange: Last 60 days

Operation name: All

Credential: All

Actor: All

Exclude actor: None

Number of application and service principals updated by authentication method (Last 60 days)

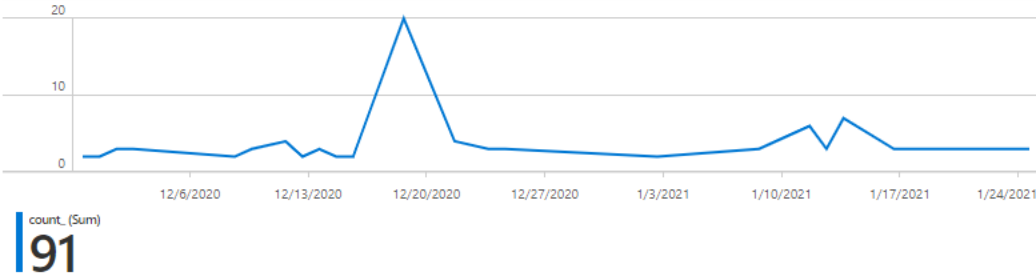


Top actors updating authentication methods (Last 60 days)

Search

Actor	Actor_Type	ServicePrincipalsChanged
Managed Service Identity	App	12
jeffs@woodgrove.ms	User	3
joeyc@woodgrove.ms	User	3
Azure AD Application Proxy	App	2
Domain Controller Services	App	1
Azure ESTS Service	App	1

Updates to service principal authentication methods over time



Recent updates to application/service principal authentication methods

Search

TimeGenerated	OperationName	Actor	Actor_Type	Service_Principal_Name	credential	Service_Principal_ID
1/25/2021, 2:03:34 AM	Add service principal credentials	Managed Service Identity	App	woodgrovechecklist	Other/not logged	1af2f52c-f74f-4a86-8eec-d
1/25/2021, 2:03:34 AM	Add service principal credentials	Managed Service Identity	App	woodgrovechecklist	AsymmetricX509Cert	1af2f52c-f74f-4a86-8eec-d
1/25/2021, 2:03:34 AM	Add service principal credentials	Managed Service Identity	App	woodgrovechecklist	Other/not logged	1af2f52c-f74f-4a86-8eec-d
1/24/2021, 1:03:46 PM	Add service principal credentials	Managed Service Identity	App	woodgrove-app	Other/not logged	dcfce8f2-17b4-4139-8d97-

01.

Aplicación, credenciales de servicio y métodos de autenticación modificados

Todas las nuevas credenciales agregadas a las aplicaciones y entidades de seguridad, incluido el tipo de credenciales

Principales actores y cantidad de modificaciones de credenciales que han realizado

Escala de tiempo para todos los cambios de credenciales

02.

Configuración de federación modificada

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights
- Troubleshooting + Support
- Virtual assistant (Preview)
- New support request

Workbooks

Edit

- Modified application and service principal credentials/authentication methods
- New permissions granted to service principals
- Directory role and group membership updates to service principals

Modified federation settings

Modified federation settings

This section monitors when a user or application modifies the federation settings on the domain. For example, this alert will trigger when a new Active Directory Federated Service (ADFS) TrustedRealm object, such as a signing certificate, is added to the domain. Modification to domain federation settings should be rare. Confirm the added or modified target domain/URL is legitimate administrator behavior.

- To understand why an authorized user may update settings for a federated domain in Office 365, Azure, or Intune, see: <https://docs.microsoft.com/office365/troubleshoot/active-directory/update-federated-domain-office-365>.
- For details on security realms that accept security tokens, see the ADFS Proxy Protocol (MS-ADFSPP) specification: https://docs.microsoft.com/openspecs/windows_protocols/ms-adfspp/e7b9ea73-1980-4318-96a6-da559486664b.

TimeRange: Last 60 days

Operation: All

InitiatingUserOrApp: All

TimeGenerated	OperationName	InitiatingUserOrApp	AADOperationType	targetDisplayName	TargetResources	Result	UserAgent
12/18/2020, 8:59:57 PM	Set federation settings on domain	jeffs@woodgrove.ms	Update	woodgrove.net	[{"displayName":"woodgrove.net","administrativeUnits":[],...	success	
12/7/2020, 3:37:54 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10.0.17134.0)
12/7/2020, 3:12:05 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10.0.17134.0)
12/7/2020, 3:11:40 PM	Add unverified domain	joeyc@woodgrove.ms	Add	pre2.woodgrove.ms	[{"displayName":"pre2.woodgrove.ms","administrativeUnits":...	success	Mozilla/5.0 (Windows NT 10.0.17134.0)
12/7/2020, 3:10:58 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10.0.17134.0)

02.

Configuración de federación modificada

Los cambios realizados a confianzas de federación de dominios

Adición de nuevos dominios y confianzas



03.

Nuevos permisos
concedidos a las
entidades de seguridad

Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
 - Sign-ins
 - Audit logs
 - Provisioning logs (Preview)
 - Logs
 - Diagnostic settings
 - Workbooks
 - Usage & insights
- Troubleshooting + Support
 - Virtual assistant (Preview)
 - New support request

Workbooks

Edit

New permissions granted to service principals

This section monitors for changes to OAuth 2.0 permissions granted to Service Principals. For example, this alert will trigger when a Service Principal is granted Application (AppOnly) permissions to read mail through the Microsoft Graph API. When this occurs, the Service Principal is added to an App Role with a value of Mail.Read.

An attacker could elevate their privileges by using a compromised account to grant new permissions to a Service Principal they control, or by tricking a user into granting permissions. Investigations should focus on high privilege permissions that either grant access to sensitive data, or represent opportunities for lateral movement by attackers.

The first view in this section focuses specifically on Application permissions, which generally (but not always) represent higher risk. The second view is broader- it includes Delegated (App+User) permissions grants and additional audit events.

TimeRange: Last 60 days

ClientApp: All

Resource: All

New Application (AppOnly) permissions added to service principals

Search

Resource	↑↓	ClientApp	↑↓	Role_Added	↑↓	Explanation	↑↓	InitiatingUserOrApp	↑↓	TimeGenerated	↑↓
Office 365 Exchange Online (4)											
JeffTestCreds2" (4)											
Microsoft Graph (4)											
JeffTestCreds2" (3)											
		JeffTestCreds2"		Application.Read.All"		"Read all applications"		jeffs@woodgrove.ms		12/20/2020, 1:54:46 PM	
		JeffTestCreds2"		"Mail.Send"		"Send mail as any user"		jeffs@woodgrove.ms		12/22/2020, 11:56:24 AM	
		JeffTestCreds2"		"Mail.ReadWrite"		"Read and write mail in all mailboxes"		jeffs@woodgrove.ms		12/22/2020, 11:56:24 AM	
Mimorony AuthTS API" (1)											
Office 365 SharePoint Online (1)											
JeffTestCreds2" (1)											

TimeRange: Last 48 hours

Operation: All

InitiatingUserOrApp: All

Recent app permissions activity

TimeGenerated	↑↓	InitiatingUserOrApp	↑↓	OperationName	↑↓	ClientApp	↑↓	Resource	↑↓	Result	↑↓
1/26/2021, 4:25:23 PM		jerryw@woodgrove.ms		Consent to application		CCE Test		Not logged		success	

04.

Información general de los cambios realizados a las suscripciones a las entidades de seguridad

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
 - Sign-ins
 - Audit logs
 - Provisioning logs (Preview)
 - Logs
 - Diagnostic settings
 - Workbooks
 - Usage & insights
- Troubleshooting + Support
 - Virtual assistant (Preview)
 - New support request

Workbooks

Edit

Sensitive Operations Report - Apps, Service Principals and Federation Settings

Workspace: All

This workbook is intended to help identify suspicious application and service principal activity that may indicate compromises in your environment. [Learn more](#) about best practices to protect M365 from attacks.

- Modified application and service principal credentials/authentication methods
- New permissions granted to service principals

Directory role and group membership updates to service principals

Directory role and group membership updates to service principals

This section monitors for Service Principals being as members of Directory Roles (admin roles) or Groups. For example, this alert will trigger when a Service Principal is added to the Company Administrator or Application Administrator role.

An attacker could elevate their privileges by adding a Service Principal they control to a high privileged role or a group that is used to protect access to sensitive resources. Investigations should focus on administrator rules and Groups that either grant access to sensitive data or represent opportunities for lateral movement by attackers.

TimeRange: Last 60 days

Operation: Add member to role

InitiatingUserOrApp: All

TimeGenerated	InitiatingUserOrApp	ServicePrincipalDisplayName	GroupOrRoleNameAddedTo
12/22/2020, 11:49:13 AM	jeffs@woodgrove.com	JeffTestCreds2	"Application Administrator"
12/22/2020, 11:52:28 AM	jeffs@woodgrove.com	Risky App	"Global Administrator"
12/20/2020, 7:46:25 PM	jeffs@woodgrove.com	JeffTestCreds2	"Security Operator"

Select

☐ All

☒ Add member to role

☐ Add eligible member to role

☐ Add scoped member to role

☐ Add member to group

Modified federation settings

Siguientes pasos

01 Ve el Solorigate Serie de videos en esta ubicación

02 Visita Seguridad de Microsoft para ver más actualizaciones:

**[www.microsoft.com/es-mx/
security/business](https://www.microsoft.com/es-mx/security/business)**

03 Lee las publicaciones del blog en:

www.microsoft.com/security/blog/

<https://aka.ms/solorigate>

