



Azure AD 工作簿

Daniel Wood

项目经理

Azure AD Identity 安全性

2021 年 2 月 18 日

使用 Azure AD 工作簿帮助了解常见攻击模式的重要性

01. 如何访问 Azure AD 工作簿
02. 第 1 部分：修改后的应用程序和服务凭据以及身份验证方法
03. 第 2 部分：修改后的联合身份验证设置
04. 第 3 部分：授予服务主体的新权限
05. 第 4 部分：对服务主体成员资格所做更改的概述

01.

登录到 **Azure**
门户。

02.

导航到“**Azure Active**
Directory”>“**监视**”>
“**工作簿**”

03.

在“**疑难解答**”部分中，
打开“**敏感操作报表**”

01.

修改后的应用程序和 服务主体凭据/身份 验证方法

- 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)

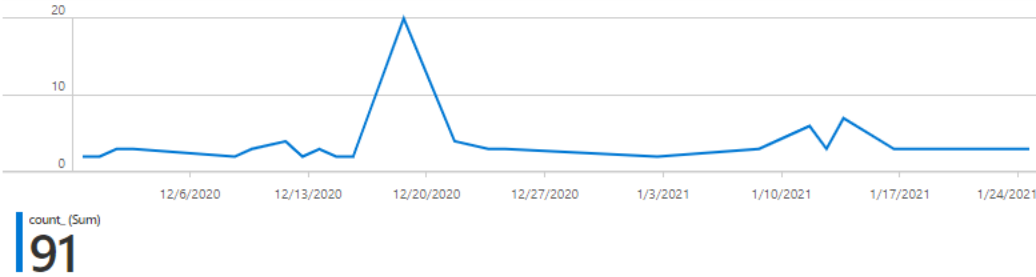


Top actors updating authentication methods (Last 60 days)

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.

修改后的应用程序和服务凭据以及身份验证方法

添加到应用程序和服务主体的所有新凭据，包括凭据类型

最佳行动者及其执行的凭据修改数量

所有凭据更改的时间线

02.

修改后的联合身份验证设置

- 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...
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...
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...
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...

02.

修改后的联合身份验证设置

对现有域联合身份验证信任执行的更改

添加新的域和信任

03.

授予服务主体的新权限

- 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.

对服务主体成员资格所做 更改的概述

- 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 Refresh Undo Redo Help

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

Select

All

Add member to role

Add eligible member to role

Add scoped member to role

Add member to group

TimeGenerated	InitiatingUser	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"

Modified federation settings

Solorigate 概述

后续步骤

- 01 在此位置观看 Solorigate 视频系列
- 02 请访问 Microsoft 安全以获取更多更新：
www.microsoft.com/en-us/security/business
- 03 阅读博客文章：
www.microsoft.com/security/blog/

<https://aka.ms/solorigate>

