

## Sổ làm việc Azure AD

### **Daniel Wood**

Người quản lý Chương trình

Bảo mật Danh tính Azure AD

18/02/2021

### Tầm quan trọng của việc sử dụng Sổ làm việc Azure AD để giúp phát hiện các kiểu tấn công phổ biến

## **01.** Cách truy nhập Sổ làm việc Azure AD

- **02.** Phần 1: Sửa đổi thông tin xác thực và phương pháp xác thực của ứng dụng và dịch vụ
- **03.** Phần 2: Sửa đổi các cài đặt liên kết
- **04.** Phần 3: Cấp những quyền mới cho tên chính của dịch vụ
- **05.** Phần 4: Tổng quan về những thay đổi được thực hiện cho tư cách thành viên tên chính của dịch vụ



Đăng nhập vào Cổng thông tin Microsoft Azure.



Dẫn hướng đến Azure Active Directory > Giám sát > Sổ làm việc



Trong mục Khắc phục sự cố, mở **Báo cáo hoạt động nhạy cảm** 



### Sửa đổi thông tin xác thực/phương pháp xác thực của ứng dụng và tên chính của dịch vụ

		E 다 Ф ? 😳 dawoo@woodgrove.ms 🥌 woodgrove							
Home > Woodgrove									
Woodgrove   Workboo	oks   Sensitive Operations Report 🛷	×							
«	🞽 Workbooks 🖉 Edit 🔚 🕐 👶 🖈 😳								
External Identities	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.								
and administrators 🕹									
Administrative units									
Enterprise applications									
Devices	TimeRange: Last 60 days 🗸 Operation name: All 🗸 Credential: All 🗸 Actor: All 🗸 Exclude actor: No	one Y							
App registrations									
Identity Governance	Number of application and service principals updated by authentication method (Last 60 days)								
Application proxy	AsymmetricX509Cert Other/not logged Password X509CertAndPassword	d							
🔓 Licenses	15 23 6 1								
🔶 Azure AD Connect									
루 Custom domain names									
Ø Mobility (MDM and MAM)	Top actors undating authentication methods (Last 60 days)	Undates to service principal authentication methods over time							
📍 Password reset		20							
Company branding	>> Search								
🖏 User settings	Actor ↑↓ Actor_Type ↑↓ ServicePrincipalsChanged ↑↓	10							
Properties	Managed Service Identity App 12								
Security	jeffs@woodgrove.ms User 3								
Monitoring	joeyc@woodgrove.ms User 3	12/6/2020 12/13/2020 12/20/2020 12/27/2020 1/3/2021 1/10/2021 1/17/2021 1/24/2021 count_ (Sum)							
Sign-ins	Azure AD Application Proxy App 2	91							
Audit logs	Domain Controller Services App 1								
Provisioning logs (Preview)	Azure ESTS Service App 1	•							
Loas	Recent updates to application/service principal authentication methods								
<ul> <li>Diagnostic settings</li> </ul>									
Workbooks	2 Search								
🙀 Usage & insights	TimeGenerated $\uparrow \downarrow$ OperationName $\uparrow \downarrow$ Actor	$\uparrow_{\downarrow} Actor_Type \uparrow_{\downarrow} Service_Principal_Name \qquad \uparrow_{\downarrow} credential \qquad \uparrow_{\downarrow} Service_Principal_ID$							
	1/25/2021, 2:03:34 AM Add service principal credentials Managed Service Identity	App woodgrovechecklist Other/not logged 1af2f52c-f74f-4a86-8eec-d							
Iroubleshooting + Support	1/25/2021, 2:03:34 AM Add service principal credentials Managed Service Identity	App woodgrovechecklist AsymmetricX509Cert 1af2f52c-f74f-4a86-8eec-d							
Virtual assistant (Preview)	1/25/2021, 2:03:34 AM Add service principal credentials Managed Service Identity	App woodgrovechecklist Other/not logged 1af2f52c-f74f-4a86-8eec-d							
New support request	1/24/2021, 1:03:46 PM Add service principal credentials Managed Service Identity	App woodgrove-app Other/not logged dcbce8f2-17b4-4139-8d97-							



### Sửa đổi thông tin xác thực và phương pháp xác thực của ứng dụng và dịch vụ

Thêm thông tin xác thực hoàn toàn mới vào các ứng dụng và tên chính của dịch vụ, bao gồm cả loại thông tin xác thực

Những kẻ tấn công hàng đầu và số lượt sửa đổi thông tin xác thực chúng đã thực hiện

Đường thời gian cho tất cả các thay đổi thông tin xác thực



### Sửa đổi các cài đặt liên kết

WOODGROVE

 $\times$ 

Home > Woodgrove

#### Woodgrove | Workbooks | Sensitive Operations Report 🛷

Azure Active Directory

_		
<b>1</b> 0	External	Identitie

Devices

🔓 Licenses

Roles and administrators Administrative units

Enterprise applications

App registrations

Identity Governance

Application proxy

Azure AD Connect

Password reset

Company branding 🐯 User settings Properties Security Monitoring Sign-ins Audit logs

Custom domain names

Mobility (MDM and MAM)

🞽 Workbooks 🖉 Edit 🔚 🕐 👶 🖈 😳

V 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 🗸

- 1	TimeGenerated	$\uparrow_{\downarrow}$	OperationName	$\uparrow_{\downarrow}$	InitiatingUserOrApp	$\uparrow_{\downarrow}$	AADOperationType $\uparrow_{\downarrow}$	targetDisplayName $\uparrow_{\downarrow}$	TargetResources	$\uparrow_{\downarrow}$	Result	$\uparrow_{\downarrow}$	UserAgent
- 1	12/18/2020, 8:59:57 PM		Set federation settings on domain		jeffs@woodgrove.ms		Update	woodgrove.net	[{"displayName": "woodgrove.net", "administrativeUnit	s":[],	success		
- 1	12/7/2020, 3:37:54 PM		Add verified domain		joeyc@woodgrove.ms		Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"	nod	failure		Mozilla/5.0 (Windows NT 10
- 1	12/7/2020, 3:12:05 PM		Add verified domain		joeyc@woodgrove.ms		Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"	nod	failure		Mozilla/5.0 (Windows NT 10
- 1	12/7/2020, 3:11:40 PM		Add unverified domain		joeyc@woodgrove.ms		Add	pre2.woodrove.ms	[{"displayName":"pre2.woodrove.ms","administrativel	Jnits	success		Mozilla/5.0 (Windows NT 10
- 1	12/7/2020, 3:10:58 PM		Add verified domain		joeyc@woodgrove.ms		Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"	nod	failure		Mozilla/5.0 (Windows NT 10

Provisioning logs (Preview)

P Logs

Diagnostic settings

Workbooks

M Usage & insights

Troubleshooting + Support

Virtual assistant (Preview)

New support request



### Sửa đổi các cài đặt liên kết

Thực hiện thay đổi đối với các mục tin cậy liên kết miền hiện có

Thêm các miền và mục tin cậy mới



### Cấp những quyền mới cho tên chính của dịch vụ

#### Home > Woodgrove Woodgrove | Workbooks | Sensitive Operations Report 🛷 $\times$ Azure Active Directory 🞽 Workbooks 🖉 Edit 🔚 🕐 👶 🖈 😳 External Identities New permissions granted to service principals Roles and administrators 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 Administrative units Principal is added to an App Role with a value of Mail.Read. Enterprise applications 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. Devices 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. App registrations Identity Governance TimeRange: Last 60 days 🗸 ClientApp: All 🗸 Resource: All V Application proxy Licenses New Application (AppOnly) permissions added to service principals Azure AD Connect ₽ Search Custom domain names Resource ↑↓ ClientApp ↑↓ Role\_Added ↑↓ Explanation ↑↓ InitiatingUserOrApp ↑↓ TimeGenerated Λ↓ Mobility (MDM and MAM) ✓ Office 365 Exchange Online (4) Password reset > "JeffTestCreds2" (4) Company branding ✓ Microsoft Graph (4) 🐯 User settings ✓ "JeffTestCreds2" (3) Properties "JeffTestCreds2" "Application.Read.All" "Read all applications" jeffs@woodgrove.ms 12/20/2020, 1:54:46 PM Security "JeffTestCreds2" "Mail.Send" "Send mail as any user" jeffs@woodgrove.ms 12/22/2020, 11:56:24 AM Monitoring "JeffTestCreds2" "Read and write mail in all mailboxes" jeffs@woodgrove.ms "Mail.ReadWrite" 12/22/2020, 11:56:24 AM Sign-ins > "Mimorony AuthTS API" (1) Audit logs ✓ Office 365 SharePoint Online (1) Provisioning logs (Preview) > "JeffTestCreds2" (1) P Logs Diagnostic settings Workbooks TimeRange: Last 48 hours ∨ InitiatingUserOrApp: All 🗸 Operation: All 🗸 艏 Usage & insights Recent app permissions activity Troubleshooting + Support Virtual assistant (Preview) TimeGenerated ↑↓ InitiatingUserOrApp Λ⊥ OperationName ↑↓ ClientApp ↑ L Resource ↑↓ Result ↑↓ New support request 1/26/2021, 4:25:23 PM Consent to application CCE Test Not logged jerryw@woodgrove.ms success

04.

# Tổng quan về những thay đổi được thực hiện cho tư cách thành viên tên chính của dịch vụ

Microsoft Azure	∠ Search resources, services, and docs (G+/)	N THE D TO CONCERNS WOODGROVE					
Home > Woodgrove							
Woodgrove   Workbo	oks   Sensitive Operations Report 🛷	×					
	Workbooks 2 Edit 品 ひ 命 交 ②						
🌓 External Identities	Sensitive Operations Report - Apps Service Principals and Federation Settings						
👃 Roles and administrators	sensitive operations heporte Apps, service i micipus and reactation settings	Workspace: All 🗸					
Administrative units	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.						
Enterprise applications							
Devices	Modified application and service principal credentials/authentication methods						
App registrations	$\sim$ New permissions granted to service principals						
Identity Governance							
Application proxy	∧ Directory role and group membership updates to service principals						
Licenses	Directory role and group membership updates to service principals						
Azure AD Connect	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.						
Custom domain names	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						
Mobility (MDM and MAM)	or represent opportunities for lateral movement by attackers.						
Password reset	TimeRange: Last 60 days X Operation: Add member to role						
Company branding	Select						
🔅 User settings	TimeGenerated $\uparrow_{\downarrow}$ InitiatingU       All $\uparrow_{\downarrow}$ ServicePrincipalDisplayName $\uparrow_{\downarrow}$ GroupOrRoleNameAddedTo $\uparrow_{\downarrow}$						
Properties	12/22/2020, 11:49:13 AM jeffs@woo Items e JeffTestCreds2 "Application Administrator"						
Security	12/22/2020, 11:52:28 AM jeffs@woo 🗸 Add member to role e Risky App "Global Administrator"						
Monitoring	12/20/2020, 7:46:25 PM jeffs@woo Add eligible member to role e JeffTestCreds2 "Security Operator"						
➔ Sign-ins	Add scoped member to role						
Audit logs	Add member to group						
Provisioning logs (Preview)							
🧬 Logs							
Diagnostic settings							
Workbooks							
🚮 Usage & insights							
Troubleshooting + Support							
🕎 Virtual assistant (Preview)							
New support request							
	X MODILIED LEDELTINGE						

Tổng quan về Solorigate

### Bước tiếp theo

01 Xem chuỗi video về Solorigate tại vị trí này 02 Truy nhập Microsoft Security để biết thêm thông tin cập nhật: https://www.microsoft.com/vivn/security/business 03 Đọc bài đăng blog trên: www.microsoft.com/security/blog/

https://aka.ms/solorigate



