Microsoft

# Sổ làm việc Azure AD

**Daniel Wood**

Người quản lý Chương trình

Bảo mật Danh tính Azure AD

**18/02/2021**

Chuỗi video về Solorigate

# 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

Microsoft Security

01.

Đăng nhập vào **Cổng thông tin Microsoft Azure**.

02.

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

03.

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

01.

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

# Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory





## 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)

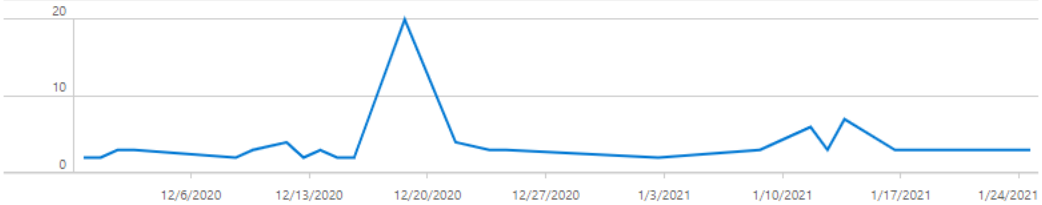
| AsymmetricX509Cert | Other/not logged | Password | X509CertAndPassword |
|---|---|---|---|
| 15 | 23 | 6 | 1 |

### 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




count_ (Sum)
91

### 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 | dcbce8f2-17b4-4139-8d97- |

01.

# 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

02.

# Sửa đổi các cài đặt liên kết

# Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory





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 1C |
| 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 1C |
| 12/7/2020, 3:11:40 PM | Add unverified domain | joeyc@woodgrove.ms | Add | pre2.woodrove.ms | [{"displayName":"pre2.woodrove.ms","administrativeUnits... | success | Mozilla/5.0 (Windows NT 1C |
| 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 1C |

02.

# 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

03.

# Cấp những quyền mới cho tên chính của dịch vụ

# Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory



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.

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

# Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory



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

Select
- All

Items
- Add member to role
- Add eligible member to role
- Add scoped member to role
- Add member to group

| TimeGenerated | InitiatingU | ServicePrincipalDisplayName | GroupOrRoleNameAddedTo |
|---|---|---|---|
| 12/22/2020, 11:49:13 AM | jeffs@woo | JeffTestCreds2 | "Application Administrator" |
| 12/22/2020, 11:52:28 AM | jeffs@woo | Risky App | "Global Administrator" |
| 12/20/2020, 7:46:25 PM | jeffs@woo | JeffTestCreds2 | "Security Operator" |

Modified federation settings

# 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/vi-vn/security/business

03 Đọc bài đăng blog trên: www.microsoft.com/security/blog/

https://aka.ms/solorigate

Microsoft