

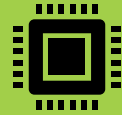


Virtual Smart Cards for Lab Environments

About Me



B.S. Management Information Systems (Hybrid Business/IT)



Started in IT at 17. 23 years experience in various jobs, (IE. Help Desk, Desktop, Analyst, Server/Datacenter, and Management)



Current focus is on Active Directory/Security, Microsoft Client/Server System Hardening, Office 365/Azure cloud security, and Active Directory Certificate Services.

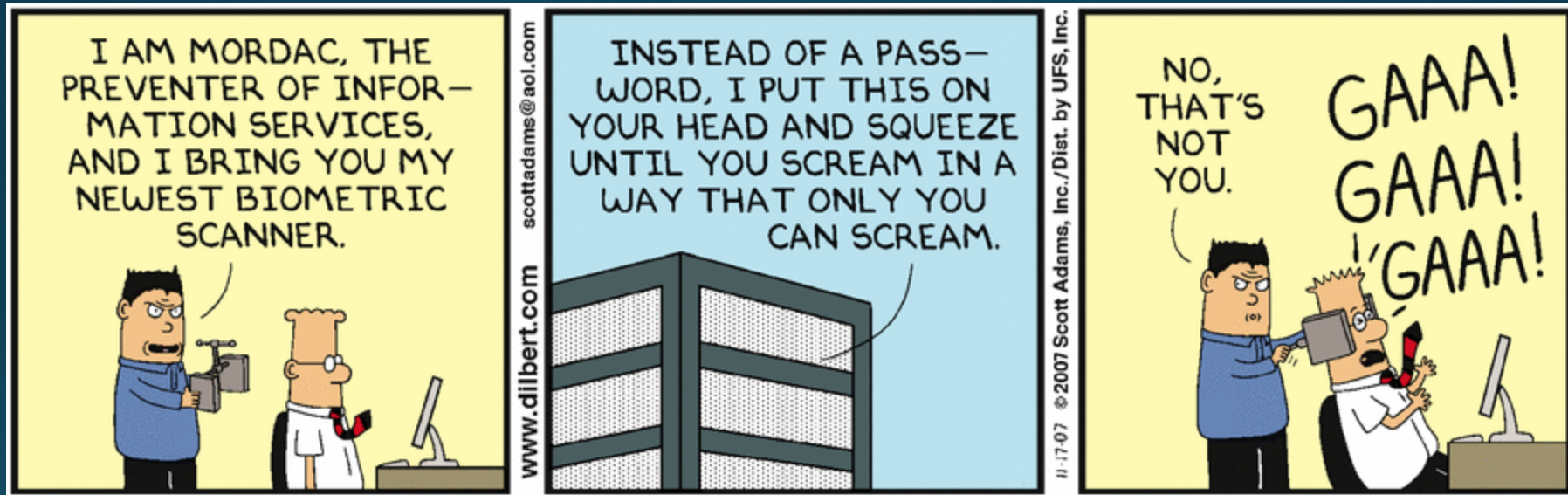


Spent the past 7 years as a Board Member at a historical non profit museum. During that time I learned a ton about Azure/EMS/Azure AD. Donating your time to non profits has interpersonal and professional benefits!

Link to Slide Decks and Content

- <https://github.com/rootsecdev/Virtual-Smart-Cards>

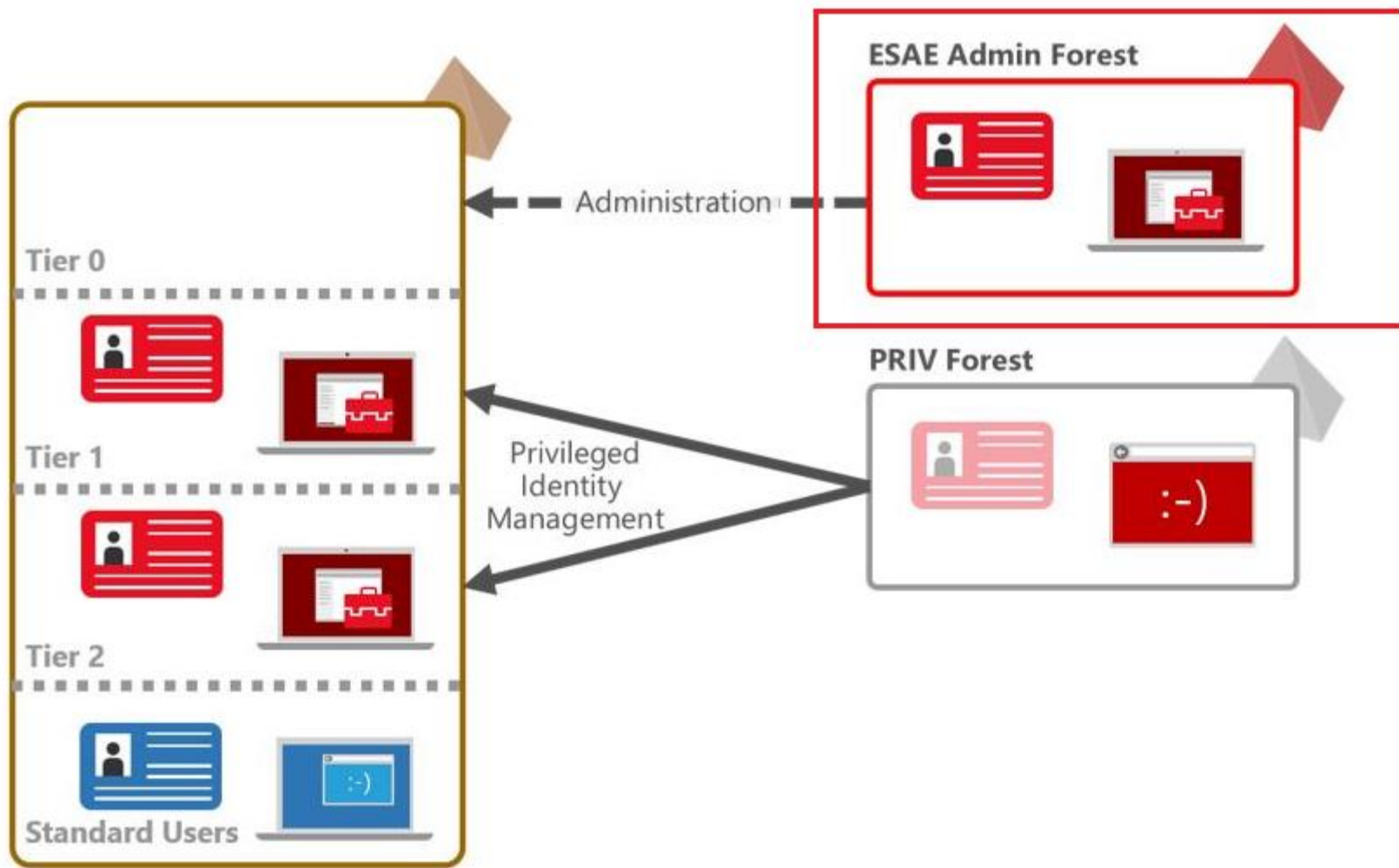
Passwords

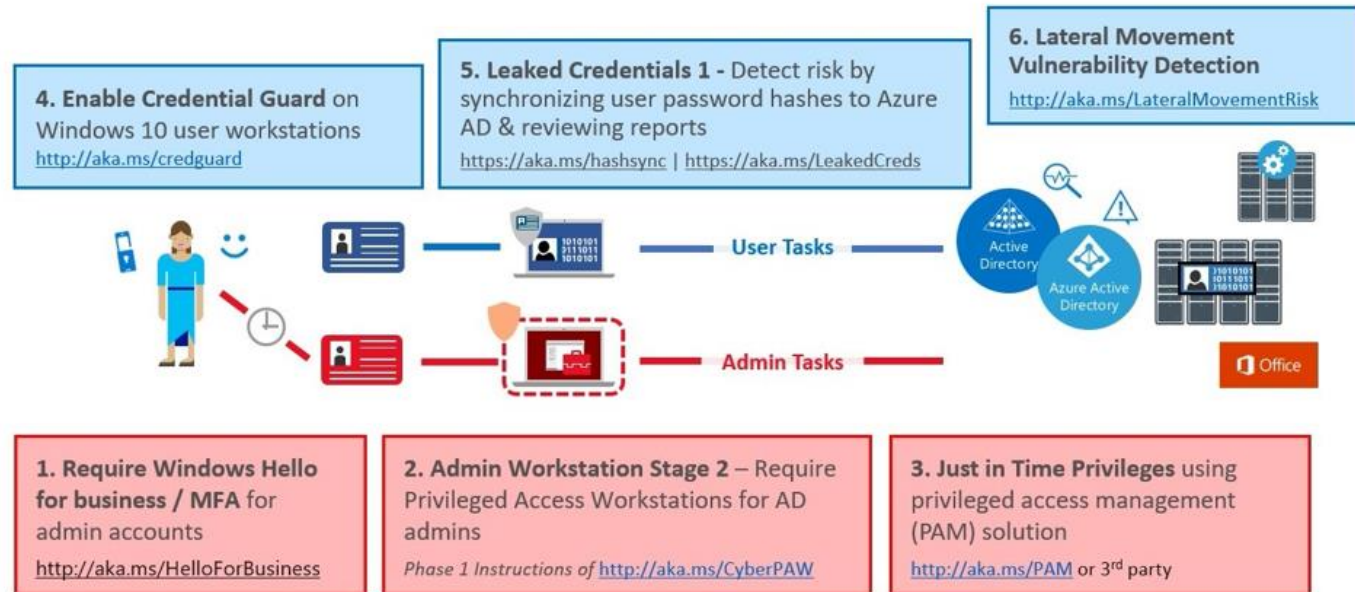


Password Domain Security

- New recommended default
- No password changes required!
- End users have a bad habit of choosing bad passwords because of short max password age. (IE 90 Days)
- This should be used in conjunction with a passwordless strategy
- Fine Grain password policies for SmartCard/Win10 Hello enforced users!

MSFT Windows 10 1903 and Server 1903 - Domain Security	
Scope	Details Settings Delegation Status
MSFT Windows 10 1903 and Server 1903 - Domain Security	
Data collected on: 8/22/2019 6:33:52 AM	
General	
Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Account Policies/Password Policy	
Policy	Setting
Enforce password history	24 passwords remembered
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Policies/Account Lockout Policy	
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes





~~1. Require Windows Hello for Business and MFA~~

~~Administrators can benefit from the ease of use associated with Windows Hello for Business. Admins can replace their complex passwords with strong two-factor authentication on their PCs. An attacker must have both the device and the biometric info or PIN, it's much more difficult to gain access without the employee's knowledge. More details about Windows Hello for Business and the path to roll out can be found in the article [Windows Hello for Business Overview](#)~~

~~Enable multi-factor authentication (MFA) for your administrator accounts in Azure AD using Azure MFA. At minimum enable the [baseline protection conditional access policy](#) more information about Azure Multi-Factor Authentication can be found in the article [Deploy cloud-based Azure Multi-Factor Authentication](#)~~

Luke Skywalker Properties



Organization	Published Certificates			Member Of
Password Replication	Object	Security	COM+	Attribute Editor
General	Address	Account	Profile	Telephones

User logon name:

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

☐ Account is disabled
☒ Smart card is required for interactive logon
☐ Account is sensitive and cannot be delegated
☐ Use only Kerberos DES encryption types for this account

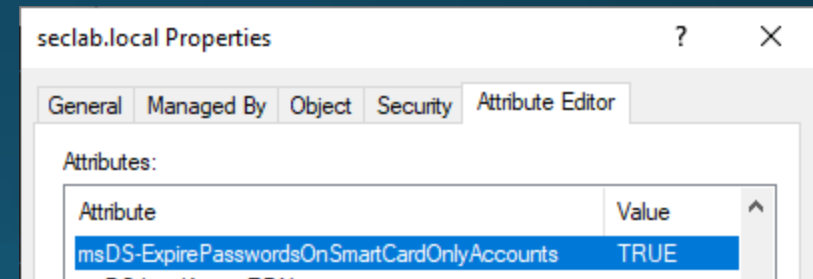
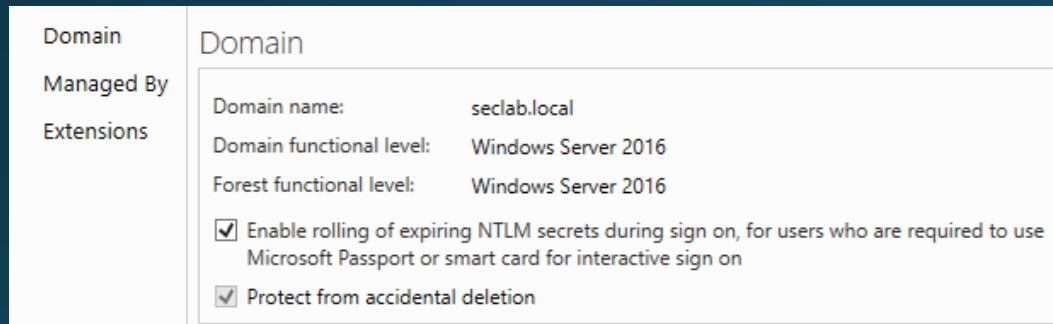
Account expires

☒ Never
☐ End of:

'Smart card is required for interactive logon' forces two factor authentication at logon: i.e. something we have (the smart card), and something we know (a PIN). This increases account security. When SCRIL is configured, the account's password hash is replaced with a hash derived from a 120-character random value.

We still have a hash... even though SCRIL users are using a smart card and not a password for interactive logon, a high-entropy secret is created to prevent a dictionary attack on NTLM network logons... and, where there are hashes, there's the potential for a [Pass-The-Hash](#) attack from a compromised system. Now, here's the rub: the hashes for SCRIL users don't change, so if their credentials are stolen, the attacker can reuse these ad infinitum.

Automatic rolling of expiring NTLM secrets



Password Settings

Directly Applies To

Extensions

Password Settings

Name: * SmartCardPasswordPolicy

Precedence: * 1

☒ Enforce minimum password length

Minimum password length (characters): * 120

☒ Enforce password history

Number of passwords remembered: * 24

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:

Password age options:

☒ Enforce minimum password age

User cannot change the password within (days): * 1

☒ Enforce maximum password age

User must change the password after (days): * 2

☒ Enforce account lockout policy:

Number of failed logon attempts allowed: * 10

Reset failed logon attempts count after (mins): * 30

Account will be locked out

☒ For a duration of (mins): * 30

☐ Until an administrator manually unlocks the account

Directly Applies To

Name

Mail

Smart_Card_Users

Add...

Remove

Deny access to this computer from the network

ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests, NT AUTHORITY\Local account

Deny log on as a batch job

ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS

Deny log on as a service

ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS

Deny log on locally

ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests

Deny log on through Terminal Services

ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests, NT AUTHORITY\Local account



DISCLAIMER

Warnings

- This slide deck and demo is a lab only environment. Please do not replicate this lab environment in a production enterprise environment.
- Deploying an Enterprise Root CA role to a domain controller could lead to a resume generating event
- PKI can be complex to roll out. Since I have 30 mins we will roll out a 1 tier ADCS environment (not recommended)



More Disclaimers

About those virtual smart cards

- They will be depreciated...
- <https://github.com/MicrosoftDocs/windows-itpro-docs/blob/master/windows/security/identity-protection/hello-for-business/hello-faq.md>
- This lab talk is mean to show a low-cost way of implementing smart cards/security keys with no extra hardware required.

There is a bright side

- Much of what I will show you will apply to Yubikey 5 NFC
- Path moving forward is Windows 10 Hello for Business
- If non Office365/Azure Customer/or using ESAFE and isolated identities then smart card is the path to take

VSC LAB

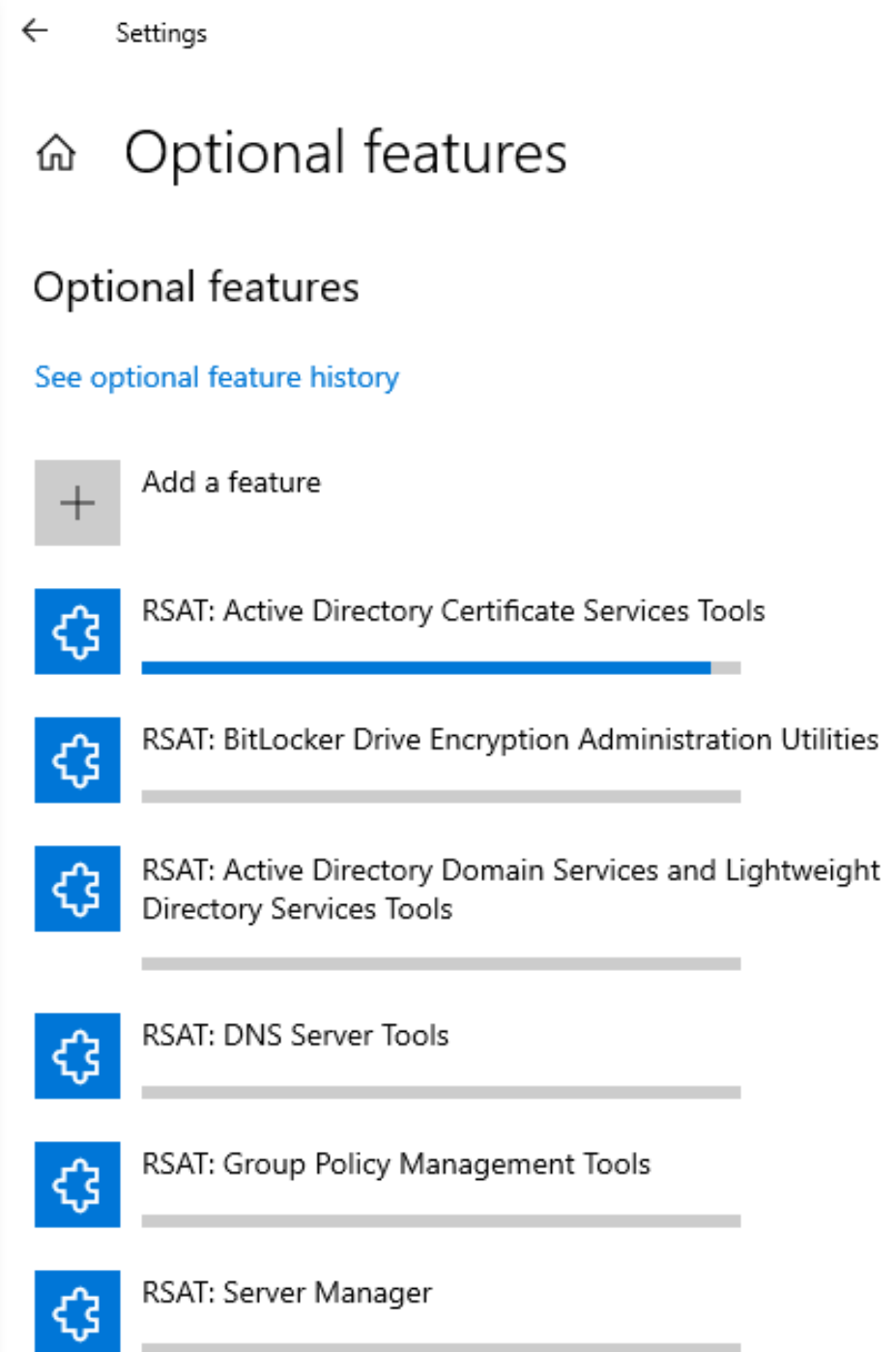
- Prerequisites:
- Hyper-V workstation or Server/Vmware-Workstation
- ~~Offline Root CA (Server 2019)~~
- Server 2019 Core VM - Domain Controller, DNS Server, ~~Enterprise Sub-CA,~~ Enterprise CA
- Windows 10 V1903 Client with Virtual TPM Enabled

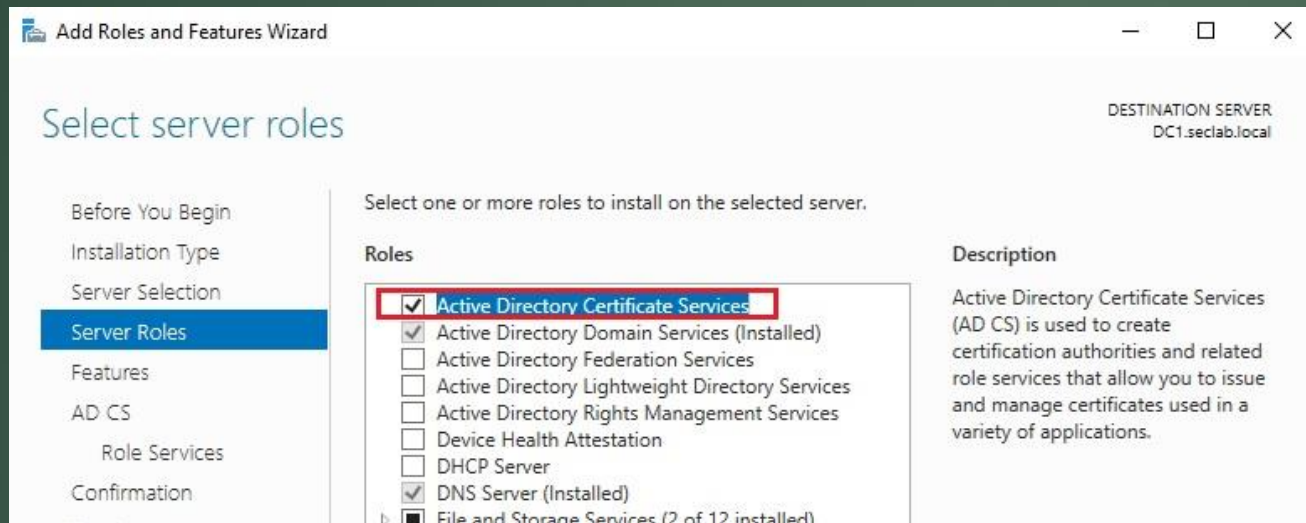
VSC LAB

- Server Core 2019
- Roles – Domain Controller, Global Catalog, DNS, ADCS
- - Do Not Disable IPv6. Instead prefer IPv4 over IPv6
- A) <https://support.microsoft.com/en-us/help/929852/guidance-for-configuring-ipv6-in-windows-for-advanced-users>
- Use “sconfig” to set static IP
- Install ADDS and Confirm domain controller is running
- Video: The Quick dirty way of building your own DC.

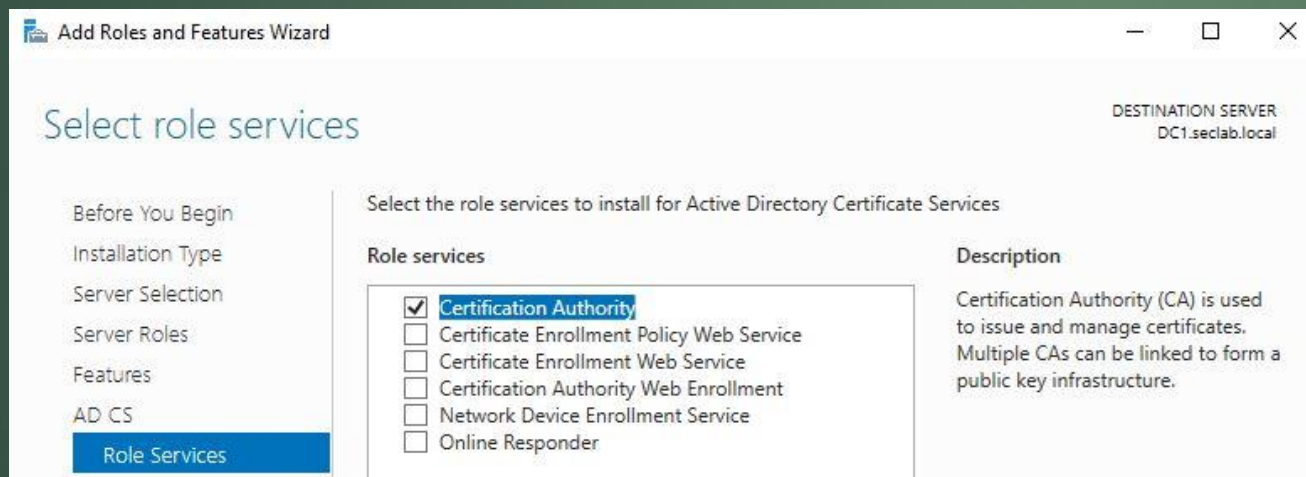
VSC LAB

- Install RSAT on Windows 10 Machine
- RSAT can only be installed through optional features starting in builds 1809 and up
- Windows Admin Center
- Use Server Manager on Windows 10 machines to add the ADCS role on your Server Core DC





VSC LAB



Active Directory Certificate Services

Additional steps are required to configure Active Directory Certificate Services on the destination server

Configure Active Directory Certificate Services on the destination server

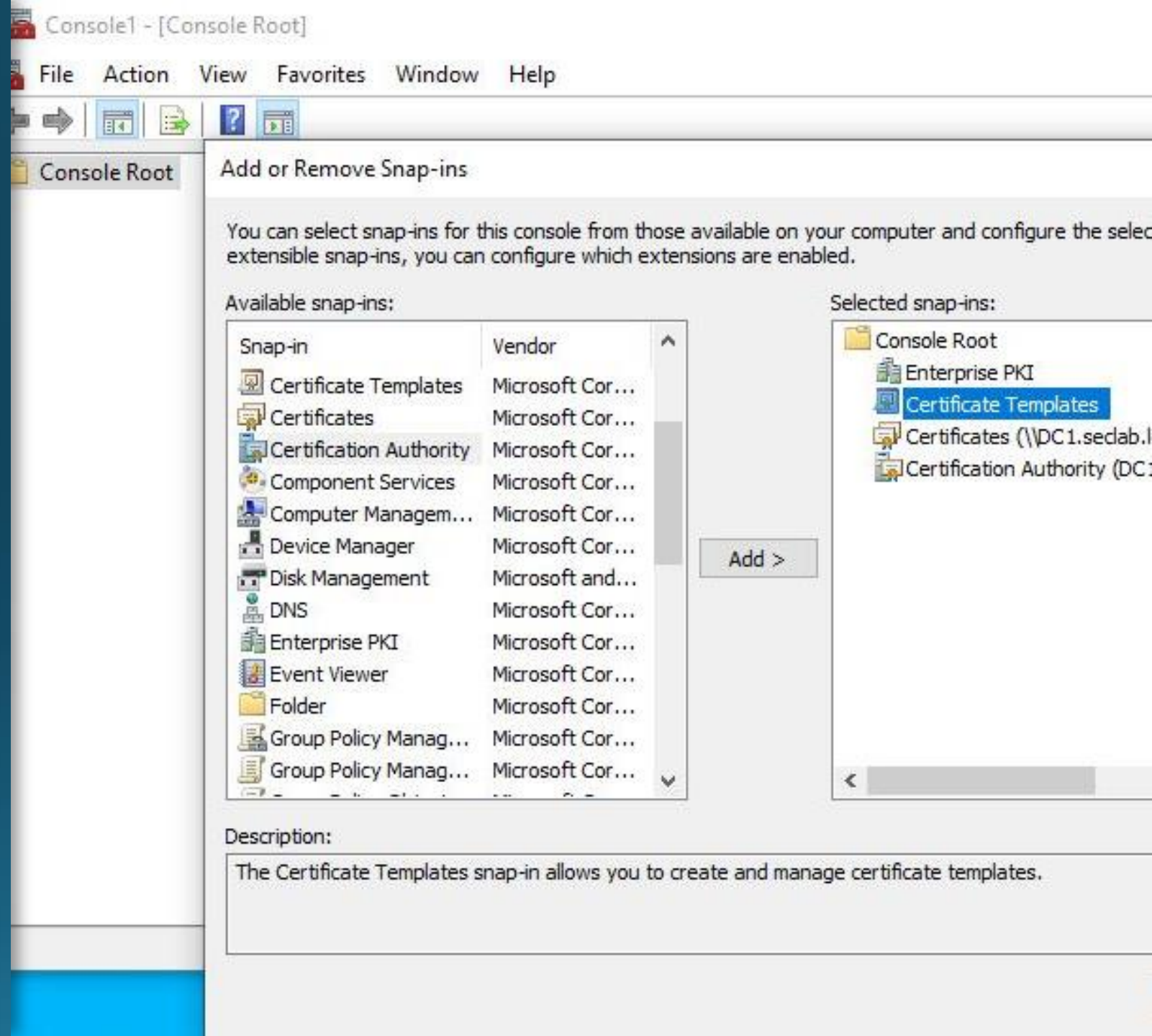
Certification Authority

VSC LAB Demo

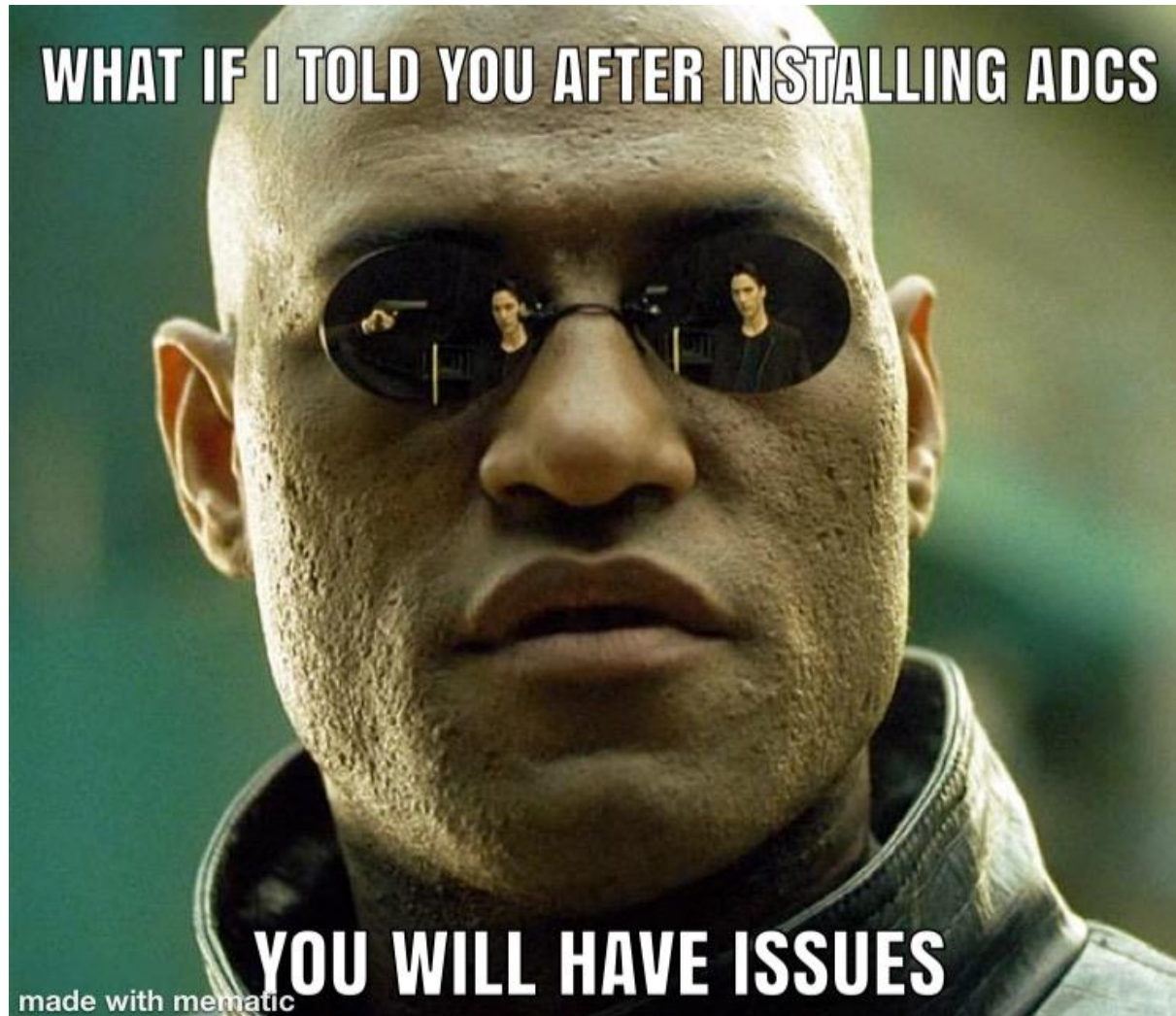


VSC LAB MMC Tools

- Enterprise PKI
- Certificate Template
- Certificates
(Computer/Point to
Domain Controller)
- Certification
Authority (Point to
Domain Controller)



WHAT IF I TOLD YOU AFTER INSTALLING ADCS



YOU WILL HAVE ISSUES

made with mematic

VSC Lab Errors

- By default we have an untrusted root CA. Fix by issuing gupdate/force

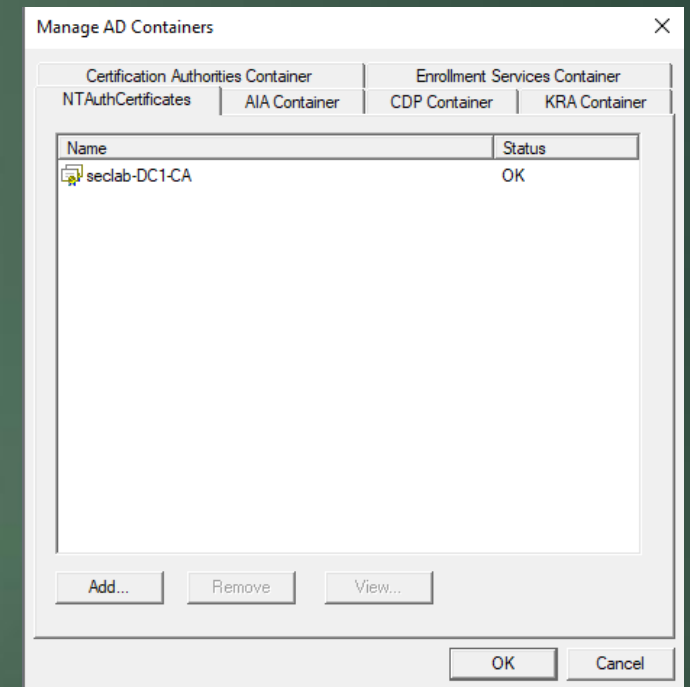
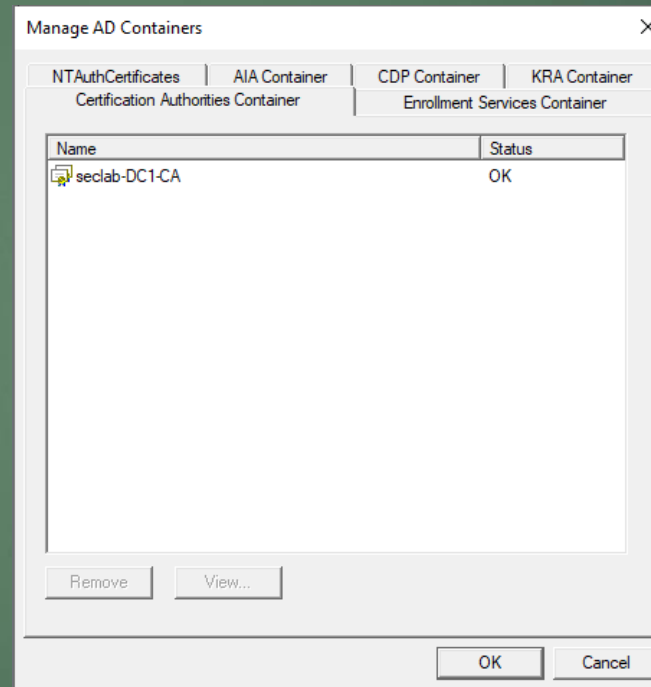
Console Root	Name	Status	Expiration Date	Location
Enterprise PKI	CA Certificate	Untrusted Root	7/27/2029 7:20 ...	
seclab-DC1-CA (V0.0)	AIA Location #1	Untrusted Root	7/27/2029 7:20 ...	Idap:///CN=seclab-DC1-CA,CN=AIA,CN=Public
Certificate Templates	CDP Location #1	OK	8/3/2019 7:30 ...	Idap:///CN=seclab-DC1-CA,CN=DC1,CN=CDP,C
Certificates (\\DC1.seclab.local)	DeltaCRL Location #1	OK	7/28/2019 7:30 ...	Idap:///CN=seclab-DC1-CA,CN=DC1,CN=CDP,C
Certification Authority (DC1)				

Console Root	Name	Status	Expiration Date	Location
Enterprise PKI	CA Certificate	OK	7/27/2029 7:20 ...	
seclab-DC1-CA (V0.0)	AIA Location #1	OK	7/27/2029 7:20 ...	Idap:///CN=seclab-DC1-CA,CN=AIA,CN=Public
Certificate Templates	CDP Location #1	OK	8/3/2019 7:30 ...	Idap:///CN=seclab-DC1-CA,CN=DC1,CN=CDP,C
Certificates (\\DC1.seclab.local)	DeltaCRL Location #1	OK	7/28/2019 7:30 ...	Idap:///CN=seclab-DC1-CA,CN=DC1,CN=CDP,C
Certification Authority (DC1)				

Enterprise PKI

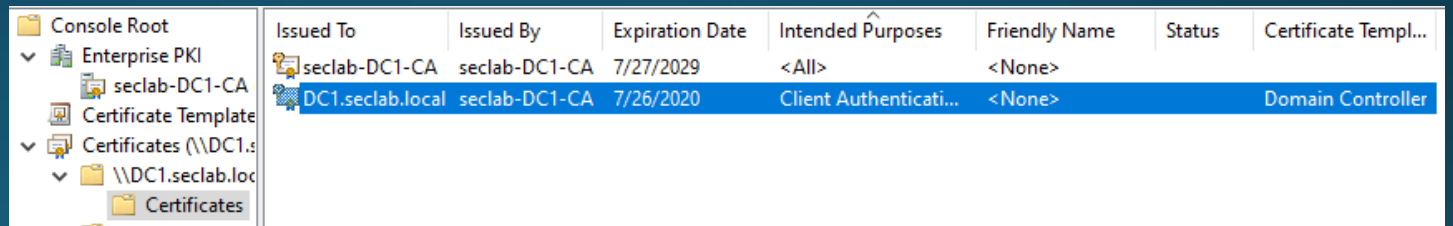
Manage AD Containers

- Manage certificate authorities here
- Root CA certificate is your NTAUTHCertificate



VSC LAB Fixes

- Domain Controller Template issued for AD Auth = Smart Card Problems!
- Fix by issuing Kerberos Authentication certificate to domain controller.
- Disable Domain Controller Template. Domain Controller Certificate can be safely deleted.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Templ...
seclab-DC1-CA	seclab-DC1-CA	7/27/2029	<All>	<None>		
DC1.seclab.local	seclab-DC1-CA	7/26/2020	Client Authenticati...	<None>		Domain Controller

VSC LAB Domain Controller Certificates Explained.

- Reference URL:
<https://blogs.technet.microsoft.com/russellt/2016/06/03/custom-ldap-certs/>
- Written by Russell Thompson (PFE MSFT)
- Use **Kerberos Authentication!**

Our Domain Controllers by default will use one of the 3 built-in certificate templates for LDAP over TLS purposes. These templates were introduced consecutively with each OS release. The templates are the:

- *Domain Controller* (Windows Server 2000)
- *Domain Controller Authentication* (Windows Server 2003)
- *Kerberos Authentication* (Windows Server 2008 and above)

Our modern domain controllers can use any one these 3 certificate templates, however we really want your DC's to be using the Kerberos Authentication template. By default, it includes multiple SAN entries that represent the Domain Controller, Active Directory Domain FQDN and the Active Directory NetBIOS name. Additionally it contains a new Enhanced Key Usage to allow strict KDC validation to be enabled on all modern clients that are performing smart-card based (PKINIT) logons.

Demo

- Remove/revoke Domain Controller Certificate
- Add Kerberos Authentication to your certificate authority through powershell



```
Administrator: Windows PowerShell
[dc1]: PS C:\Users\lskywalker\Documents> Get-Certificate -Template KerberosAuthentication -CertStoreLocation cert:\LocalMachine\My

Status Certificate
-----
Issued [Subject]...

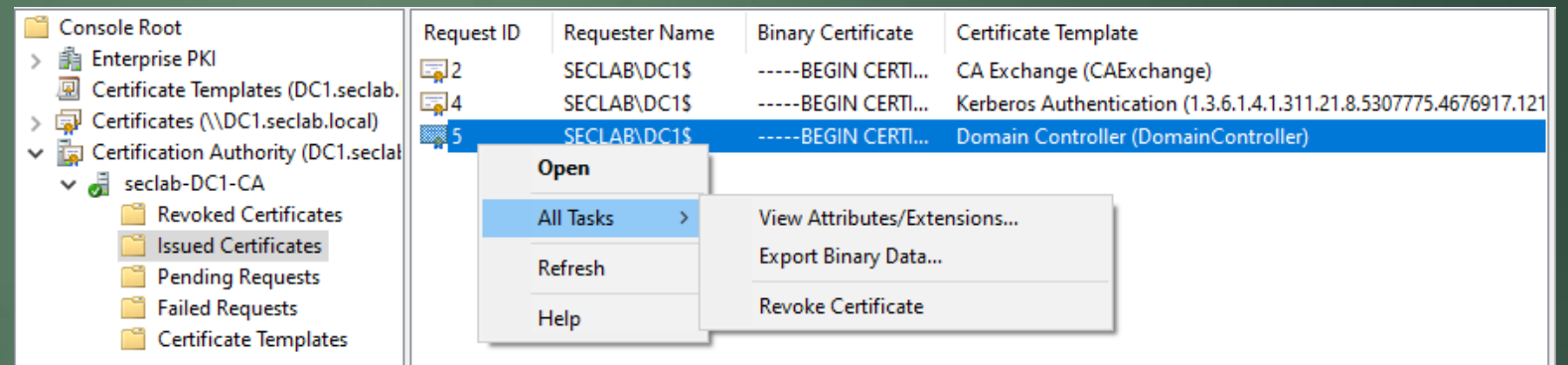
[dc1]: PS C:\Users\lskywalker\Documents> █
```

VSC Lab Fixes

- 2 ways to issue Kerberos authentication certificate on Server Core 2019
- PS remoting following by Get-Certificate command
- Directly on the domain controller in powershell using Get-Certificate command.

VSC LAB

- Revoking issued certificates



Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

USING SHA512 HASH



TO PROTECT MYSELF FROM NSA

made with mematic

hashicorp / vault

Watch 535

Star 13,631

Fork 2,027

Code

Issues 428

Pull requests 80

Security

Insights

LDAP auth: Cannot establish TLS1.2 connection with Active Directory server using SHA-512 certificates #2058

New issue

Closed

glennmcallister opened this issue on Nov 2, 2016 · 8 comments



glennmcallister commented on Nov 2, 2016

Contributor + 😊 ...

Vault Release: 0.6.2

Reproduction Steps:

1. Setup Active Directory DC with TLS, using a SHA-512 hash cert. Yep, this is a pain.
2. Setup the LDAP auth method to communicate with this DC.
3. Attempt to authenticate.

Expected behaviour: Successful authentication.

Actual behaviour: Connection failure.

```
$ vault auth --method=ldap username=glenn.mcallister
Password (will be hidden):
Error making API request.
```

```
URL: PUT http://127.0.0.1:8200/v1/auth/ldap/login/glenn.mcallister
Code: 400. Errors:
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Notifications

Customize

🔊 Subscribe

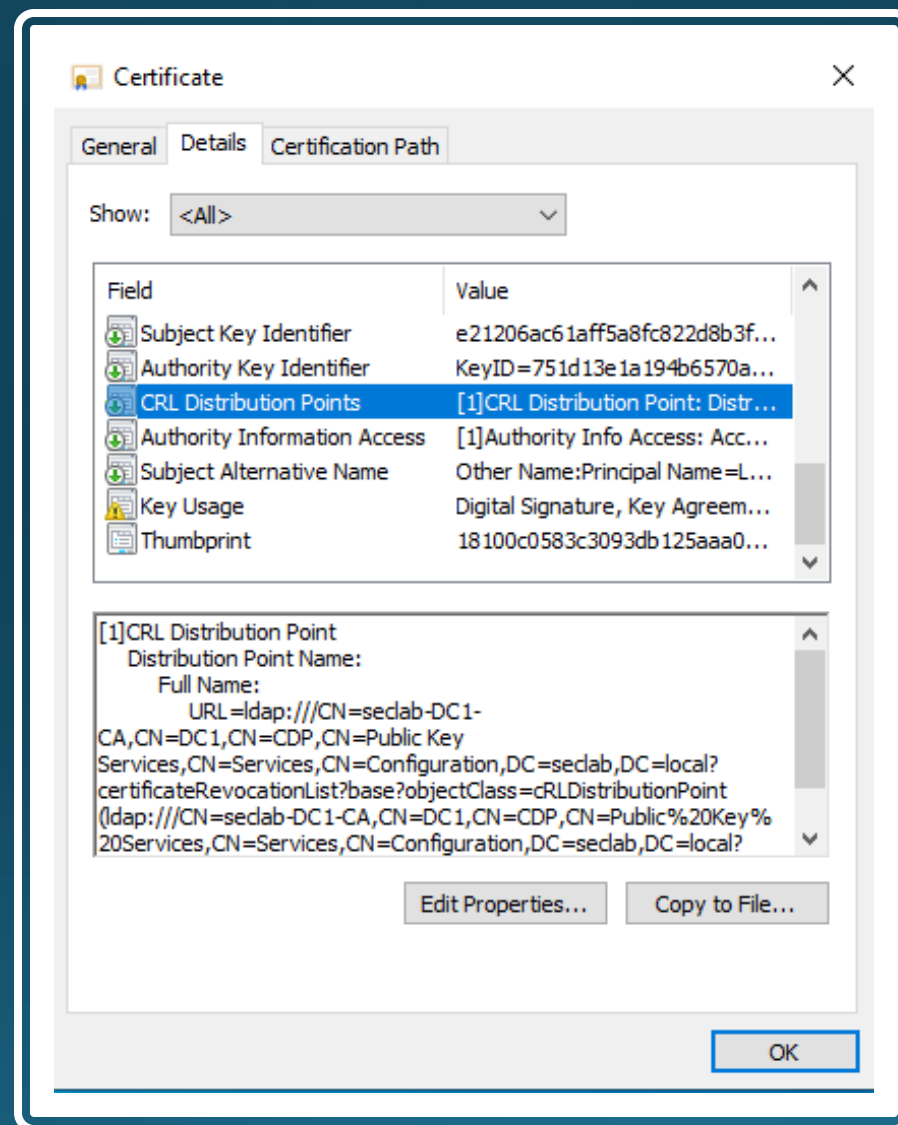
You're not receiving notifications from this thread.

VSC Lab LDAP Auth Issues

- SSL over LDAP is perfect example on why you shouldn't use exotic or crazy hashing on CA's. (SHA512=No cipher support)
- If security auditing is your thing vulnerability scans will pick up your 2019 DC with 3DES Ciphers enabled (IE. Sweet 32 attacks)
- The security community has yet to see practical attacks on sweet32. Disable anyway!

```
[rootsecdev@localhost ~]$ nmap -sV --script ssl-enum-ciphers -p 636
Starting Nmap 6.40 ( http://nmap.org ) at 2019-08-10 06:13 CDT
Nmap scan report for 172.16.2.2
Host is up (0.0018s latency).
PORT      STATE SERVICE VERSION
636/tcp   open  ssl/ldap
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - strong
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA256 - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA256 - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 12.62 seconds
```

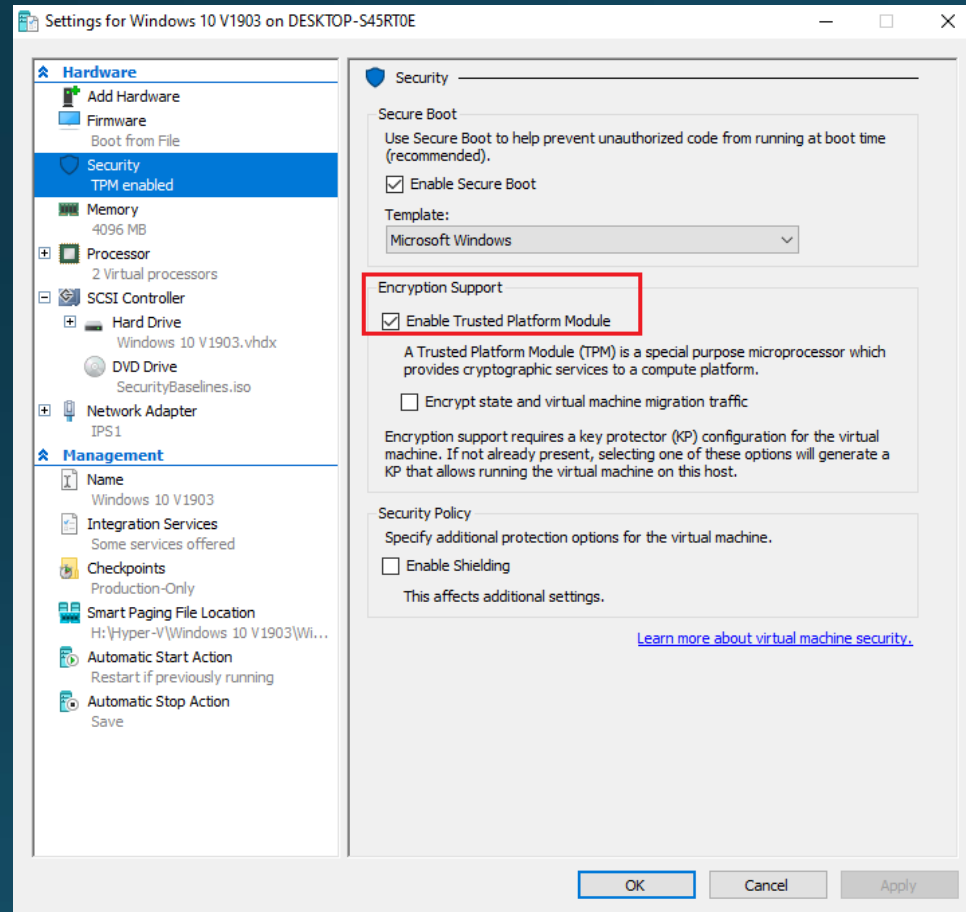


VSC LAB LDAP

- I'm focusing on LDAP because lab is using 1 tier hierarchy for ADCS
- Authority Information Access and CRL Distribution will rely on LDAP for Certificate Revocation
- Refer to >>



VSC Lab Workstation Config



```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

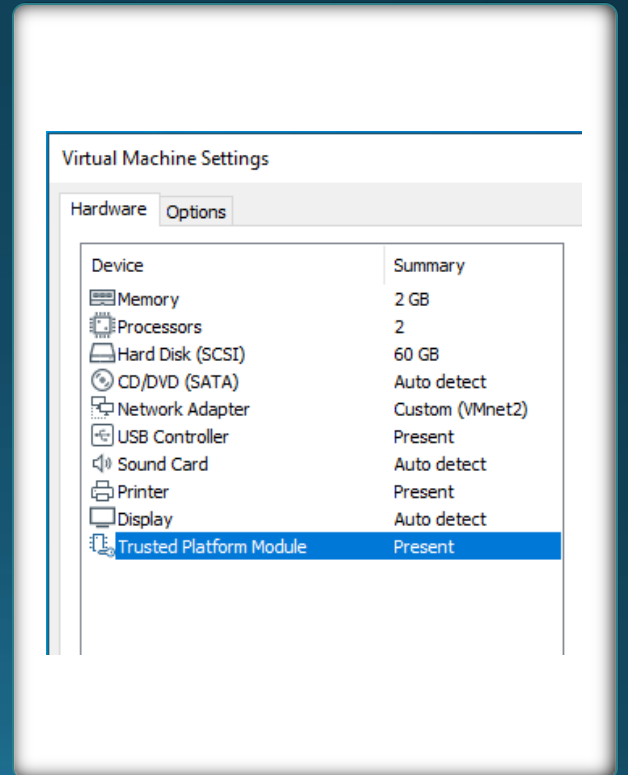
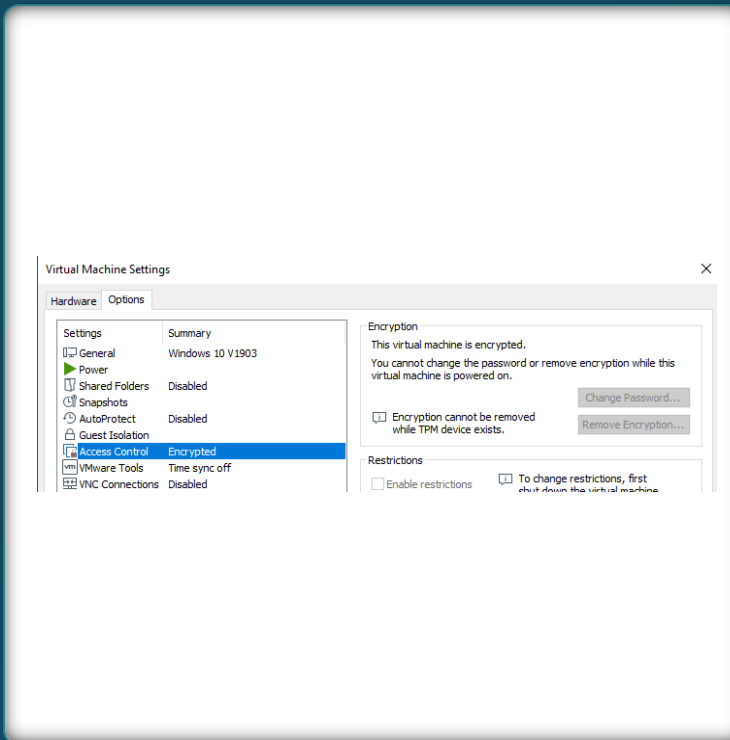
PS C:\WINDOWS\system32> Get-TPM

TpmPresent           : False
TpmReady             : False
ManufacturerId       : 0
ManufacturerIdTxt    :
ManufacturerVersion  :
ManufacturerVersionFull120 :
ManagedAuthLevel    : Full
OwnerAuth            :
OwnerClearDisabled   : True
AutoProvisioning     : NotDefined
LockedOut            : False
LockoutHealTime      :
LockoutCount         :
LockoutMax           :
SelfTest             :
```

PS C:\WINDOWS\system32>

Yes...this works for VMware

- Encrypt VM in Settings > Options
- Add TPM in Hardware tab
- In that order!



TPMVSCMGR

- TPMSVSCMGR Reference >>
<https://docs.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-tpmvscmgr>

```
Administrator: Command Prompt

C:\Windows\system32>tpmvscmgr.exe create /name VSC /pin prompt /adminkey random /generate
Enter PIN:
*****
Confirm PIN:
*****
Creating TPM Smart Card...
Initializing the Virtual Smart Card component...
Creating the Virtual Smart Card component...
Initializing the Virtual Smart Card Simulator...
Creating the Virtual Smart Card Simulator...
Initializing the Virtual Smart Card Reader...
Creating the Virtual Smart Card Reader...
Waiting for TPM Smart Card Device...
Authenticating to the TPM Smart Card...
Generating filesystem on the TPM Smart Card...
TPM Smart Card created.
Smart Card Reader Device Instance ID = ROOT\SMARTCARDREADER\0000

C:\Windows\system32>
```

TPMVSCMGR

- You can destroy what you create!

```
C:\Windows\system32>tpmvscmgr.exe destroy /instance root\smartcardreader\0000
Destroying TPM Smart Card...
Initializing the Virtual Smart Card Reader...
Destroying the Virtual Smart Card Reader...
Initializing the Virtual Smart Card Simulator...
Destroying the Virtual Smart Card Simulator...
Initializing the Virtual Smart Card component...
Destroying the Virtual Smart Card component...
TPM Smart Card destroyed.

C:\Windows\system32>
```


VSC LAB

Smart Card Template creation and virtual smart card provisioning walkthrough



- Reference URL: Get Started with Virtual Smart Cards: Walkthrough Guide
- <https://docs.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-get-started>

VSC LAB Reference Links

- Best Practices for securing active directory - <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>
- Password-less Strategies - <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy>
- Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy - [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831348\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831348(v=ws.11))

VCS LAB

- Microsoft Security Baselines can be downloaded at URL:
- <https://www.microsoft.com/en-us/download/details.aspx?id=55319>
- Securing privileged access <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

Addendum Slides (Yubikeys)

- https://developers.yubico.com/PIV/Introduction/Certificate_slots.html

Slot 9a: PIV Authentication

This certificate and its associated private key is used to authenticate the card and the cardholder. This slot is used for things like system login. The end user PIN is required to perform any private key operations. Once the PIN has been provided successfully, multiple private key operations may be performed without additional cardholder consent.

Slot 9c: Digital Signature

This certificate and its associated private key is used for digital signatures for the purpose of document signing, or signing files and executables. The end user PIN is required to perform any private key operations. The PIN must be submitted every time immediately before a sign operation, to ensure cardholder participation for every digital signature generated.

Slot 9d: Key Management

This certificate and its associated private key is used for encryption for the purpose of confidentiality. This slot is used for things like encrypting e-mails or files. The end user PIN is required to perform any private key operations. Once the PIN has been provided successfully, multiple private key operations may be performed without additional cardholder consent.

Slot 9e: Card Authentication

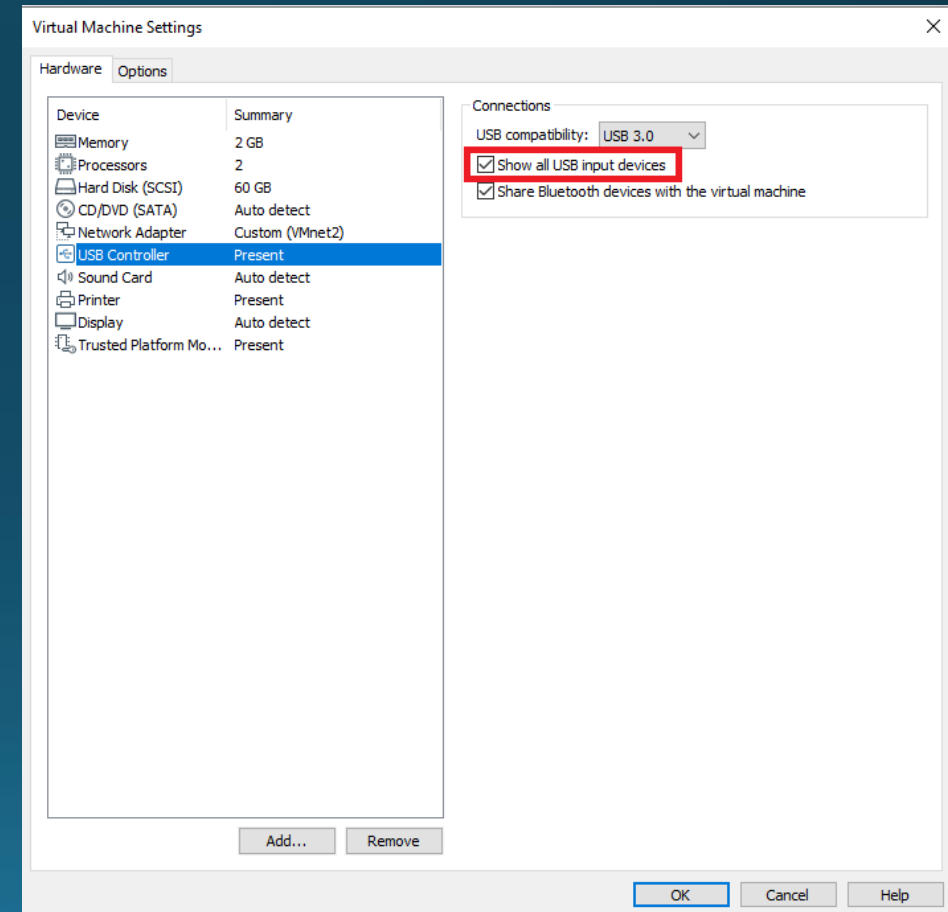
This certificate and its associated private key is used to support additional physical access applications, such as providing physical access to buildings via PIV-enabled door locks. The end user PIN is NOT required to perform private key operations for this slot.

Yubikeys

- Yubikey Smart Card Deployment Guide
https://support.yubico.com/support/solutions/articles/15000006456-yubikey-smart-card-deployment-guide#Use_Multiple_Authentication_Credentialsobpsn4
- If yubikey 4 it may be vulnerable to weak RSA Key Generation
<https://www.yubico.com/support/security-advisories/ysa-2017-01/>
- Generate ECC on Yubikeys if possible

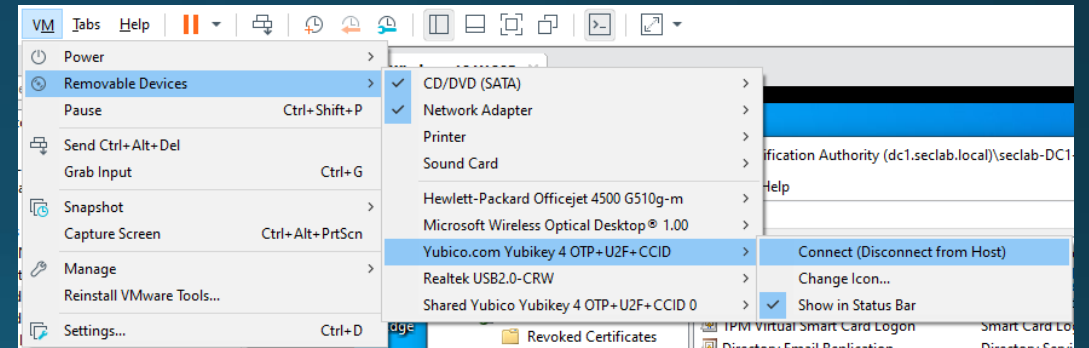
Yubikeys

- VMware Workstation Guidance
- <https://support.yubico.com/support/solutions/articles/15000008891-troubleshooting-vmware-workstation-device-passthrough>

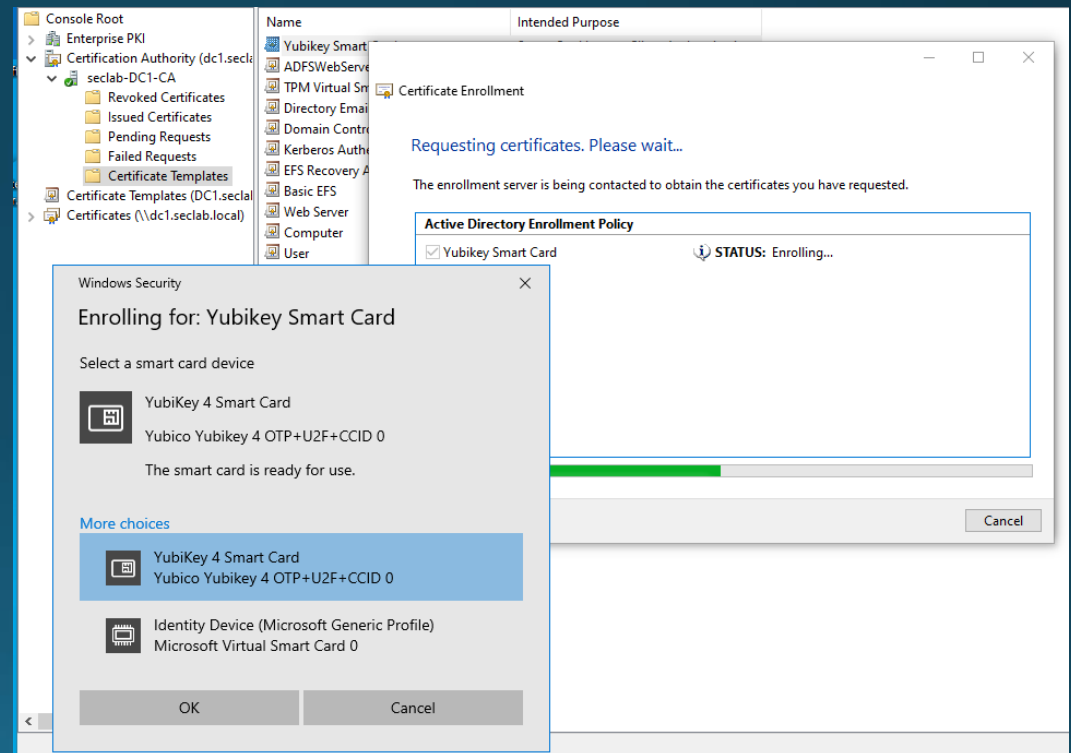


Yubikeys

- Don't use Shared Yubikey if using vmware. Use the Yubikey 4 OTP
- Otherwise the card will not function



- Use enrollment with minicard driver.
- You can do native enrollment through Windows certificate manager if yubikey minidriver is installed
- <https://www.yubico.com/products/services-software/download/>



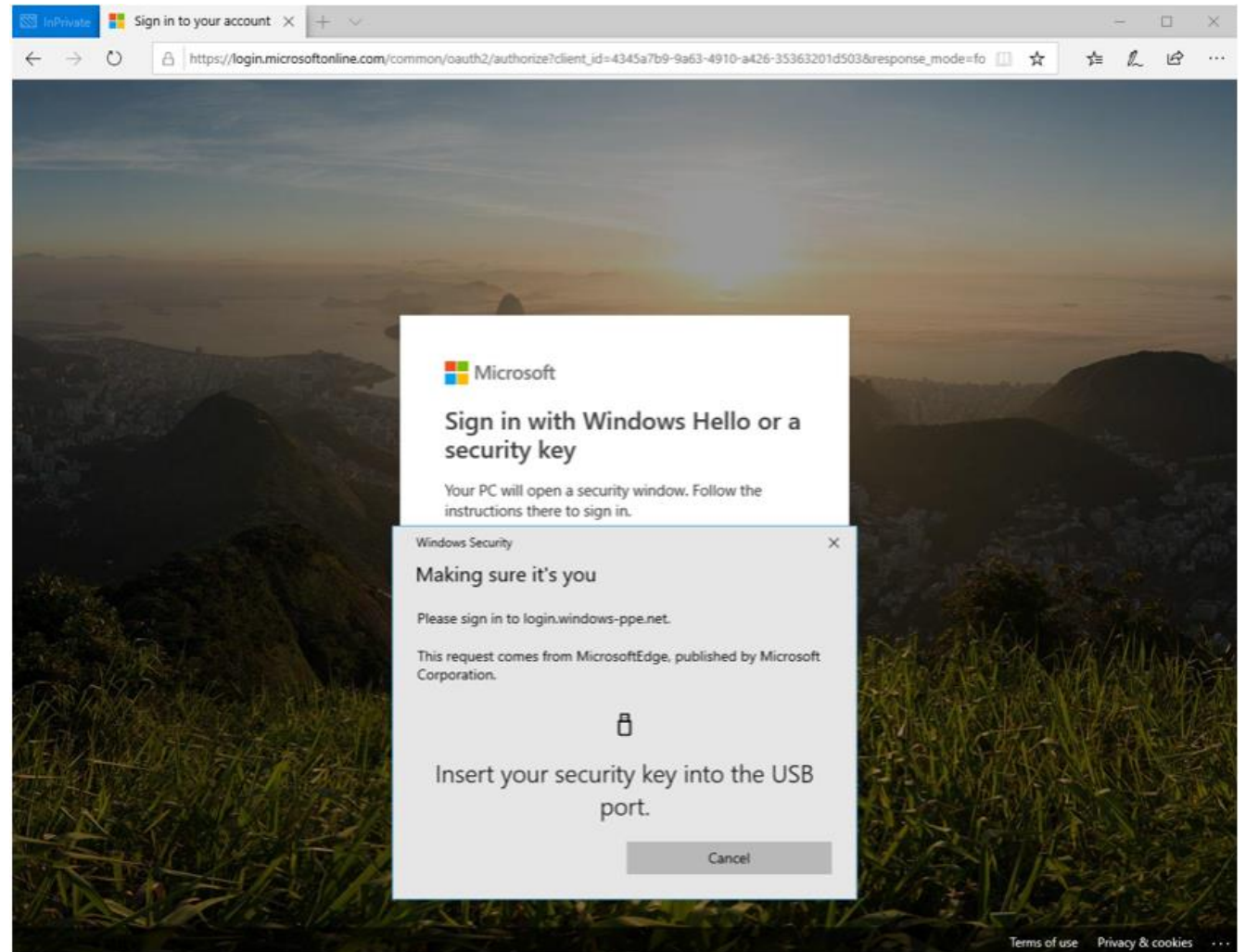
Yubikeys

- Allow ECC keys through GPO.
Not on by default

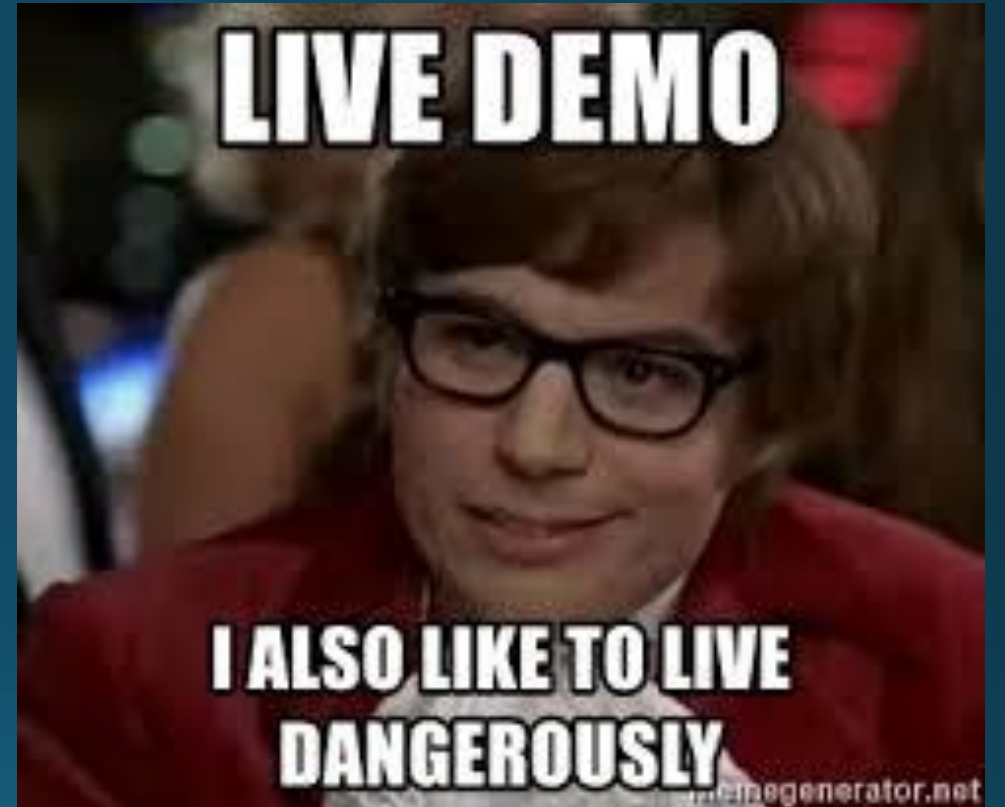
Windows Components/Smart Card	
Policy	Setting
Allow ECC certificates to be used for logon and authentication	Enabled

Bonus Extend to azure (in preview)

- How to enroll
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-o-authentication-passwordless-security-key>
- Works with Yubikey 5



Yubikey Demo



Thank You Derbycon!

