yubico

AD Certificate Services Smart Card Deployment

yubico

Workshop Agenda

Topic	Estimated Duration
Welcome & Introductions	0:05
What is a YubiKey?	0:05
YubiKey as a Smart Card	0:20
Prerequisites and Considerations	0:15
PIV Overview	0:30
Administration	0:15
Use Case Demos	0:10
Resources, Questions, and Wrap-up	0:15
Total	**1:55**

Yubico's Professional Services Team

Deployment Advisors

Molly Babcock

Laura Eppley

Jeff Olives

Engineers

Greg Whitney

Dante Melo

Mitchell Armenta

Kanchan Thakur

Scott Truger

What is a YubiKey?

Technical Overview

Easy, Fast, & Reliable Authentication

YubiKey does not require a battery or network connection.

FIDO2 CERTIFIED

Waterproof

Crush Resistant

YubiKey as a Smart Card

yubico

Why YubiKeys as Smart Cards?

- Durable - waterproof, crush resistant
- Various form factors
- FIPS 140-2 hardware options
- Strong, Password-less Authentication
- Native Microsoft support
- Works for various use-cases
- Simple user experience

YubiKey Smart Card Capabilities

- Smart Card functionality based on the Personal Identity Verification (PIV) interface specified in NIST SP 800-73, (Cryptographic Algorithms and Key Sizes for PIV)
- Performs RSA or ECC sign/decrypt operations using a private key stored on the smart card, through common interfaces such as PKCS#11 (Multi-platform) and a Smart Card Minidriver for Microsoft Windows
- Available on YubiKey 5, YubiKey 5 Nano, YubiKey 5C, YubiKey 5C Nano, YubiKey 5Ci, and YubiKey FIPS

YubiKey Smart Card Capabilities (Cont.)

- Supports 24 key slots on the YubiKey 5 (max per certificate size of 3,052 bytes)
  - Only available when using the YubiKey Minidriver
- Key Slots have different use cases and are assigned functional roles like:
  - PIV Authentication
  - Digital Signature
  - Key Management
- Each slot is capable of holding an X.509 certificate, along with its accompanying private key
- Key support:
  - RSA
  - ECC
- All functionality is available over both USB and NFC interfaces

YubiKey Smart Card: YubiKey Minidriver

- Allows the YubiKey to work as a smart card out-of-the-box on Microsoft Windows Server 2008 R2+ and Microsoft Windows 7+
- Provides certificate and PIN management via the native Windows user interface, support for ECC key algorithms, set touch policy for private key use
- Enrollment from a Windows Certification Authority, based on templates
- Import existing certificate to the YubiKey (including a .pfx file)
- Supports all Windows smart card behaviors, including lock on removal
- Identifies as a YubiKey Smart Card using YubiKey smart card minidriver

What is a Minidriver?

- Software that allows applications to interact directly with a vendor smart card
- A minidriver acts as a software bridge, enabling Windows operating systems to communicate with smart cards like the YubiKey using standard smart card interfaces
- Extends the basic functionality of the YubiKey, allowing Windows to not only recognize it as a smart card but also to manage certificates stored on the device

Prerequisites and Considerations

Prerequisites

This presentation is designed to help with configuring certificate templates, and best practices for an organization that has a PKI environment deployed.

- PKI environment deployed and up to date
- PKI admin available to create certificate templates
- Admin who can deploy YubiKey smart card minidriver

Considerations

Certificates

- Do you want self-enrollment, enroll on-behalf of, or both?
- How long do you want certificates to be valid?
- How do you want the renewal process to be?

Software Deployment

- How will you deploy minidriver and any other desired software?
- Do you want to deploy Yubico Authenticator for user management?

PKI Management and Maintenance

- CA backup and restore
- CA monitoring and reporting

PIV Overview

Registration - the first step to eliminating the dependence on passwords.

What is PIV?

- US Federal government standard for credentials
- Defined in NIST.SP.800-73-4
- Specifies the PIV data model, application programming interface (API), and card interface requirements necessary to comply with the use cases
- In short: a PIV card is a smart card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assure appropriate levels of security
- PIV provides different ways of authentication (card holder, card to server, physical access to facilities, etc, plus data encryption, signature)

PIV Credential Model

PIV logical credentials fall into the following three categories:

1. Credential elements used to prove the identity of the cardholder to the card (PIN)
2. Credential elements used to prove the identity of the card management system to the card (PIV Card Application Administration Key)
3. Credential elements used by the card to prove the identity of the cardholder to an external entity (CHUID, biometric credentials, symmetric keys, and asymmetric keys)

PIV Smart Card Access

- PIV provides two different levels of access:
  - End-user (cardholder) level, which is protected by a PIN. This level allows normal day-to-day usage of the PIV functionality
  - Administrator level, which is protected by a management key. This level allows provisioning of credentials
  - Note: The management key does not need to be changed when using the minidriver
- End-user functionality is guarded by a PIN, which needs to be provided by the user to perform private key operations
- PIN can be up to 8 characters long, and supports any type of alphanumeric characters
- If the PIN is entered incorrectly 3 times consecutively, it will be blocked
- If the PIN is lost or blocked it can be reset using a PUK

Administration

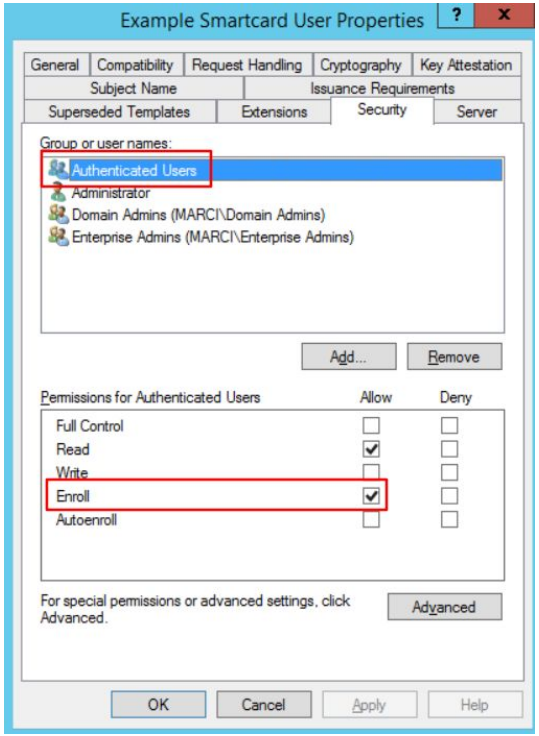
Administrative functions of using YubiKeys as smart cards.

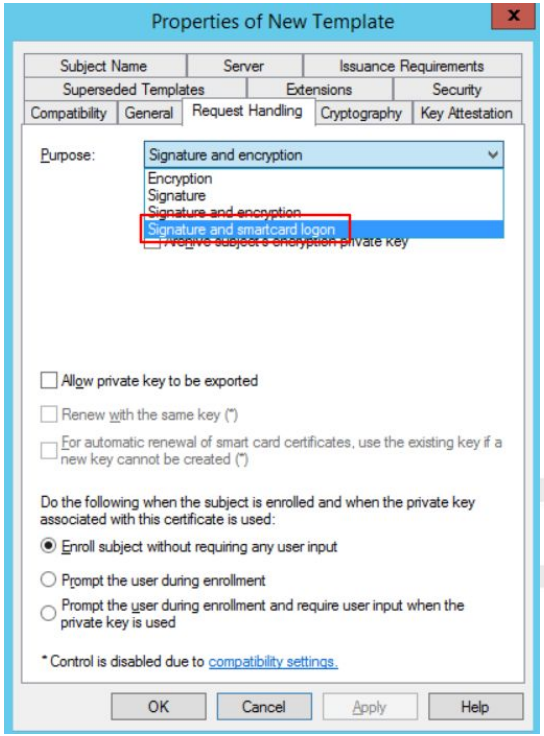
Certificate Templates

- Template enrollment types
  - Self-enrollment
    - Enables users to enroll and renew their own certificates
  - Enroll on-behalf of
    - Enables admins to enroll certificates for users
- Renewal types
  - Automatic renewal
    - More complicated to deploy and support for admins
    - Easier and more seamless for end users
  - Manual renewal
    - Easier to deploy for admins
    - Requires end user training to renew their certificates

Certificate Templates (Cont.)

- Any group granted **Enroll** access can enroll smart cards on YubiKeys
  - For self-enroll **Authenticated Users**
  - For enroll on-behalf **Domain Admins**
- Ensure the purpose is for **Signature and smartcard logon**





Certificate Life Cycle

- Enrollment
  - Available for members of the AD groups assigned Enroll permissions
  - Mechanisms
    - Windows notification prompt
    - Certificate Manager (Personal, certificates, All tasks, Request New Certificate)
- Revocation
  - CA console: Select certificate from Issued Certificates folder, then Revoke
- Renewal
  - Available 6 weeks before expiration
  - Mechanisms
    - Windows notification prompt
    - Certificate Manager (Personal, certificates, All tasks, Renew Certificate)

Machine Level Enforcement

- Once this policy is applied to a workstation no one will be able to login to it with anything but a smart card
- Hard to manage exceptions
- Hard to obtain reports on what users are doing
- Recommended in cases where access is mostly done by admins and there are almost no exceptions
- Users still have a functioning password (that they can use for other machines)
    - This password needs to be managed

User Level Enforcement

- Done on a per-user basis by modifying the "Smart Card Required for Interactive Logon" (SCRIL) user account control flag on the AD user object
- This sets the password to a high entropy 120 character random value (password hash), so that the user does not know the password
- This password hash can be scrambled at will, by flipping the flag off and then flipping it back
- Administrators can reset the user’s password for them and they can use it for network logons

User Support

- Changing a PIN
- Managing loss of YubiKey
  - Certificate revocation, and re-issuance
- Managing forgotten PIN
  - Using PUK

Planning for Enrollment

- Enroll On Behalf
  - Microsoft Management Console (MMC)
  - Enrollment Station
- Self-Enrollment
  - Script
  - Auto-enrollment

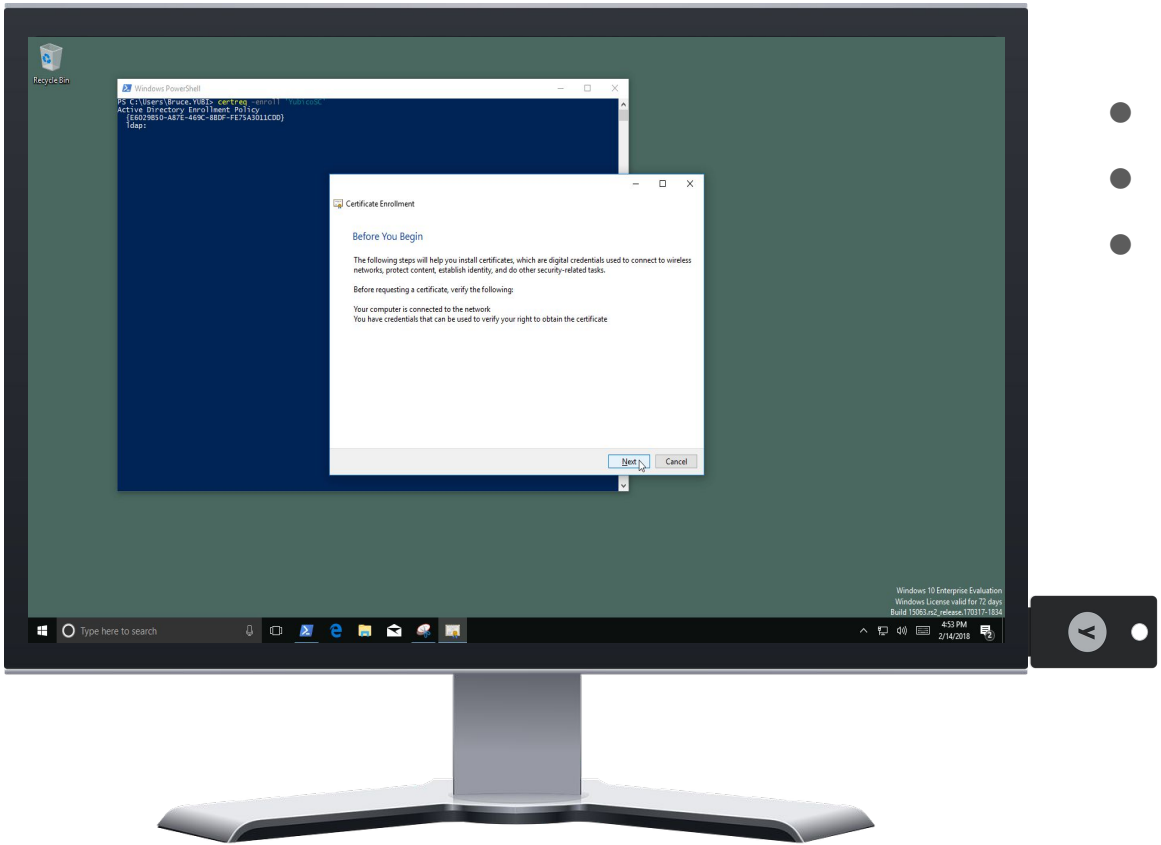
Use Case Demos

Using and managing YubiKeys beyond Windows logon

Use Case Demos Overview

- User Self-Enrollment
  - Smart card enrollment steps for user
- Auto-Enrollment
  - How the auto-enrollment process will look for users
- Remote Desktop
  - RDP with smart card authentication
- Offline Logon
  - Logging in with smart card not connected to the network
- Web App Support
  - Logging into web applications with smart cards
- Change PIN
  - How to change a smart card PIN on Windows
- Revoke Access
  - Revoking a certificate for authentication

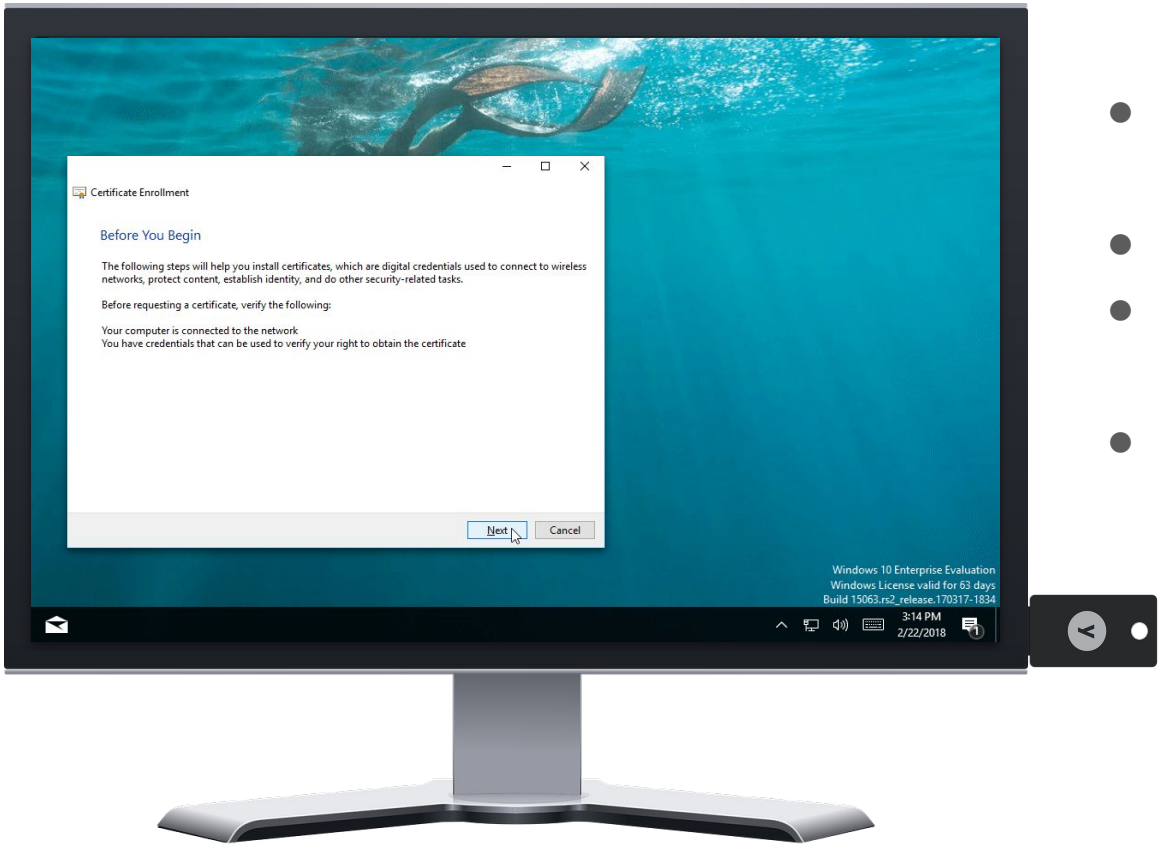
User Self-Enrollment



- User driven enrollment
- Enroll when ready
- Simple, just a few steps

yubico

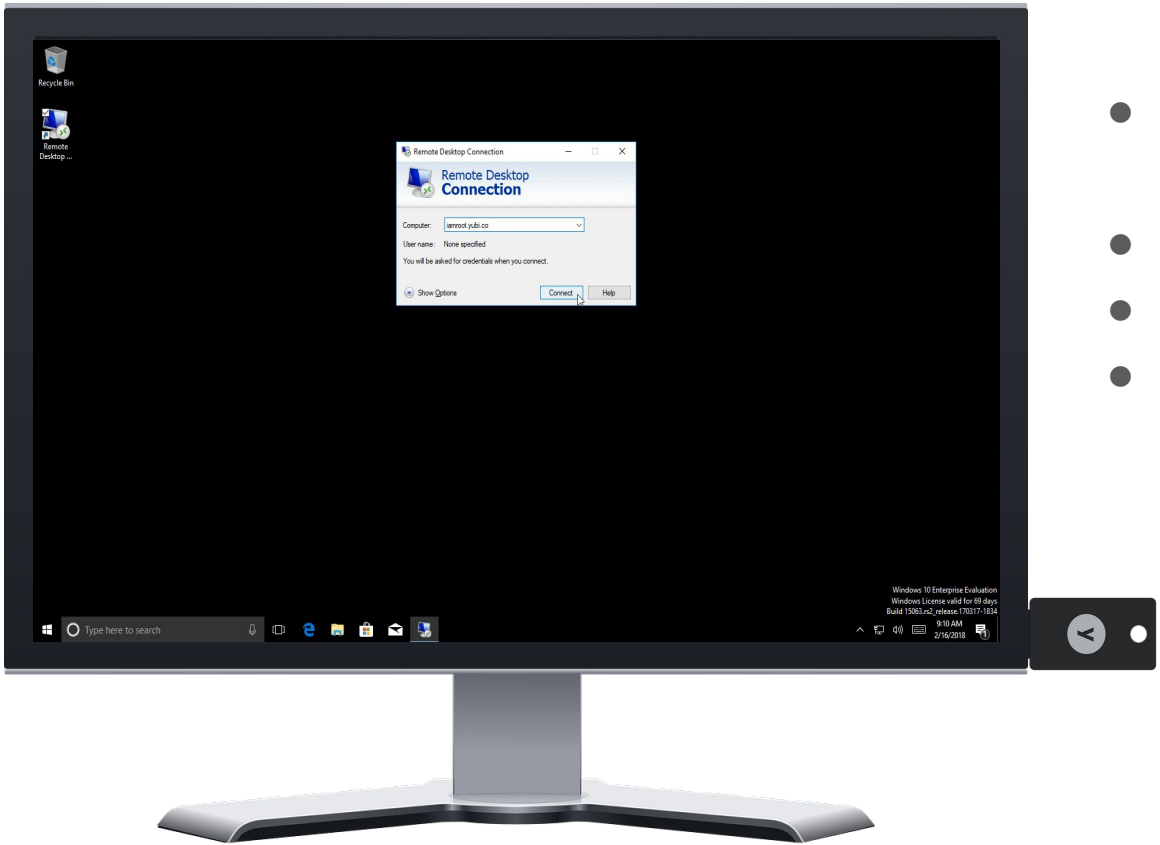
Auto-Enrollment



- Triggered enrollment (e.g. at log on)
- Windows prompts user
- Target specific groups or devices (GPO)
- Quick and easy

yubico

Remote Desktop



- Strong auth for remote user access
- Secure privileged users
- Protect server access
- **Note**: This does require installing the minidriver on the remote machines with the legacy node option.

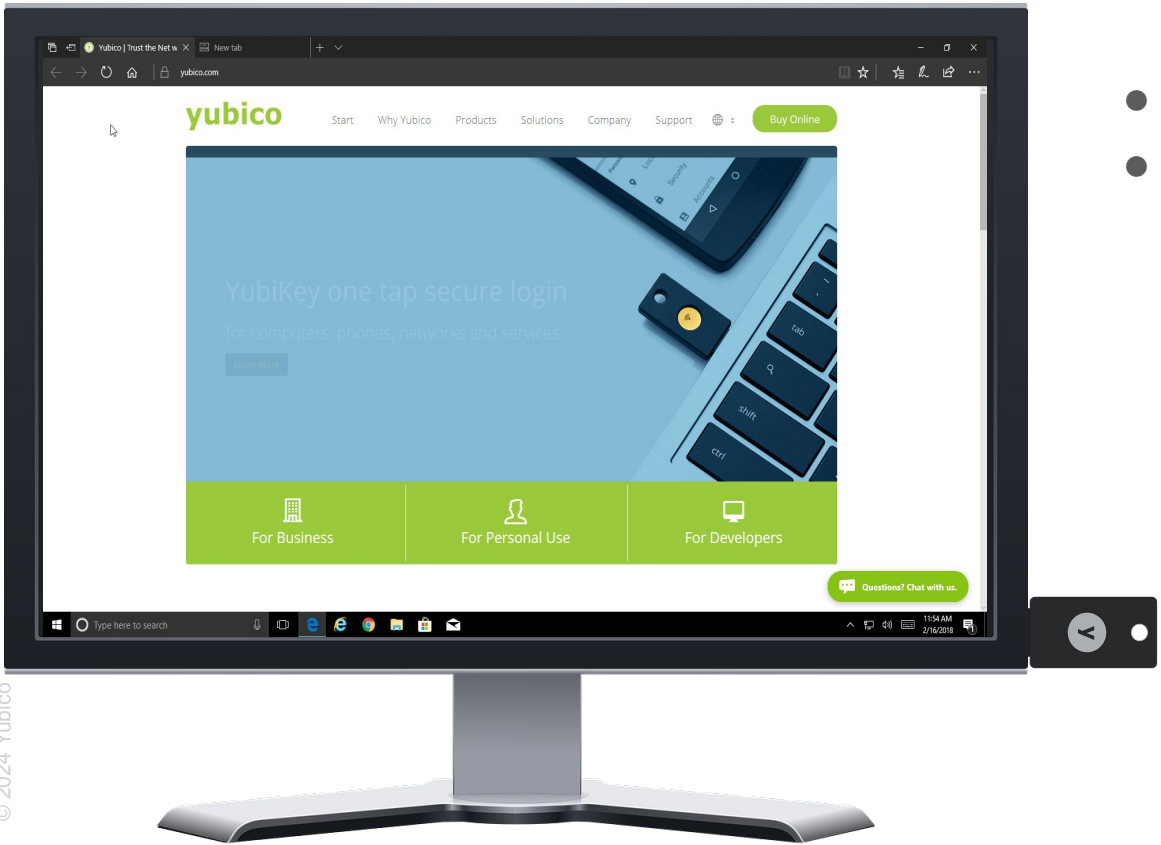
yubico

Offline Logon

- Strong auth in intermittent/limited connectivity scenarios

yubico

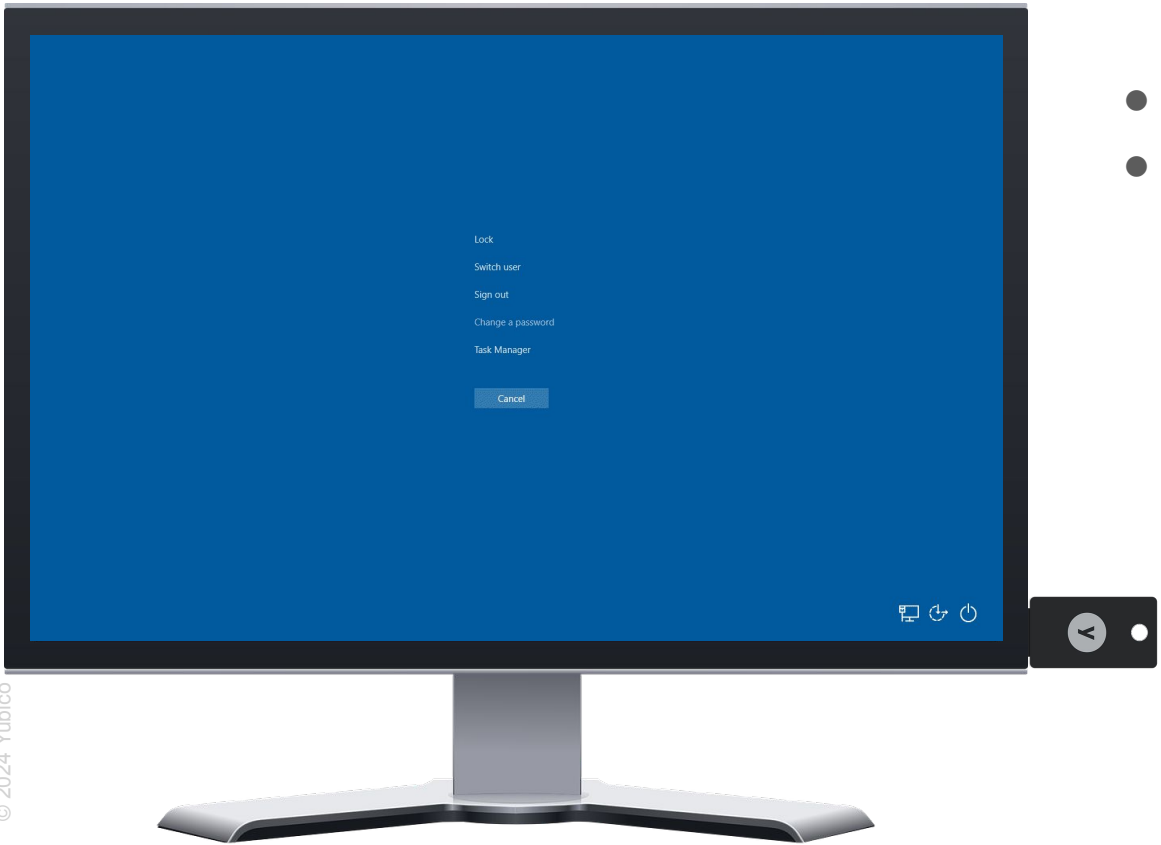
Web App Support



- Strong auth to web apps
- Single-sign on experience using SAML and ADFS

yubico

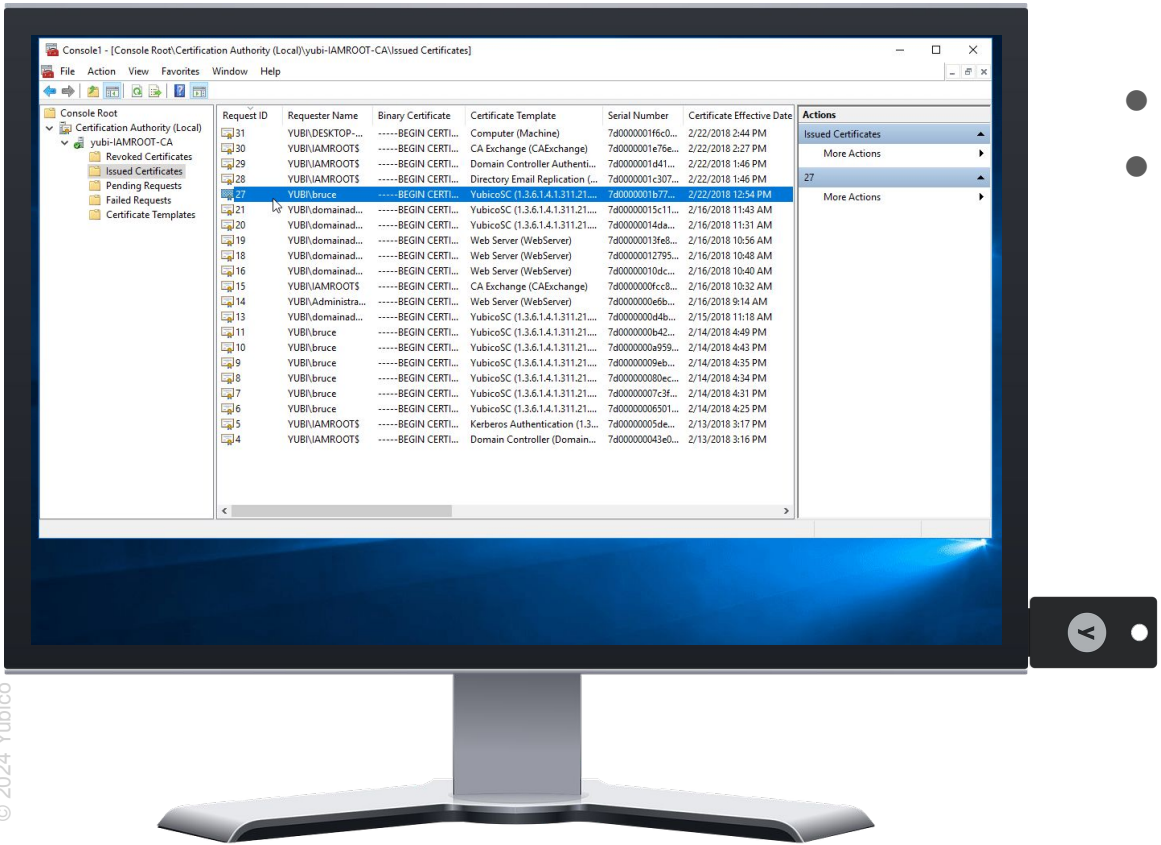
Change PIN



- Native GUI support
- Optional, scripting with Yubico tools

yubico

Revoke Access



- Native GUI support
- Script with PowerShell

yubico

Resources, Questions, and Wrap-up

Yubico Smart Card Resources

- YubiKey as a Smart Card Overview
- Smart Card Drivers and Tools
- Smart Card Documentation and Guides