Quest ONE IDENTITY ccess

# Card

## The problems it solves (and the ones it doesn't)

Quest Software/One Identity

Dan Conrad – Federal CTO

# Disclaimer

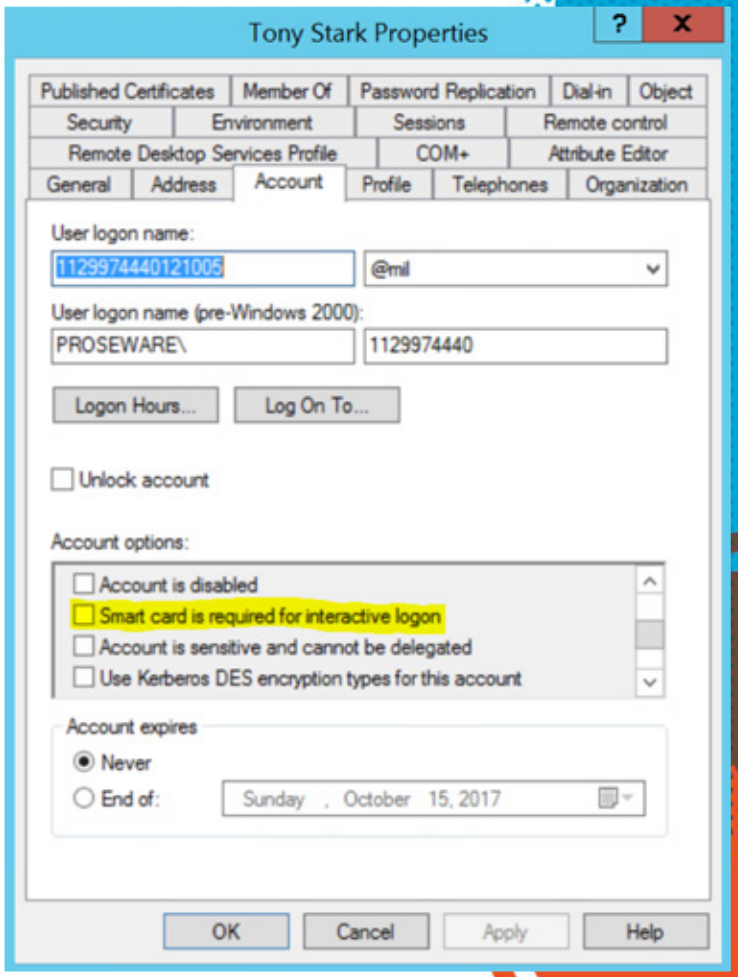
The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

# Open discussion topics

- The Common Access Card and Active Directory (specifically)
- Before CAC – how did we function?
- Why CAC – the vulnerabilities it eliminates
- The vulnerabilities we think it eliminates but doesn't

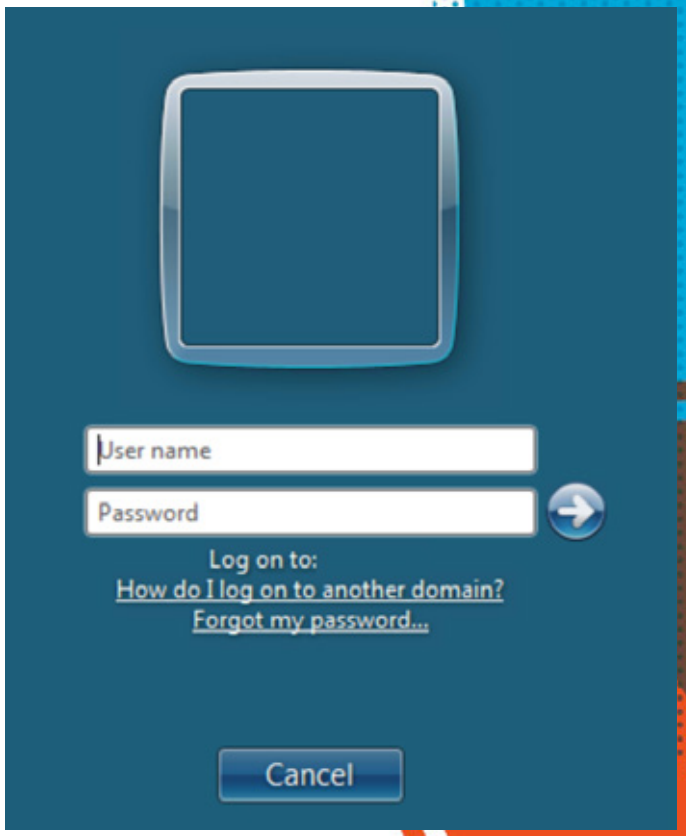
# The CAC and AD

- What we're **not** talking about
  - 3rd party external applications
  - Web applications
  - Anything outside of Active Directory authentication
- We **are** talking about
  - Active Directory authentication
  - What happens in Active Directory



# Before CAC..... If you can remember

- Ah. The passwords we've seen.



# Why CAC? A short history

- Significantly reduced vulnerability of user impersonation compared to username/passw nonrepudiation
- Holds encryption certificates for secure communication (email)
- Used for physical security access control
- Certificate based authentication provides single point to **revoke logical access**
- Prevent password compromise via Phishing attacks

# Where we are today

- CAC enabled/forced ALL of users
- MFA, alternate tokens for ALL administrato

So all passwords are gone.  Except for

# All passwords are gone, except for…

- Service accounts, local accounts, routers, switches, firewalls, appliances, DRACs, ILOs, etc

And…

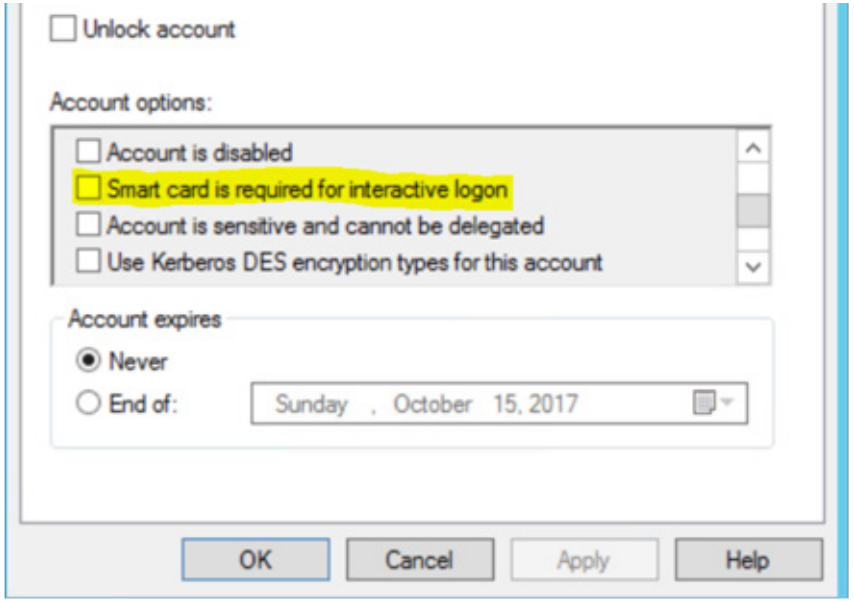
- ALL Active Directory user accounts

# Smart Card…

- Enabled
- Enabled/Enforced
- Enabled/Enforced…. But knows password

# An over examination of ….

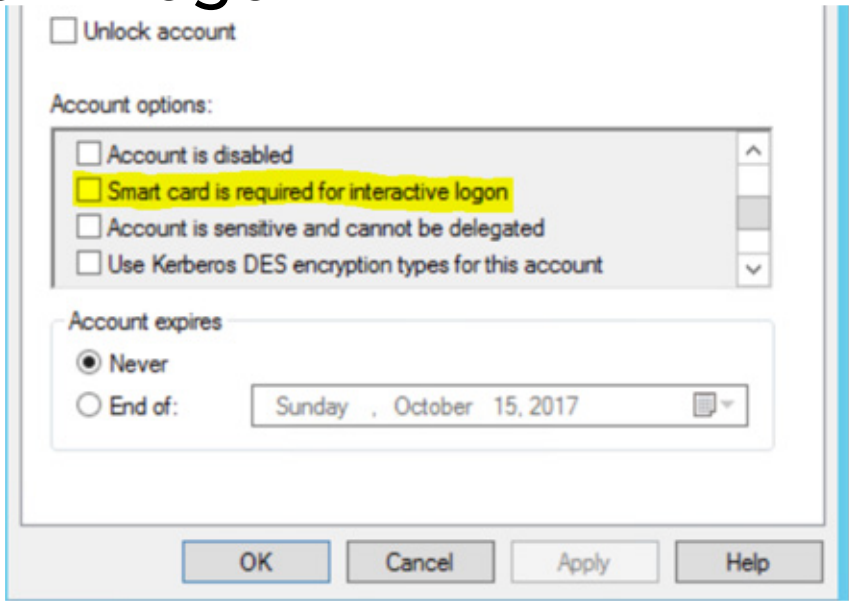
"Smart card required…  a.k.a "SCRIL"




Sometimes, what it **doesn't** say is more important.

# What it doesn't say

- Doesn't say ..
  - "Smart card required for **Authentication**"
  - "Smart card required for **Network Logon**"



# There's more than one logon type?

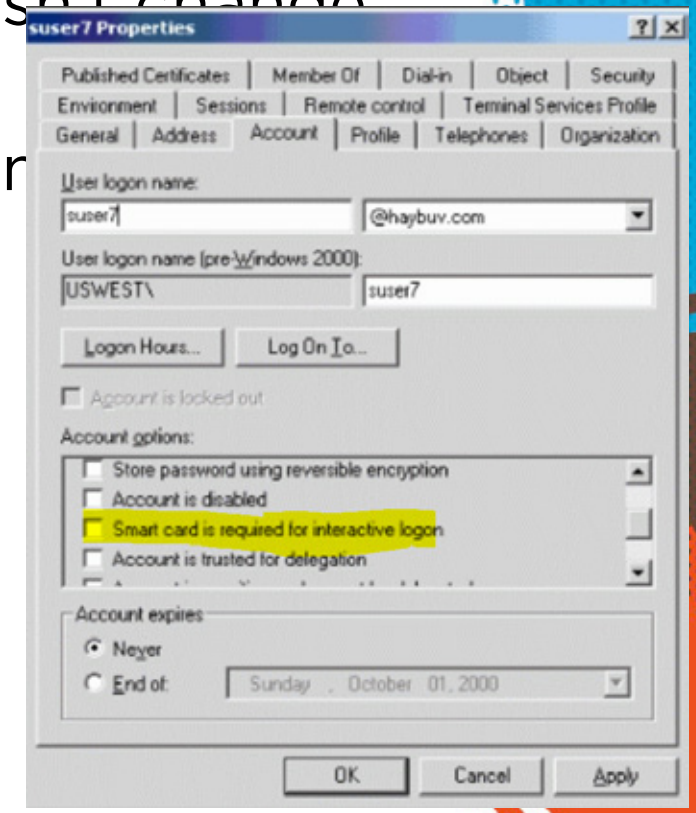
Here's the one SCRIL addresses

- Logon Type 0 = System Only
- Logon Type 1 = *unknown*
- Logon Type 2 = Interactive Logon
- Logon Type 3 = Network
- Logon Type 4 = Batch
- Logon Type 5 = Service
- Logon Type 6 = (proxy logon)
- Logon Type 7 = Unlock Workstation
- Logon Type 8 = Network Clear Text
- Logon Type 9 = New Credentials
- Logon Type 10 = Remote Interactive
- Logon Type 11 = Cached Interactive
- Logon Type 12 = CachedRemoteInteractive
- Logon Type 13 = CachedUnlock

Here's the one used for PtH exploit

# The “Smart Card Required” vulnerability

- When “SCRIL” is checked
  - NTLM hash doesn’t expire since password doesn’t change
  - A problem for standard user accounts?
  - Serious problem with elevated privilege accounts

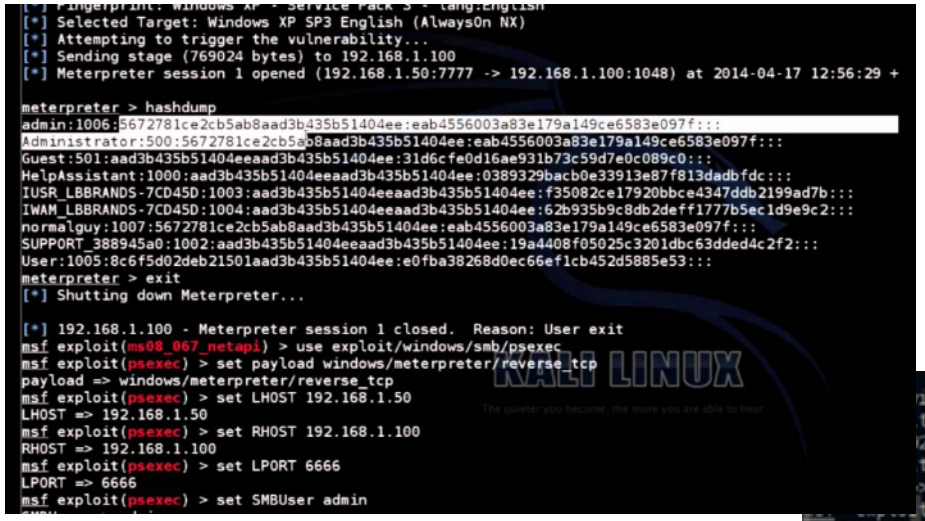


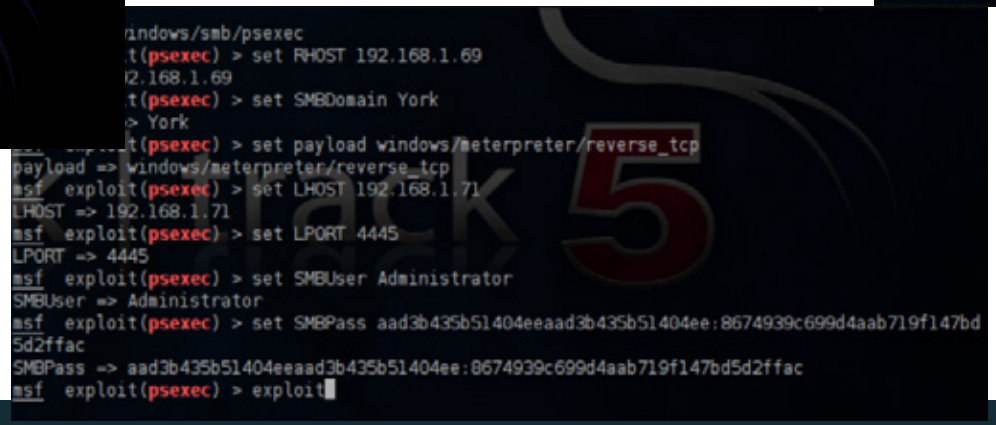
# From Microsoft

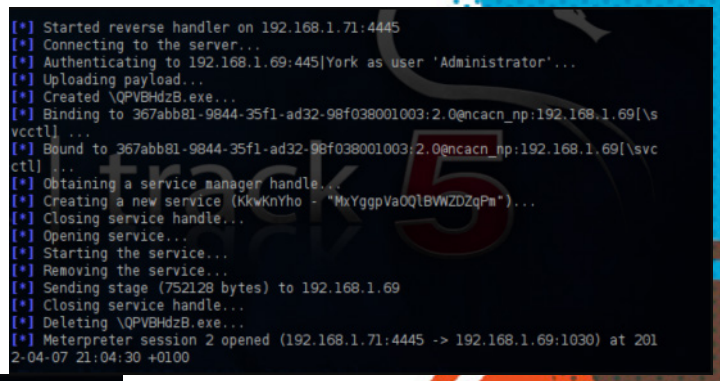
- Ticking the ‘Smart Card is required for interactive logon checkbox for a user resets the password for that user to a random complex password that is unknown to anyone and the UserAccountControl attribute of the user gets the flag SMARTCARD_REQUIRED added to it.
- In addition to this, the DONT_EXPIRE_PASSWORD flag on the account is set so that the user’s password never expires. The GINA or LogonUI components on the client check for the presence of the SMARTCARD_REQUIRED flag during an interactive logon (console or RDP) and reject the logon if it isn’t made with a smartcard when it is set for the user.

# We thought we fixed this

- Pass-the-hash https://pentestlab.blog/2012/04/08/pass-the-hash-attack/

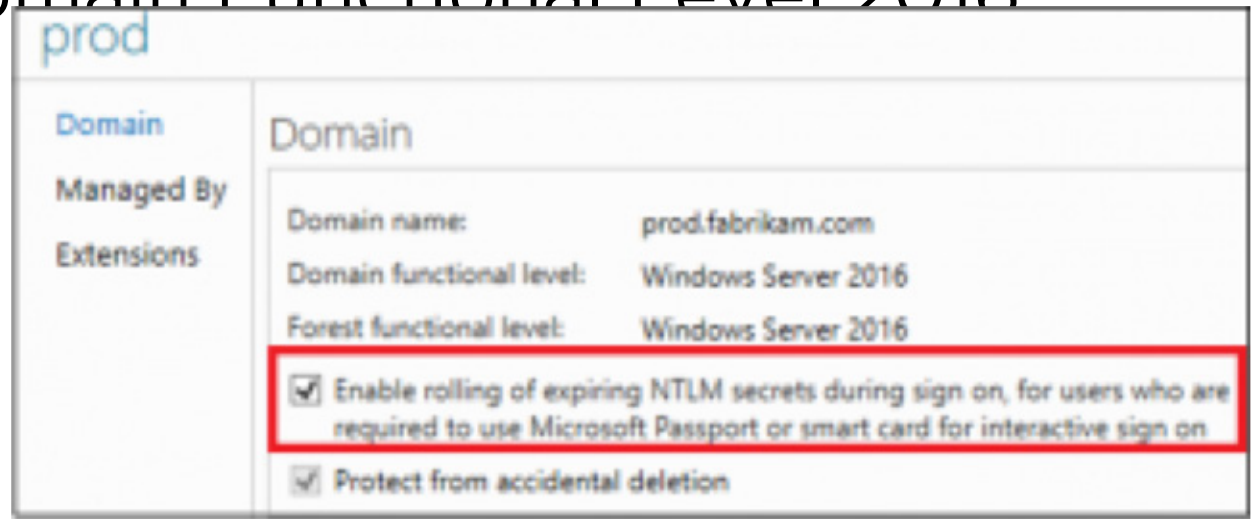


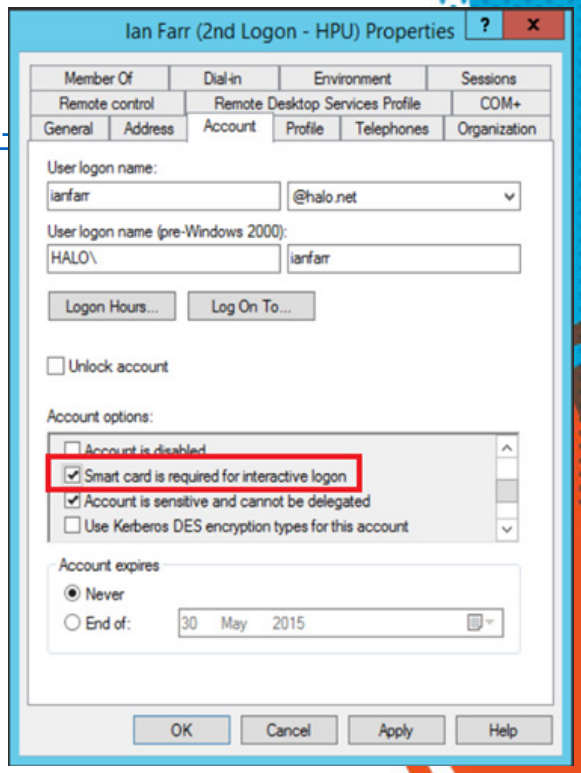



# Mitigations for the CAC Vulnerability

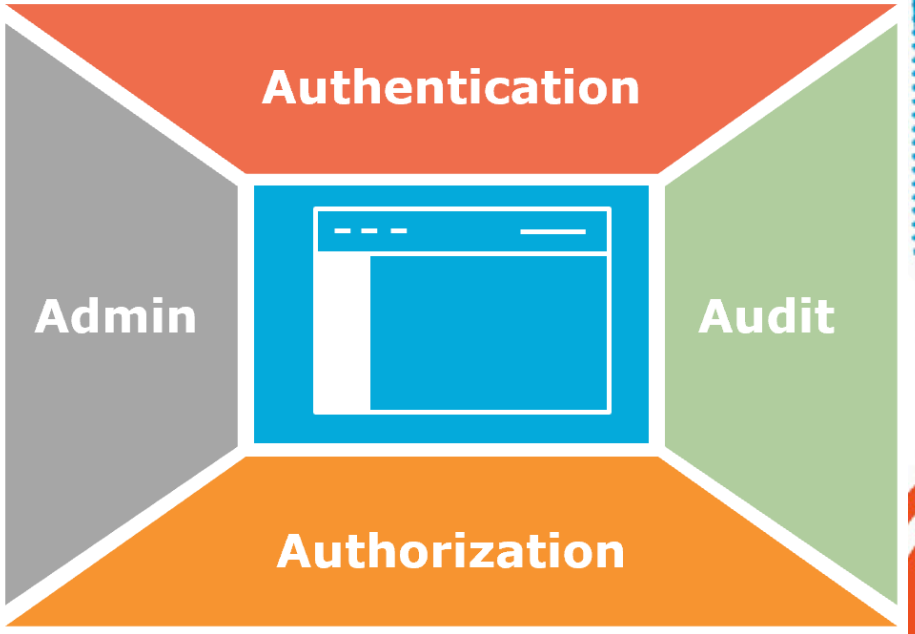
- Combination of Forest Functional Level and a strong password policy
  - https://secureidentity.se/expire-passwords-on-smart-card-only-accounts/
  - https://blogs.technet.microsoft.com/positivesecurity/2017/05/17/smartcard-and-pass-
  - Script to check and uncheck SCRIL
- Domain Functional Level 2016



# How does this effect accounts with elevated privileges?

- Service  Accounts
- Privileged users
- Local accounts
- SCRIL users
- nonWindows systems



# Using a Privileged Account Management solution

- Manages passwords for any system which changes the hash
- CAC-enabled check out = nonrepudiation
- Purpose built for security
- Hardened appliance

**Hardened Appliance**

One Identity Provides

| | |
|---|---|
| Hardware | BIOS pre-secured |
| | Hard disk encryption enabled |
| | TPM used for key storage |
| System Software | System software pre-installed |
| | Pre-hardened |
| | No middleware or patching maintenance |
| | No malware or virus care needed |
| Application Software | Embedded OS |
| | Backup/restore |

ONE IDENTITY

## Access Management

### CHALLENGES

- Managing and securing hybrid Active Directory environments
- Streamlining the IT workload for user lifecycle management
- Unifying user logons and strengthening authentication
- Password management
- Secure remote access

### KEY PRODUCTS

- **Active Roles** – overcome the shortcomings of native tools to streamline AD and AAD user and group administration and increase security over administrator access in the hybrid AD environment
- **Cloud Access Manager** – Web access management, single sign-on and federation along with secure remote access and adaptive risk-based security
- **Password Manager** – self service password resets, granular password policy, and helpdesk automation for AD and beyond
- **Enterprise Single Sign-on** – single sign-on and security for legacy applications
- **Defender** – flexible, affordable, and powerful multifactor authentication

## Identity Governance

### CHALLENGES

- Unifying enterprise provisioning
- Quickly embrace the move to the cloud
- Enabling users and the line-of-business
- Governance for access, data, and privileged accounts
- Adaptive risk-based security

### KEY PRODUCTS:

- **Identity Manager** – enterprise provisioning and governance including end-to-end identity lifecycle management, line-of-business self-service, attestation/recertification, process orchestration, and rapid response to changing requirements
- **Identity Manager – Data Governance Edition** – governance, request, and fulfillment for unstructured data including file shares, SharePoint, and other sources
- **Connect for Cloud** – easily extend the capabilities of One Identity Manager to cloud-based applications and services without heavy programing and onerous integration burdens

## Privileged Management

### CHALLENGES

- Assigning individual accountability to administrator access and activities
- Eliminate password sharing
- Audit activities performed with elevated credentials
- Enforce separation of duties (SoD)

### KEY PRODUCTS:

- **Privileged Password Manager** – password vaulting for any elevated credential with powerful workflows, approvals, and automation including service accounts, A2A, and A2DB access scenarios on an ultra-secure appliance
- **Privileged Session Manager** – Session audit for activities performed via Privileged Password Manager
- **Privileged Access Suite for Unix** – Active Directory bridging, Unix/Linux root delegation, and sudo management

TECH BRIEF

The Department of Homeland Security program, Continuous Diagnostics and Mitigation (CDM), is one of the most significant advancements in cybersecurity by the federal government. If you haven't heard of it, here's how it is described on the DHS web site: "The CDM program is a dynamic approach to fortifying the cybersecurity of government networks and systems." Despite this program delivering tools and technologies necessary to protect sensitive information and enable access to essential government services, one of the

TECH BRIEF

Managing th
Privileged A
Privileged P
Civilian Age

Reduce Risk while St
Administrative Workf

**Abstract**

Even IT environments that have two-factor authentication in place must still deal with many different types of passwords: service account, local account, Windows local administrator and Unix/Linux root account passwords. Managing them in a way that meets requirements can be a tedious full-time job, and can make even a "simple" job, like applying a hotfix, a complex, multi-step process that introduces far too much risk.

With One Identity Privileged Password Manager and Priv Session Manager from One I managing privileged passw is easy and far more secure white paper explains how.

**Introduction**

**Why civilian agencies are adopting two-factor authentication**

Civilian agencies have come long way with authenticatio Instead of allowing users to authenticate with just user and passwords, organizatio

TECH BRIEF

Managing the R
Privileged Acco
Privileged Passv
Defense Organi

Reduce risk while streamlin administrative workflows

**Abstract**

Even IT environments that have two-factor authentication in place must still deal with passwords: service account passwords, local account passwords, Windows local administrator passwords and Unix/Linux root account passwords. Managing them in a way that meets requirements can be a tedious full-time job and can make even a simple job, such as applying a hotfix, a complex, multi-step process that introduces far too much risk.

With One Identity Privileged Password Manager and Privileged Session Manager, managing privileged passwords is easy and far more secure. This white paper explains how.

**Introduction**

**Even with two-factor authentication in place, passwords still present challenges.**

The Defense community has come a long way with authentication. Instead of allowing users to authenticate with just user names

administrative functions. This provides a solid level of assurance of who the users are and ensures non-repudiation.

ONE IDENTITY

TECH BRIEF

# How does the DoD protect its authentication infrastructure?

Use these recommendations and highlighted product features to find the ideal solution for your organization

**Introduction**

The Department of Defense operates some of the largest Active Directory (AD) infrastructures in the world. Some of them are dispersed across multiple forests while others are centralized. Like commercial organizations, the military relies heavily on AD to provide authentication to desktops, applications, collaboration sites and many other mission-critical resources.

The DoD Common Access Card (CAC) has added a layer of multifactor security to ensure that this AD authentication can be trusted. Since AD is, by far, the largest authenticator for the DoD, it is imperative that the administration of AD is vigilantly executed with unwavering commitment to policies.

**The importance of rules and policies**

The accounts and privileges in AD are key targets for the

'bad actors' looking to exploit the privileged accounts and the resources they manage. While securing and controlling AD for any size organization can be a challenge, many DoD organizations have chosen to consolidate directories in an effort to wrap more controls around fewer directories. Obviously, managing fewer directories creates fewer targets and therefore should be easier to control and secure, but if weak controls and policies

ONE IDENTITY