

PROTECT TOKENS WITH INTUNE & CONDITIONAL ACCESS

ARNO VAN DIJK

SECURITY MEETUP 18-09-25



INHOUDSOPGAVE

- 1 Onderwerp 2
- 2 Onderwerp 4
- 3 Onderwerp 6
- 4 Onderwerp 8

TOPICS

- WHOAMI
- Wat is een Token
- Wat is Token Theft
- Standaard Windows Setting
- Intune Settings
- Conditional Access Settings
- Key Take Aways

WHOAMI

WORK

- Arno van Dijk
- Tribelead Workspace @RawWorks
- MVP Microsoft Intune
- Microsoft Certified Trainer
- Blogger: xplorethecloud.nl

NON-WORK

- Samenwonend in Enschede
- 2 kinderen + 1 onderweg ;)
- Klushuis, Bierbrouwen, Lego, Familie



WAT IS
EEN
TOKEN?



WAT IS EEN TOKEN?

Access tokens in the Microsoft identity platform

05/14/2025

Access tokens are a type of security token designed for authorization, granting access to specific resources on behalf of an authenticated user. Information in access tokens determines whether a user has the right to access a particular resource, similar to keys unlocking specific doors in a building. These individual pieces of information that make up tokens are called claims. Therefore, they are sensitive credentials and pose a security risk if not handled correctly. Access tokens differ from **ID tokens** which serve as proof of authentication.

WAT IS EEN TOKEN



Persoon &
Ticket

+



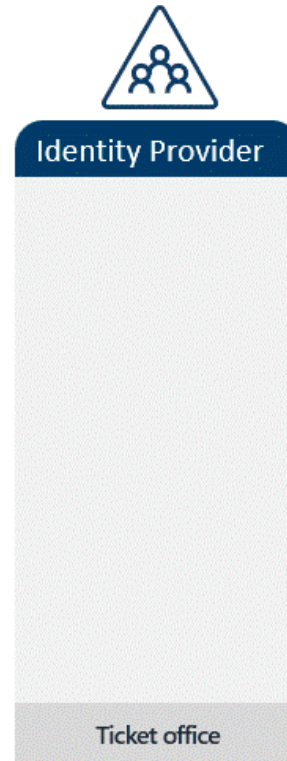
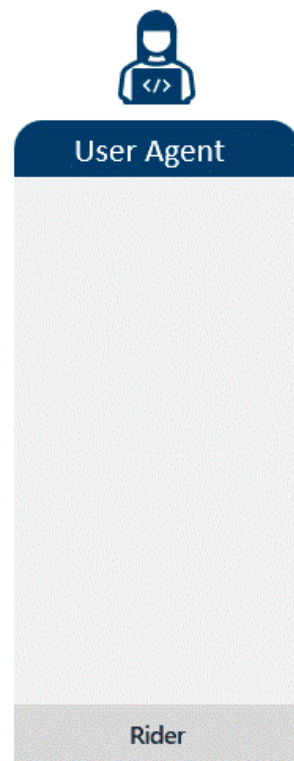
Locatie & Controle

=



Toegang

WAT IS EEN TOKEN?



TOKENS ENTRA ID SIGN-IN LOGS

Activity Details: Sign-ins



Token Protection - Sign In Session Bound

Basic info

Location

Device

Service principal name

Date

Resource service principal ID

Request ID

Unique token identifier

Correlation ID

Token issuer type

Microsoft Entra ID

Authentication requirement

Token issuer name

Agent Type

Incoming token type

Primary refresh token

Status

Authentication Protocol

None

Continuous access evaluation

Additional Details

Latency

78ms

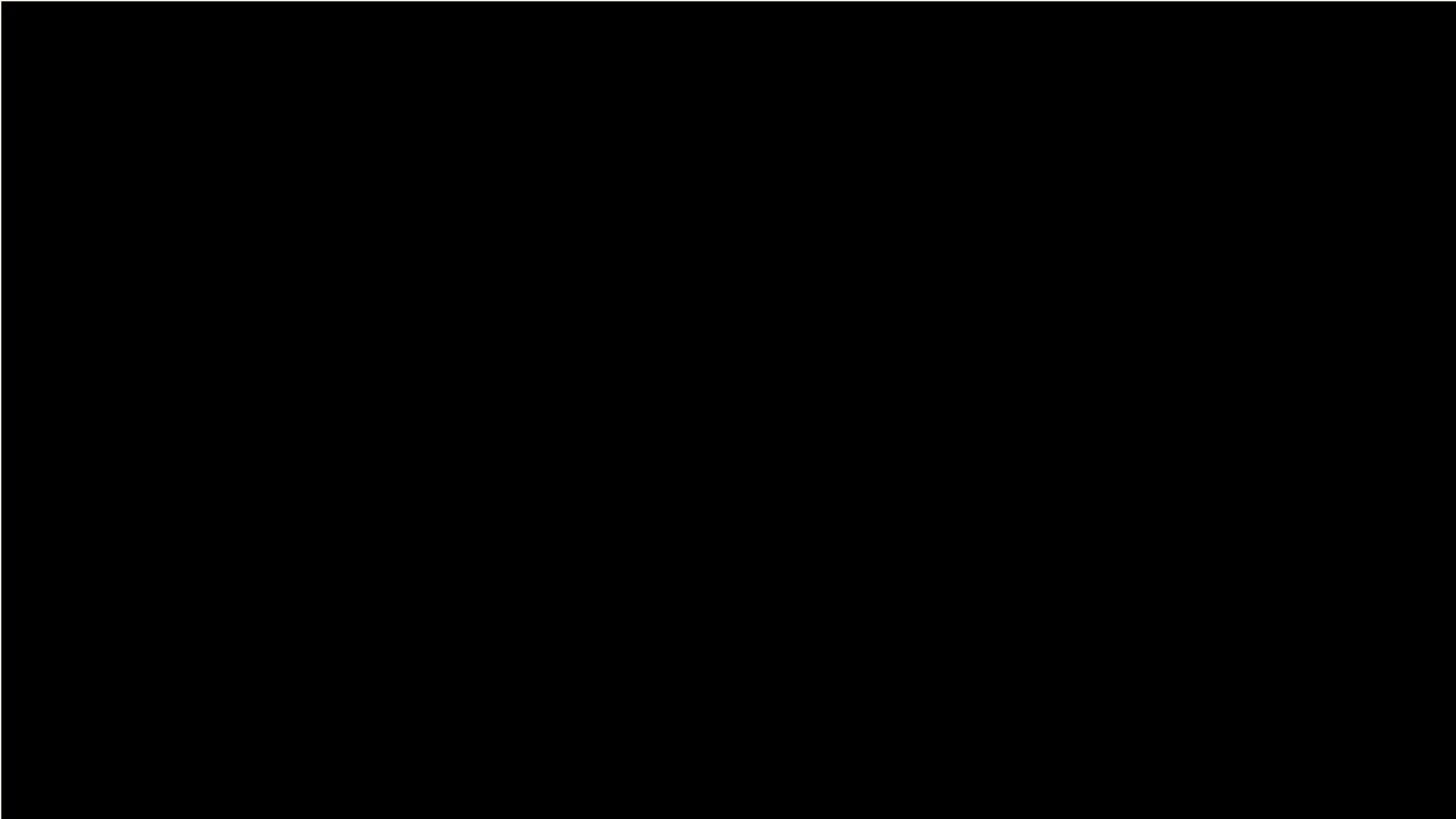
Flagged for review

No

User agent

Windows-AzureAD-Authentication-Provider/1.0

TOKENS ENTRA ID SIGN-IN LOGS (SHORT WALKTHROUGH)





TOKEN THEFT

- TOKEN THEFT
- METHODES
- LIFETIME TOKEN

WAT IS TOKEN THEFT

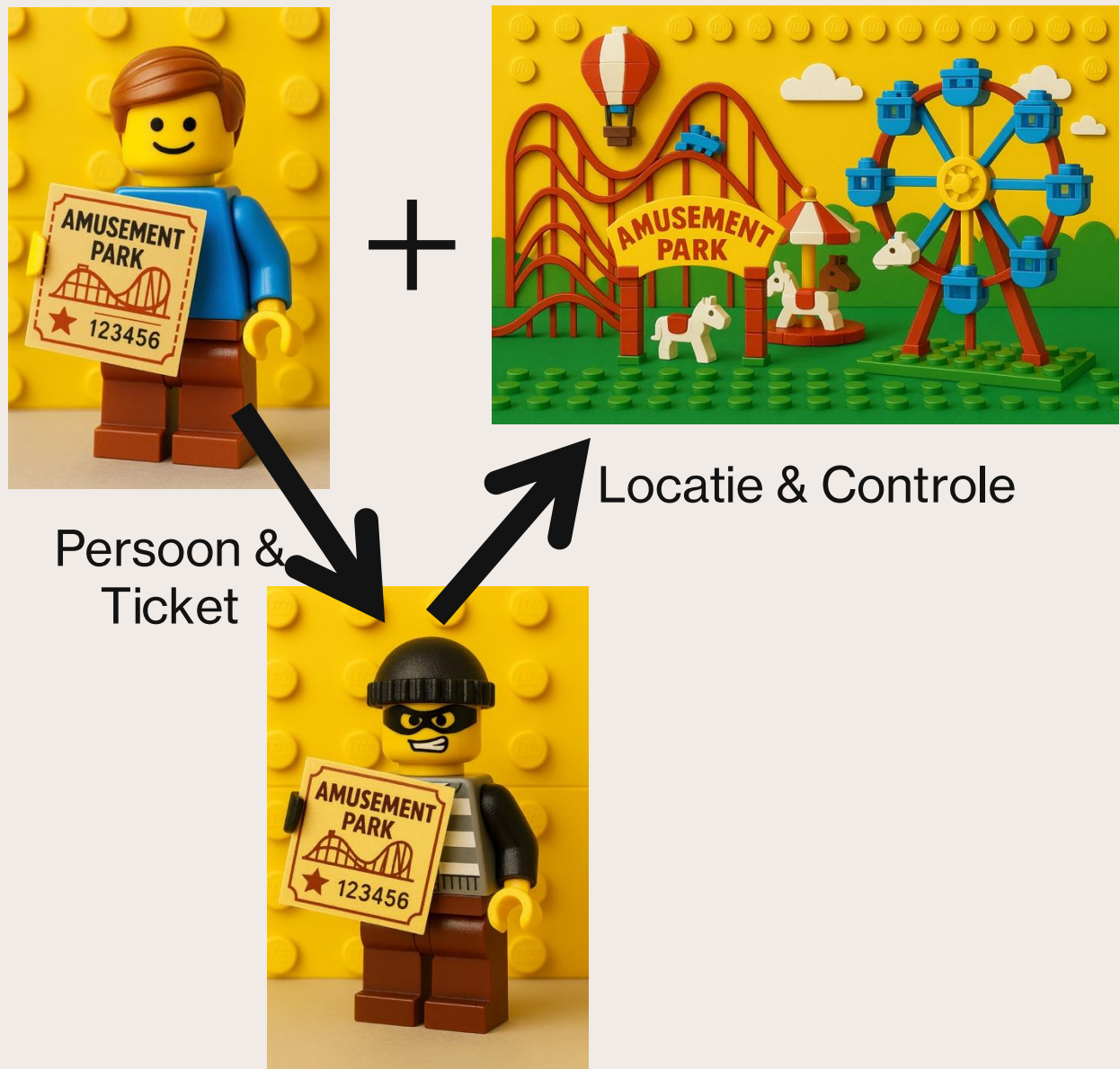
Token theft playbook

03/07/2024

This article, and its accompanying [decision tree](#), provide guidance for security analysts and incident responders to identify and investigate token theft attacks in an organization. As organizations increase their security posture, threat actors use more sophisticated techniques to compromise resources. Quick response is needed to investigate, contain, and remediate damage resulting from token theft attacks.

A token theft attack occurs when threat actors compromise and replay tokens issued to a user, even if that user has satisfied multifactor authentication. Because authentication requirements are met, the threat actor is granted access to organizational resources by using the stolen token.

WAT IS TOKEN THEFT?



=



Toegang

TOKENTHEFT METHODES

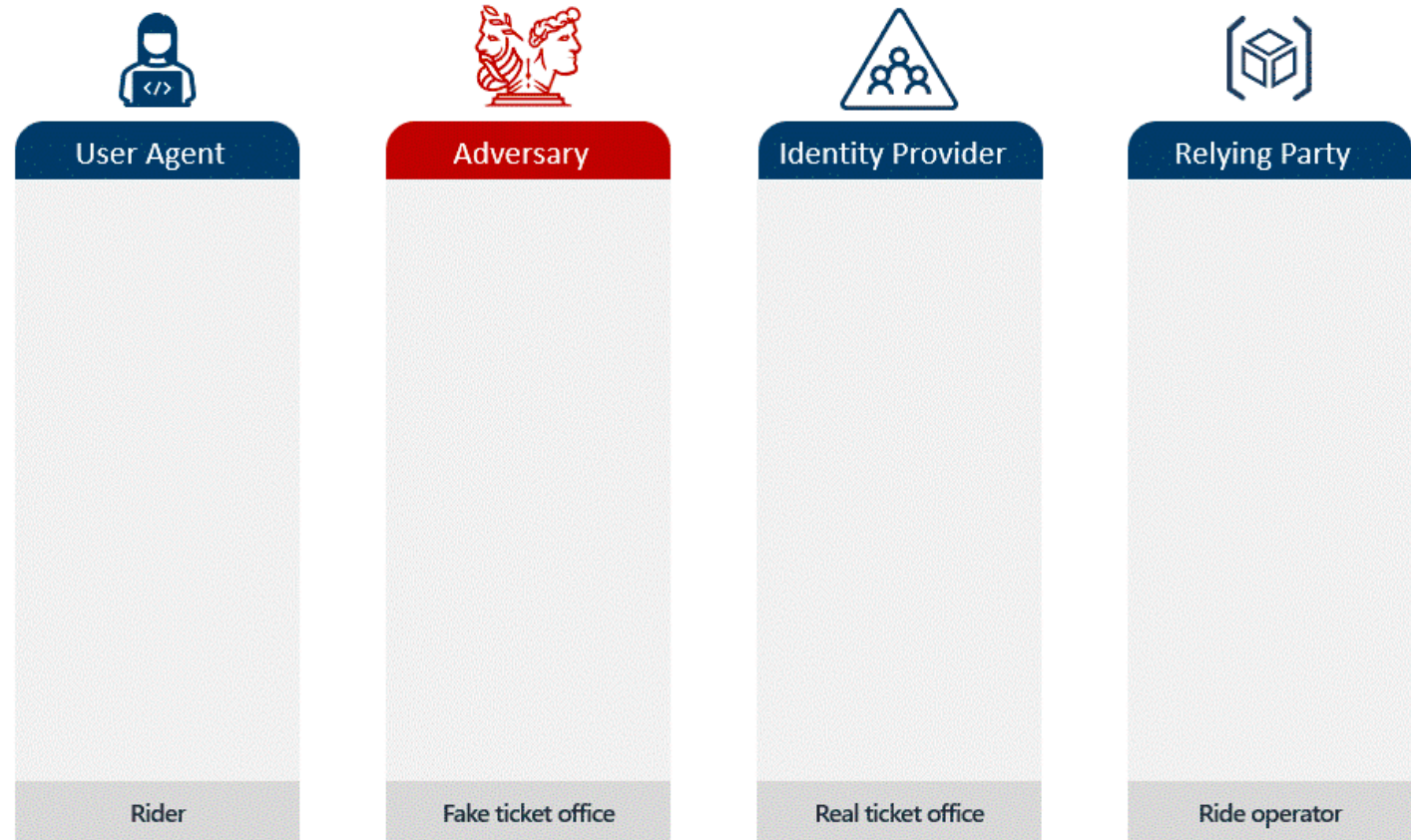
Malware



User

TOKEN THEFT METHODS

AiTM
(Adversary-in-the-Middle)



LIFETIME TOKENS

Token Type	Issued by	Purpose	Scoped to Resource	Lifetime	Revocable	Renewable
Primary Refresh Token (PRT)	Entra ID	Request Access Tokens	No – Can request an access token for any resource	14 days*	Yes	Yes
Refresh Token	Entra ID	Request Access Tokens	Yes	90 days*	Yes	Yes
Access Token	Entra ID	Access the resource	Yes	Variable 60-90 minutes	Yes, if CAE capable	No
App auth cookie	Web app	Access the resource	Yes	Determined by application	Depends on application	No

Source: <https://learn.microsoft.com/en-us/entra/identity/devices/concept-tokens-microsoft-entra-id>

STANDAARD WINDOWS SETTING

- CREDENTIAL
GUARD
- LOCAL SECURITY
AUTHORITY (LSA)
- WALKTHROUGH



CREDENTIAL GUARD – DEFAULT SETTINGS

Starting in Windows 11, 22H2 and Windows Server 2025, VBS and Credential Guard are enabled by default on devices that meet the requirements.

*The default enablement is **without UEFI Lock**, thus allowing administrators to disable Credential Guard remotely if needed.*



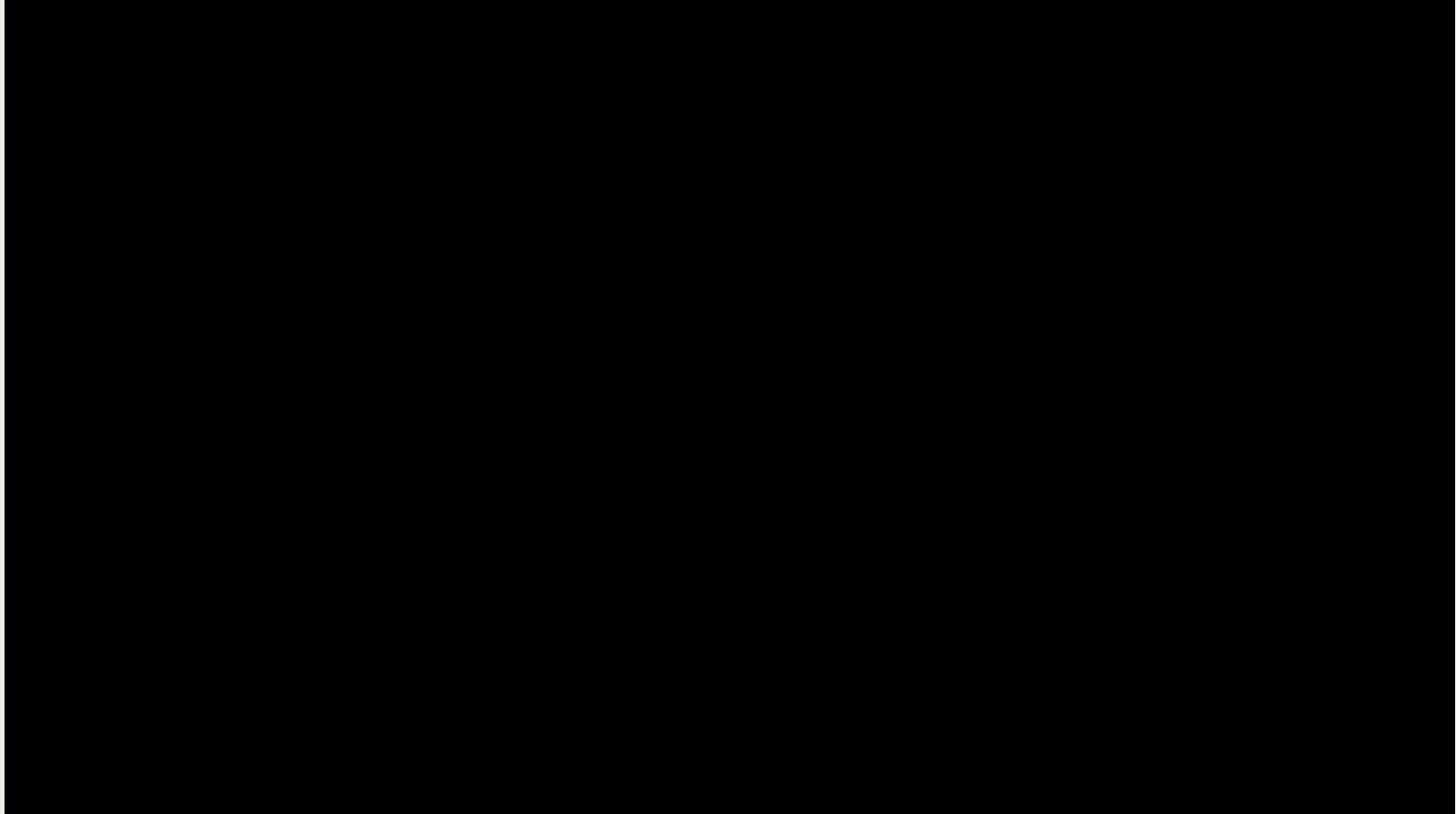
LOCAL SECURITY AUTHORITY – DEFAULT SETTTINGS

*Automatic enablement of added LSA protection on Windows 11 version 22H2 and later **doesn't set a UEFI** variable for the feature. If you want to set a UEFI variable, you can use a registry configuration or policy*



LOCAL SECURITY AUTHORITY – DEFAULT SETTTINGS - WALKTHROUGH

DISABLE & ENABLE
MET REGISTER









INTUNE SETTINGS

- CREDENTIAL GUARD

TOKEN THEFT PROTECTION – CREDENTIAL GUARD

Credential Guard overview

02/25/2025 •

Applies to:  Windows 11,  Windows 10,  Windows Server 2025,  Windows Server 2022,  Windows Server 2019, 
Windows Server 2016

Credential Guard prevents credential theft attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets (TGTs), and credentials stored by applications as domain credentials.

Credential Guard uses [Virtualization-based security \(VBS\)](#) to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks like *pass the hash* and *pass the ticket*.

INTUNE SETTINGS – CREDENTIAL GUARD SETTING

Settings Catalog / **Device Guard**

Credential Guard

Setting: **Enabled with UEFI lock**

Virtualization Based security: **Enabled**

^ Device Guard

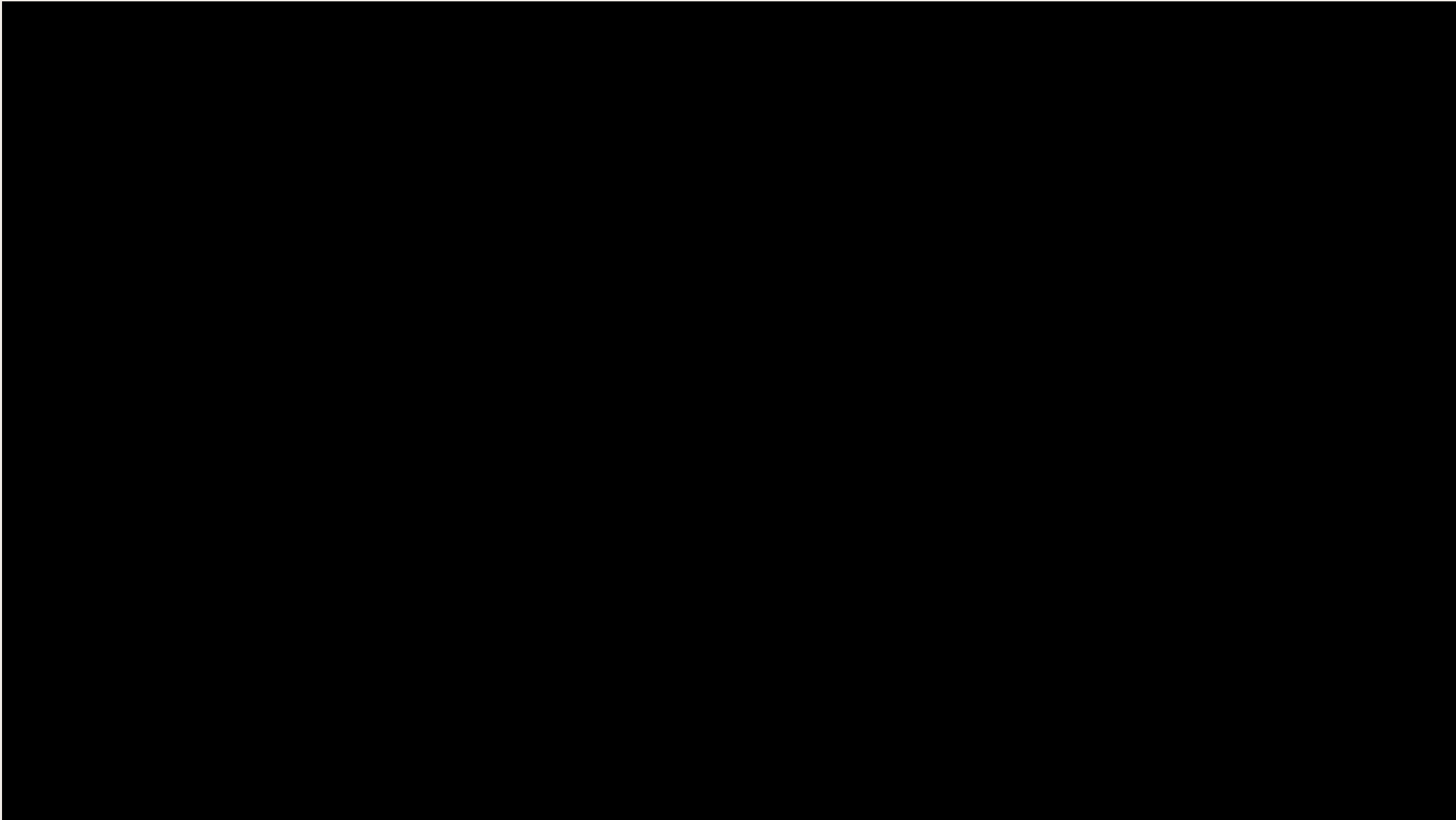
Credential Guard ⓘ

(Enabled with UEFI lock) Turns on Credential Guard with UEFI lock.

Enable Virtualization Based Security ⓘ

enable virtualization based security.

INTUNE SETTINGS – CREDENTIAL GUARD SETTING - WALKTHROUGH



CREDENTIAL GUARD SETTING – CHECK

Windows Logs > System

Wininit Event ID 13

Event Properties - Event 13, Wininit

General

Details

Credential Guard was started and will protect LSA credentials.

Log Name: System

Source: Wininit

Event ID: 13

Level: Information

User: SYSTEM

OpCode: Info

Logged: 25/06/2025 20:19:36

Task Category: None

Keywords:

Computer: WIN-2PVUQSJIM6P

Copy

Close

System Information

Virtualization-based Security Services Running

Virtualization-based security	Running
Virtualization-based security Re...	Base Virtualization Support, Secure Boot, DMA Protection
Virtualization-based security Av...	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly.
Virtualization-based security Se...	Credential Guard, Hypervisor enforced Code Integrity
Virtualization-based security Se...	Credential Guard, Hypervisor enforced Code Integrity
App Control for Business policy	Enforced

CREDENTIAL GUARD UEFI – OPT-OUT - WALKTHROUGH

DISABLE WITH UEFI LOCK
MET SCRIPT

KEY

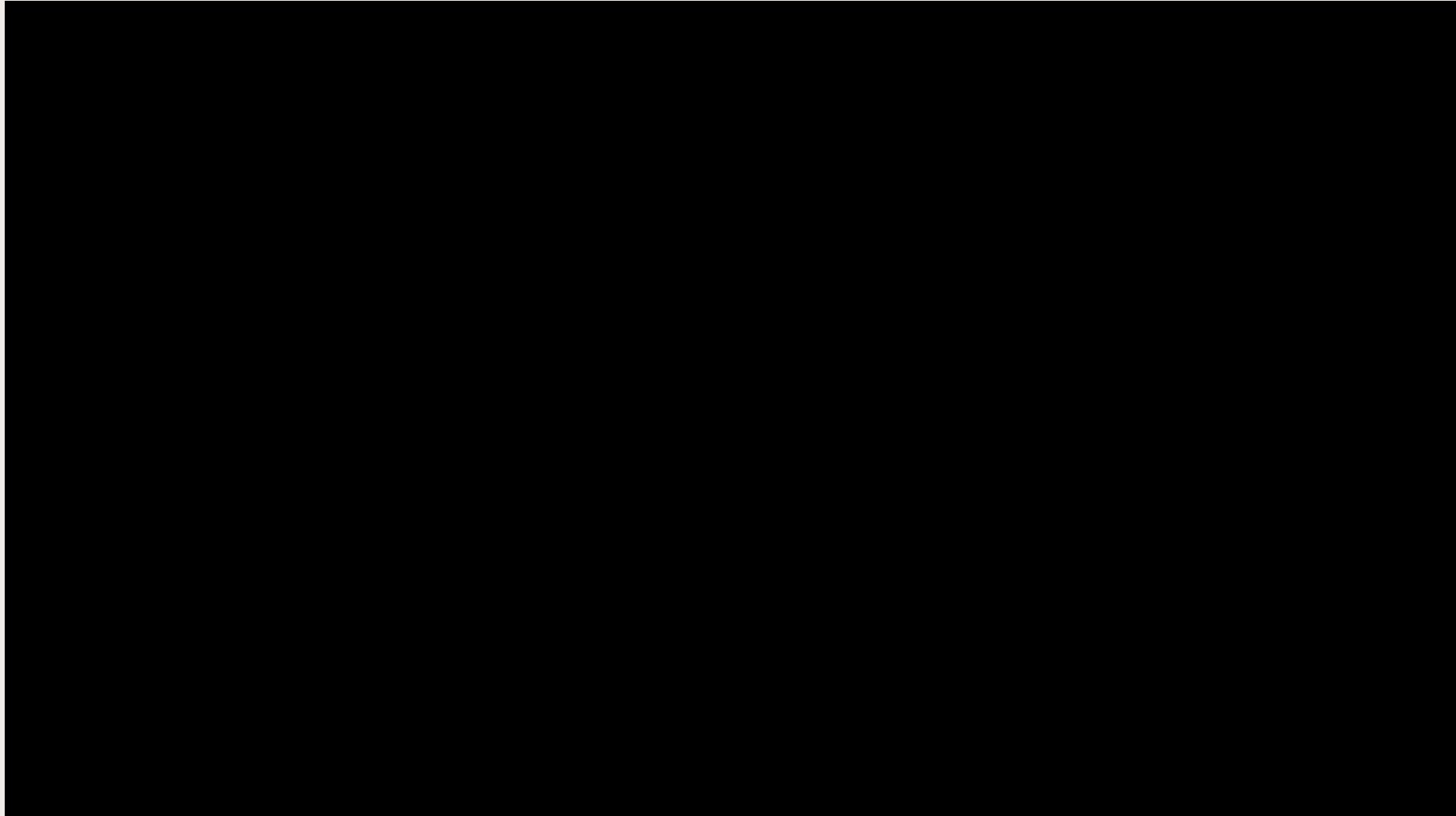
NAME: LSACFGFLAGS

TYPE: REG_DWORD

VALUE:

1 (TO ENABLE
CREDENTIAL GUARD
WITH UEFI LOCK)

2 (TO ENABLE
CREDENTIAL GUARD
WITHOUT LOCK)





INTUNE SETTINGS

- LOCAL SECURITY AUTHORITY (LSA) PROTECTION

TOKENTHEFT PROTECTION – LSA PROTECTION

Enable and configure added LSA credentials protection

You can configure added LSA protection for devices running Windows 8.1 or later, or Windows Server 2012 R2 or later, by using the procedures in this section.

Devices that use Secure Boot and UEFI

When you enable LSA protection on x86-based or x64-based devices that use Secure Boot or UEFI, you can store a UEFI variable in the UEFI firmware by using a registry key or policy. When enabled with UEFI lock, LSASS runs as a protected process, and this setting is stored in a UEFI variable in the firmware.

When the setting is stored in the firmware, the UEFI variable can't be deleted or changed to configure added LSA protection by modifying the registry or by policy. The UEFI variable must be reset by using the instructions in [Remove the LSA protection UEFI variable](#).

INTUNE SETTINGS – LOCAL SECURITY AUTHORITY

Settings Catalog / **Local Security Authority**

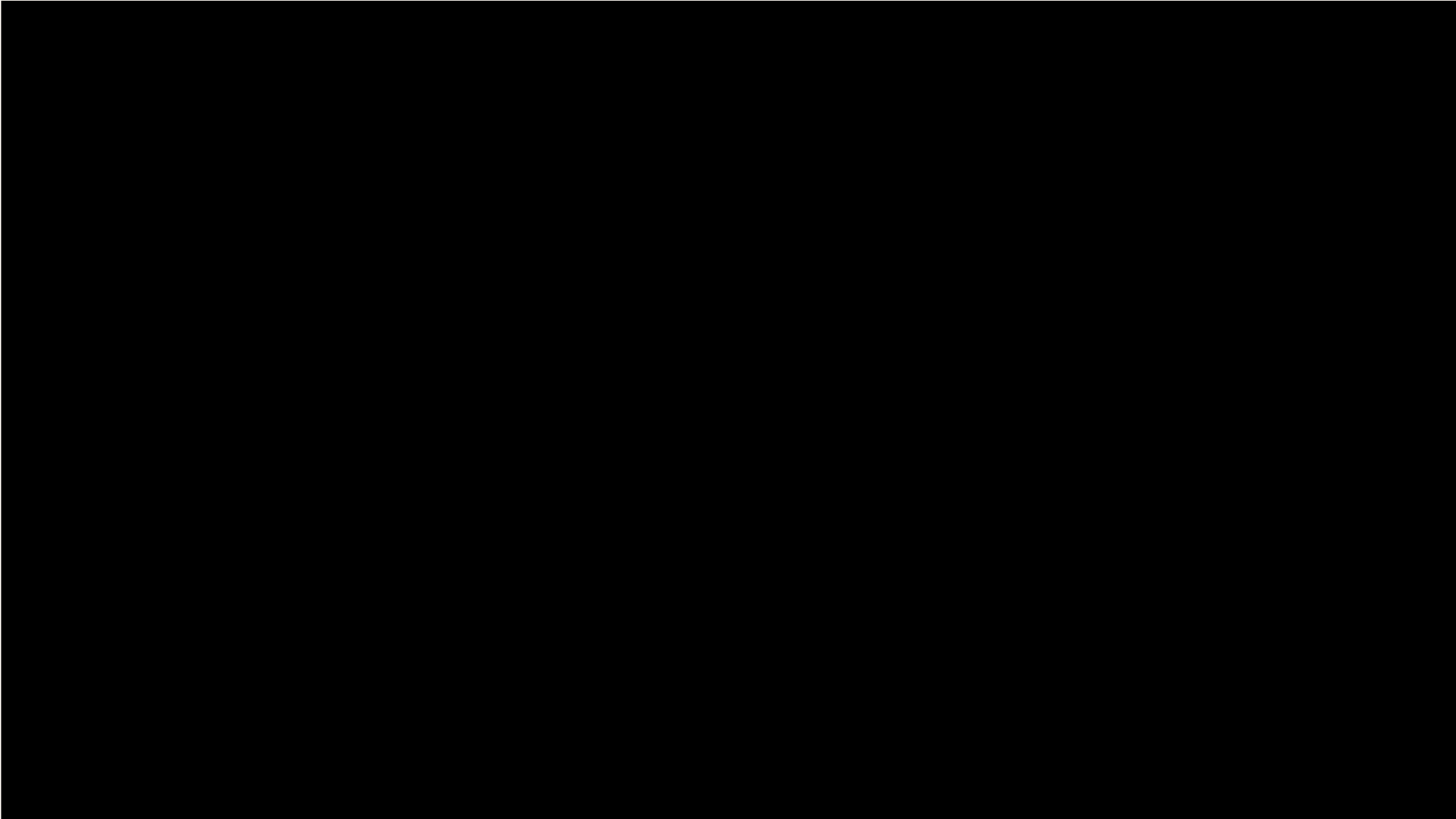
Setting:
Enabled with UEFI lock

^ Local Security Authority

Configure Lsa Protected Process ⓘ

Enabled with UEFI lock. LSA will run as protected process and this configuration is UEFI locked.

INTUNE SETTINGS – LOCAL SECURITY AUTHORITY - WALKTHROUGH



LOCAL SECURITY SETTING – CHECK

Windows Logs > System

Wininit Event ID 12

Event Properties - Event 12, Wininit

GeneralDetails

LSASS.exe was started as a protected process with level: 4.

Log Name: System

Source: Wininit

Event ID: 12

Level: Information

User: SYSTEM

OpCode: Info

Logged: 27/08/2025 08:58:03

Task Category: None

Keywords:

Computer: TestLaptop

Copy

Close

Core Isolation

LSA protection

This setting is managed by your administrator.

Local Security Authority protection

Helps protect user credentials by preventing unsigned drivers and plugins from loading into the Local Security Authority.

☒ On

[Learn more](#)

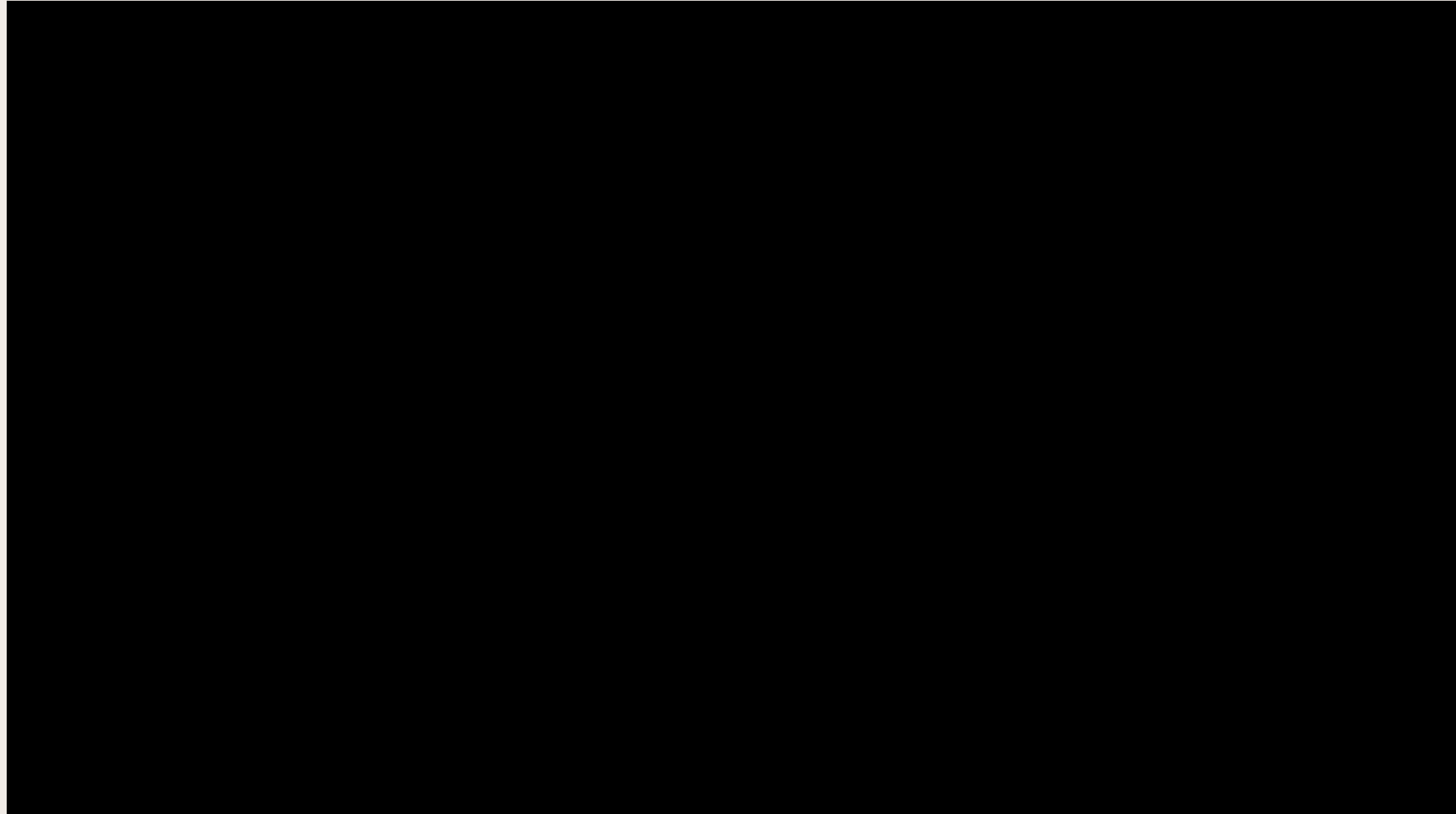
Credential Guard

Credential Guard is protecting your account login from attacks.

LSA – UEFI OPT-OUT - WALKTHROUGH

Tool en script:

Disable the registry key
RunAsPPL.





INTUNE SETTINGS

- CUSTOM COMPLIANCE

INTUNE SETTINGS – CUSTOM COMPLIANCE SCRIPT

Custom Compliance / Compliance Script

Controle op Device Guard
proces running

Author: Jörgen Nilsson

Source: <https://github.com/Ccmexec/Intune-MEM/tree/master/Custom%20Compliance>

Custom Compliance Script Credential Guard ...

Basics [Edit](#)

Name	Custom Compliance Script Credential Guard
Description	Custom Compliance Script Credential Guard
Publisher	No Publisher
Version	1

Settings [Edit](#)

Detection script

```
1 $DevGuard = Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard
2 $CredGuardStatus = @{"CredentialGuardRunning" = ($DevGuard.SecurityServicesRunning -contains 1)}
3 Return $CredGuardStatus | ConvertTo-Json -Compress
```

Run this script using the logged on credentials	No
Enforce script signature check	No
Run script in 64 bit PowerShell Host	Yes

INTUNE SETTINGS – CUSTOM COMPLIANCE

Compliance Settings / Custom Compliance

Selecter Script
Upload JSON File

Author: Jörgen Nilsson

Source: <https://github.com/Ccmexec/Intune-MEM/tree/master/Custom%20Compliance>

1 Compliance settings

2 Review + save

Custom Compliance

Custom compliance ①

Select your discovery script

Upload and validate the JSON file with your custom compliance settings

Require

Not configured

Custom Compliance Script Credential Guard

Select a file

Setting name	Operator	Value
No results.		

```
1 {
2   "Rules": [
3     {
4       "SettingName": "CredentialGuardRunning",
5       "Operator": "IsEquals",
6       "DataType": "Boolean",
7       "Operand": true,
8       "MoreInfoUrl": "https://xplorethecloud.nl",
9       "RemediationStrings": [
10        {
11          "Language": "en_US",
12          "Title": "Credential Guard is not enabled",
13          "Description": "Please make sure that Credential Guard is enabled on yo
14        }
15      ]
16    }
17  ]
}
```

INTUNE SETTINGS – CUSTOM COMPLIANCE - CHECK

Intune Portal / Devices /
Compliance


Compliance Policy Windows









Policy setting compliance

 Refresh  Export  Columns 

 Search



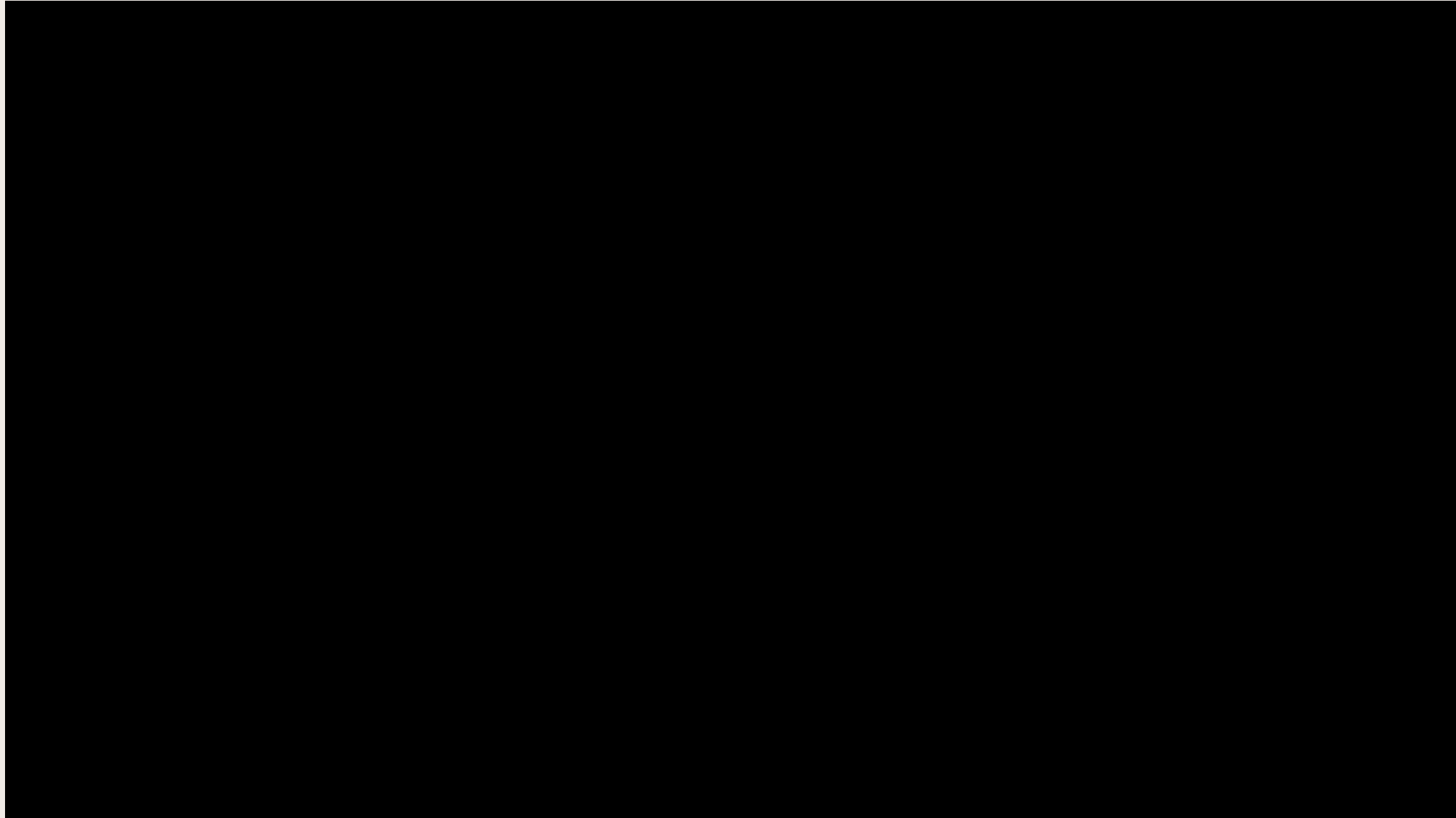
 Add filters

Setting	State	State details
CredentialGuardRunning	 Compliant	
Firewall	 Compliant	
Anti-Spyware	 Compliant	
Antivirus	 Compliant	
BitLocker	 Compliant	
Code Integrity	 Compliant	
Microsoft Defender Antimalware	 Compliant	
Simple Passwords	 Compliant	

Author: Jörgen Nilsson

Source: <https://github.com/Ccmexec/Intune-MEM/tree/master/Custom%20Compliance>

INTUNE SETTINGS – CUSTOM COMPLIANCE



CONDITIONAL ACCESS SETTINGS



CA SETTINGS – POLICY

Target Resources:

- **Microsoft Team Services**
- **Office 365 Exchange Online**
- **Office 365 SharePoint Online**
- **Windows 365**
- **Azure Virtual Desktop** (9cdead84-a844-4324-93f2-b2e6bb768d07)



Tip

The app name was previously *Windows Virtual Desktop*. If you registered the *Microsoft.DesktopVirtualization* resource provider before the display name changed, the application will be named **Windows Virtual Desktop** with the same app ID as Azure Virtual Desktop.

Target resources ⓘ

5 resources included

Network **NEW** ⓘ

Not configured

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

1 control selected

☐ All resources (formerly 'All cloud apps')

☒ Select resources

Edit filter

None

Select

Windows Virtual Desktop and 4 more

MT	Microsoft Teams Services cc15fd57-2c6c-4117-a88c-83b1d56b4bbe	...
O3	Office 365 Exchange Online 00000002-0000-0ff1-ce00-000000000000	...
O3	Office 365 SharePoint Online 00000003-0000-0ff1-ce00-000000000000	...
W3	Windows 365 0af06dc6-e4b5-4f28-818e-e78e62d137a5	...
WV	Windows Virtual Desktop 9cdead84-a844-4324-93f2-b2e6bb768d...	...

CA SETTINGS – POLICY

Conditions: Device platforms

- **Windows**

Conditions: Client apps

- **Mobile apps and desktop clients**

Device platforms

×

Apply policy to selected device platforms.
[Learn more](#)

Configure ⓘ

Yes No

Include

Exclude

☐ Any device

☒ Select device platforms

☐ Android

☐ iOS

☐ Windows Phone

☒ Windows

☐ macOS

☐ Linux

Client apps

×

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

Yes No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☒ Mobile apps and desktop clients

Legacy authentication clients

☐ Exchange ActiveSync clients

☐ Other clients ⓘ

CA SETTINGS – POLICY

Grant

- **Require Device to be marked as compliant**

Session

- **Require Token protection for sign-in sessions**

Grant



Control access enforcement to block or grant access. [Learn more](#)

- ☐ Block access
- ☒ Grant access

☐ Require multifactor authentication

☐ Require authentication strength

☒ Require device to be marked as compliant

Don't lock yourself out! Make sure that your device is compliant. [Learn more](#)

Session



This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. [Learn more](#)

☐ Use Conditional Access App Control

☐ Sign-in frequency

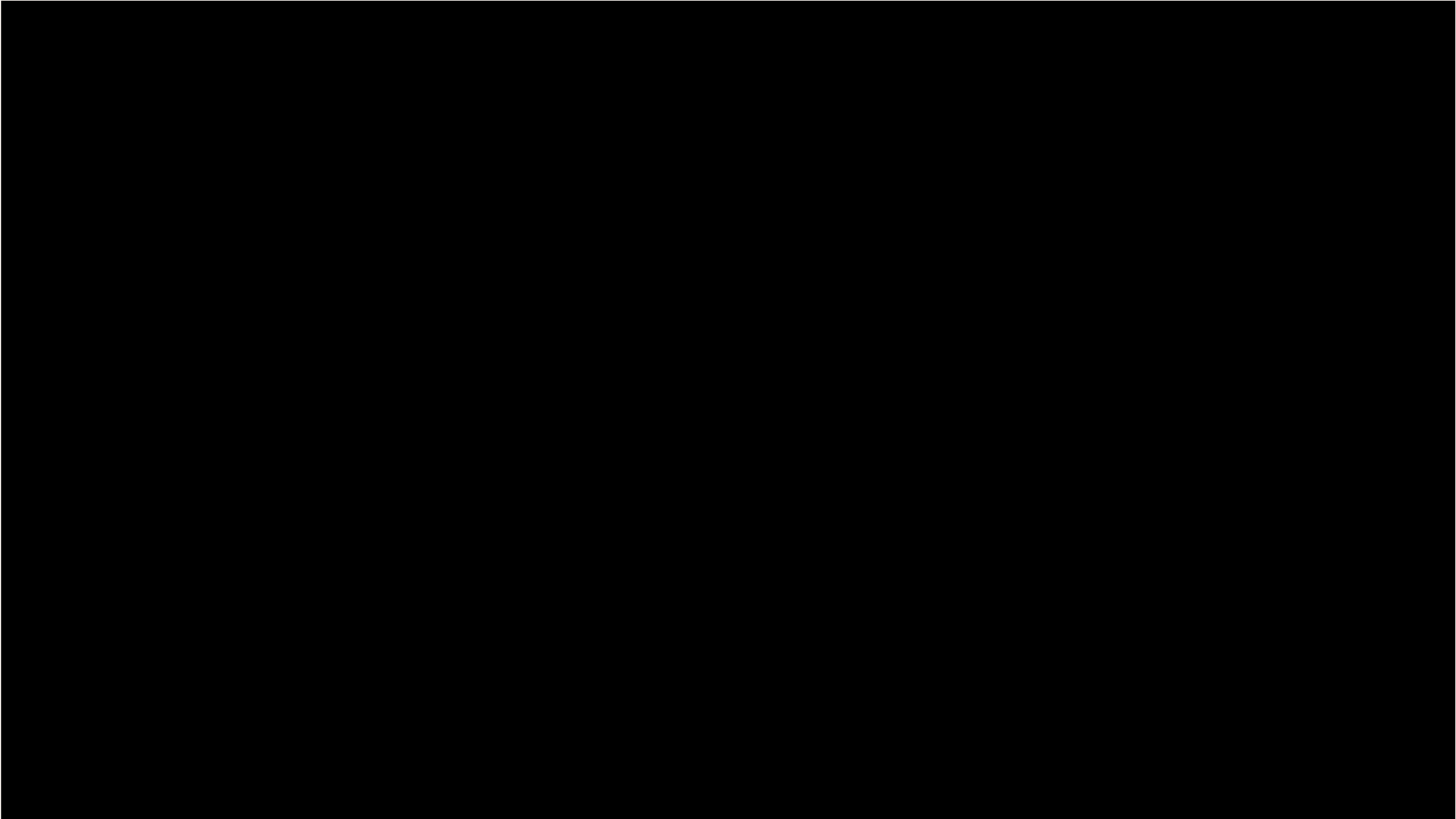
☐ Persistent browser session

☐ Customize continuous access evaluation

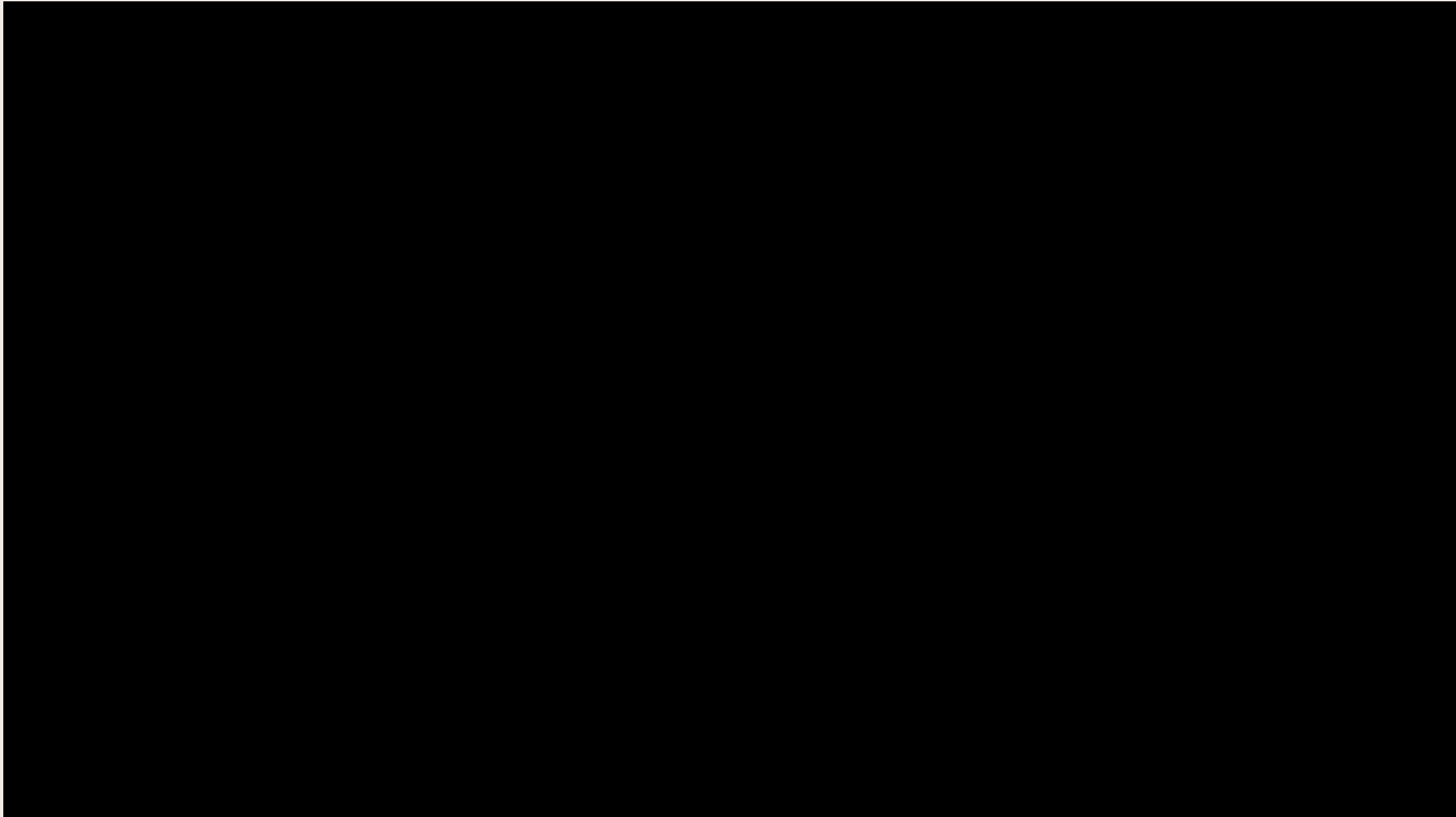
☐ Disable resilience defaults

☒ Require token protection for sign-in sessions (Generally available for Windows. Preview for MacOS, iOS)

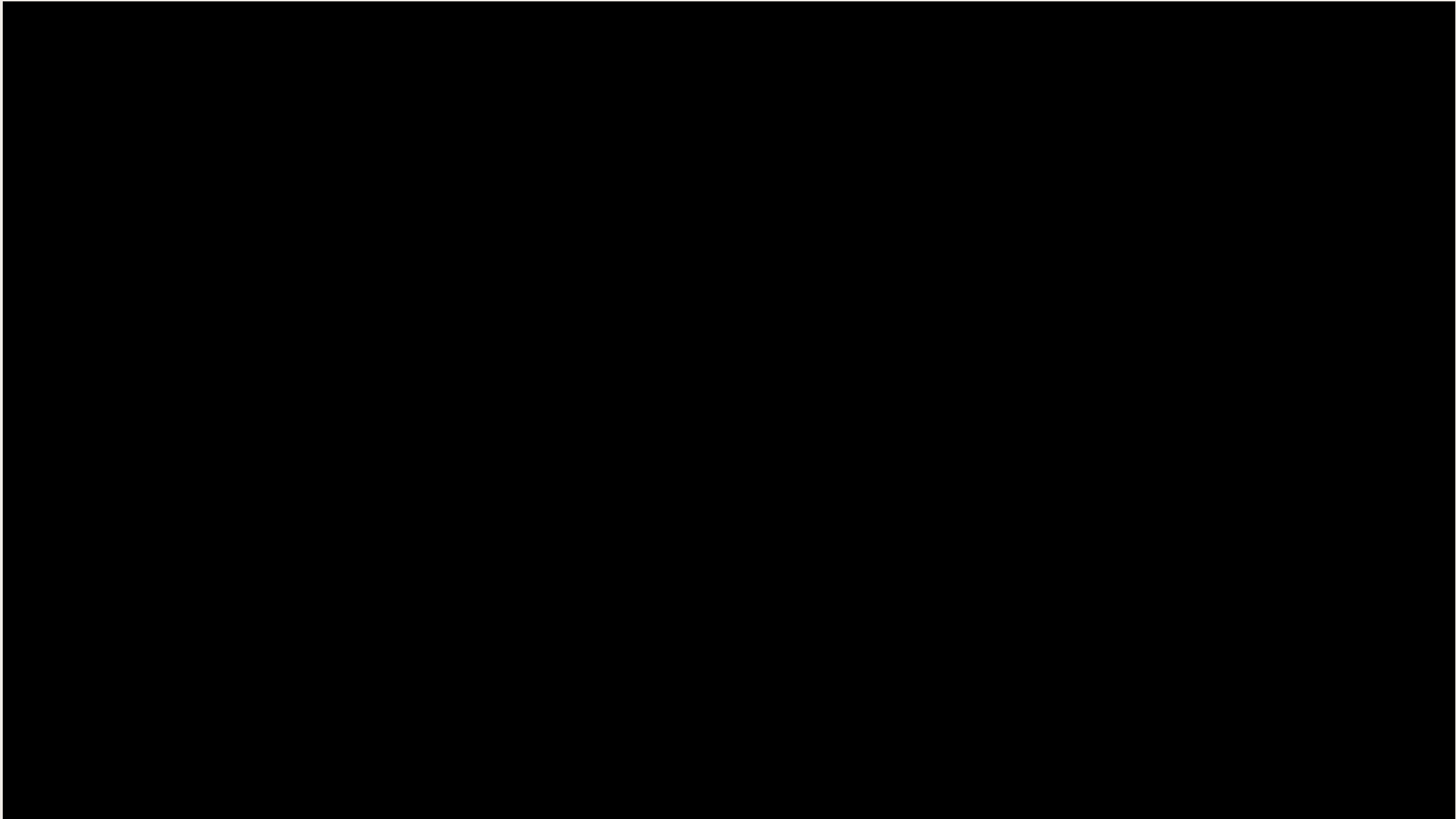
CA SETTINGS - VIDEO



CA RULE – SUCCESS



CA SETTINGS – LOGS BLOCK – USER EXPERIENCE



CA SETTINGS – LOGS BLOCK

Authentication requirement	Multifactor authentication
Agent Type	Not Agentic
Status	Failure
Continuous access evaluation	No
Sign-in error code	530084
Failure reason	Access has been blocked by conditional access token protection policy configured by this organization. To learn more, see https://aka.ms/TBCADocs .

ENTRA ID Sign-in Logs

Token Protection- Unbound

Client app	Mobile Apps and Desktop clients
Client credential type	None
Service principal ID	[REDACTED]
Original transfer method	None
Token Protection - Sign In Session	Unbound (statusCode: 1002)
Service principal name	
Resource service principal ID	[REDACTED]
Unique token identifier	[REDACTED]



KEY TAKE AWAYS



KEY TAKE

AWAYS

- GEBUIKERS GEEN LOCAL ADMIN RECHTEN
- CONTROLEER LSA & CREDENTIAL GUARD INSTELLINGEN
- STEL LSA & CREDENTIAL GUARD IN MET INTUNE MET UEFI LOCK
- CUSTOM COMPLIANCE CHECK CREDENTIAL GUARD
- CA REGEL VOOR TOKEN BOUND



KEY TAKE

AWAYS

- GEBUIKERS GEEN LOCAL ADMIN RECHTEN
- CONTROLEER LSA & CREDENTIAL GUARD INSTELLINGEN
- STEL LSA & CREDENTIAL GUARD IN MET INTUNE MET UEFI LOCK
- CUSTOM COMPLIANCE CHECK CREDENTIAL GUARD
- CA REGEL VOOR TOKEN BOUND