White Paper
September 2022

Credential Guard and Device Guard for DeltaV™ Systems

This white paper presents two new protections that can be implemented on a DeltaV™ system based on Microsoft features introduced in Windows 10 and Windows Server 2016.

Table of Contents

Introduction

In a Windows network, the Microsoft security protocols suite used for authentication is called Windows NT LAN Manager, also known as: NTLM. Users' passwords are not exchanged in clear text within this network, instead a hash is used by the underlying applications to respond to a challenge-response authentication scheme. If the hashes are discovered, they can be used to authenticate within a given Windows network in place of passwords.

A known cyber-attack called pass-the-hash targets the system hashes by compromising endpoints. There are different ways to implement this attack, but most of them are initiated by compromising computers within a system with specific toolkits that allow the hashes to be obtained. The hashes are either obtained as they are created (upon user's authentication once the password is entered) or by attacking the Windows secrets vault that resides in the system computers.

The main goal of the pass-the-hash cyber-attack is to obtain the hashes of high privilege accounts. These accounts' hashes are not usually cached and not used as frequently as other lower privileged accounts. Therefore, this attack is implemented in stages, where the attacker:

1. Compromises computer(s).
2. Obtains any valid hash in the system.
3. Uses the known hashes to force abnormal conditions on behalf of a legitimate user.
4. Forces an awkward user's experience which is reported to the system administrator.
5. Learns the system administrator's hash once he/she logs into the system for troubleshooting.
6. Use the learned hashes to compromise the whole system locally or remotely.

In theory, any system that uses NTLM for authentication can be exposed to the pass-the-hash attack including Microsoft Windows and UNIX-based operating systems. Microsoft released two solutions within Windows 10 and Windows Server 2016 operating systems that can be used together to protect system hashes and the boot-up sequence of computers in a network. These solutions are called Credential Guard and Device Guard respectively. The intent of this whitepaper is to explain how these protection mechanisms work in DeltaV systems with a brief description followed by an FAQ – for a detailed description of Credential Guard /Device Guard applied to DeltaV systems, please check Guardian Support Knowledge Base Articles and DeltaV Books Online.

Microsoft Credential Guard (also known as Windows Defender Credential Guard) is a specific feature within Windows that is used to isolate and harden user secrets against compromises. Microsoft Device Guard (also known as Windows Defender Device Guard) is a group of features designed to harden a computer and prevent malicious code execution. Although different, Credential Guard and Device Guard are complementary and have variations that must be evaluated and implemented accordingly to deliver the protection layers for workstations and servers.

Virtual Secure Mode (VSM) is the base for Credential Guard and Device Guard. VSM leverages the processor's virtualization support to extend its functionality to isolate critical processes and memory areas. The isolated virtualized area does not have a user interface and is protected against tampering by means of hardware and software components detailed in the next sections of this whitepaper. One key component that is added to the secured virtual environment is the Local Security Authority (LSA), which is where the secrets of a Windows operating system are stored, and therefore, Credential Guard / Device Guard elevates LSA to the secured virtual environment, thereby protecting against the pass the-hash cyber-attack.

Overall Considerations

Microsoft presents a list of requirements that must be followed before Credential Guard or Device Guard are enabled. The minimum set of features required to enable these features include, but are not limited to:

- Windows 10 or Windows Server 2016 64-bit O/S
- Domain environments (protection is provided to domain accounts only)
- UEFI – Unified Extensible Firmware Interface with Secure Boot enabled
- Computer's CPU with virtualization extensions (e.g., Intel-VT)
- Trusted Platform Module (TPM) version 2.0 or higher

Please refer to Guardian Support Knowledge Base Articles with detailed information about minimum requirements to enable Credential Guard / Device Guard on DeltaV workstations, as well as the steps to implement these features on your DeltaV system.

Most modern computers ship with UEFI instead of BIOS to improve security, support large hard drives and, speed up boot times among other enhancements. Secure boot adds security to the boot up sequence which is an essential step in preventing attacks that target workstations and servers. TPM is a hardware component that is installed on the computers' motherboard and is used to add physical security to the boot up sequence in combination with Secure Boot – please consult with your local Emerson sales office for details about how to deploy Credential Guard / Device Guard in your country if any limitations or restrictions apply.

In DeltaV v14.3, two new features were introduced to address the minimum requirements of Credential Guard and Device Guard. Independent DeltaV Domain Controller (IDDC) enables domain controller isolation which is essential if you require Credential Guard to be enabled on a DeltaV system. And, all DeltaV service accounts have been changed to domain members which is an important step to address specific requirements to implement Credential Guard – the use of interactive and local service accounts with administrative privileges can defeat the purpose of Credential Guard. Please check Guardian Support Knowledge Base Articles for a complete list of DeltaV workstations and servers that meet the minimum requirements to enable Credential Guard / Device Guard on DeltaV systems.

IDDC helps with the deployment of Credential Guard but is not sufficient on its own. Systems with Credential Guard enabled must not cache credentials since caching is done locally on each computer in a system and outside of the secured virtualized environment. Cached credentials in a domain environment are used to prevent authentication issues in case domain members cannot contact the domain controllers of the system. It is highly recommended to implement backup domain controllers on systems that do not cache credentials . Emerson recommends you enable Credential Guard and Device Guard, implement redundant IDDC Domain Controllers, and disable credentials caching on DeltaV systems.

If Credential Guard is implemented on an existing DeltaV system, it is recommended to change all users' passwords to make sure any compromised hashes are not used to breach the system.

Device Guard is not implemented in its full extent for DeltaV systems. A full-blown Device Guard implementation is like allow-listing which is already offered for DeltaV systems with the Application Allow-listing solution provided by Emerson (powered by McAfee). The Device Guard setup supported on DeltaV systems targets the protection of the boot up sequence so that workstations and servers on a DeltaV network cannot be tampered with during boot.

Scenarios Not Protected by Credential Guard

The following scenarios are not protected by Credential Guard:

- Software that manages credentials outside of the Windows feature protection.
- Local accounts (all DeltaV service accounts in v14.3 and later are domain accounts).
- Credential Guard does not protect the Active Directory database running on domain controllers. It also does not protect credential input pipelines, such as Windows Server 2016 servers running Remote Desktop Gateway.
  - If you're using a Windows Server 2016 server as a client PC, it will get the same protection as it would when running Windows 10 Enterprise.
- Key loggers.
- Physical attacks.
- Attacks based on malware that uses elevated privileges on compromised workstations and servers. We recommend using dedicated workstations and servers for high value accounts, such as IT Pros and users with access to high value assets in your organization.
- Integration of tested and approved applications that are running outside of the DeltaV network and in a workgroup environment.

Frequently Asked Questions

- What is the performance impact on a DeltaV system if Credential Guard or Device Guard are enabled?

  Re.: Emerson has not experienced performance degradation after enabling Credential Guard and Device Guard under the standard validation and soaking tests for DeltaV v14.3. It is important to follow the recommendations provided by Emerson when enabling these features in DeltaV systems.

- Is DeltaV Backup & Recovery compatible with DeltaV workstations and servers running Credential Guard and/or Device Guard?

  Re.: Yes. Credential Guard and Device Guard require Secure Boot which would prevent full disk images being restored with DeltaV Backup & Recovery solution. However, Secure Boot can be temporarily disabled during a complete machine restore from an image backup created by DeltaV Backup & Recovery.

- Can I enable Credential Guard or Device Guard on a DeltaV v13.3.1 system running on Windows 10 and Windows Server 2016 O/S?

  Re.: No. Although DeltaV v13.3.1 can also run on Windows 10 and Windows Server 2016 O/S, the configuration changes to enable Credential Guard and Device Guard were not fully tested with DeltaV v13.3.1. Moreover, the support for service accounts as domain members and the IDDC functionality are only available on DeltaV v14.3 and later.

- Can Credential Guard or Device Guard be enabled on a system that is not following all requirements listed by Emerson and Microsoft?

  Re.: Failing to meet the requirements listed in Books Online and the specific Knowledge Base Articles to deploy either Credential Guard or Device Guard will not guarantee the protection expected from these features on a DeltaV system. Emerson provides support for DeltaV systems running Credential Guard and/or Device Guard if these features are implemented as described in the user's documentation.

- Do I need to purchase any specific software license (DeltaV or Windows specific) to enable Credential Guard or Device Guard on a DeltaV system?

  Re.: No. If the DeltaV system meets the requirements to deploy Credential Guard or Device Guard, then these features can be enabled anytime following the guidelines in Books Online and Guardian Support Knowledge Base Articles. No additional licenses are required to implement these features.

- Is the Independent DeltaV Domain Controller a mandatory requirement to enable Credential Guard on a DeltaV system?

  Re.: No, it is not a mandatory requirement, but the Independent DeltaV Domain Controller (IDDC) is highly recommended as Credential Guard is not supported on domain controllers (per Microsoft guidelines). If, instead of IDDC, the domain controllers are the ProfessionalPLUS and Application stations, the Credential Guard functionality will not be enabled on these DeltaV stations, and since these servers are usually connected to external networks, the DeltaV system can be vulnerable to the pass-the-hash cyber-attack even with Credential Guard enabled on all other workstations and servers in the same network.

- Can I run Credential Guard and Device Guard on DeltaV workstations and servers that do not have TPM 2.0 installed on them? Are TPM 1.2 or TCM supported?

  Re.: No. TPM 2.0 is a mandatory requirement to enable Credential Guard or Device Guard per Microsoft. Microsoft states that TPM 2.0 is required (not v1.2) and TCM (Trusted Cryptography Module) is not listed by Microsoft as a supported cryptography component to enable these features.

- Is there an upgrade option for DeltaV workstations and servers that do not have TPM 2.0 (or have other TPM versions)?

  Re.: Certain DeltaV workstations and servers can be upgraded. Dell provides an upgrade kit to install TPM 2.0 for very specific hardware models. The updated list of DeltaV stations that can be upgraded to TPM 2.0 is available in Guardian Support Knowledge Base Articles that describe Credential Guard and Device Guard functionality for DeltaV systems.

- Does Emerson support full-blown Device Guard deployment on DeltaV systems?

  Re.: No. The code integrity protection available as part of the Device Guard feature is not compatible with DeltaV systems and can also conflict with the Application Allow-listing for DeltaV systems if they both run on the same workstations or servers. Therefore, this specific feature is not enabled in the steps that describe how to configure Device Guard for DeltaV systems.

- Is my system vulnerable if after enabling Credential Guard the system passwords are not changed?

  Re.: Yes. Although this risk is low if appropriate network segmentation is already in place, it is still better to change all system's passwords after enabling Credential Guard to make sure hashes are not compromised.

- Can I enable Credential Guard on a DeltaV system that has stations that do not meet all requirements specified by Microsoft?

  Re.: A partially deployed Credential Guard protection will not provide full protection against credentials theft. Moreover, many of the requirements are checked by Windows during Credential Guard implementation – Credential Guard will show it is configured but not running on all stations that do not comply with all requirements to enable the protection.

- Is there any impact to Credential Guard if the ProfessionalPLUS is unavailable in the network?

  Re.: Credential Guard should be deployed in domain environments with Independent DeltaV Domain Controllers deployed. There is no impact to the protection features in this case if the ProfessionalPLUS is not available in the network for any specific reason.

Where to find more information

- Guardian Support Portal
- DeltaV Books Online
- Microsoft document: “Protect derived domain credentials with Windows Defender Credential Guard” (**https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard**)
- Microsoft document: “Requirements and deployment planning guidelines for Windows Defender Device Guard” (**https://docs.microsoft.com/en-us/windows/device-security/device-guard/requirements-and-deployment-planning-guidelines-for-device-guard**)
- Microsoft Technet article: “Windows 10 Device Guard and Credential Guard Demystified” (**https://blogs.technet.microsoft.com/ash/2016/03/02/windows-10-device-guard-and-credential-guard-demystified/**)

Contact Us
www.emerson.com/contactus