COALFIRE

IMPLEMENTING MICROSOFT CREDENTIAL GUARD FOR ISO 27001, PCI, AND FEDRAMP

North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

INTRODUCTION

The threat of a cyber-attack is a constant factor all organizations must consider when developing their information security posture. A particular area of concern is the exploitation of information system derived domain credentials and credential artifacts, which present attackers the opportunity to pass-the-hash or pass-the-ticket with derived domain credentials such as NTLM password hashes or Kerberos tickets. Credential Guard is a set of new security features for Windows Server 2016 and the Windows 10 operating system which helps organizations prevent derived credentials from being compromised by advanced attacks or from being exposed during certain authentication workflows.

In order to help customers implement this new capability for compliance with ISO, PCI, or FedRAMP, Microsoft worked closely with Coalfire, a recognized third-party IT compliance firm, to define each security and compliance objective in relation to the capabilities of Credential Guard. In addition, Appendix A contains mappings between Credential Guard and the security control requirements present in ISO 27001, PCI DSS, and FedRAMP.

OVERVIEW OF CREDENTIAL GUARD

Credential Guard provides robust protections against local pass-the-hash or pass-the-ticket attacks on derived credentials by providing advanced virtualization-based isolation for certain authentication workflows within normal Windows system operation. Previously, during authentication workflows that required NTLM or Kerberos authentication, Windows stored derived credentials in process memory associated with the Local Security Authority (LSA). With this approach, an attacker could compromise the credential artifacts by retrieving them directly from memory associated with the LSA. Now, with Credential Guard, derived credentials are isolated from process memory to ensure they remain inaccessible to any process running within the operating system, including processes running with administrative privileges. Credential Guard is also used to enforce acceptable authentication workflows, and does not allow the configuration or use of unconstrained Kerberos delegation, NTLMv1, MS-CHAPv2, Digest, CredSSP, or Kerberos DES encryption.

Credential Guard protections actually consist of two discrete, closely related features:

> **Credential Guard**: Credential Guard functionality is used to protect and isolate derived credentials generated by local authentication to domain accounts or domain resources, in accordance with the overview in the previous section.
>
> **Remote Credential Guard**: Remote Credential Guard functionality extends the same protections to remote RDP sessions by preventing RDP authentication from exposing derived credentials, even when initiating RDP connections to machines that are potentially compromised.

CREDENTIAL GUARD AND VIRTUALIZATION-BASED SECURITY

Credential Guard leverages new virtualization-based security (VBS) capabilities within Windows Server 2016 and Windows 10 to implement strong isolation for derived credentials. VBS capabilities are used by Credential Guard to isolate Windows services critical to the security and integrity of the system from user and kernel modes, including from host administrator action, essentially acting as a barricade to most authentication attack vectors.

VBS is used by the Hyper-V hypervisor to restrict sections of physical memory from Windows kernel access in order to provide a secure place to store credentials, signatures, and other system-critical artifacts. This prevents attackers from compromising system-critical functions even if they compromise the Windows kernel or gain access to privileged administrative functions. With VBS, even if malware gains access to the kernel, the effects can be severely limited, because the hypervisor can prevent the malware from gaining access to derived credentials.

Instead of storing derived credentials and credential artifacts in process memory associated with the LSA, Credential Guard stores and protects derived credentials in a component new to the Windows kernel, called the Isolated LSA. This Isolated LSA is protected using VBS, and communicates with the LSA via remote procedure calls that are strictly controlled to ensure that common authentication attack vectors cannot compromise the Isolated LSA.

For security reasons, the Isolated LSA process does not contain any unnecessary functionality, such as device drivers. Instead, it only hosts a small subset of core operating system binaries that are required for operation. All binaries within the Isolated LSA are signed with a certificate that is trusted by VBS functionality. In order to ensure the Isolated LSA is genuine and hasn't been compromised prior to any authentication workflow, binary signatures are validated by VBS before initiating any action.

USING CREDENTIAL GUARD WITH DEVICE CERTIFICATES AND DEVICE GUARD

Credential Guard can provide mitigations against attacks on derived credentials and prevent the use of stolen credentials elsewhere. However, hosts can still be vulnerable to certain attacks, even if the derived credentials are protected by Credential Guard. These attacks can include abusing privileges and use of derived credentials directly from a compromised device, reusing previously stolen credentials acquired prior to Credential Guard protections being put in place, and abuse of management tools and weak application configurations. Because of this, additional mitigations may also need to be deployed to make the domain environment more secure.

Credential Guard can be deployed in combination with device certificates to provide additional levels of security and assurance for an organization environment. Credential Guard helps prevent user credential theft attacks, which allow the attacker to steal secrets from one device and use them from another device. However, since devices also use shared secrets for authentication, attackers can steal those secrets as well. By deploying device certificates with Credential Guard, authentication policies can require that the device authenticates with its private key. This prevents shared secrets on stolen devices from being used with stolen user passwords or Kerberos secret keys to sign on as the user.

Device certificate authentication has the following requirements:

- Device domains are Windows Server 2012 or higher and all domain controllers have certificates, which satisfy strict KDC validation (KDC EKU present and the DNS domain name matches the DNSName field of the SubjectAltName (SAN) extension).Windows 10 devices have the CA issuing the domain controller certificates in the enterprise store.
- A process is established to ensure the identity and trustworthiness of the device in a similar manner as you would establish the identity and trustworthiness of a user before issuing them a smartcard.

Similarly, Credential Guard can be deployed in combination with Device Guard to ensure that any derived credentials compromised before Credential Guard was configured cannot be used to install or execute unauthorized binaries, which can be used by attackers to escalate privileges or compromise other systems.

USING CREDENTIAL GUARD FOR COMPLIANCE WITH PCI, ISO 27001, AND FEDRAMP

In addition to providing customers a more powerful and effective way of protecting derived credentials, Credential Guard can also help customers meet compliance with several common compliance frameworks. The remainder of this document is aimed at providing Credential Guard control and requirement applicability across three common compliance frameworks: ISO 27001, PCI DSS, and FedRAMP.

Although compliance does not directly equate to security, many customers are required to adhere to different compliance standards as part of doing business in organization environments. This new solution is broadly applicable to numerous different controls within ISO 27001, PCI DSS, and FedRAMP, and provide customers an easier and more efficient way to meet applicable control requirements that are already in place.

PROTECTION OF AUTHENTICATION ASSOCIATED WITH LOCAL ACCESS

Deploying Credential Guard for local authentication to domain accounts provides coverage for numerous compliance requirements present in all three frameworks. Numerous controls within ISO, PCI, and FedRAMP are directed at securing authentication workflows, enforcing replay resistance, and providing strong credential protections to ensure credentials are not compromised prior to use. Although Credential Guard will not provide complete coverage for certain mapped control objectives due to the need for organizations to establish processes in order to support the control objective, implementing Credential Guard gives organizations the ability to start with a technical foundation when creating a compliance program for those specific control areas.

PROTECTION OF AUTHENTICATION ASSOCIATED WITH REMOTE ACCESS

In addition to the protections provided by Credential Guard, implementing Remote Credential Guard extends credential protections to session authenticity and secure remote access.

APPENDIX A: CREDENTIAL GUARD MAPPING TO PCI, ISO 27001, AND FEDRAMP

Credential Guard Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.2	FedRAMP; NIST 800-53 Revision 4
Protection of Authentication Associated with Local Access	A.9.2.4 – Management of Secret Authentication Information of Users A.9.3.1 – Use of Secret Authentication Information of Users A.9.4.1 – Information Access Restriction A.9.4.2 – Secure Logon Procedures A.9.4.3 – Password Management System A.10.1.2 – Key Management A.14.1.3 – Protecting Application Services Transactions	2.2.4 – Configure System to Prevent Misuse 3.6.2 – Secure Cryptographic Key Distribution 3.6.3 – Secure Cryptographic Key Storage 3.6.7 – Prevention of Unauthorized Key Substitution 8.1.2 – Control User IDs and Credentials 8.2.1 –Protect User Credentials (Passwords) 8.2.2 – Verify User Credential Modification 8.6 – Protect User Credentials (Other Authenticators)	AC-3 – Access Enforcement AC-4 – Information Flow Enforcement AC-6 (10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions IA-2 (8) – Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts – Replay Resistant IA-5 – Authenticator Management IA-5 (6) – Authenticator Management | Protection of Authenticators IA-6 – Authenticator Feedback IA-7 – Cryptographic Module Authentication SC-2 – Application Partitioning SC-4 – Information in Shared Resources SC-12 – Cryptographic Key Establishment and Management SC-12 (2) – Cryptographic Key Establishment and Management | Symmetric Keys
Protection of Authentication Associated with Remote Access	A.9.1.2 – Access to Networks and Network Services A.9.2.4 – Management of Secret Authentication Information of Users	2.2.3 – Enable Additional Control for Insecure Services, Protocols, Daemons 2.2.4 – Configure System to Prevent Misuse	AC-3 – Access Enforcement AC-4 – Information Flow Enforcement AC-6 (10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions AC-17 – Remote Access

Credential Guard Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.2	FedRAMP; NIST 800-53 Revision 4
	A.9.3.1 – Use of Secret Authentication Information of Users A.9.4.1 – Information Access Restriction A.9.4.2 – Secure Logon Procedures A.9.4.3 – Password Management System A.10.1.2 – Key Management A.13.1.2 – Security of Network Services A.14.1.2 – Securing Application Services of Public Networks A.14.1.3 – Protecting Application Services Transactions	3.6.2 – Secure Cryptographic Key Distribution 3.6.3 – Secure Cryptographic Key Storage 3.6.7 – Prevention of Unauthorized Key Substitution 8.1.2 – Control User IDs and Credentials 8.2.1 –Protect User Credentials (Passwords) 8.2.2 – Verify User Credential Modification 8.6 – Protect User Credentials (Other Authenticators)	IA-2 (8) – Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts – Replay Resistant IA-5 – Authenticator Management IA-5 (6) – Authenticator Management | Protection of Authenticators IA-6 – Authenticator Feedback IA-7 – Cryptographic Module Authentication SC-2 – Application Partitioning SC-4 – Information in Shared Resources SC-8 – Transmission Confidentiality and Integrity SC-8 (1) – Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection SC-12 – Cryptographic Key Establishment and Management SC-12 (2) – Cryptographic Key Establishment and Management | Symmetric Keys SC-23 – Session Authenticity