PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) V4.0

Multifactor Authentication

CHANGES TO MULTIFACTOR AUTHENTICATION

The Payment Card Industry Security Standards Council (PCI SSC) released V4.0 of the PCI Data Security Standards (PCI DSS) on March 31, 2022. The new PCI V4.0 standards include changes to address evolving threats, updates to clarify guidance, and a reorganization of content. Among the PCI V4.0 standard updates are some specific changes to the requirements regarding multifactor authentication (MFA) and access to the cardholder data environment (CDE).

The specific PCI requirements addressing multifactor authentication include:

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

8.4.2 MFA is implemented for all access into the CDE.

8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:

- All remote access by all personnel, both users and administrators, originating from outside the entity's network.
- All remote access by third parties and vendors.

8.5.1 MFA systems are implemented as follows:

- The MFA system is not susceptible to replay attacks.
- MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.
- At least two different types of authentication factors are used.
- Success of all authentication factors is required before access is granted.

Requirements 8.4.2 and 8.5.1 are future-dated new requirements in the PCI V4.0 standard. As future-dated new requirements, they are only recommended for implementation until March 31, 2025. After that date, PCI Requirements 8.4.2 and 8.5.1 are mandatory.

WHAT IS THE IMPACT OF THE MFA CHANGES?

The changes to the MFA requirements primarily cover access to the CDE, non-console administrative access to the CDE, and remote access including the CDE.

PCI Requirements 8.4.1 and 8.4.3 both exist in the PCI v3.2.1 standard but have had some changes to their formatting and guidance.

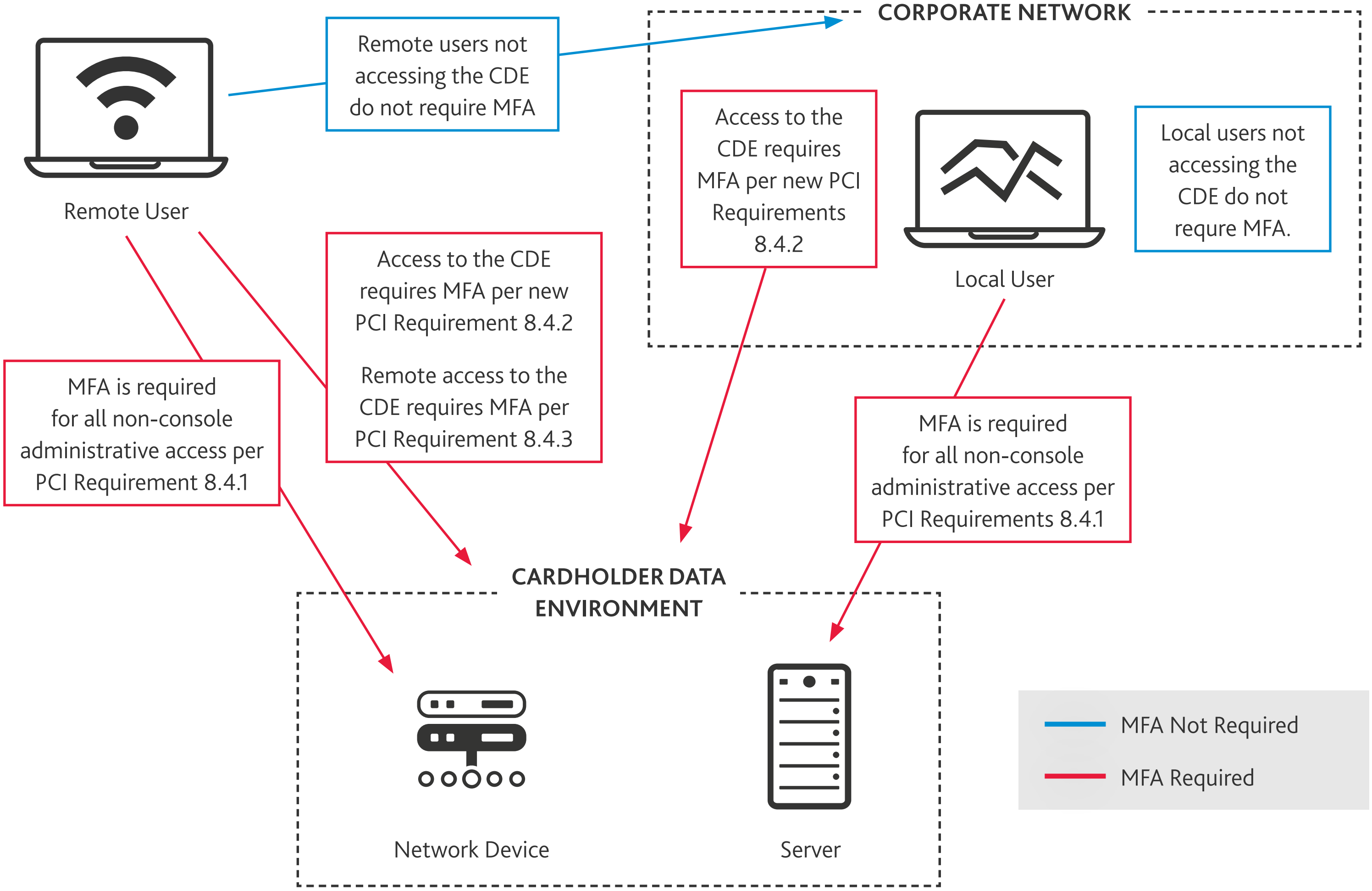
Clarification has been added to PCI Requirement 8.4.3. Any access that originates from outside the organization's network that either connects to the CDE or could impact the CDE must use MFA. This means that MFA is not required if the remote access is to a part of the network that is properly segmented from the CDE. MFA is required if the remote access leads to, or could lead to, access into the CDE.

The most notable change to MFA is the introduction of the new future-dated PCI Requirement 8.4.2. With this change, organizations are required to control all access to the CDE via multifactor authentication. This means all users accessing the CDE must be validated with MFA before they are granted access. This includes both users and administrators.

The important thing to note is the requirement to use MFA for access to the CDE and the requirement to use MFA for non-console administrative access are separate requirements, and both controls must be in place for PCI compliance. This means MFA must be used to authenticate access to the CDE and for non-console access separately. For example, if an administrator is accessing a server in the CDE, the administrator must use MFA to access the CDE, and then use MFA a second time to authenticate access to the server.

Whether or not an organization uses segmentation to isolate their CDE can also have an impact on how MFA is implemented and enforced. When organizations are using segmentation to reduce their PCI scope, users not accessing the CDE are not required to use MFA. Without segmentation, MFA must be implemented for all access.

SEGMENTATION



Remote users not accessing the CDE do not require MFA

Access to the CDE requires MFA per new PCI Requirements 8.4.2

Local users not accessing the CDE do not requre MFA.

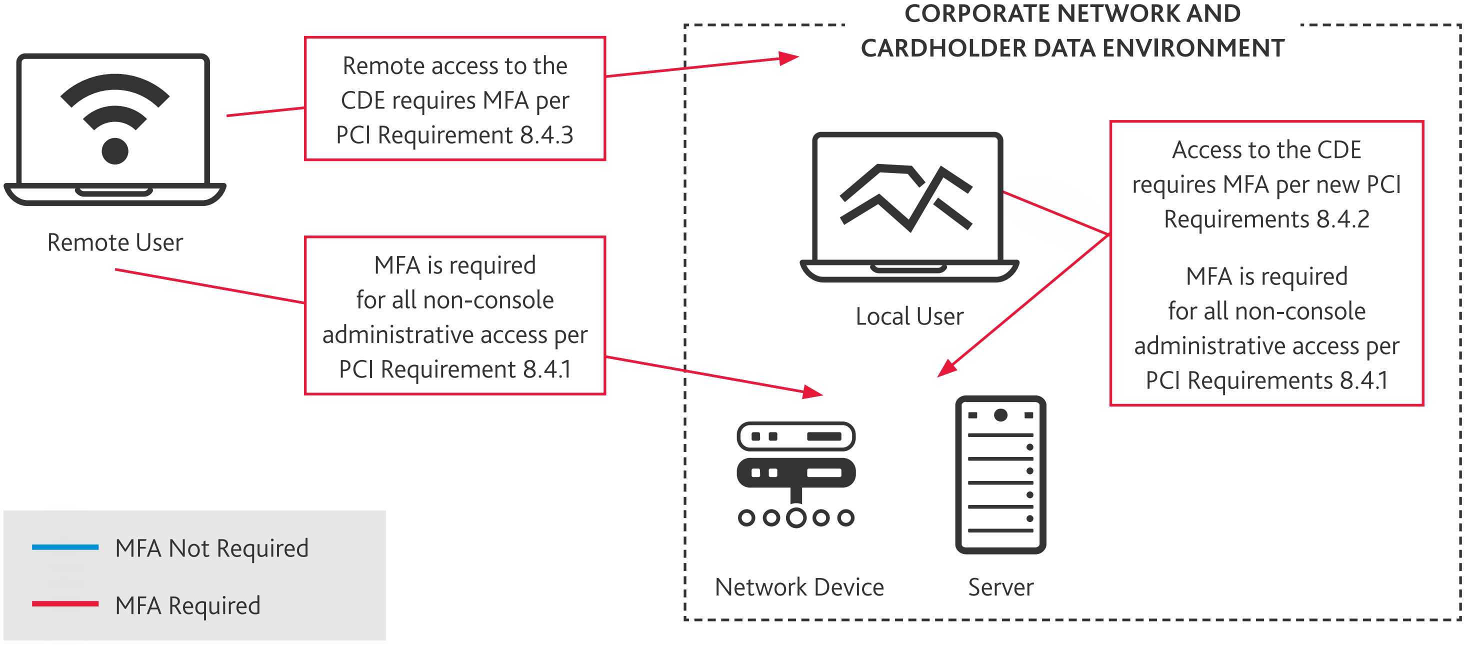
Access to the CDE requires MFA per new PCI Requirement 8.4.2

Remote access to the CDE requires MFA per PCI Requirement 8.4.3

MFA is required for all non-console administrative access per PCI Requirement 8.4.1

MFA is required for all non-console administrative access per PCI Requirements 8.4.1

NO SEGMENTATION


CORPORATE NETWORK AND CARDHOLDER DATA ENVIRONMENT
Remote User
Remote access to the CDE requires MFA per PCI Requirement 8.4.3
MFA is required for all non-console administrative access per PCI Requirement 8.4.1
Local User
Access to the CDE requires MFA per new PCI Requirements 8.4.2
MFA is required for all non-console administrative access per PCI Requirements 8.4.1
Network Device
Server
MFA Not Required
MFA Required

Another situation to consider is connections to the cardholder data environment through a jump box. This is where a connection is made from an insecure environment outside the CDE to a system in the CDE to make connections to applications or systems within the CDE. When connecting to the jump box, MFA is required to connect to the CDE, and MFA is also required for any non-console administrative connection in the CDE — including non-console administrative access to the jump box.

The following table lists some high-level scenarios involving the use of multifactor authentication:

SCENARIO	MFA REQUIRED	EXPLANATION
Local (LAN-based) access to corporate network (CDE segmented)	No	Access would not permit direct access to any cardholder data systems or cardholder data.
Local (LAN-based) access to corporate network (non-segmented)	Yes	The entire network is part of the CDE and access would permit direct access to cardholder data systems and cardholder data. 8.4.2 MFA is implemented for all access into the CDE. This new future-dated requirement is best practice until March 31, 2025, when it becomes mandatory.
Remote access (ex: VPN) to corporate network (CDE Segmented)	No (recommended)	Access would not permit direct access to any cardholder data systems or cardholder data.
Remote access (ex: VPN) to corporate network (non-segmented)	Yes	The entire network is part of the CDE and access would permit direct access to cardholder data systems and cardholder data. 8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE
Local (LAN-based) access to CDE from corporate network (CDE segmented)	Yes	Access to cardholder data environment requires MFA per new V4.0 requirement. 8.4.2 MFA is implemented for all access into the CDE. This new future-dated requirement is best practice until March 31, 2025, when it becomes mandatory.

SCENARIO	MFA REQUIRED	EXPLANATION
Non-console administrative access to any cardholder data system (remote or LAN-based).	Yes	All non-console access to the CDE requires multifactor authentication. If the system resides in the CDE, admins must be authenticated to the CDE with MFA prior to authenticating to any CDE device with MFA. 8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.
Connecting to any cardholder data system (remote or LAN-based) through a jump box.	Yes	Access to cardholder data environment requires MFA per new V4.0 requirement. All non-console access to the CDE requires multifactor authentication. If the system resides in the CDE, admins must be authenticated to the CDE with MFA prior to authenticating to any CDE device with MFA. All non-console access to the CDE requires multifactor authentication. If the system resides in the CDE, admins must be authenticated to the CDE with MFA prior to authenticating to any CDE device with MFA. 8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

PCI Requirement 8.5.1 includes new testing procedures to follow for validating how MFA systems are implemented. Assessors will need validate the MFA implementation details per the requirement. Requirements 8.4.2 and 8.5.1 are future-dated new requirements in the PCI V4.0 standard. As future-dated new requirements, they are only recommended for implementation until March 31, 2025. After that date, PCI Requirements 8.4.2 and 8.5.1 are mandatory.

IMPLEMENTATION TIMELINE

The PCI v3.2.1 standards will remain active until March 31, 2024, and organizations are not required to use the PCI V4.0 standard until that time.

PCI V4.0 includes future dated new requirements and testing procedures. These future dated new requirements are designated as best practice until March 31, 2025. After March 31, 2025, the future dated new requirements become mandatory and must be considered during an organization's PCI DSS assessment.

BDO USA Can Help

As a Qualified Security Assessor Company (QSAC), BDO USA has experienced QSAs who can assist your organization in understanding and transitioning to the new PCI V4.0 standards.

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

GREG SCHU
Cybersecurity, Compliance, and Assessments Services Principal
gschu@bdo.com

BRIAN HILL
Cybersecurity, Compliance, and Assessments Services Managing Director
bhill@bdo.com

FRED BRANTNER
Cybersecurity, Compliance, and Assessments Services Director
fbrantner@bdo.com

JAMES ROMAN
Cybersecurity, Compliance, and Assessments Services Senior Manager
james.roman@bdo.com