

# Requirement 8: Identify and Authenticate Access to System Components

---



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire [www.withoutfire.com](http://www.withoutfire.com)



## Requirement 8



**Manage user accounts**

**User authentication**

**Multi-factor authentication for higher risk activities**

**Educate users about authentication**

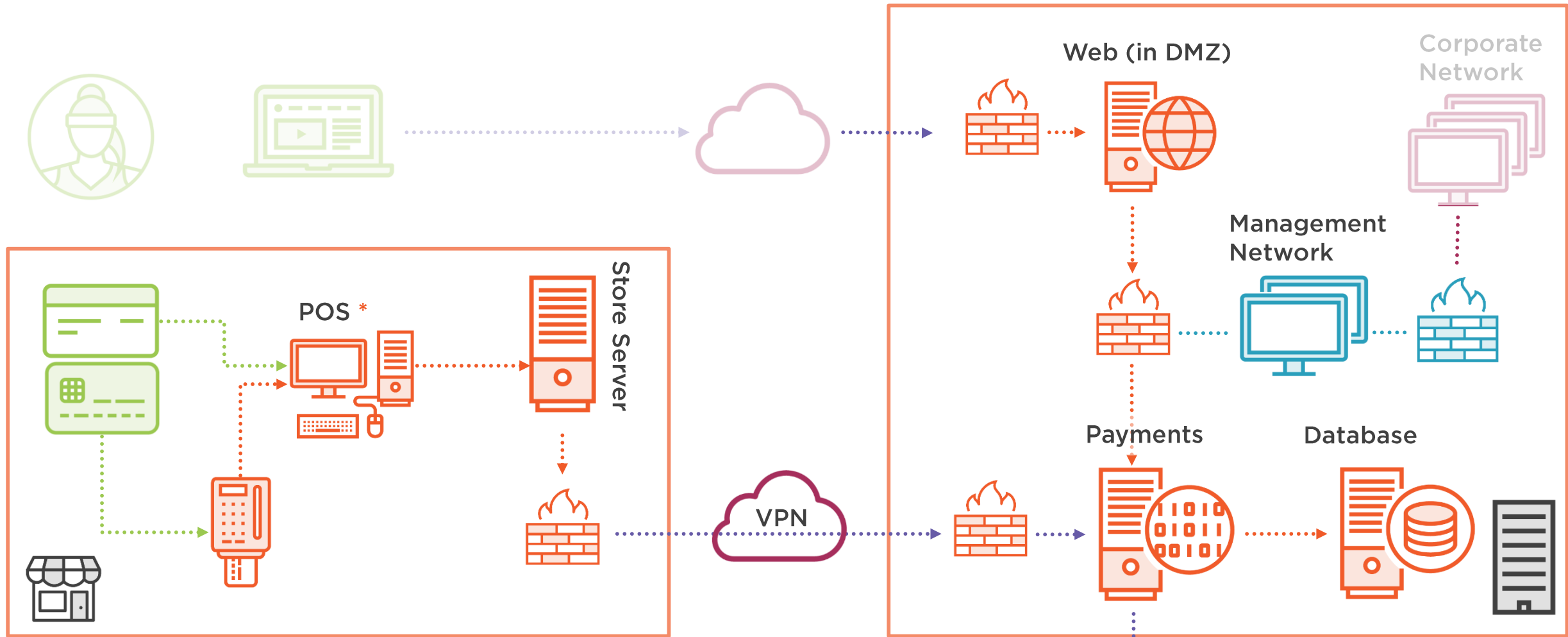
**Limit shared accounts**

**Control physical factors**

**Restrict access to databases**

**Have policies and procedures**





- Cardholder's card and systems
- Stores, processes or transmits
- Connected to or security affecting
- Out of scope of PCI DSS

- Unencrypted cardholder data
- Encrypted cardholder data
- Physical card read
- Management network
- Corporate network





All administrative accounts

All accounts used to view cardholder data

All accounts used to access cardholder data

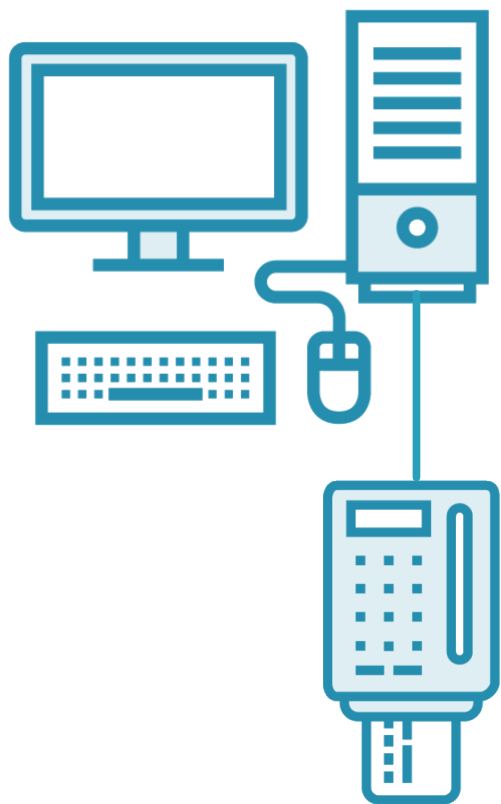
All accounts used to access systems with cardholder data (even if the account has no access to the data itself)

Vendors and third parties



Requirement 8 does not  
apply to customers,  
consumers, or cardholders





## Some requirements \* .....

“are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts)”





## Requirement 8.1

Have policies and processes to manage users, and follow them



## Requirement 8.1

Define and implement policies and procedures to ensure proper user identification management for **non-consumer users** and **administrators** on all system components as follows:

See 8.1.1 through 8.1.8



## Requirement Guidance

- There's no specific guidance for requirement 8.1



# 1.1 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	<b>Y</b>	<b>Policies and procedures</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	





## Requirement 8.1.1 \*

Have unique user IDs





### Requirement 8.1.1 \*

Assign all users a **unique ID before** allowing them to access system components or cardholder data.



### Requirement Guidance

- By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.

## 8.1.1 \* Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	-	
<b>Examine records</b>	-	
<b>Interview people</b>	Y	System administrators





## Requirement 8.1.2 & 8.1.3

Effective joiners, movers and leavers (JML)



### Requirement 8.1.2

Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.



### Requirement Guidance

- To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.



### Requirement 8.1.3

**Immediately revoke** access for any **terminated users**.



### Requirement Guidance

- If an employee has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account. To prevent unauthorized access, user credentials and other authentication methods therefore need to be revoked promptly (as soon as possible) upon the employee's departure.

## 8.1.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Verify user ID authorizations and privileges</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Approval records</b>
<b>Interview people</b>	<b>-</b>	





## 8.1.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>User access lists</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Terminated users</b>
<b>Interview people</b>	<b>-</b>	





## Requirement 8.1.4

Deactivate inactive user accounts





#### Requirement 8.1.4

**Remove** or **disable** inactive user accounts **within 90 days**.



#### Requirement Guidance

- Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.

## 8.1.4 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Any inactive user accounts</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.1.5

Management of third party user IDs used for  
“remote access”





## Requirement 8.1.5

**Manage IDs** used by **third parties** to access, support, or maintain system components **via remote access** as follows:

**Enabled only during the time period needed and disabled when not in use.**

**Monitored** when **in use**.



## Requirement Guidance

- Allowing vendors to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed, and disabling it as soon as it is no longer needed, helps prevent misuse of these connections.
- Monitoring of vendor access provides assurance that vendors are accessing only the systems necessary and only during approved time frames.

## 8.1.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Processes used by 3<sup>rd</sup> parties</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 8.1.6 \* & 8.1.7 \*

Lock accounts after six failed logins for at least 30 minutes





### Requirement 8.1.6 \*

Limit repeated access attempts by **locking out** the **user ID** after not more than **six attempts**.



### Requirement Guidance

- Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.



### Requirement 8.1.7 \*

Set the **lockout duration** to a minimum of **30 minutes** **or until** an **administrator** enables the user ID.



### Requirement Guidance

- If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the admin or help desk can validate that it is the actual account owner requesting reactivation.

## 8.1.6 & 8.1.7 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configuration settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.1.8 \*

Lock inactive user sessions after 15 minutes





### Requirement 8.1.8 \*

If a **session** has been **idle** for more than **15 minutes**, require the **user** to **re-authenticate** to re-activate the terminal or session.



### Requirement Guidance

- When users walk away from an open machine with access to critical system components or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse.
- The re-authentication can be applied either at the system level to protect all sessions running on that machine, or at the application level.

## 8.1.8 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configuration settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.2 \*

At least single-factor authentication





## Requirement 8.2 \*

In **addition to** assigning a unique **ID**, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at **least one** of the following to authenticate all users:

Something **you know**, like a password or passphrase  
Something **you have**, like a token device or smart card  
Something **you are**, like a biometric.



## Requirement Guidance

- These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Note that a digital certificate is a valid option for “something you have” as long as it is unique for a particular user.
- Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.



## 8.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe an authentication</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Authentication methods</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.2.1

Encrypt password in transit  
and storage with strong cryptography

“Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices”

## **Strong Cryptography**

[www.pcisecuritystandards.org/documents/PCI\\_DSS\\_Glossary\\_v3-2.pdf](http://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf)

*See: NIST Special Publication 800-57 Part 1*





## Requirement 8.2.1

Using **strong cryptography**, render all authentication credentials (such as passwords/phrases) unreadable during **transmission** and **storage** on all system components.



## Requirement Guidance

- Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a “sniffer,” or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access.

## 8.2.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Configuration settings, password files, data transmissions</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Vendor documentation</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.2.2

Check if someone is who they say they are before changing their security things





## Requirement 8.2.2

**Verify user identity** before **modifying** any authentication **credential**— for example, performing password resets, provisioning new tokens, or generating new keys.



## Requirement Guidance

- Many malicious individuals use “social engineering”— for example, calling a help desk and acting as a legitimate user — to have a password changed so they can utilize a user ID. Consider use of a “secret question” that only the proper user can answer to help administrators identify the user prior to re-setting or modifying authentication credentials.

## 8.2.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe security people</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Examine authentication procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	







## Requirement 8.2.3 \*

Seven character passwords

Alpha and numeric

Like **passwo1**





### Requirement 8.2.3 \*

Passwords/passphrases must meet the following:

Require a minimum length of at least **seven characters**.

Contain both **numeric** and **alphabetic** characters.

Alternatively, the passwords/passphrases must have complexity and **strength** at least **equivalent** to the parameters specified above.



### Requirement Guidance

- This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/ passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use “equivalent strength” to evaluate their alternative. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.)



## 8.2.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configuration settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.2.4 \*

Force password change every 90 days





#### Requirement 8.2.4 \*

Change user passwords / passphrases at least once every 90 days.



#### Requirement Guidance

- Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to work on breaking the password/phrase.

## 8.2.4 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configuration settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	



Doesn't this go  
against all modern  
guidance?

Yes

See FAQ 1467

*“Can organizations use alternative  
password management methods to  
meet PCI DSS Requirement 8?”*

[www.pcisecuritystandards.org/faqs](https://www.pcisecuritystandards.org/faqs)





## Requirement 8.2.5 \*

Don't allow users to repeat passwords  
(last four)







### Requirement 8.2.5 \*

Do not allow an individual to submit a new password/passphrase **that is the same as any of the last four passwords/passphrases** he or she has used.



### Requirement Guidance

- If password history isn't maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period of time reduces the likelihood that passwords that have been guessed or brute-forced will be used in the future.

## 8.2.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>System configuration settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.2.6

Ensure initial passwords are unique and must be changed by the user when they first login





### Requirement 8.2.6

Set passwords/passphrases for **first-time use** and upon reset to a **unique value for each user**, and **change immediately** after the **first use**.

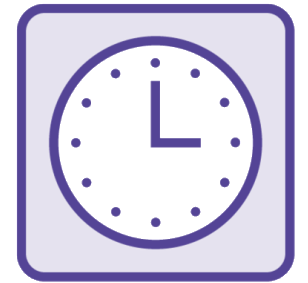


### Requirement Guidance

- If the same password is used for every new user, an internal user, former employee, or malicious individual may know or easily discover this password, and use it to gain access to accounts.

# Unique Passwords

This is the 45<sup>th</sup>  
time this week  
I've had to think  
of a unique  
password!



TownHall15



## 8.2.6 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe security personnel and system configuration</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Password procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.3

Require MFA for:

1. All non-console admin access
2. All remote access to the CDE





### Requirement 8.3

Secure all individual non-console administrative access and all remote access to the CDE using **multi-factor** authentication.

Know	password
Have	token
Are	biometric



### Requirement Guidance

- Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted.
- Multi-factor authentication is **not required** at **both** the **system-level** and **application-level** for a particular system component. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component.



## 8.3 Testing Procedures

**There really are no specific testing procedures for 8.3**

**Observe/examine  
systems and settings**

-

**Examine documentation**

-

**Examine records**

-

**Interview people**

-





### Requirement 8.3.1

Incorporate **multi-factor authentication** for all **non-console access** into the CDE for personnel with **administrative** access.



### Requirement Guidance

- If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use MFA either when logging onto the CDE network or onto a system.
- If the CDE is segmented from the rest of the network, an administrator should use MFA when connecting to a CDE system from a non-CDE network. MFA can be implemented at network level or at system/application level; it does not have to be both. If the administrator uses MFA when logging into the CDE network, they do not also need to use MFA to log into a particular system or application within the CDE.



### Requirement 8.3.2

Incorporate **multi-factor authentication** for all **remote** network access (both **user and administrator**, and including third-party access for support or maintenance) originating from outside the entity's network.



### Requirement Guidance

- This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, MFA for remote access to that network would not be required. However, MFA is required for any remote access to networks with access to the CDE, and is recommended for all remote access to the entity's networks.



### Requirement 8.3.2

Incorporate **multi-factor authentication** for all **remote network access** (both **user and administrator**, and including third-party access for support or maintenance) originating from outside the entity's network.



### Requirement Guidance

- This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, MFA for remote access to that network would not be required. However, MFA is required for any remote access to networks with access to the CDE, and is recommended for all remote access to the entity's networks.





### Requirement 8.3.2

Incorporate **multi-factor authentication** for all **remote network access** (both **user and administrator**, and including third-party access for support or maintenance) **originating from outside the entity's network.**



### Requirement Guidance

- This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, MFA for remote access to that network would not be required. However, MFA is required for any remote access to networks with access to the CDE, and is recommended for all remote access to the entity's networks.



## 8.3.1 & 8.3.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Examine system configurations for remote access</b> <b>Observe logins</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 8.4

Let users know the authentication rules





## Requirement 8.4

**Document & communicate** authentication **policies** and **procedures** to all users including:

**Selecting strong** authentication credentials and how to **protect** authentication **credentials**. Instructions **not to reuse passwords** and to **change passwords if** there is any suspicion the password could be **compromised**.



## Requirement Guidance

- Communicating password/authentication policies and procedures helps users understand and abide by the policies.
- Guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don't contain dictionary words, and that don't contain information about the user. Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files, and being alert for malicious individuals who may attempt to exploit their passwords.



## 8.4 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Authentication policies and procedures for users
<b>Examine records</b>	-	
<b>Interview people</b>	Y	Users





## Requirement 8.5 \*

Don't use generic or shared IDs

(In some circumstances shared IDs are OK)





## Requirement 8.5 \*

**Do not use group, shared, or generic IDs**, passwords, or other authentication methods as follows:

1. **Generic user IDs** are **disabled** or **removed**.
2. **Shared** user **IDs** do **not** exist for system **administration** and other critical functions.
3. **Shared** and generic user IDs are **not** used to **administer** any system components.



## Requirement Guidance

- If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.

## 8.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>User ID lists</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Authentication policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>System administrators</b>





## Requirement 8.5.1

Remote access for service providers – use unique credentials for each customer



## Requirement 8.5.1

*Additional requirement for service providers only:* **Service providers** with **remote access** to customer premises (for example, for support of POS systems or servers) must use a **unique authentication credential** (such as a password / phrase) **for each customer**.



## Requirement Guidance

- To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer.
- Technologies, such as multi-factor mechanisms, that provide a unique credential for each connection (for example, via a single-use password) could also meet the intent of this requirement.

## 8.5.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Authentication policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Users / administrators</b>





## Requirement 8.6

Physical authentication factors must not be shared







## Requirement 8.6

Where other authentication mechanisms are used, use of these mechanisms must be assigned as follows:

- Authentication mechanisms must be **assigned to an individual account** and not shared among multiple accounts.
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.



## Requirement Guidance

- If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism.

## 8.6 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Configuration settings and/or physical controls</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Authentication policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Security personnel</b>





## Requirement 8.7

Prohibit direct query access to databases containing cardholder data (except DBAs)





## Requirement 8.7

All access to **any database containing cardholder data is restricted** as follows:

All **user access** is through **programmatic** methods.

Only **database administrators** have the ability to directly access or **query databases**.

Application IDs for database applications can only be used by the applications.



## Requirement Guidance

- Without user authentication for access to databases and applications, the potential for unauthorized or malicious access increases, and such access cannot be logged since the user has not been authenticated and is therefore not known to the system. Also, database access should be granted through programmatic methods only (for example, through stored procedures), rather than via direct access to the database by end users (except for DBAs, who may need direct access to the database for their administrative duties).



## 8.7 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Database and application configuration and database access control settings</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





# Requirement 8.8

Policies and procedures





## Requirement 8.8

Ensure that **security policies** and operational **procedures** for identification and authentication are **documented, in use**, and **known** to all affected parties.



## Requirement Guidance

- Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.

## 8.8 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Security policies, Operational procedures
<b>Examine records</b>	-	
<b>Interview people</b>	Y	People who need to know the policies and procedures





# That's Fine in Theory

