

# Requirement 2: Do Not Use Vendor-supplied Defaults

---



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

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



## Requirement 2



**Default parameters**

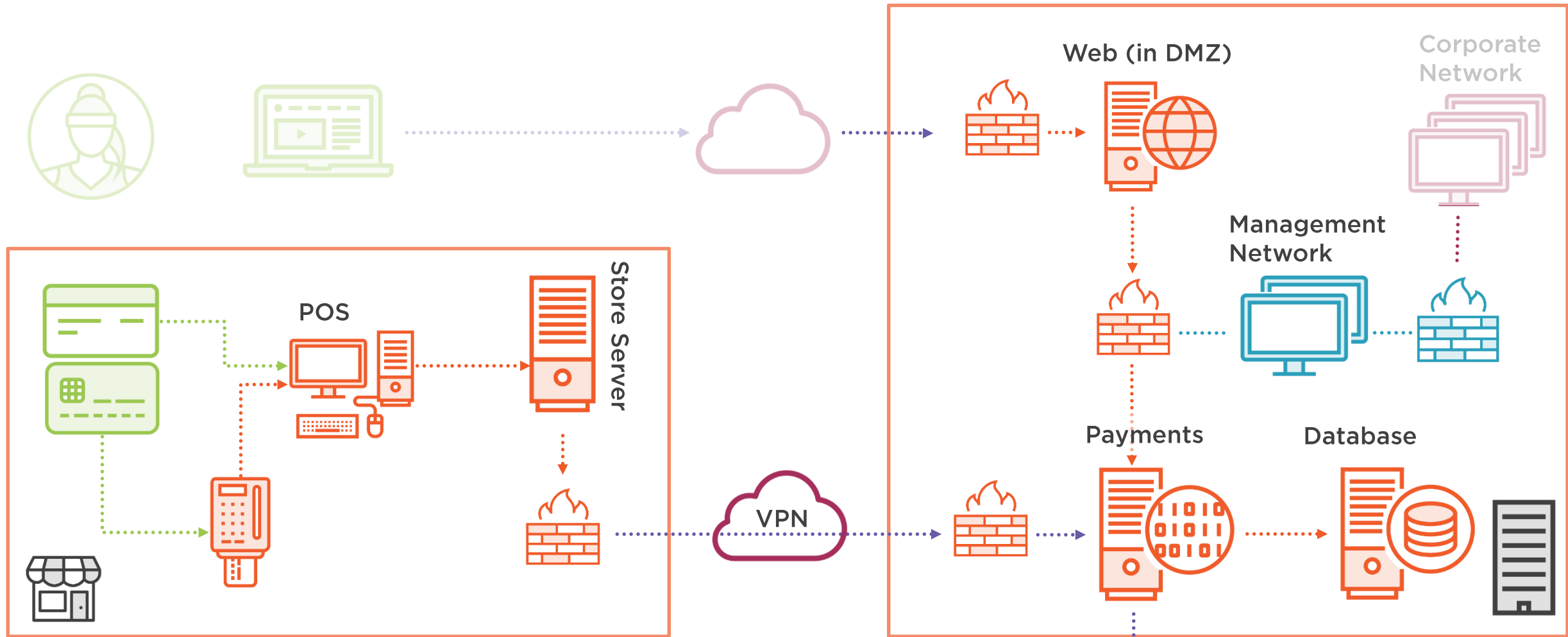
**Hardened builds**

**Encrypt admin access**

**Inventories**

**Policies and procedures**







## Requirement 2.1

New system?

- a) Change default passwords
- b) Remove or disable default accounts





## Requirement 2.1

Always **change** vendor-supplied defaults and remove or **disable** unnecessary default accounts **before** installing a system on the network



## Requirement Guidance

- Malicious individuals often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack.
- Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

## 2.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Attempt default log on to sample components</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Supporting documents</b>
<b>Examine records</b>	<b>Y</b>	<b>Accounts on sample components</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.1.1

Change all defaults on wireless networks.

Don't use WEP





### Requirement 2.1.1

For wireless environments connected to the cardholder data environment or transmitting cardholder data, change **ALL** wireless **vendor defaults** at installation, including but not limited to **default wireless encryption keys, passwords**, and SNMP community strings.



### Requirement Guidance

- If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network.
- In addition, the key-exchange protocol for older versions of 802.11x encryption (Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.





## 2.1.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Wireless configuration settings</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Supporting documents, vendor documents, policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.2

Develop secure configuration standards for everything



## Requirement 2.2

Develop **configuration standards** for **all system components**. Assure that these standards address all known security vulnerabilities and are consistent with **industry-accepted system hardening standards**.



## Requirement Guidance

- There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses.
- System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.



[www.cisecurity.org/cis-benchmarks/](http://www.cisecurity.org/cis-benchmarks/)



## 2.2 Testing Procedures

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

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.2.1

Servers: You had one job ...



## Requirement 2.2.1

Implement only **one primary function per server** to prevent functions that require different security levels from co-existing on the same server.

(For example, web servers, database servers, and DNS should be implemented on separate servers.)

.



## Requirement Guidance

- If server functions that need different security levels are located on the same server, the security level of the functions with higher security needs would be reduced due to the presence of the lower-security functions. Additionally, the server functions with a lower security level may introduce security weaknesses to other functions on the same server. By considering the security needs of different server functions as part of the system configuration standards and related processes, organizations can ensure that functions requiring different security levels don't co-exist on the same server.

## 2.2.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Configurations on components and virtualization technologies</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters







## Requirement 2.2.2

Only enable necessary things



### Requirement 2.2.2

Enable only **necessary** services, protocols, daemons, etc., as required for the function of the system.



### Requirement Guidance

- As stated in Requirement 1.1.6, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. Including this requirement as part of an organization's configuration standards and related processes ensures that only the necessary services and protocols are enabled.

## 2.2.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Enabled services etc. on system components</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 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.2.3

Secure the insecure

(services, protocols, etc.)





### Requirement 2.2.3

Implement **additional security features** for any required services, **protocols**, or daemons that are considered to be **insecure**.



### Requirement Guidance

- Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations.
- Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network.
- Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).



## 2.2.3 Testing Procedures

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

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.2.4

Use the security functions  
available in the systems



#### Requirement 2.2.4

Configure system security parameters to prevent misuse.



#### Requirement Guidance

- System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use.
- In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.



## 2.2.4 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Sample of system components</b>
<b>Examine documentation</b>	<b>Y</b>	<b>System configuration standards</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>System administrators</b>

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.2.5

Remove all unnecessary functionality





### Requirement 2.2.5

**Remove all unnecessary functionality**, such as scripts, drivers, features, subsystems, file systems, and **unnecessary web servers**.



### Requirement Guidance

- Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. By removing unnecessary functionality, organizations can focus on securing the functions that are required and reduce the risk that unknown functions will be exploited.
- Including this in server-hardening standards and processes addresses the specific security implications associated with unnecessary functions (for example, by removing/disabling FTP or the web server if the server will not be performing those functions).



## 2.2.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Sample of system components</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Functionality documents</b>
<b>Examine records</b>	<b>Y</b>	<b>Security parameters</b>
<b>Interview people</b>	<b>-</b>	

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters

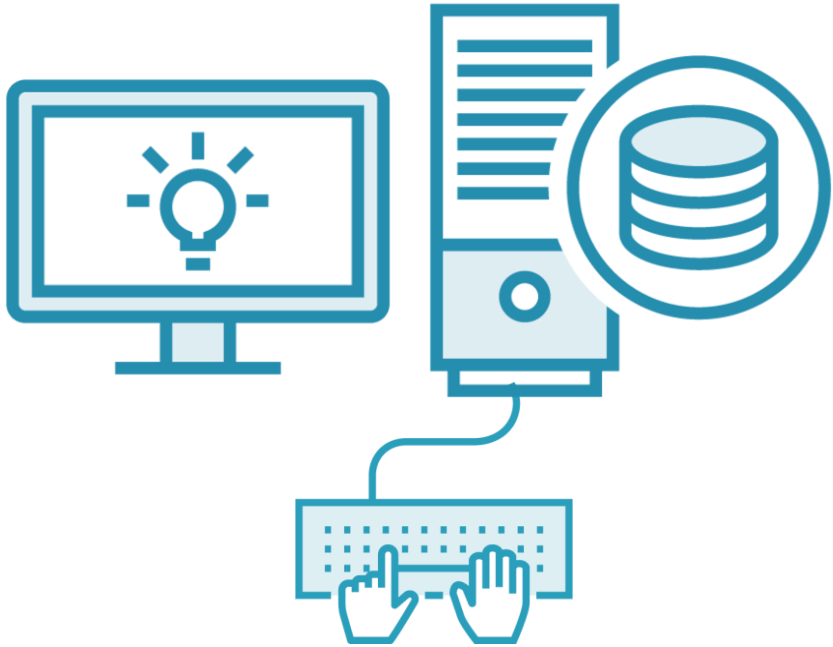




## Requirement 2.3

Encrypt non-console admin access

# Console



# Non-console





### Requirement 2.3

Encrypt all non-console administrative access using **strong cryptography**.



### Requirement Guidance

- Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information.
- To be considered “strong cryptography,” industry- recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to “strong cryptography” in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)



“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*





## 2.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Admin logins to a sample of systems and system components</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Vendor documents</b>
<b>Examine records</b>	<b>Y</b>	<b>System configurations Services and parameter files</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.4

Maintain an inventory of system components that are in scope for PCI DSS

(That's really 2005 talking)





## Requirement 2.4

Maintain an inventory of system components that are in scope for PCI DSS.



## Requirement Guidance

- Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards.

## 2.4 Testing Procedures

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

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.5

Have the necessary policies, procedures, and standards



## Requirement 2.5

Ensure that **security policies** and operational procedures for managing vendor defaults and other security parameters are **documented, in use**, and **known** to all affected parties.



## Requirement Guidance

- Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.

## 2.5 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	<b>Security policies and operational procedures</b>
<b>Examine records</b>	-	
<b>Interview people</b>	Y	<b>Responsible people and people who need to know</b>

Requirement 2 | Do not use vendor-supplied defaults for system passwords and other security parameters





## Requirement 2.6

Shared hosting providers must meet the requirements in *Appendix A1*





## Requirement 2.6

Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers*.



## Requirement Guidance

- This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients. This allows clients to add insecure functions and scripts that impact the security of all other client environments; and thereby make it easy for a malicious individual to compromise one client's data and thereby gain access to all other clients' data. See *Appendix A1* for details of requirements.



# That's Fine in Theory

