Dell Networking Support for Payment Card Industry Data Security Standard

A Dell Best Practices Guide

Dell Engineering
January 2014
## Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2014</td>
<td>Version 1.0</td>
<td>Tracy Alonzo</td>
</tr>
</tbody>
</table>
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisions</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>1 Build and Maintain a Secure Network</td>
<td>9</td>
</tr>
<tr>
<td>1.1 Install and Maintain a Firewall Configuration to Protect Cardholder Data</td>
<td>9</td>
</tr>
<tr>
<td>1.2 Inventory network</td>
<td>9</td>
</tr>
<tr>
<td>1.3 Secure and synchronize configuration files</td>
<td>9</td>
</tr>
<tr>
<td>2 Do not use Vendor-supplied Defaults for System Passwords and other Security Parameters</td>
<td>10</td>
</tr>
<tr>
<td>2.1 Change vendor-supplied defaults before installing into network including wireless environments</td>
<td>10</td>
</tr>
<tr>
<td>2.2 Use secured technologies such as SSH, HTTPS and IPSEC in place of services like Telnet and HTTP</td>
<td>10</td>
</tr>
<tr>
<td>2.3 Encrypt non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for WEB based management</td>
<td>10</td>
</tr>
<tr>
<td>3 Maintain a vulnerability management program</td>
<td>11</td>
</tr>
<tr>
<td>3.1 Ensure a system is protected by having the latest vendor-supplied security patches</td>
<td>11</td>
</tr>
<tr>
<td>4 Implement Strong Access Control Measures</td>
<td>12</td>
</tr>
<tr>
<td>4.1 Restrict access to cardholder data to authorized individuals only</td>
<td>12</td>
</tr>
<tr>
<td>4.1.1 Restrict user access rights from least privileges to most privileges</td>
<td>12</td>
</tr>
<tr>
<td>4.1.2 Default Deny all setting</td>
<td>12</td>
</tr>
<tr>
<td>4.2 Assign a unique ID to each person with computer access</td>
<td>12</td>
</tr>
<tr>
<td>4.2.1 Assign all users a unique ID before allowing them system access to cardholder data</td>
<td>13</td>
</tr>
<tr>
<td>4.2.2 Secure remote access</td>
<td>13</td>
</tr>
<tr>
<td>4.2.3 Render all passwords unreadable during transmission and when stored</td>
<td>13</td>
</tr>
<tr>
<td>4.2.4 Remove/disable inactive user accounts at least every 90 days</td>
<td>13</td>
</tr>
<tr>
<td>4.2.5 Change user passwords at least every 90 days</td>
<td>14</td>
</tr>
<tr>
<td>4.2.6 Provide a minimum password length of at least seven characters</td>
<td>14</td>
</tr>
<tr>
<td>4.2.7 Use passwords containing both numeric and alphabetic characters</td>
<td>14</td>
</tr>
<tr>
<td>4.2.8 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used</td>
<td>14</td>
</tr>
<tr>
<td>4.2.9 Limit repeated access attempts by locking out the user after six attempts</td>
<td>14</td>
</tr>
<tr>
<td>4.2.10 Set the lockout duration to a minimum of 30 minutes or until the administrator enables the user ID</td>
<td>15</td>
</tr>
<tr>
<td>4.2.11 If a session has been idle for more than 15 minutes, ask the user to re-authenticate to re-activate the terminal or session</td>
<td>15</td>
</tr>
</tbody>
</table>
4.2.12 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment................................................................. 15
4.2.13 Restrict physical access to publically assessable network jacks ................................................................. 15
5 Regularly Monitor and Test the Network ........................................................................................................... 17
5.1 Track and Monitor all Access to Network Resources and Cardholder Data......................................................... 17
5.1.1 Monitor all actions taken by any individual with root or administrative privileges ........................................ 17
5.1.2 Log access to audit trails .......................................................................................................................... 17
5.1.3 Log invalid access attempts ....................................................................................................................... 17
5.1.4 Log the user identifications and authentications in the audit trail ............................................................. 18
5.1.5 Initialization of audit logs ......................................................................................................................... 18
5.1.6 Create and delete system level objects ....................................................................................................... 18
5.1.7 Log user identification in log entries ......................................................................................................... 18
5.1.8 Include type of events in logs ..................................................................................................................... 19
5.1.9 Include date and time stamp in log entries ................................................................................................. 19
5.1.10 Log successful and failed events ............................................................................................................. 19
5.1.11 Include origin of events in logs ................................................................................................................. 20
5.1.12 Include name of modified or altered system components in logs ............................................................. 20
5.1.13 Ensure that time data is protected ........................................................................................................... 20
5.1.14 Limit viewing of audit trails to those with a job-related need ............................................................... 21
6 Other Recommendations ................................................................................................................................... 22
6.1 SNMP Community Strings ............................................................................................................................. 22
6.2 Shutdown Unused Switch Ports ..................................................................................................................... 22
6.3 Secure Telnet Switch Access ........................................................................................................................ 22
6.4 Secure Console Switch Access .................................................................................................................... 23
6.5 Secure Shell Switch Access .......................................................................................................................... 23
Additional resources .......................................................................................................................................... 24
Executive Summary

The Payment Card Industry (PCI) Data Security Standard (DSS) applies to any organization that transmits, processes, or stores payment card transactions or cardholder Information. It is the responsibility of the organization to protect the privacy and confidentiality of debit and credit card data. The PCI DSS standard was created and enforced by the major credit card companies. Dell provides a product portfolio which includes the N-Series switch portfolio for deployments that support PCI compliance and contribute to recommended best practices in network security.

As with other regulations and guidelines, PCI DSS compliance cannot be achieved through technology alone. It requires the organization to build, maintain and monitor a secure network to protect the privacy and confidentiality of debit and credit card data. This paper guides you on how to create a network that meets the requirements of PCI DSS utilizing Dell’s Networking N-Series switch solutions.

Introduction

The PCI DSS consists of six major categories encompassing twelve security areas defined within DSS 3.0. Dell supports PCI compliance through network products and security policies and procedures. Dell networking N-Series switches provide the features to support an organization’s ability to successfully achieve PCI compliance. The following table summarizes these requirements:

<table>
<thead>
<tr>
<th>Build and maintain a secure network</th>
<th>Requirement</th>
<th>Applicable Requirements</th>
<th>Dell Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
<td>1.1.2 Inventory network</td>
<td>Dell networking Open Manage Network Manager, OpenManage Essentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.2.2 Secure and synchronize configuration files</td>
<td>Dell networking N-Series</td>
<td></td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>2.1 Change vendor supplied defaults before installing into network including wireless environments</td>
<td>Dell networking N-Series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2.2 Use secured technologies such as SSH, IPSec , and HTTPs in place of services like Telnet, and HTTP</td>
<td>Dell networking N-Series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.3 Encrypt non console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for WEB based management</td>
<td>Dell networking N-Series</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protect cardholder data</th>
<th>Requirement</th>
<th>Applicable Requirements</th>
<th>Dell Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Protect stored cardholder data</td>
<td>3.1 to 3.6.8 Implement data retention and disposal policies, procedures, and processes for all cardholder data storage</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>4. Encrypt transmissions of cardholder data</td>
<td>4.1 to 4.2 Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>across open, public networks</td>
<td>individuals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Maintain a vulnerability management program**

<table>
<thead>
<tr>
<th>5. Use and regularly update anti-virus software or programs</th>
<th>5.1 to 5.2 Deploy anti-virus software on all systems commonly affected by malicious software</th>
<th>Not Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Develop and maintain secure systems and applications</td>
<td>6.1 Provide methods to maintain current vendor security patches and updated patches</td>
<td>Dell networking N-Series</td>
</tr>
</tbody>
</table>

**Implement strong access control measures**

<table>
<thead>
<tr>
<th>7. Restrict access to cardholder data by business need to know</th>
<th>7.1.1 Restrict access rights to privileged user IDs to least privileges necessary to perform job responsibilities</th>
<th>Dell networking N-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.2.3 Default &quot;deny-all&quot; settings</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access</td>
<td>8.1 Assign all users a unique ID for system access</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.2 Users must be authenticated to access system</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.3 Secure Remote Access</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.4 Render all passwords unreadable during transmission and storage</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.5 Inactive accounts can be removed from system</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.9 Change user password at least every 90 days</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.10 Require minimum password length</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.11 Use passwords containing both numeric and alphabetic characters</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.12 New passwords cannot be same as previous used passwords</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.13 User locked out after six invalid logon attempts</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.14 Lockout duration of 30 minutes and/or administrative reset</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td></td>
<td>8.5.15 Idle timeout for 15 minutes or less</td>
<td>Dell networking N-Series</td>
</tr>
<tr>
<td>9. Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment</td>
<td>9.1.2 Restrict physical access to publically assessable network jacks</td>
<td>Dell networking N-Series</td>
</tr>
</tbody>
</table>

**Regularly monitor and test networks**
| 10. Track and monitor all access to network resources and cardholder data | 10.2.4  Monitor actions taken by any individual with root or administrator privileges | Dell networking N-Series |
| | 10.2.3  Log access to audit trails | Dell networking N-Series |
| | 10.2.4  Log invalid access attempts | Dell networking N-Series |
| | 10.2.5  Log user identifications and authentications in the audit trail | Dell networking N-Series |
| | 10.2.6  Initialization of audit logs | Dell networking N-Series |
| | 10.2.7  Log creation and deletion of system level objects | Dell networking N-Series |
| | 10.3.1  User identification included in log entries | Dell networking N-Series |
| | 10.3.2  Type of event included in log entries | Dell networking N-Series |
| | 10.3.3  Date and time included in log entries | Dell networking N-Series |
| | 10.3.4  Failure indications are included in log entries | Dell networking N-Series |
| | 10.3.5  Origin of events included in log entries | Dell networking N-Series |
| | 10.3.6  Identity or name of changed system component is included in log entries | Dell networking N-Series |
| | 10.4.1  System clocks and times are synchronized with industry accepted time resources | Dell networking N-Series |
| | 10.5.1  Restrict audit trail views to need to know basis | Dell networking N-Series |
| | 10.2.2  Log administrative privilege actions | Dell networking N-Series |

| 11. Regularly test security systems and processes | 11.1 to 11.5 System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment | Not Applicable |

| Maintain an information security policy | 12. Maintain a policy that addresses information security for all personnel | 12.1 to 12.9.6 Establish, publish, maintain, and disseminate a security policy that accomplishes all PCI requirements, includes annual policy reviews, incorporates operational security procedures | Not Applicable |

Table 1  PCI Requirements Checklist
1 Build and Maintain a Secure Network

This section describes the steps to build and maintain a secure network.

1.1 Install and Maintain a Firewall Configuration to Protect Cardholder Data

Firewalls are devices that not only control traffic allowed between an entity’s internal networks and external untrusted networks but also into and out of sensitive areas such as cardholder data within an entity’s internal trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

1.1.2 Inventory network

Dell N-Series together with Open Manage Network Manager and OpenManage Essentials maintains an inventory of the network infrastructure.

1.1.3 Secure and synchronize configuration files

Dell N-Series switches allow for the running configuration file to be used for normal operations and startup configuration file to be used when the switch is rebooted. The files are fully synchronized with the same configuration.
2 Do not use Vendor-supplied Defaults for System Passwords and other Security Parameters

Malicious individuals (external and internal to an organization) often use vendor default passwords and other default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

2.1.1 Change vendor-supplied defaults before installing into network including wireless environments

Dell N-Series switches do not supply default username and passwords. Although this is a good practice, there are a number of other default settings that should be changed, such as SNMP community strings. (See Section 4.1 for recommended configuration).

2.1.2 Use secured technologies such as SSH, HTTPS and IPSEC in place of services like Telnet and HTTP

Dell N-Series switches and W-Series controllers support SSH, and HTTPS secure technologies as alternatives to insecure technologies such as Telnet and HTTP.

2.1.3 Encrypt non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for WEB based management

Dell N-Series switches provide encrypted technologies such as SSH and HTTPS for WEB based and Out-of-band management.
3  Maintain a vulnerability management program

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by security patches provided by the vendor, which must be installed by the entities that manage the system. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

3.1.1  Ensure a system is protected by having the latest vendor-supplied security patches

Dell N-Series switches support several methods to update system firmware as new images become available. The following command is an example of how the firmware image on the switch is updated using a remote TFTP server:

```
console#copy tftp://172.25.114.14/N4000_6108.stk active
```

Reset the switch to boot the system with the new image.

```
console#reload
Are you sure you want to continue? (y/n)y
```

Reloading all switches...

The system will reboot. After the system reboots, type the following commands:

```
console #boot system active
console#show bootvar
```

The screen displays the following information:

Image Descriptions

active :

backup :

Images currently available on Flash

unit active backup current-active next-active

----- ------------ ---- ------------ ----

1  6.19.03  6.19.03  6.19.03  6.19.03
4. Implement Strong Access Control Measures

This section describes the steps to implement strong access control.

4.1. Restrict access to cardholder data to authorized individuals only

To ensure that critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on the need-to-know and the job responsibilities.

4.1.1. Restrict user access rights from least privileges to most privileges

The Dell N-Series switches support the ability to limit and/or control access to what is only necessary to the user. The following example creates a user login restricting the user to level 1 access:

```
console# username pci password test privilege level 1
```

In this example, a user login is created allowing access to privilege level 15:

```
Console(config)#username xyz password xxxyyyyzzz privilege level 15
```

The Dell N-Series support two access levels to the switch, access level 1 for read privilege and access level 15 for Read/Write privileges

4.1.2. Default Deny all” setting

The Dell N-Series switches default to implicit deny all rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit deny all rule is applied and the packet is dropped.

The implicit deny all statement at the end of the access list is not shown and is not editable.

4.2. Assign a unique ID to each person with computer access

Assigning a unique identification to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by and can be traced to, known and authorized users.
4.2.1 Assign all users a unique ID before allowing them system access to cardholder data

The Dell N-Series switches support the ability to assign user names and passwords to control user access to the switch. The following is an example of a command to create a user identification with password to control access to the switch:

```
Console(config)#username xyz password xxxyyyyzzz
```

4.2.2 Secure remote access

The Dell N-Series switches and provide RADIUS and TACACS as secure remote access method.

4.2.3 Render all passwords unreadable during transmission and when stored

The Dell N-Series switches encrypt passwords for all access methods. The following example shows password protected by encryption:

Type the following command:

```
console#show startup-config
```

The following information is displayed on the screen:

```
username "admin" password 0390edfae62dd382b6ecbd6e425f499b privilege 15 encrypted
username "abc" password c2545ed1142f2f4ac9956800bdb13e2e privilege 1 encrypted
aaa authentication login "defaultList" local enable line
line console
password f96aa76938f30f0ff60f2ccce864ed0 encrypted
exit
snmp-server engineid local 800002a203001ec9ded247
snmp-server agent boot count 3
enable password 76cc181783fd2d191d08e5d2ec07ffa0 encrypted
```

4.2.4 Remove/disable inactive user accounts at least every 90 days

The Dell N-Series switches provide the capability to remove inactive user accounts. The following example shows a user login history that has been inactive greater than 90 days then the account is removed from the local database:

```
Console#show users login-history
```

Login Time Username Protocol Location
4.2.5  Change user passwords at least every 90 days
The Dell N-Series switches support password expiration up to 365 days. The following example changes the password age limit to 90 days:

Console(config)#password aging 90

4.2.6  Provide a minimum password length of at least seven characters
Dell N-Series switches support a range of 8–64 minimum password characters. The following example sets the minimum password length to 9 characters:

Console(config)#password min-length 9 (system defaults to 8 characters)

4.2.7  Use passwords containing both numeric and alphabetic characters
Dell N-Series switches are configurable to require both numeric and alphabetic characters in the login password. The following example sets the password to require both numeric and alphabetic characters:

console(config)#passwords strength check enabled
console(config)#passwords strength minimum numeric-characters 3
console(config)#passwords strength minimum uppercase-letters 6
Console(config)#password strength minimum character-class 2

4.2.8  Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
The Dell N-Series switches support the ability to set the number of previous passwords to store. When a user changes password, the user is not able to reuse any of the passwords stored in password history. The following is an example of a command that sets the number of previous passwords remembered by the switch to four:

Console(config)#password history 4

4.2.9  Limit repeated access attempts by locking out the user after six attempts
The Dell N-Series switches support the ability to lock out user accounts that fail login due to wrong password. The following is an example of a command that sets the number of user attempts before lock-out at 6:

Console(config)#password lock-out 6
4.2.10 Set the lockout duration to a minimum of 30 minutes or until the administrator enables the user ID

If the user is locked out, the Dell N-Series switches remain locked out until the administrator resets the password or clears the configuration by accessing the switch through the serial console port.

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

The Dell N-Series switches allow for idle timeout settings. If user has been logged on and the idle timer expires, the user is logged off and required to re-authenticate. The following example sets the idle timeout to 15 minutes before session is logged off:

```
console(config)#line console
console(config-line)#exec-timeout 15
```

4.2.12 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

4.2.13 Restrict physical access to publically assessable network jacks

The Dell N-Series switches provide port security. MAC Locking remembers the MAC address connected to the switch port and allows only that MAC address to communicate on that port. If any other MAC address tries to connect, the port security disables port.

The following example enables port security over a range of switch ports to limit the number of source MAC addresses that can be learned to 10 and then discard unlearned frames:

```
console(config)#int range gi1/0/3-10
console(config-if)#port security max 10
console(config-if)#port security discard
```

```
console(config)#do show ports security

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Action</th>
<th>Maximum</th>
<th>Trap</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>------</td>
<td>-----------</td>
</tr>
<tr>
<td>Gi1/0/1</td>
<td>Unlocked</td>
<td>-</td>
<td>100</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Unlocked</td>
<td>-</td>
<td>100</td>
<td>Disable</td>
<td>30</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Port Speed</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/3</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>Unlocked</td>
<td>10</td>
<td>Disable</td>
<td>30</td>
</tr>
</tbody>
</table>
5 Regularly Monitor and Test the Network
This section describes the procedures to regularly monitor and test the network.

5.1 Track and Monitor all Access to Network Resources and Cardholder Data
Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something goes wrong. Determining the compromise is difficult, if not impossible, without system activity logs. Every activity on the network can be monitored and any compromise on security can be traced back to the exact cause with the help of system activity logs.

5.1.1 Monitor all actions taken by any individual with root or administrative privileges
The Dell N-Series switches can log administrator privilege level 15 actions. The following example shows the logging activity of a privileged user into and out of the switch:

```
<190> Nov  6 03:36:53 172.25.114.50-1 CLI_WEB[109122276]: cmd_logger_api.c(260) 1285 %% [CLI:admin:EIA-232] User admin logged in to enable mode.
<190> Nov  6 03:36:04 172.25.114.50-1 CLI_WEB[109122276]: cmd_logger_api.c(260) 1284 %% [CLI:admin:EIA-232] User has successfully logged in
<189> Nov  6 03:33:30 172.25.114.50-1 TRAPMGR[109122276]: traputil.c(739) 1283 %% Multiple Users: CPU
<190> Nov  6 03:34:33 172.25.114.50-1 CLI_WEB[109122276]: cmd_logger_api.c(260) 1282 %% [CLI:admin:EIA-232] User has logged out
```

5.1.2 Log access to audit trails
Dell N-Series switches can log who has been accessing audit trail logs: The following example shows the enabled events being logged:

```
console#show logging
```

5.1.3 Log invalid access attempts
The Dell N-Series switches support logging of invalid access attempts. The following example shows a guest user failing login:

```
<189> Nov  6 04:02:57 172.25.114.50-1 TRAPMGR[108689556]: traputil.c(696) 1302 %% An invalid user tried to login through CLI from 0.0.0.0
<190> Nov  6 04:02:57 172.25.114.50-1 CLI_WEB[109122276]: cmd_logger_api.c(260) 1301 %% [CLI:guest:0.0.0.0] User login authentication failed
```
5.1.4 Log the user identifications and authentications in the audit trail
The Dell N-Series switches support logging of user identifications and authentications. The following example shows a guest user account being created with access privilege:

```
<190> Nov  6 04:04:11 172.25.114.50-1 CLI_WEB[109122276]: cmd_logger_api.c(260) 1314 %% [CLI:admin:EIA-232] Access level of user guest1 has been set to 1
```

```
<190> Nov  6 04:04:11 172.25.114.50-1 CLI_WEB[109122276]: cmd_logger_api.c(260) 1312 %% [CLI:admin:EIA-232] New user guest1 has been added
```

5.1.5 Initialization of audit logs
The Dell N-Series switches support audit log clearing. The following example shows the user clearing the RAM buffer:

```
clear logging
```

```
Buffer Log:
```

```
<189> Nov  6 04:26:04 172.25.114.50-1 CMDLOGGER[109122276]: cmd_logger_api.c(83) 1 %% CLI:EIA-232:admin:clear logging
```

5.1.6 Create and delete system level objects
The Dell N-Series switches log removal and tampering of system log files. The following example shows the user deleting the operational log file from the system:

```
<190> Nov  6 04:20:21 172.25.114.50-1 CMDLOGGER[109122276]: cmd_logger_api.c(83) 1323 %% CLI:EIA-232:admin:delete olog2.txt
```

```
```

5.1.7 Log user identification in log entries
The Dell N-Series switches log user identification in log entries. The following example shows a guest user CLI commands sequence used while navigating the switch including enabling global configuration mode and setting BPDU protection:

```
<189> Nov  6 04:51:45 172.25.114.50-1 CMDLOGGER[109122276]: cmd_logger_api.c(83) 23 %% CLI:172.25.114.3:admin:show
```
5.1.8 Include type of events in logs

The Dell N-Series switches include events types in logs. The following example shows an events log for change in port status and spanning tree protocol:

5.1.9 Include date and time stamp in log entries

The Dell N-Series switches include time stamp with each log entry. The following example shows the time stamp with each log:

5.1.10 Log successful and failed events

The Dell N-Series switches support logging of successful and failed events. The following example shows a guest user failed login followed by a successful login:
20
Dell Networking Support for Payment Card Industry Data Security Standard

5.1.11 Include origin of events in logs
The Dell N-Series switches include the origin of events in logs. The following example shows the origin of an event:

<189> Nov 7 00:29:29 172.25.114.50-1 TRAPMGR[119710284]: traputil.c(696) 1235 %%
Gi1/0/43 is transitioning from the Forwarding state to the Blocking state in instance 0

<189> Nov 7 00:29:29 172.25.114.50-1 TRAPMGR[119710284]: traputil.c(696) 1234 %% Link on
Gi1/0/43 is failed

5.1.12 Include name of modified or altered system components in logs
The Dell N-Series switches include the names of system components that have been modified or altered in logs. The following example shows an event log for the real time clock being changed:

<190> Dec 25 01:12:34 172.25.114.50-1 SIM[120142900]: usmdb_util.c(5615) 1291 %% System
time is changed from 1:12:34 12/25/2013 to 1:12:34 12/7/2013

<190> Nov 7 01:11:02 172.25.114.50-1 SIM[120142900]: usmdb_util.c(5615) 1290 %% System
time is changed from 1:11:2 11/7/2013 to 1:11:2 12/25/2013

5.1.13 Ensure that time data is protected
The Dell N-Series switches ensure that logs are correct and have not been tampered with. The following example sets the correct time and date by synchronizing with the SNTP server:

Console(config)#sntp unicast client enable

Console(config)#sntp server 172.25.10.20
5.1.14 Limit viewing of audit trails to those with a job-related need

The Dell N-Series switches can be configured to restrict user logins to user exec mode with level 1 privilege. The following example restricts guest users from gaining access to and/or viewing log files and messages:

```
Console(config)#aaa authentication login default local
Console(config)#line console
Console(line-config)#login authentication default
Console (line-config)#exit
Console(config)#enable password xxxyyyzzz
Console(config)#username admin password wwwxxxxyy privilege 15
Console(config)#username guest password wwwxxxxyy privilege 1
```
6 Other Recommendations

6.1 SNMP Community Strings

Do not use default community strings on the switch or the Network Management System. Use unique community strings as SNMP v2c community strings are passed in plain text. This way, if the community string and/or device becomes compromised, the rest of the network may not be at risk.

The following example configures read-only access on the switch using the community string <Austin>, and read-write access on the switch using the community string <Texas>.

```
console(config)#snmp-server community Austin ro
console(config)#snmp-server community Texas rw
console(config)#snmp-server enable traps all
console(config)#snmp-server host 192.168.114.65 Austin
console(config)#exit
```

6.2 Shutdown Unused Switch Ports

The Dell N-Series switches enable all ports by default. It is best practice to shutdown all unused ports. The following example shuts down a range of switch ports assumed to be unused in the network:

```
console(config)# int range gi1/0/3-10
console(config-if)#shutdown
console(config-if)#exit
console(config)#do show ports interface status
```

6.3 Secure Telnet Switch Access

The following example sets a password authentication for Telnet:

```
console(config)#aaa authentication login default line
console(config)#line telnet
console(config-line)#password xxxyyyyzzz
console (config-line)#login authentication default
console(config-line)#exit
console(config)#Do write
console(config)#exit
console#exit
```
6.4 Secure Console Switch Access

If no password is set for the switch console, by default, an intruder can access user mode and then into other modes if no passwords are set there either. The console port is typically the initial point of entry to configure the switch. It is critical to set a password on the console port to protect against an intruder gaining access to the switch. To ensure that only authorized users can access and change the configuration of the switch, users should be authenticated.

```
console(config)#aaa authentication login default line
console(config)#line console
console(config-line)#password xxxyyzzz
console(config-line)#login authentication default
console(config-line)#exit
console(config)#do write
console(config)#exit
console#exit
console>logout
console>user:
```

By the default, no authentication is required for console access. If the "User" login prompt is not displayed, then authentication for the console port is not configured.

6.5 Secure Shell Switch Access

The following example sets a password authentication for SSH:

```
console(config)#aaa authentication login default line
console(config)#line ssh
console(config-line)#password xxxyyzzz
console(config-line)#login authentication default
console(config-line)#exit
console(config)#do write
```
console(config)#exit

console#exit

console>logout

console>User

### Additional resources


[Dell Tech Center](#) is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products.

This document references the Payment Card Industry Security Standards Council. For more information including proposed updates to the standard: [PCI Security Standards Council](#)

Dell can help organizations meet and maintain each of the Payment Card Industry Data Security Standard requirements with a combination of hardware, software, and services. For more information visit: [Achieving and Maintaining PCI Compliance and Security with Dell Solutions](#)