



## **MultiFactor SecureAuth® for VPN and Web Applications delivers certified, affordable user authentication for PCI compliance**

### **An Overview of PCI DSS Security Requirements**

The PCI DSS is a set of security requirements intended to help organizations protect the account data of credit and debit cardholders. PCI DSS was created to prevent credit card fraud, identify theft, hacking and other security threats. The standards apply to all organizations that store, process or transmit cardholder data and offer guidance to software developers and the creators of applications and devices used in card transactions. Any organization that handles cardholder data must be PCI DSS compliant or risk audits, fines or the loss of the right to process payments via credit or debit card.

#### **Definitions**

PCI DSS security requirements apply to all “system components” that capture, store or transmit cardholder data. These system components are defined as any network component, server, or application that is included in or connected to the cardholder data environment.

The “cardholder data environment,” in turn, is any part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications

#### **Annual Reviews**

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted, unless otherwise specified.



For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example, employee remote access or third-party payment card company access for processing and maintenance).
- All connections to and from the authorization and settlement environment (for example, connections for employee access or for devices such as firewalls and routers).
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS.
- Any point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location, such as a retail store, restaurant, hotel property, gas station, supermarket, or other POS location.
- If there is no external access to the merchant location (by Internet, wireless, virtual private network (VPN), dial-in broad band, or publicly accessible machines such as kiosks), the POS environment may be excluded.

## PCI DSS Requirement 8

**SecureAuth** meets or exceeds all requirements for access to external connections into the networks and connections to and from the authorization and settlement environment. These specific requirements are called out in PCI DSS Compliance Requirement 8. Below is a mapping of the specific Requirement 8 PCI DSS requirements, information on how the Security Standards Council will be testing for them, and specifically how SecureAuth meets each section in Requirement 8.

For most organizations, PCI DSS Requirement 8 is what must be addressed first. Requirement 8 covers user access. Most organizations already adhere to requirements



1-6, which require organizations to have a firewall, maintain up-to-date antivirus signatures, encrypt stored data and the like.

Requirements 7-9 address access controls, and the most fundamental access control is how users gain access to applications. Requirement 7 states that organizations must “restrict access to cardholder data by business need-to-know.”

Requirement 8 states that organizations must “assign a unique ID to each person with computer access,” and requirement 9 addresses the physical access to systems.

For most organizations, Requirement 8 is the most immediate concern. If user access isn’t uniquely tied to an individual, other access requirements are undermined. This document will specifically address PCI DSS Requirement 8.

### **PCI DSS Requirement 8 Overview**

Requirement 8 states that organizations must assign a unique ID to each person with computer access. Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

**PCI DSS Requirement 8.1** – Calls for organizations to identify all users with a unique user name before allowing them to access system components or cardholder data.

**Testing Procedure 8.1** – For a sample of user IDs, review user ID listings and verify that all users have a unique username for access to system components or cardholder data.

**SecureAuth Compliance 8.1** – SecureAuth creates a secure user credential which is mapped to an enterprise UserID.

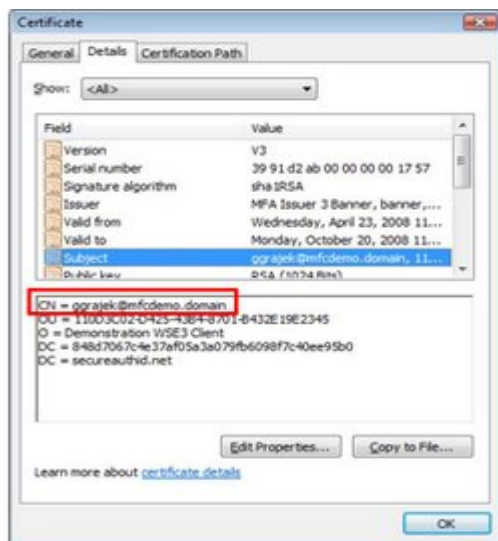
**PCI DSS Requirement 8.2** – In addition to assigning a unique ID, you must employ at least one of following methods to authenticate users: passwords, token devices, certificates, public keys, or biometrics.

**Testing Procedure 8.2** – To verify that users are authenticated using a unique ID and additional authentication, such as a password, for access to the cardholder environment, you should perform the following:

- Obtain and examine documentation describing the authentication method(s) used.

- For each type of authentication method used and for each type of system component, observe an authentication to verify that the authentication is functioning consistent with documented authentication method(s).

**SecureAuth Compliance 8.2** – SecureAuth creates a secure user credential which is mapped to an enterprise-mapped UserID. The SecureAuth credential is utilized to securely identify and authenticate the user. The UserID is in the SecureAuth credential presented upon attempted access by the end-user (See Figure #1).



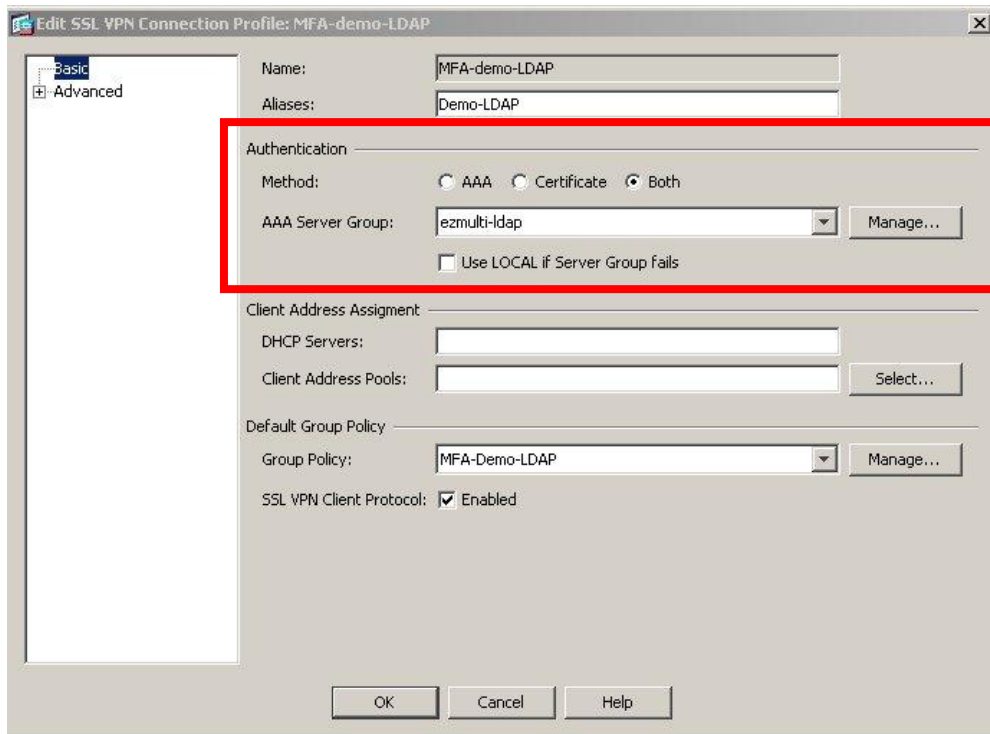
**Figure # 1** – SecureAuth creates and utilizes a unique ID per user.

**PCI DSS Requirement 8.3** – Organizations must implement two-factor authentication for remote access to the network by employees, administrators, and third parties. You must use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens or a VPN (based on SSL/TLS or IPSEC) with individual certificates.

**Testing Procedure 8.3** – To verify that two-factor authentication is implemented for all remote network access, observe an employee connecting remotely to the network and verify that both a password and an additional authentication item (SecureAuth certificate) are required.

**SecureAuth Compliance 8.3** – VPN authentication works in conjunction with a VPN appliance to authenticate a user with a securely delivered SecureAuth X.509 credential. (The SecureAuth X.509 credential meets the 8.5 PCI DSS requirement

of an “individual certificate.”) The VPN is set to utilize “AAA + Certificate” authentication, thus enabling true 2-factor authentication. The user must have the SecureAuth certificate and input the password associated with the user’s account (See Figure #2)



**Figure #2 – The VPN is set to utilize both “AAA + SecureAuth Certificate” authentication.**

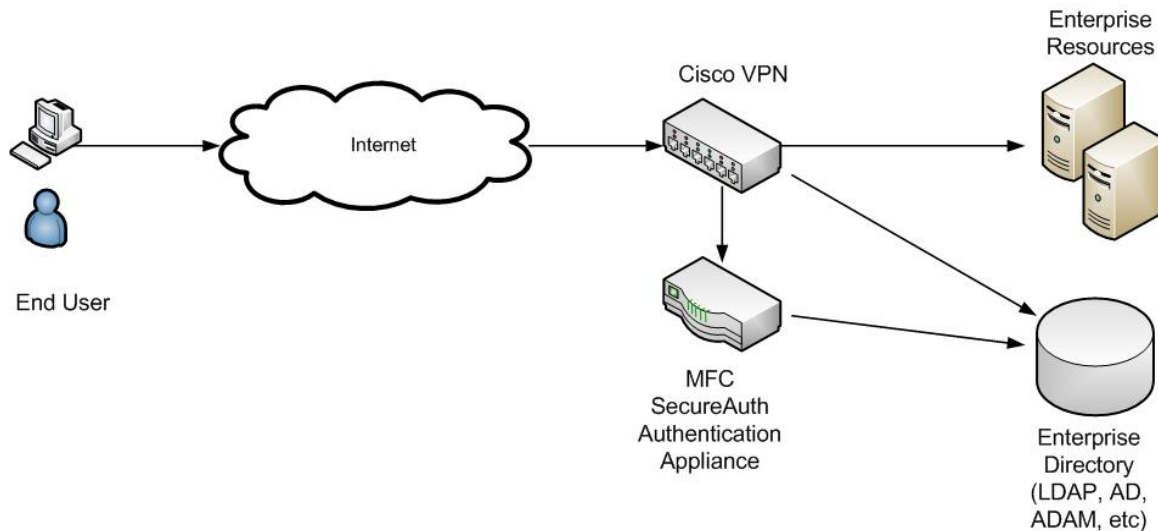
**PCI DSS Requirement 8.4 –** You must encrypt all passwords during transmission and storage on all system components.

**Testing Procedure 8.4.a –** For a sample of system components, critical servers, and wireless access points, you should examine password files to verify that passwords are unreadable.

**For Service Providers only –** Observe password files to verify that customer passwords are encrypted.

**SecureAuth Compliance 8.4 –** SecureAuth does NOT have its own user credential and password data store. SecureAuth utilizes the directory (AD, ADAM,

LDAP) that the VPN or web application is using natively. This helps the enterprise meet PCI DSS Requirement 8.4. The enterprise does NOT have to create, sync and encrypt an additional new set of data information.



**Figure #3 – SecureAuth utilizes the native user store the enterprise has connected to the VPN.**

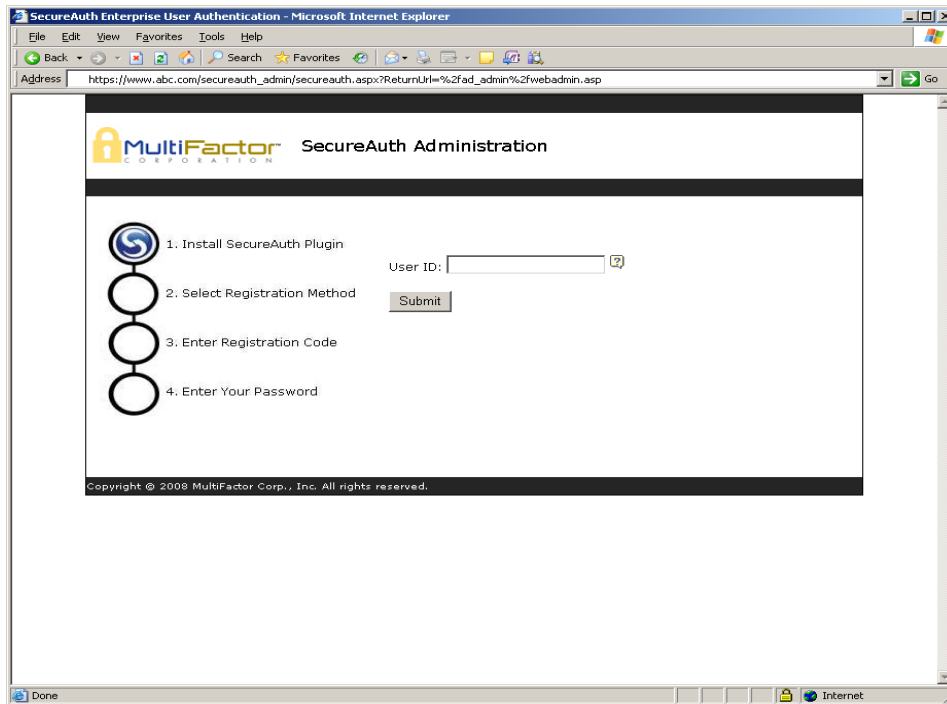
**PCI DSS Requirement 8.5** – Organizations must ensure proper user authentication and password management for non-consumer users and administrators on all system components.

**Testing Procedure 8.5** – Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management by performing the following: Select a sample of users IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following:

Obtain and examine an authorization form for each ID.

Verify that the sampled user IDs are implemented in accordance with the authorization form.(including with privileges as a specified and all signatures obtained), by tracing information from the authorization form to the system.

**SecureAuth Compliance 8.5** – The SecureAuth appliance is administered via a secure GUI. All administrators are required to authenticate via strong 2-factor, SecureAuth authentication (certificate plus UserID/password).



**Figure #4 – SecureAuth administrators must uniquely authenticate and utilize secure 2-factor X.509 authentication.**

**PCI DSS Requirement 8.5.1 – Organizations must control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.**

**Testing Procedure 8.5.1.a – Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following:**

- Obtain and examine an authorization form for each ID
- Verify that the sampled User IDs are implemented in accordance to the authorization form (with privileges as specified and all signatures obtained) by tracing information from the authorization form to the system

**8.5.1.b – Verify that only administrators have access to management consoles for wireless networks.**



**SecureAuth Compliance 8.5.1** – Administration accounts are uniquely created and associated with individual accounts, so configuration modifications are associated with specific administrators.

**PCI DSS Requirement 8.5.2** – Organizations must verify a user’s identity before performing password resets.

**Testing Procedure 8.5.2** – Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, email, web, or other non-face-to-face method, the user’s identity is verified before the password is reset.

**SecureAuth Compliance 8.5.2** – SecureAuth requires end-users to perform a 2-factor authentication (certificate + password) before they are allowed to modify their passwords. The PCI DSS 8.5.2 requirement is met by forcing users to strongly authenticate before modification of their password.

**PCI DSS Requirement 8.5.3** – Organizations must set first-time passwords to a unique value for each user and users must change them immediately after first use.

**Testing Procedure 8.5.3** – Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use.

**SecureAuth Compliance 8.5.3** – SecureAuth works in conjunction with VPNs and web applications for resetting the password on first usage.

**PCI DSS Requirement 8.5.4** – You must immediately revoke access for any terminated users.

**Testing Procedure 8.5.4** – Select a sample of employees terminated in the past six months and review current user access lists to verify that their IDs have been inactivated or removed.

**SecureAuth Compliance 8.5.4** – SecureAuth is unique among X.509 authentication solutions by providing instant revocation by checking the data store of record to ensure that the user is still in existence. This facilitates one-button revocation (*See Figure #3*)

SecureAuth requires the end-user to have both a valid SecureAuth certificate and authenticate with a valid password (*See figure #2*). If the user is revoked on the data store, SecureAuth will not grant access to the user.



**PCI DSS Requirement 8.5.5** – Organizations must remove inactive accounts at least every 90 days.

**Testing Procedure 8.5.5** – For a sample of user IDs, verify that there are no inactive accounts over 90 days old.

**SecureAuth Compliance 8.5.5** – SecureAuth can set its credentials for any time period. An enterprise can set the SecureAuth credential to be 90 days or less, thereby forcing users to re-authenticate every 90 days.

**PCI DSS Requirement 8.5.6** – You must enable accounts used by vendors for remote maintenance only during the time period needed.

**Testing Procedure 8.5.6** – Verify that any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used.

**SecureAuth Compliance 8.5.6** – SecureAuth has a configurable certificate length that can be set in accordance to security and resource requirements. This is completed in a simple administrator GUI.

**PCI DSS Requirement 8.5.7** – Communicate password procedures and policies to all users who have access to cardholder data.

**Testing Procedure 8.5.7** – Interview the users from a sample of user IDs to verify that they are familiar with password procedures and policies.

**SecureAuth Compliance 8.5.7** – SecureAuth is a user self-enrollment product that walks an end-user through a simple process to obtain a secure credential. Additionally, the product utilizes the enterprise data store, which allows it to follow the enterprise's existing policies.

**PCI DSS Requirement 8.5.8** – Do not use group, shared, or generic accounts and passwords.

**Testing Procedure 8.5.8.a** – For a sample of system components, critical servers, and wireless access points, examine user ID lists to verify the following

- Generic User IDs and accounts are disabled or removed
- Shared User IDs for system administration activities and other critical functions do not exist.



- Shared and generic User IDs are not used to administer wireless LANs and devices.

**8.5.8.b** – Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited.

**8.5.8.c** – Interview system administrators to verify that group and shared passwords are not distributed, even if requested.

**SecureAuth Compliance 8.5.8-** SecureAuth's unique self-enrollment for X.509 credentials makes sharing of the certificate impossible without having access to the user's machine, as well as access to their user name and password information.

**PCI DSS Requirement 8.5.9** – Organizations must change user password at least every 90 days.

**Testing Procedure 8.5.9** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require password changes at least every 90 days.

**For Service Providers only** – Review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when and under what circumstances passwords must change.

**SecureAuth Compliance 8.5.9** – SecureAuth requires the end-user to change his or her security credential every 90 days (or whatever time period the enterprise determines). The SecureAuth authentication credential can be set from 1 hour to 10 years. SecureAuth enables an enterprise to meet the requirement today, but also to adjust accordingly if this requirement changes (*See Figure #5*).



The screenshot shows a configuration window titled "Certificate Expiration Settings". It contains two input fields: "Long Term Certificate Duration" with a value of 90 and "Short Term Certificate Duration" with a value of 2. The units are "days (2 to 730 days)" and "hours (2 to 48 hours)" respectively. A red rectangular box highlights the entire settings area.

Certificate Expiration Settings	
Long Term Certificate Duration:	90 days (2 to 730 days)
Short Term Certificate Duration:	2 hours (2 to 48 hours)

**Figure #5 - Enterprises can select the length of time certificates are valid for end users.**

**PCI DSS Requirement 8.5.10** – You must require a minimum password length of at least seven characters.

**Testing Procedure 8.5.10** – For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords of at least seven characters.

**For Service Providers only** – Review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements.

**SecureAuth Compliance 8.5.10** – SecureAuth utilizes the enterprise’s data store (See Figure #3). Whatever configuration the enterprise sets is enforced by the SecureAuth appliance during certificate enrollment.

**PCI DSS Requirement 8.5.11** – You must require passwords that contain both numeric and alphabetic characters.

**Testing Procedure 8.5.11** – For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords that contain both numeric and alphabetic characters.



**SecureAuth Compliance 8.5.11** – SecureAuth utilizes the enterprise’s data store (See Figure #3). Whatever configuration the enterprise sets is enforced by the SecureAuth appliance during certificate enrollment.

**PCI DSS Requirement 8.5.12** – 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.

**Testing Procedure 8.5.12** – For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.

**For Service Providers only** – Review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords.

**SecureAuth Compliance 8.5.12** – SecureAuth utilizes the enterprise’s data store (See Figure #3). All policies and configurations existing in the enterprise’s data store will be honored by SecureAuth.

**PCI DSS Requirement 8.5.13** – Limit repeated access attempts by locking out the user ID after no more than six attempts.

**Testing Procedure 8.5.13** – For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that a user’s account is locked out after no more than six invalid logon attempts.

**For Service Providers only** – Review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after no more than six invalid access attempts.

**SecureAuth Compliance 8.5.13** – SecureAuth has a lock-out feature for registration. The default for this configurable feature is three attempts.

**PCI DSS Requirement 8.5.14** – Set the lockout duration to thirty minutes or until administrator enables the user ID.

**Testing Procedure 8.5.14** - For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to



verify that password parameters are set to require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account.

**SecureAuth Compliance 8.5.14** – In accordance with requirement 8.5.14 accounts can be locked out for a given time period. This is configurable in the enterprise data store that SecureAuth uses (*See Figure #3*).

**PCI DSS Requirement 8.5.15** – If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.

**Testing Procedure 8.5.15** – For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that system/session idle time-out features have been set to 15 minutes or less.

**SecureAuth Compliance 8.5.15** – SecureAuth relies on VPN and web application settings for session duration and session idle enforcement.

**PCI DSS Requirement 8.5.16** – Authenticate all access to any database containing cardholder data. This includes access applications, administrators, and all other users.

**Testing Procedure 8.5.16.a** – Review database configuration settings for a sample of databases to verify that access is authenticated, including for individual users, applications, and administrators.

**SecureAuth Compliance 8.5.16** – The policies contained in the enterprise's data store can be used for SecureAuth with no additional effort for a new data store.