WHITE PAPER

JUMPCLOUD DIRECTORY-AS-A-SERVICE® PLATFORM FOR PCI DSS

ANDREY SAZONOV | CISA, QSA(P2PE), PA-QSA(P2PE)

JumpCloud®
Directory-as-a-Service®

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

JumpCloud, Inc. (JumpCloud) engaged Coalfire, a respected Payment Card Industry (PCI) Payment Application – Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of their JumpCloud Directory-as-a-Service® (DaaS) platform. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire will describe that the JumpCloud DaaS platform can be implemented to support the PCI Data Security Standard (PCI DSS) v3.2.1 authentication and logging requirements based on the sample testing and evidence gathered during this assessment. All references to the PCI DSS requirements should be assumed to refer to the PCI DSS v3.2.1.

JumpCloud's solution can be implemented to help address PCI DSS compliance and help reduce compliance efforts when it comes to management of user authentication within a company's environment.

ABOUT THE JUMPCLOUD DAAS PLATFORM

The JumpCloud DaaS platform is a cloud-based solution for a single point of authority to authenticate, authorize, and manage the identities of a business's employees and systems. DaaS securely connects employees with systems, applications, files, networks, and other resources through a single unified cloud-based directory, replacing the need for on-premises solutions such as Active Directory and LDAP. The JumpCloud DaaS platform supports most major operating system (OS) platforms (Windows, Linux, and macOS) and is designed to control and manage user access to both internal and external IT resources such as servers and applications.

AUDIENCE

This assessment white paper has three target audiences:

1. **QSA and Internal Audit Community:** This audience may be evaluating the JumpCloud DaaS platform to assess a merchant or service provider environment for PCI DSS.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating the JumpCloud DaaS platform for use within their organization for compliance requirements of PCI DSS.
3. **Merchant and Service Provider Organizations:** This audience may be evaluating the JumpCloud DaaS platform for deployment in their cardholder data environment and the benefits this solution can offer.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using the below industry and audit best practices. Coalfire conducted testing within the JumpCloud hosted infrastructure as well as in the Coalfire test lab. Testing was conducted from April 12, 2018 to May 14, 2018.

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full solution and its components (JumpCloud Agent and JumpCloud Web Service).
2. Implementation of the JumpCloud Agent software in the Coalfire lab environment on all supported platforms (Windows, Linux, macOS).
3. Review and testing of the functionality provided to enforce authentication controls on tested systems.
4. Confirmation that authentication controls can be configured to meet PCI DSS Requirement 8 controls and are enforced on the system upon configuration.
5. Confirmation that appropriate logging takes place in accordance with PCI DSS Requirement 10.
6. Review of the systems to verify passwords are handled in a PCI DSS compliant manner.

It's important to note that during a PCI DSS audit, a merchant would need to collaborate with JumpCloud in order to verify scope and applicable controls for the requirements.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- When properly implemented following vendor guidance, the JumpCloud DaaS platform can provide coverage for applicable sections of PCI DSS Requirement 8 (Identify and authenticate access to system components) and Requirement 10 (Track and monitor all access to network resources and cardholder data).
- The JumpCloud Agent securely integrates with the underlying OS authentication methods (Windows 10 Professional 64 bit, Ubuntu 16.06 LTS, macOS Sierra 10.12 were tested) and allows for performing user management tasks according to the policies configured within the JumpCloud cloud environment.
- The JumpCloud DaaS platform adequately generated logs of all user actions and could be traced in accordance with PCI DSS requirement 10. All logs are able to be imported to a centralized logging platform of choice.
- Coalfire verified that the JumpCloud DaaS platform cannot be disabled by unauthorized users.
- No user passwords were found to be stored either locally on the system or within the JumpCloud DaaS platform cloud environment in a non-compliant manner. The JumpCloud Agent does not have access to cleartext user passwords.
- No user passwords were found to be transmitted over the local or public network in the clear or in a non-compliant manner. Passwords are protected in transit using the TLS 1.2 protocol.

ASSESSOR COMMENTS

The assessment scope focused on validating the use of the JumpCloud DaaS platform in a PCI DSS environment, to include its impact on applicable sections of PCI DSS Requirement 8 and Requirement 10.

The JumpCloud DaaS platform, when properly implemented following guidance from JumpCloud, can be utilized to meet the technical portions of PCI-DSS Requirement 8 and 10. However, as most computing environments and configurations vary drastically, it is important to note that use of this product does not guarantee security by default, and user management processes can fail when improperly implemented or methods of social engineering are implemented as an attack. A defense-in-depth strategy that provides multiple layers of protection should be followed as a best practice. Please consult with JumpCloud for policy and configuration questions and best practices.

It should also not be construed that the use of the JumpCloud DaaS platform guarantees full PCI DSS compliance. Disregarding PCI requirements and security best practice controls for systems and networks inside or outside of PCI DSS scope can introduce many other security or business continuity risks to merchants or service providers. Security and business risk mitigation should be any merchant's or service provider's goal and focus for selecting security controls.

APPLICATION ARCHITECTURE

The JumpCloud DaaS platform provides real-time user management for multiple supported OS endpoints and, at a high level, utilizes the following two components as shown in Figure 1:

- JumpCloud Agent: A lightweight software client designed to synchronize all settings with the JumpCloud Web Service and integrate securely with the underlying OS authentication functionality by taking over the account where it is initially set up. The JumpCloud Agent supports multiple flavors of Linux, macOS, and Windows OSs and has the ability to add, modify, and delete local user accounts, including setting passwords, updating full name fields, and changing group membership.
- JumpCloud Web Service – Hosted in the cloud and managed by the vendor, JumpCloud provides a web interface for all administrative user and system management functionality. This component interacts with the agent software installed on each system in the organization to synchronize users, policies, and configurations, as configured by the administrator. In addition, the architecture of the JumpCloud DaaS platform allows further integration with other services including Google G Suite, Amazon Web Services (AWS), Microsoft Office 365, as well as provides a bridge to existing Active Directory instances and other services; however, this functionality is out of scope for this white paper.

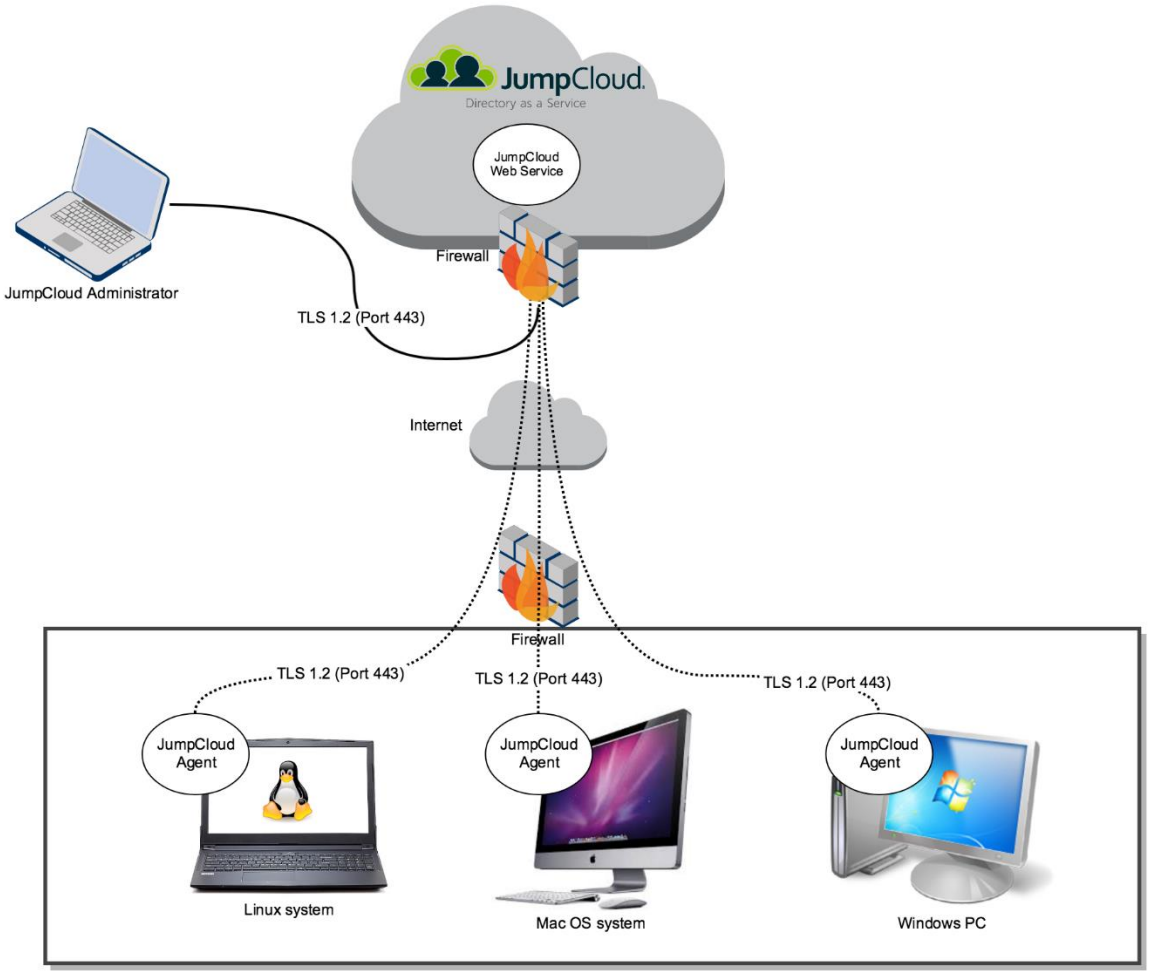

Figure 1: The JumpCloud DaaS Platform Architecture Diagram

TECHNICAL SECURITY ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the potential PCI DSS coverage of the solution:

1. Initial configuration of the JumpCloud DaaS platform in accordance with policies enforced by PCI DSS.
2. Deployment of the JumpCloud Agent software to multiple platforms: Windows, Linux, and macOS. Examination of end-point configuration to confirm the JumpCloud Agent cannot be turned off by non-administrators.
3. Observation of integration with the underlying OS authentication and logging mechanisms and verification that these mechanisms could operate in a PCI DSS compliant manner.
4. User creation, deletion, and configuration using steps provided by JumpCloud. Testing of all deployment and configuration scenarios to address any PCI DSS requirements that may apply.
5. Evaluation of methodologies for password protection in transit.
6. Forensic analysis of the hard drive to confirm that none of the clear-text passwords used are stored by the JumpCloud Agent.
7. Review of administrative functionality and role-based access control (RBAC) in place for using different types of accounts.
8. Evaluation of the multi-factor authentication (MFA) functionality.
9. Evaluation of the agent software update process to verify secure distribution processes.

ASSESSMENT ENVIRONMENT

The JumpCloud Agent was installed on the following systems:

- Windows 10 Professional 64 bit in a virtual environment
- Ubuntu 16.06 LTS in a virtual environment
- macOS Sierra 10.12 running on the MacBook Pro laptop

A separate laptop was used to access the JumpCloud Web Service using a web browser to perform all administrative configurations.

INITIAL CONFIGURATION

The initial configuration of the solution included installation of the client software on all OSs being tested:

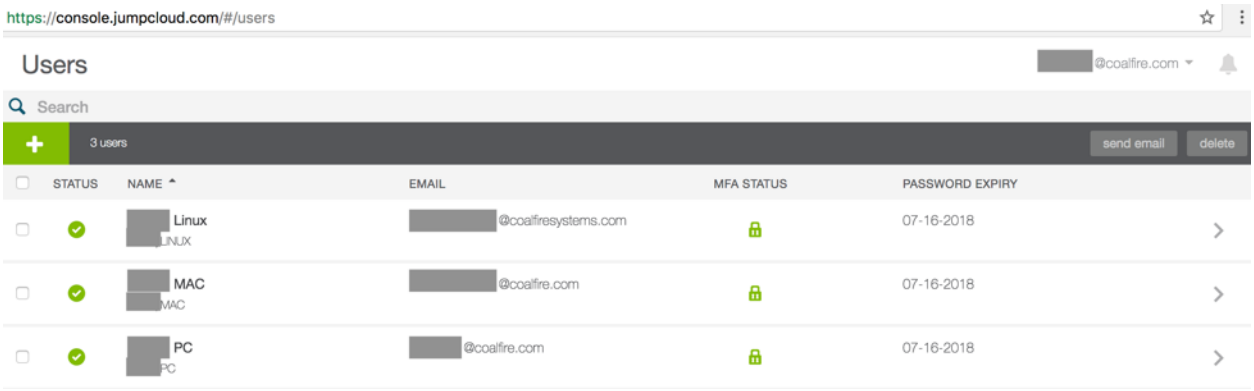

Figure 2: JumpCloud Users Configured

A local account was configured with matching username and password on each tested OS with a local instance of the JumpCloud Agent installed to allow for administrative control of this system:

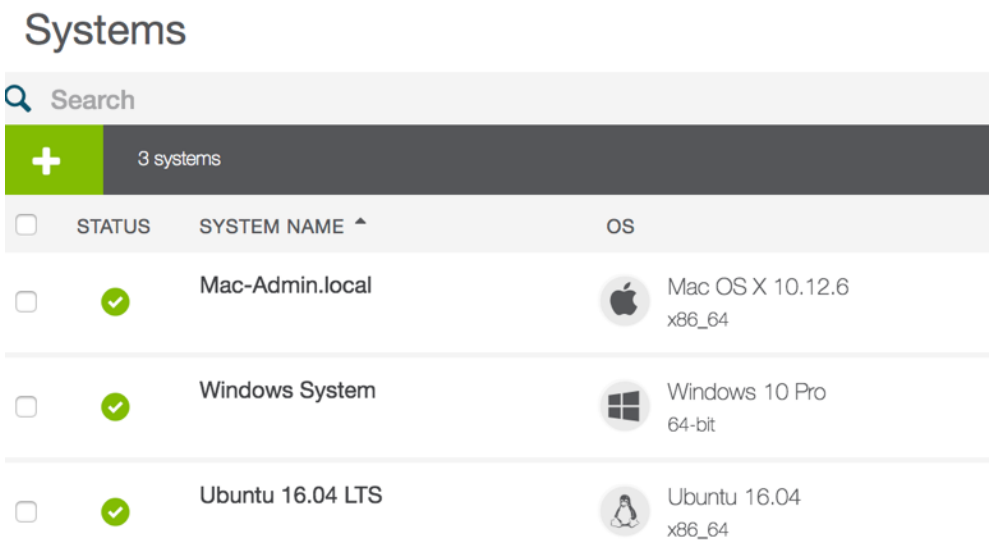

Figure 3: JumpCloud Systems Configured

The initial configuration also required the following security settings on the JumpCloud Web Service that would enforce PCI policies as addressed in Appendix A of this white paper:

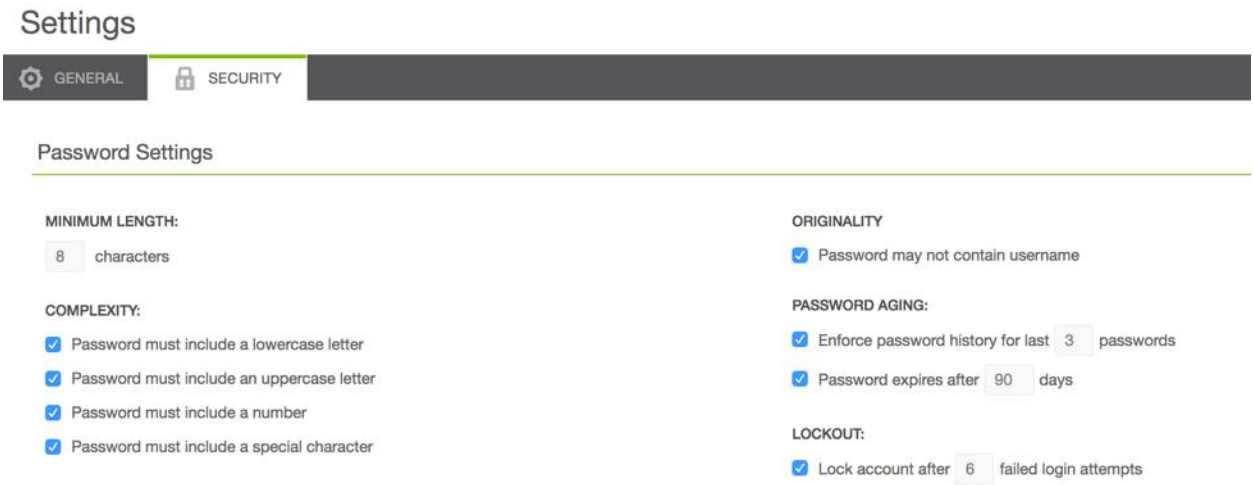

Figure 4: Initial Security Configuration

The "Policies" functionality of the JumpCloud DaaS platform was used to configure a fifteen-minute inactivity timeout as well as disable the default guest account and provide additional functionality that could be enforced as needed:

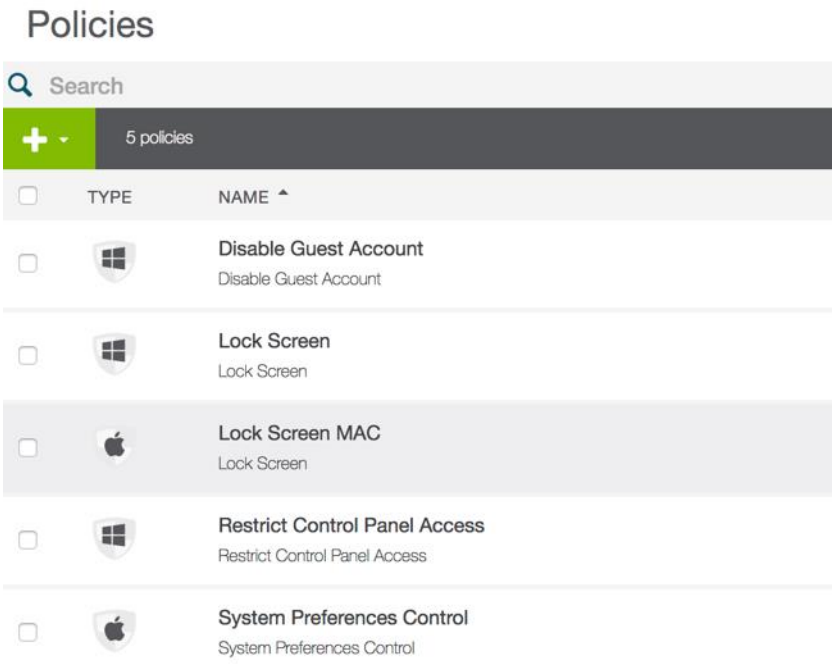

Figure 5: The JumpCloud DaaS Platform Policies Configured

It is important to note that the JumpCloud DaaS platform natively supports the "inactivity timeout" feature for the Windows and macOS platforms, but requires additional configuration for Linux Systems (using the JumpCloud Command Runner feature) to meet PCI DSS requirements.

Lastly, MFA (multi-factor authentication) was configured for the macOS and Ubuntu operating systems. Native MFA for Windows is in development by the vendor.

All administrator access to the JumpCloud Web Service web interface was configured to use two-factor authentication.

INTEGRATION OF THE JUMPCLOUD AGENT WITH THE UNDERLYING OPERATING SYSTEM

The JumpCloud Agent operates by relying on the underlying OS authentication functionality. There are no additional authentication mechanisms or features for the application to introduce, other than the one provided by the underlying OS (Windows, Linux, or Mac).

Coalfire confirmed that, when configured with the guidance provided by JumpCloud, the end user could not disable the JumpCloud Agent and bypass the policies enforced.

Coalfire performed interviews to understand the integration mechanisms of the JumpCloud Agent software and confirmed with testing that it is not possible to disable, uninstall, or block the JumpCloud Agent software by non-administrators, as depicted in the figures below.

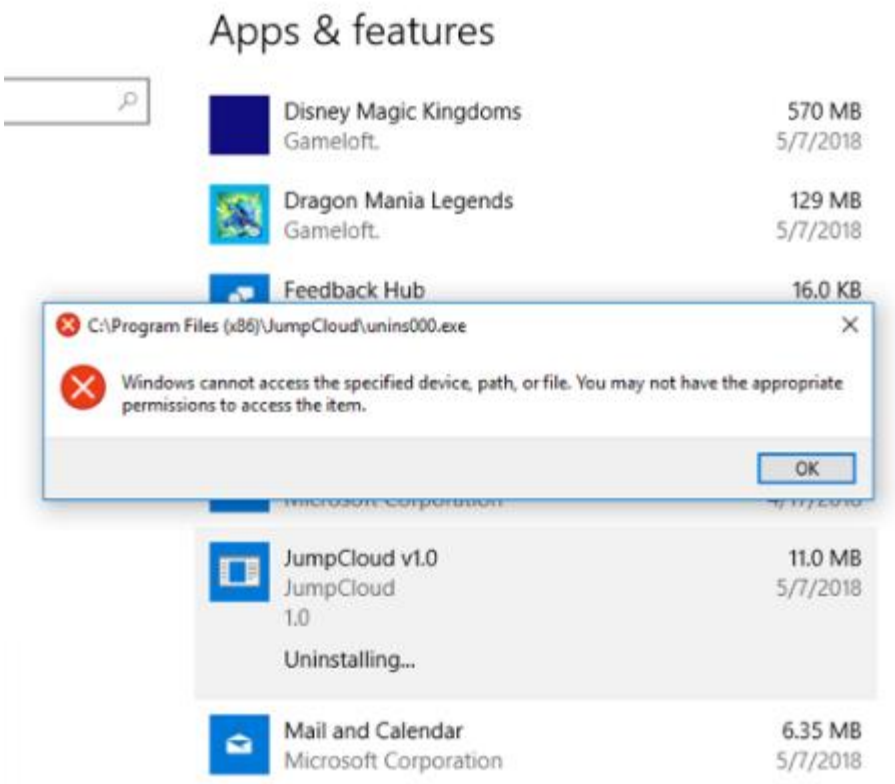

Figure 6: Failed Attempts to Uninstall the JumpCloud Agent

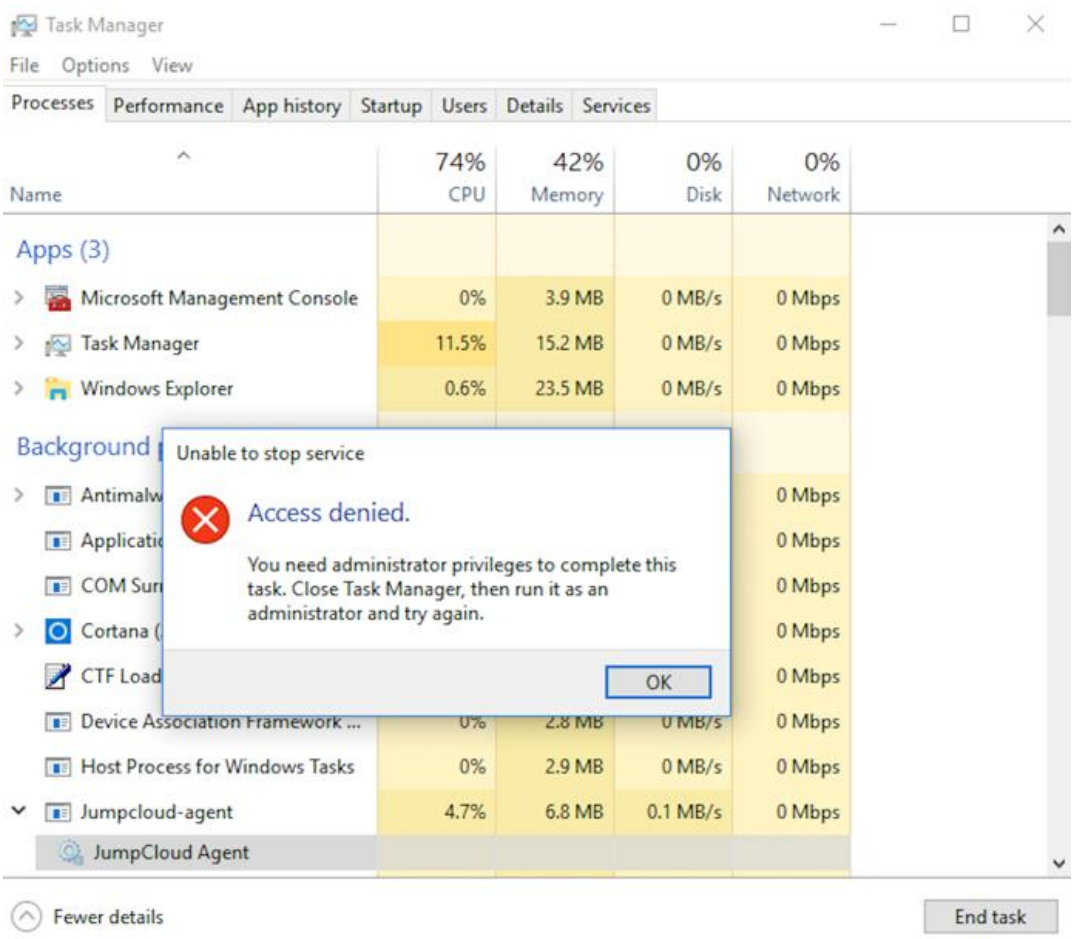

Figure 7: Failed Attempts to Disable or Block the JumpCloud Agent

AUTHENTICATION POLICY ENFORCEMENT

Coalfire has reviewed all PCI DSS authentication controls required to be met by the JumpCloud DaaS platform with the primary goal to verify that the solution would be able to help companies meet requirements and controls enforced by PCI DSS.

Coalfire has observed that policies are enforced by the JumpCloud Agent software and were properly implemented for all systems tested in a way that is compliant with PCI DSS. See Appendix A for details.

LOGS REVIEWED

Logging functionality was reviewed specifically for authentication features.

Since the JumpCloud Agent relies on underlying OS authentication functionality, appropriate logging was performed by the underlying OS as well. It was observed that the mechanisms were in place by all tested OSs to properly log and monitor all actions performed by users. See Appendix A for details.

Additionally, logs were implemented on the JumpCloud Web Service to address all authentication requirements posted by the PCI DSS requirements. See Appendix A for details.

NETWORK TRAFFIC ASSESSMENT

A Wireshark Ethernet port sniffer was used to monitor the following traffic for components within the test environment:

Traffic from the JumpCloud Agent to the JumpCloud Web Service (Figure 8): No sensitive data is transmitted over the network from the JumpCloud Agent running on the local system to the JumpCloud Web Service and all communication (login information, log requests, policy synchronization, and any other requests) is encrypted over the TLS 1.2 protocol.

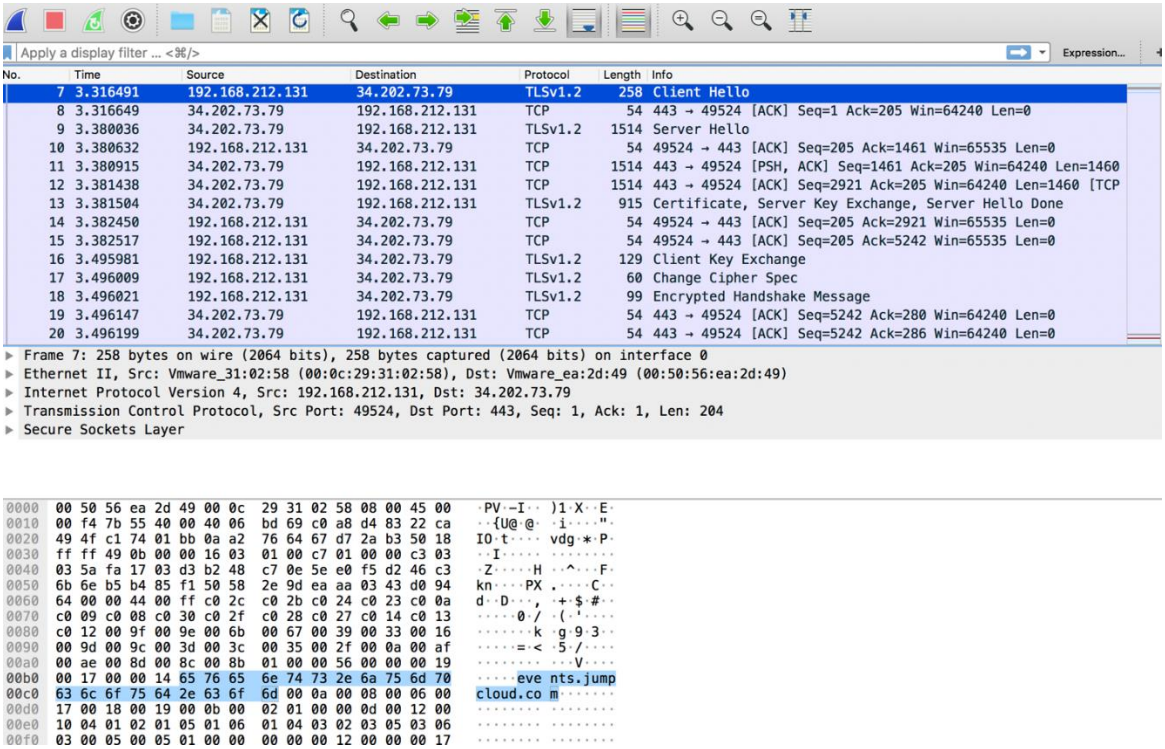

Figure 8: Communication between the JumpCloud Agent and the JumpCloud Web Service

FORENSIC ANALYSIS

The technical assessment included a forensic examination of the hard drive of the system running the JumpCloud Agent.

The process for examining the hard drive was as follows:

1. The whole disk image of the systems with the JumpCloud Agent were captured for forensic analysis. A total of three images were produced (Windows, macOS, Ubuntu).
2. The FTK forensic toolkit was used to search disk images for clear text passwords.

No findings were identified with the image when searched using the FTK forensic toolkit. The following represents the conclusions from performing forensic analysis:

- The forensic analysis demonstrates that there is no residual password data on the system running the JumpCloud Agent.

The interview with the developers and review of the JumpCloud DaaS platform confirmed there is no intent to store any passwords in the clear for any reason.

AGENT SOFTWARE UPDATE PROCESS

The update process is performed by the JumpCloud Agent application automatically without user interaction. The update package is delivered using TLS 1.2 protocol with the digital signature verification process in place that would prevent the package from being installed if the digital signature is not valid.

TOOLS AND TECHNIQUES

Tools Coalfire utilized for this application security review included:

TOOL NAME	DESCRIPTION
FTK Forensic Toolkit	*Forensic tool for digital data and media analysis.
Wireshark	Wireshark Ethernet port sniffer was used to observe the traffic coming in and out of the system.
Additional tools	FTK Imager, Process Explorer

*Forensic tool: A tool or method for uncovering, analyzing and presenting forensic data, which provides robust ways to authenticate, search, and recover computer evidence rapidly and thoroughly.

APPENDIX A: PCI-DSS REQUIREMENTS COVERAGE MATRIX

Requirement 8: Identify and authenticate access to system components

COMPLIANCE LEVEL	DESCRIPTION
✓	Compliance directly supported via use of the JumpCloud DaaS platform
✓	Technical requirements are met by the JumpCloud DaaS solution and requires company policies for full compliance
⊘	Requires company policies for full compliance

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
Requirement 8: Identify and authenticate access to system components		
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: **8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.**	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop. **How the JumpCloud DaaS platform can help meet this requirement:** The solution provides the following features: • Can directly deploy agents that use functionality of the underlying OS authentication mechanisms (Windows, Linux, or macOS). • Direct user management capabilities for the agent deployed systems through the JumpCloud Web Service (hosted by JumpCloud in the cloud). • By default, only unique IDs can be created for all systems within the JumpCloud Agent. Actual usage of unique IDs is a policy requirement that should be followed by those JumpCloud customers pursuing PCI DSS certification. • Each OS supported at a minimum requires an administrator account, which is usually (but not required to be) delegated to the JumpCloud Agent. Local accounts can still be used outside the JumpCloud DaaS platform and would have to be managed by the organization separately.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop. **How the JumpCloud DaaS platform can help meet this requirement:** Coalfire observed how addition, deletion, and modification of user IDs and credentials can be managed using the JumpCloud Web Service (hosted by JumpCloud in the cloud) in a PCI DSS compliant manner.

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		Application local agent software is installed on each system and enforces policies that are distributed from the centralized JumpCloud Web Service. In case of addition, deletion, and modification of user IDs and credentials, the changes would be applied instantly across all platforms where the user has presence. In many cases, the process is automated and should simplify user management across multiple systems, especially when different OSs are used.
8.1.3 Immediately revoke access for any terminated users.	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop. **How the JumpCloud DaaS platform can help meet this requirement:** Coalfire observed how revoking access for any terminated user can be done via the JumpCloud Web Service and applied to all systems affected. Application local agent software is installed on each system and enforces policies that are distributed from the centralized JumpCloud Web Service. In case of revoking user access, the changes would be applied instantly across all platforms where the user has presence. In many cases, the process is automated and should simplify user management across multiple systems, especially when different OSs are used.
8.1.4 Remove/disable inactive user accounts within 90 days.	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop. **How the JumpCloud DaaS platform can help meet this requirement:** Coalfire observed that the JumpCloud DaaS platform can be configured to disable inactive users within 90 days. This configuration can be done via the JumpCloud Web Service and applied to all systems specified. Any change to the user account would be applied instantly across all platforms where the user has presence. In many cases, the process of removing/disabling users across the organization can be automated and should simplify user management across multiple systems, especially when different OSs are used.
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.**	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop. **How the JumpCloud DaaS platform can help meet this requirement:** The JumpCloud Web Service can deploy temporary access for third parties that is monitored and enabled for the

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		timeframe needed, after which it is immediately disabled. This access can be granted to as many systems as needed across multiple OS platforms by utilizing group policy and enforcing it to all agent software across the organization.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** JumpCloud administrators can set the number of login attempts that must be exceeded before locking the account and distributing notifications of the lockout event. Coalfire observed how six login attempts with an incorrect password resulted in a locked out account. This functionality was present across all OSs tested (Windows, Linux, macOS).
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** There is no configuration to set lockout duration; by default, it's locked until an administrator releases the account. Coalfire observed how six login attempts with an incorrect password resulted in a locked out account that was locked for 30 minutes, when an administrator released the account. This functionality was present across all OSs tested (Windows, Linux, macOS).
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.	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** The JumpCloud DaaS platform command execution and policies functionality can be leveraged to ensure that idle systems are locked after fifteen minutes. Coalfire observed how the system that was idle for fifteen minutes required the user to re-authenticate. This functionality was present across all OSs tested (Windows, Linux, macOS).
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 methods to authenticate all users:	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** By default, the JumpCloud DaaS platform requires a username and password for any user to authenticate. In addition, MFA is required for a user to login (the Google Authenticator application was used).

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
Something you know, such as a password or passphrase Something you have, such as a token device or smart card Something you are, such as a biometric.		
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	✓	**How the JumpCloud DaaS platform meets this requirement:** The JumpCloud Agent does not store passwords, either hashed, encrypted, or any other way. The JumpCloud Web Service does have access to passwords, which was assessed under a service provider certification (the solution uses SHA512 with a salt to protect user passwords in storage). All communication between the JumpCloud Agent and the JumpCloud Web Service is using the TLS protocol version 1.2. **Storage of passwords:** Passwords are not stored by the application; instead, the functionality of the underlying OS is used in a manner that meets secure storage best practices. The matrix below shows the method of protection of passwords in storage for each OS supported by the JumpCloud DaaS platform (and requires additional configuration within the OS): - Windows OS - NTLM v2 algorithm for storing passwords that are salted and hashed - Linux OS – SHA256 or SHA512 hashing algorithm with added salt - macOS - SHA512 using PBKDF2 algorithm Coalfire observed that the JumpCloud Agent does not store user passwords in any way. **Passwords in transit:** Passwords are transmitted using public/private key infrastructure with proper authentication provided by the TLS 1.2 protocol. Coalfire captured traffic between the JumpCloud agent and the JumpCloud Web Service to confirm passwords are protected using the TLS version 1.2 protocol while in transit.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	✓	This control requires initial configuration of two factor authentication by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** The JumpCloud DaaS platform does not currently support a secret question for resetting passwords; however, usage of MFA is leveraged as an additional factor for a password reset. Whenever authentication credentials are reset, the user will receive an email with the link to reset the password. The user

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		would need to login into the application using two-factor authentication provided by JumpCloud. Coalfire configured users with two-factor authentication and observed how any modification to authentication credentials required the user to login with two-factor authentication. The first factor was username/password and the second factor was a unique code provided by the Google Authenticator application. This functionality was present across all OSs tested (Windows, Linux, macOS).
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.**	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** The JumpCloud Web Service's password complexity builder can be configured to require that passwords be at least seven characters long and contain numeric and alphabetic characters. By using the administrator account, Coalfire configured password complexity to meet this requirement (at least seven characters and alphanumeric). Coalfire also observed how the system would force authentication requirements for all users logging into the systems. This functionality was present across all OSs tested (Windows, Linux, macOS).
8.2.4 Change user passwords/passphrases at least once every 90 days.	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** The JumpCloud Web Service's password complexity builder can be configured to require that passwords expire every 90 days. By using the administrator account, Coalfire configured the password policy using the JumpCloud DaaS platform to meet this requirement (each password to expire after 90 days). Coalfire also changed the system time locally on the test system forwarding it to 90 days from the current date and observed how the system would force password changes for all users logged into the systems. This functionality was present across all OSs tested (Windows, Linux, macOS).
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.	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:**

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		The JumpCloud Web Service's password complexity builder can be configured in a way that requires the password to be different from the last four passwords used. By using the administrator account, Coalfire configured the password history to meet this requirement (each has to be different from the last four passwords used). Coalfire changed user passwords on the test system and observed how re-using any of the last four passwords would result in a password change failure. This functionality was present across all OSs tested (Windows, Linux, macOS).
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.	✓	This control is directly met by the JumpCloud DaaS platform. **How the JumpCloud DaaS platform meets this requirement:** The JumpCloud Web Service's password is created by the user and an email link is sent out to confirm the account. The initial login requires setting up the password by the user. Therefore, there are no default passwords. However, if the company chooses to set up default password, it can be set to change after the initial login. By using the administrator account, Coalfire configured users with passwords that should be changed after the first login and observed how after a successful login the password was required to be changed. This functionality was present across all OSs tested (Windows, Linux, macOS).
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop to require Multi-Factor Authentication (MFA) for all remote access to the CDE. This requirement also requires initial configuration by the organization and technical requirements can be addressed by the JumpCloud DaaS platform and third-party solutions. **How the JumpCloud DaaS platform can help meet this requirement:** The JumpCloud DaaS platform can be configured to require MFA for Linux and macOS system access natively (at the system login screen/console login). Windows OS does not natively support MFA; however, access to the system can be configured with the use of third-party tools for MFA authentication.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
for personnel with administrative access.		should develop to require MFA for all remote access to the CDE. This requirement also requires initial configuration by the organization and technical requirements can be addressed by the JumpCloud DaaS platform and third-party solutions. **How the JumpCloud DaaS platform can help meet this requirement:** The JumpCloud DaaS platform can be configured to require MFA for Linux and macOS system access. Windows OS does not natively support MFA; however, access to the system can be configured with the use of third-party tools for MFA authentication.
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.	✓	This control requires user management procedures and policies that the company pursuing PCI DSS certification should develop to require MFA for all remote access to the CDE. This requirement also requires initial configuration by the organization and technical requirements can be addressed by the JumpCloud DaaS platform and third-party solutions. **How the JumpCloud DaaS platform can help meet this requirement:** The JumpCloud DaaS platform can be configured to require MFA for Linux and macOS system access. Windows OS does not natively support MFA; however, access to the system can be configured with the use of third-party tools for MFA authentication.
8.4 Document and communicate authentication policies and procedures to all users including: **• Guidance on selecting strong authentication credentials** **• Guidance for how users should protect their authentication credentials** **• Instructions not to reuse previously used passwords** **• Instructions to change passwords if there is any suspicion the password could be compromised.**	⊘	This is a policy requirement that requires creating and communicating documentation and policies that the company pursuing PCI DSS certification should develop. All procedures for providing authentication policies for users have to be developed by the organization.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: **• Generic user IDs are disabled or removed.**	⊘	This is a policy requirement that requires user management procedures and policies that the company pursuing PCI DSS certification should develop. All procedures for providing training guidance for users have to be developed by the organization.

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
• Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.		
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), 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		This is a policy requirement that requires user management procedures and policies that the company pursuing PCI DSS certification should develop. All physical authentication controls have to be developed by the organization.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are 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 (and not by individual users or other non-application processes).		This is a policy requirement that requires user management procedures and policies that the company pursuing PCI DSS certification should develop. All administrative access has to be restricted by the policies and procedures developed by the organization.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.		This is a policy requirement that requires user management procedures and policies that the company pursuing PCI DSS certification should develop. All security policies and procedures should be developed, in use, and known to all parties of the organization.

Requirement 10: Track and monitor all access to network resources and cardholder data

COMPLIANCE LEVEL	DESCRIPTION
✓	Compliance directly supported via use of the JumpCloud DaaS platform
✓	Technical requirements are met by JumpCloud DaaS platform and requires company policies for full compliance
⊘	Requires company policies for full compliance

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 Implement audit trails to link all access to system components to each individual user.	✓	**How the JumpCloud DaaS platform meets this requirement:** Logging requirements can be met by using a combination of logs available both locally on each system and provided by the JumpCloud DaaS platform. Therefore, there are two logging features that are used by the JumpCloud DaaS platform: • Logging of all user activities is provided by the underlying OS natively. • Logging is done by the JumpCloud Web Service and includes audit trails to link all access to system components to each user Due to the fact that all access is logged by the underlying OS, the requirement can be met by relying fully on the underlying OS controls. All access to the JumpCloud Web Service was observed to be logged in a PCI DSS compliant manner by JumpCloud.
10.2 Implement automated audit trails for all system components to reconstruct the following events: **10.2.1 All individual user accesses to cardholder data**	✓	**How the JumpCloud DaaS platform can help meet this requirement:** The JumpCloud DaaS platform manages user access to systems but cannot identify if a particular system contains cardholder data or if cardholder data was accessed on a particular system. This control requires the company to develop a policy or procedure that would implement automated audit logging for all system components where access to cardholder data could happen. When configured according to those policies, the JumpCloud DaaS platform can provide audit trails for all individual access to cardholder data.
10.2.2 All actions taken by any individual with root or administrative privileges	✓	**How the JumpCloud DaaS platform meets this requirement:** Logging requirements can be met by using a combination of logs available both locally on each system and provided by

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		the JumpCloud DaaS platform. Therefore, there are two logging features that are used by the JumpCloud DaaS platform: • Logging of all user activities is provided by the underlying OS. • Logging is also done by the JumpCloud Web Service and includes actions taken by administrators. All actions taken by an administrator are logged by the underlying OS. For all actions performed on the JumpCloud Web Service, JumpCloud provides procedures on how to access those logs.
10.2.3 Access to all audit trails	✓	**How the JumpCloud DaaS platform meets this requirement:** Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS. • Logging is also done by the JumpCloud Web Service and includes logs of all access to audit trails. All access to audit trails is logged by the underlying OS. For all actions performed on the JumpCloud Web Service, JumpCloud provides procedures on how to access those logs.
10.2.4 Invalid logical access attempts	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud solution. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS. • Logging is also done by the JumpCloud Web Service and includes logs of all invalid logical access attempts. All invalid logical access attempts are logged by the underlying OS. For all actions performed on the JumpCloud Web Service, JumpCloud provides procedures on how to access those logs.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS. • Logging is also done by the JumpCloud Web Service and includes logs of all usage and changes to authentication and identification mechanisms.

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		All use of and changes to identification and authentication mechanisms are logged by the underlying OS. For all actions performed on the JumpCloud Web Service, JumpCloud provides procedures on how to access those logs.
10.2.6 Initialization, stopping, or pausing of the audit logs	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS solution. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS. • Logging is also done by the JumpCloud Web Service and includes events of pausing, stopping or initialization of audit logs. All initialization, stopping or pausing of the audit trails is logged by the underlying OS. For all actions performed on the JumpCloud Web Service, JumpCloud provides procedures on how to access those logs.
10.2.7 Creation and deletion of system level objects	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS. • Logging is also done by the JumpCloud Web Service and includes records of creation and deletion of system level objects, where applicable. All creation and deletion of system level objects is logged by the underlying OS. For all actions performed on the JumpCloud Web Service, JumpCloud provides procedures on how to access those logs.
10.3 Record at least the following audit trail entries for all system components for each event: **10.3.1 User identification**	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS solution. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS and includes user identification. • Logging is also done by the JumpCloud Web Service and includes all required details and specifically user identification.
10.3.2 Type of event	✓	**How the JumpCloud DaaS platform meets this requirement:**

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS and includes type of event. • Logging is also done by the JumpCloud Web Service and includes all required details and specifically type of event (description).
10.3.3 Date and time	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS and includes date and timestamp. • Logging is also done by the JumpCloud Web Service and includes all required details and specifically date and timestamp.
10.3.4 Success or failure indication	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS and includes success or failure indication. • Logging is also done by the JumpCloud Web Service and includes all required details and specifically success or failure indication.
10.3.5 Origination of event	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS and includes origination of event. • Logging is also done by the JumpCloud Web Service and includes all required details and specifically where the event has originated.
10.3.6 Identity or name of affected data, system component, or resource.	✓	**How the JumpCloud DaaS platform meets this requirement:** This control is directly met by the JumpCloud DaaS platform. Where applicable, the JumpCloud Web Service and underlying OS functionality provide the following features: • Logging of all user activities is provided by the underlying OS and includes identity or name of affected data or resource.

PCI-DSS REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		• Logging is also done by the JumpCloud Web Service and includes all required details and specifically identity or name of affected data or resource.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for using time-synchronization technology.
10.5 Secure audit trails so they cannot be altered.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for securing audit trails so they cannot be altered.
10.5.1 Limit viewing of audit trails to those with a job-related need.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for limiting access of audit trails to those with a job-related need only.
10.5.2 Protect audit trail files from unauthorized modifications.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for protecting audit trail files from unauthorized modifications.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for backing up audit trail files to centralized log server or media.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for writing audit trails to a secure, centralized, internal log server, or media.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for using file integrity monitoring or change-detection software on logs to ensure existing log data cannot be changed without generating alerts.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for reviewing logs and security events for all system components to identify suspicious activity or anomalies.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	⊘	This is a policy requirement that requires that the company pursuing PCI DSS certification should develop policies for storing audit trail history for at least one year, with a minimum of three months immediately available for analysis.

CONCLUSION

After reviewing the requirements of the PCI DSS, Coalfire determined, through review of business impacts and a technical assessment, that the JumpCloud DaaS platform, as outlined in this document, can help organizations meet applicable sections of PCI DSS Requirement 8 and 10. The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of the JumpCloud DaaS platform.

During the assessment, JumpCloud demonstrated a high level of flexibility for user management, customization of policies, policy enforcement, notifications, and configurations including logging.

ABOUT THE AUTHORS AND REVIEWERS

Andrey Sazonov CISA, QSA(P2PE), PA-QSA(P2PE) | **Author** | Senior Consultant, Solution Validation, Coalfire Systems

Nick Trenc CISSP, CISA, QSA, PA-QSA | **Reviewer** | Director, Solution Validation, Coalfire Systems

Published August 2018.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com