WHITE PAPER

JUMPCLOUD DIRECTORY-AS-A SERVICE® PLATFORM FOR HIPAA

ANDREY SAZONOV | CISA, QSA(P2PE), PA-QSA(P2PE)
NICK TRENC | CISSP, CISA, QSA, PA-QSA

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 Systems Inc. (Coalfire) 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 how the JumpCloud DaaS platform can assist in satisfying the technical requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. To fully comply with the requirement, an organization must implement user management policies and procedures as well as train its employees on user management procedures. An explanation of the testing activities performed during Coalfire's review is included in this white paper.

HIPAA SECURITY AND BREACH NOTIFICATION RULES

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI) through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a Covered Entity or Business Associate of a Covered Entity. These organizations are required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against reasonably anticipated unauthorized uses or disclosures of protected health information; and
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures
- Documentation Requirements

While the administrative, physical, and technical requirements identified under HIPAA are mandatory, their implementation may differ based on the organization's type, size, and level of exposure to ePHI. Under the HIPAA Security Rule, Standards and Implementation Specifications are classified as either "Required" or "Addressable". It is important to note that neither of these classifications should be interpreted as "optional". An explanation of each is provided below:

- **Required** – Implementation specifications identified as "required" must be fully implemented by the covered organization. Furthermore, all of the HIPAA Security Rule requirements identified as "Standards" are classified as "required".
- **Addressable** – The concept of an "addressable" implementation specification was developed to provide covered organizations flexibility with respect to how the requirement could be satisfied. To meet the requirements of an addressable specification, a covered organization must: (a) implement

the addressable implementation specification as defined; (b) implement one or more alternative security measures to accomplish the same purpose; or (c) not implement either an addressable implementation specification or an alternative. Where the organization chooses an alternative control or determines that a reasonable and appropriate alternative is not available, the organization must fully document their decision and reasoning. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

The HIPAA Breach Notification Rule, 45 CFR §164.404 - 414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. The major sections of the Rule include:

- Notification in the Case of Breach
- Notification to the Media
- Notification to the Secretary
- Notification by a Business Associate
- Law Enforcement Delay

ABOUT THE JUMPCLOUD DAAS PLATFORM

The JumpCloud DaaS platform is the 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 two target audiences:

1. **Audit Community:** This audience may be evaluating the JumpCloud DaaS platform to assess the company's ability to comply with the requirements of the HIPAA Security Rule.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating the JumpCloud DaaS platform for use within their organization to meet the requirements of the HIPAA Security Rule.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using guidance from the National Institute of Standards and Technology (NIST) and the most recent Office for Civil Rights (OCR) Audit Protocols. 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 are enforced on the system and can be configured to assist in satisfying the HIPAA Security and Breach Notification Rules, when configured properly.
5. Review of the systems to verify passwords are handled in a compliant manner to support NIST recommendations and industry best practices.

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 the HIPAA Security and Breach Notification Rules
- 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 in accordance with the policies configured within the JumpCloud cloud environment.
- The JumpCloud DaaS platform adequately generated logs of all user actions and those actions could then be traced in accordance with requirements of the HIPAA Security Rule.
- Coalfire verified that the JumpCloud DaaS platform cannot be disabled by unauthorized users (non-administrators).
- 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 meeting applicable requirements of the HIPAA Security Rule.

The JumpCloud DaaS platform, when properly implemented following guidance from JumpCloud, can be utilized to help an organization implement technical controls that can assist the organization in meeting the technical requirements of the HIPAA Security Rule. 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 that user management processes can fail when improperly implemented. 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 that an organization will be in compliance with the HIPAA Security and Breach Notification Rules. Disregarding security best practice controls for systems and networks can introduce many other security or business continuity risks.

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 integrates 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, it 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.

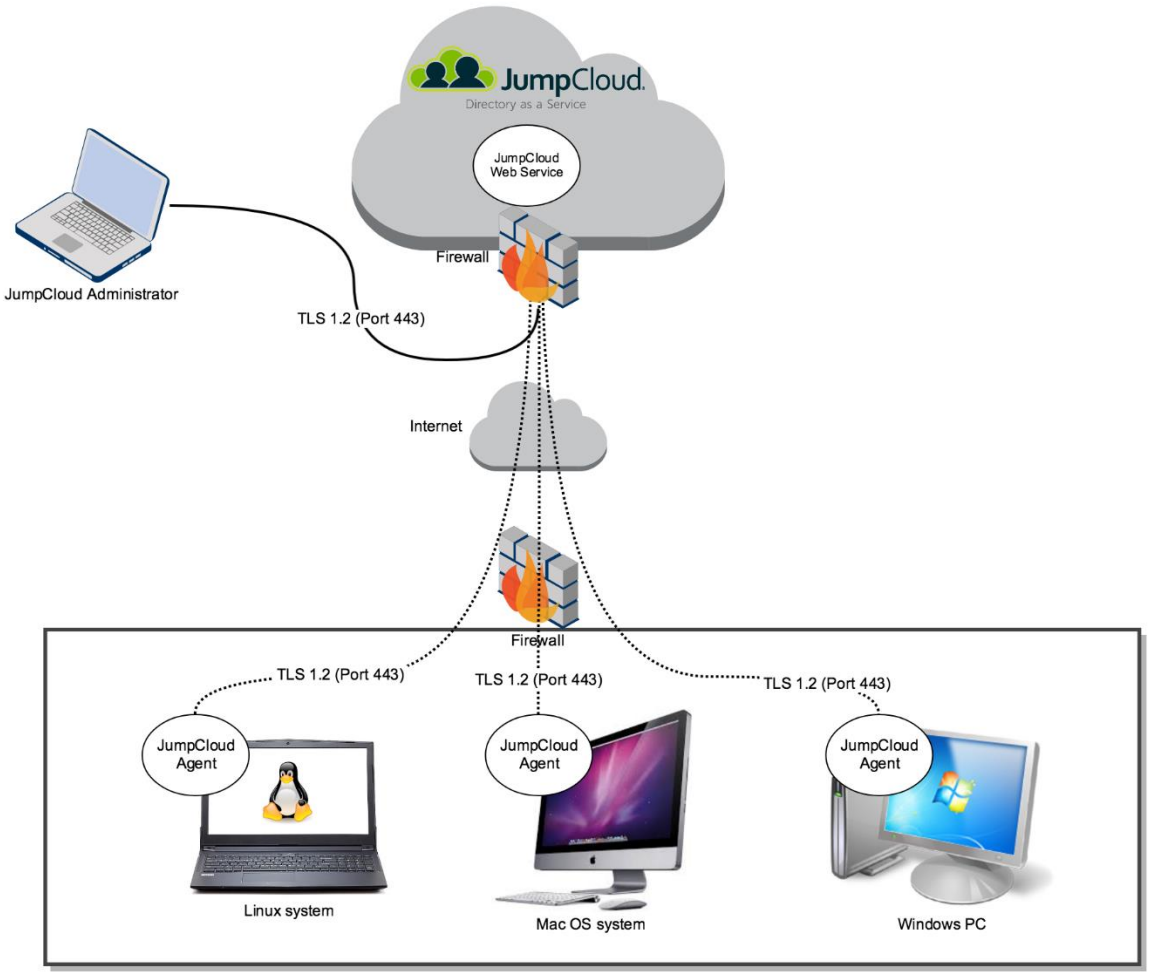

Figure 1: The JumpCloud DaaS Platform Architecture Diagram

TECHNICAL SECURITY ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the platform's alignment with the technical elements of the HIPAA Security Rule:

1. Initial configuration of the JumpCloud DaaS platform in accordance with policies generated by a system administrator and following industry best practices.
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 manner that supports the HIPAA Security Rule technical safeguard standards.
4. User creation, deletion, and configuration using guidance provided by JumpCloud. Testing of all deployment and configuration scenarios to address the technical requirements of the HIPAA Security Rule.
5. Evaluation of 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 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:

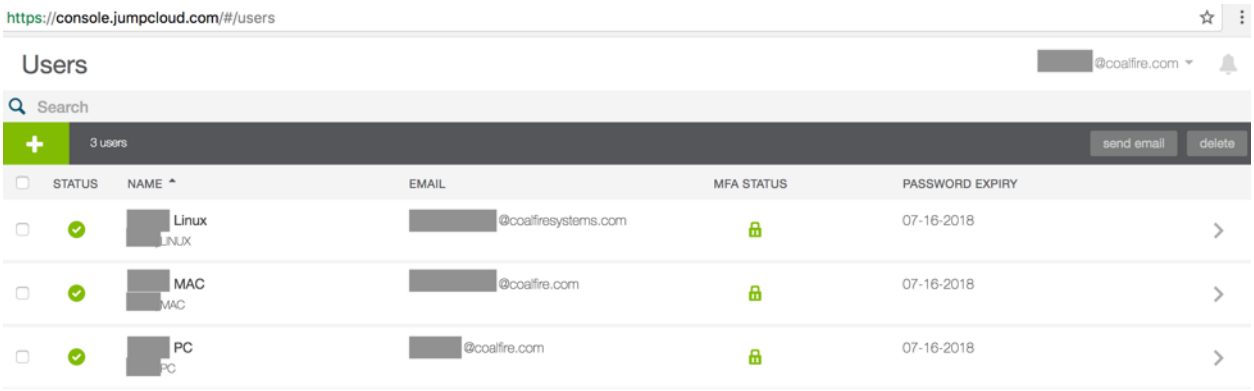

Figure 2: JumpCloud Users Configured

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

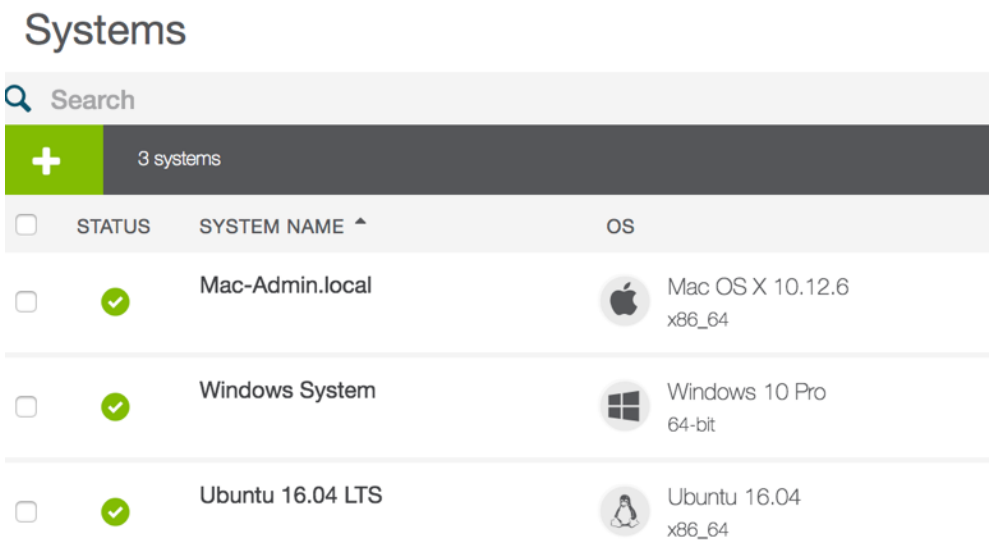

Figure 3: JumpCloud Systems Configured

The initial configuration also required the following security settings on the JumpCloud Web Service that would enforce the HIPAA Security Rule technical safeguards as addressed in Appendix A of this white paper:

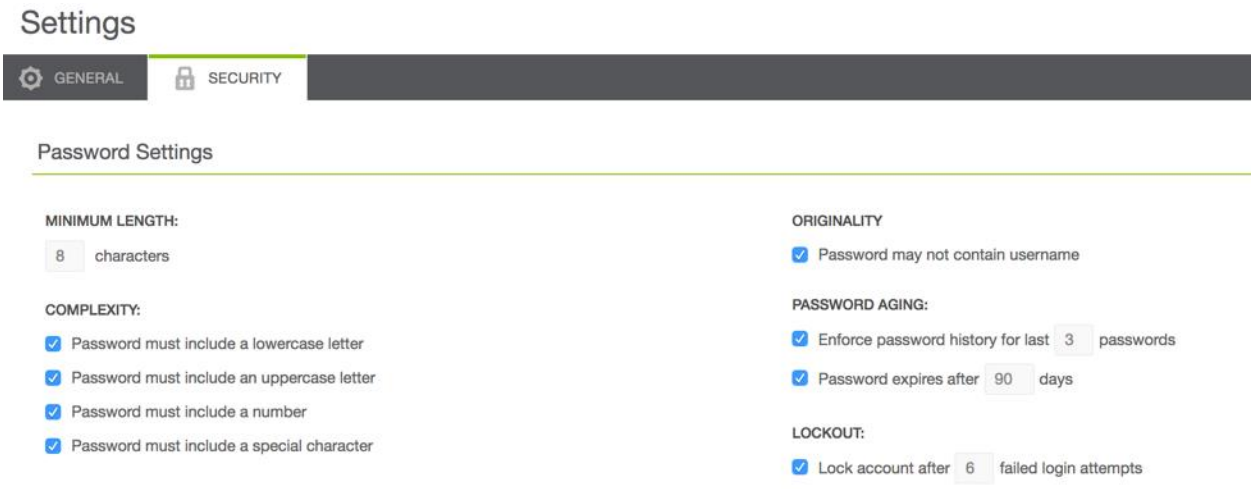

Figure 4: Initial Security Configuration

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:

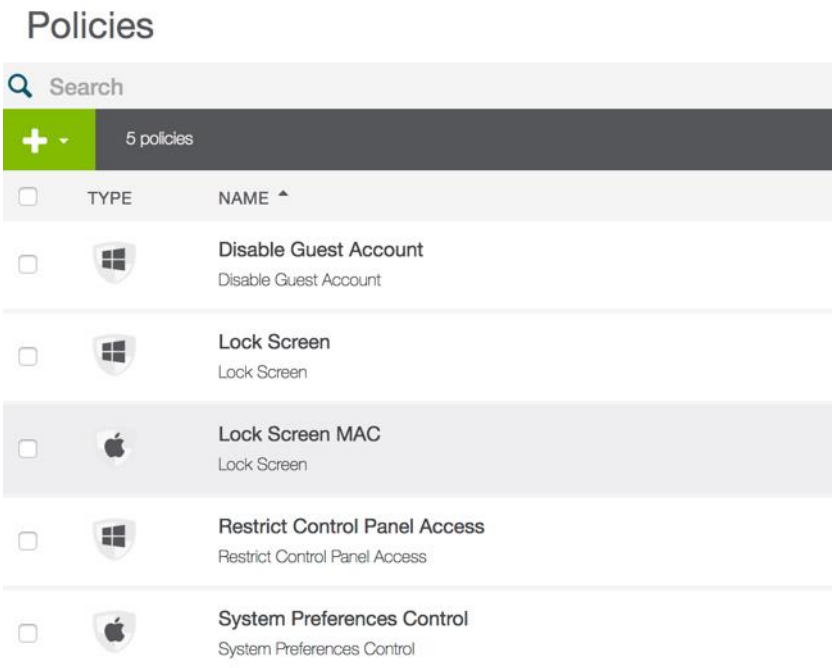

Figure 5: The JumpCloud DaaS Platform Policies Configured

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 applicable requirements of the HIPAA Security Rule.

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.

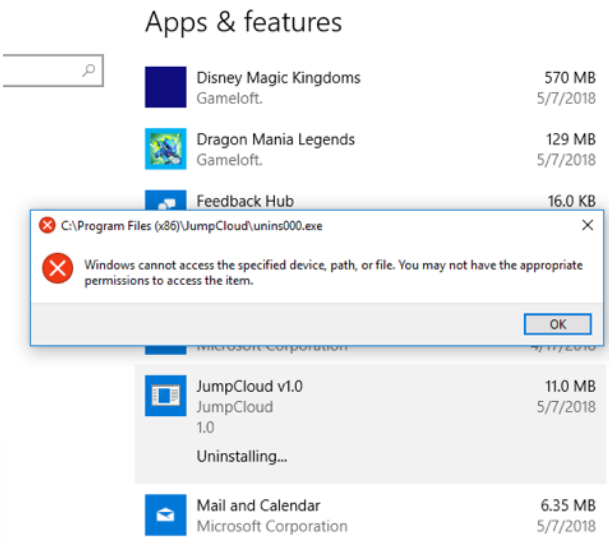

Figure 6: Failed Attempts to Uninstall the JumpCloud Agent

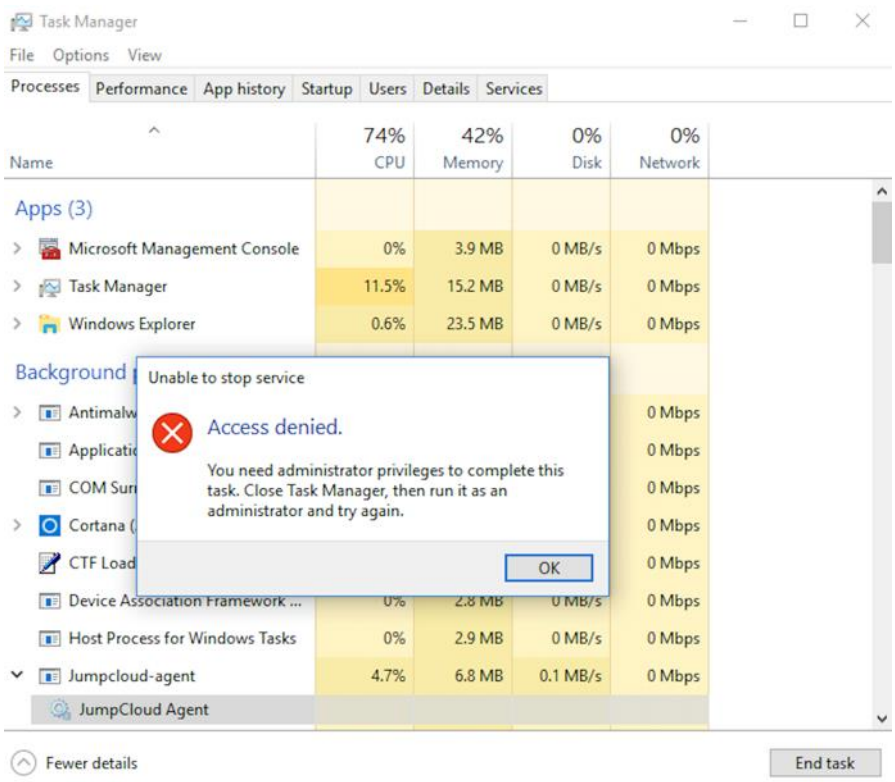

Figure 7: Failed Attempts to Disable or Block the JumpCloud Agent

TECHNICAL SAFEGUARDS – §164.312

Coalfire has observed that policies for access and audit controls are enforced by the JumpCloud Agent software and are properly implemented for all systems tested in a way that addresses technical safeguards of the HIPAA Security Rule. 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.

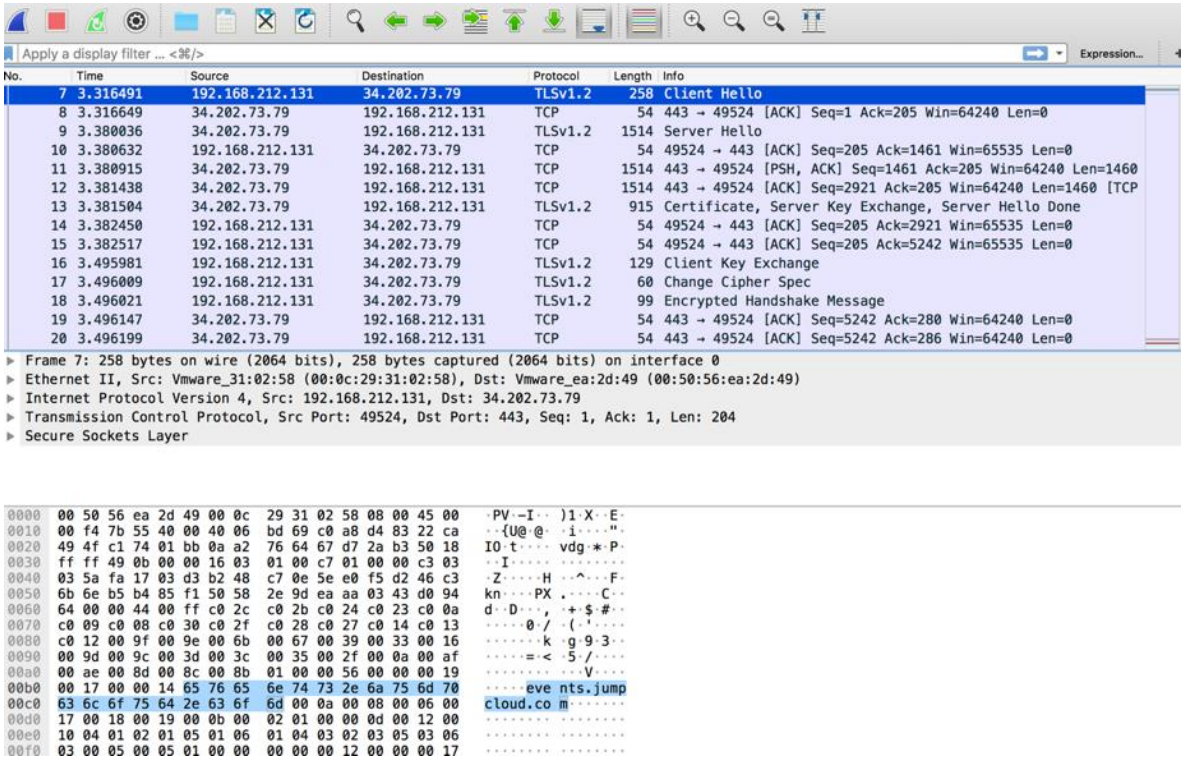

Figure 8: Communication between the JumpCloud Agent and the JumpCloud Web Service

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

No findings were identified within the disk image when searched using 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.

An 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 the 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: HIPAA REQUIREMENTS COVERAGE MATRIX

COMPLIANCE LEVEL	DESCRIPTION
✓	Technical requirements are 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

TECHNICAL SAFEGUARDS – §164.312	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
Access Control – 164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	✓	This control requires user management procedures and policies that the company 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 JumpCloud Web Service (hosted by JumpCloud in the cloud). • Each OS supported at a minimum requires an administrator account, which is usually (but not required) 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.
Unique User Identification – R 164.312(a)(2)(i) Assign a unique name and/or number for identifying and tracking user identity.	✓	This control requires user management procedures and policies that the company should develop. **How the JumpCloud DaaS platform can help meet this requirement:** The JumpCloud DaaS platform allows usage of only unique user IDs for all systems where the JumpCloud Agent is installed. The usage of user identification is a policy requirement that should be followed by the company.
Emergency Access Procedure – R 164.312(a)(2)(ii) Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	⊘	This is a procedure control related to accessing electronic protected health information, in case of user access emergency.
Automatic Logoff – A 164.312(a)(2)(iii) Implement electronic procedures that terminate an electronic session	✓	This control requires initial configuration by the organization and can be directly met by the JumpCloud DaaS platform.

TECHNICAL SAFEGUARDS – §164.312	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
after a predetermined time of inactivity.		**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 a predetermined period of inactivity. Coalfire observed how the system that was idle for fifteen minutes required user to re-authenticate. This functionality was present across all OSs tested (Windows, Linux, macOS).
Encryption and Decryption – A 164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.	⊘	This control requires implementation of encryption and decryption policies that the company should develop. JumpCloud Agent does not store or have access to any element of electronic protected health information and only operates with user accounts accessing the system.
Audit Controls – R 164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	✓	This control requires procedures and policies that the company should develop. **How the JumpCloud DaaS platform can help meet this requirement:** The logging requirements can be met by using a combination of logs available both locally on each system as well as logs provided by the JumpCloud DaaS platform. The following logging functionality can be leveraged when using the JumpCloud DaaS platform: • Logging of all user activities is provided by the underlying OS natively. • Logging is also 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, this control 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 HIPAA Security Rule compliant manner by JumpCloud.
Integrity – 164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	⊘	This control requires procedures and policies that the company should develop. The JumpCloud Agent does not store or have access to any element of electronic protected health information and only operates with user accounts accessing the system.
Person or Entity Authentication – 164.312(d) Person or Entity Authentication – R 164.312(d) Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	✓	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 default method of authentication provided by the JumpCloud DaaS platform is a username and password that

TECHNICAL SAFEGUARDS – §164.312	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		can be configured per an organization's requirements for complexity. It is also possible to configure MFA (multi-factor authentication) for Linux and macOS system access (by using the Google Authenticator application, for example). Windows OS does not natively support MFA via the JumpCloud DaaS platform (this feature is currently being developed by the vendor); however, access to the system can be configured with the use of the third-party tools for MFA.
Transmission Security – 164.312(e)(1) Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. Integrity Controls – A 164.312(e)(2)(i) Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.		This control requires user management procedures and policies that the company should develop. The JumpCloud Agent does not transmit any element of electronic protected health information and only operates with users accessing the system. The only data in transit presented by the JumpCloud DaaS platform is system account passwords that are transmitted using public/private key infrastructure with proper authentication provided by the TLS 1.2 (or higher) protocol. Captured traffic between JumpCloud Agent and JumpCloud Web Service to confirm passwords is protected using the TLS version 1.2 protocol while in transit.
Encryption – A 164.312(e)(2)(ii) Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.		This control requires user management procedures and policies that the company should develop. The JumpCloud Agent does not store any element of electronic protected health information and only operates with user accounts accessing the system. The JumpCloud Agent also does not store user passwords which was validated by capturing full disk image and scanning for passwords using FTK forensic toolkit.

CONCLUSION

After performing a review of business impacts and a technical assessment, Coalfire determined that the JumpCloud DaaS platform, as outlined in this document, can help organizations meet applicable technical requirements of the applicable controls of the Health Insurance Portability and Accountability Act Security Rule. During the assessment, the JumpCloud DaaS platform demonstrated a high level of flexibility for user management, customization of policies, policy enforcement, notifications, and configurations including logging.

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.

ABOUT THE AUTHORS

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

Tommy Abraham CISSP, CISM, CISA, CRISC, CCSFP | **Reviewer** | Director, Healthcare Assurance, 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

Copyright © 2014-2018 Coalfire Systems, Inc. All Rights Reserved. Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.