stonebranch

TECHNICAL PAPER

Universal Automation Center and PCI DSS

How UAC Complies with the Payment Card Industry Data Security Standard (PCI DSS)

In accordance with

PCI Security Standards Council™

June, 2022

Table of Contents

1. Introduction

The Payment Card Industry “Data Security Standard Requirements and Security Assessment Procedures, Version 3.2.1,” dated May 2018, describes PCI DSS as follows:

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

On a very high level, the PCI DSS requirements are defined as shown in the following table:

Category	Requirement
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 1: PCI DSS Requirement Definitions

1.1. What Do the PCI DSS Requirements Mean?

These requirements should be examined in the context of automation software, with implications for the Universal Automation Center. Both organizations already using Universal Automation Center (UAC) as their workload or process automation solution today, and prospective companies considering modernizing their IT infrastructure and migrating to Universal Automation Center as part of that process should take the requirements into consideration. The underlying philosophy behind these requirements raises an important question about the need for PCI DSS compliance. In its role of managing production processes, Universal Automation Center runs programs, scripts and applications that may process payment and personal data. Given that Universal Automation Center must be granted the authority to use powerful credentials to run these payment applications, it is reasonable to scrutinize its security setup and administration.

For example, a payment application executes as a “superuser” (or some similar powerful account) to manipulate card stripe data. When Universal Automation Center submits the batch jobs for this application, that “superuser” user ID must be specified as the credential value in the task definition. To comply with PCI DSS, it is necessary to ensure that the ability to run jobs with the “superuser” credentials is both controlled and audited. If such controls are missing, it is possible that jobs can be run either maliciously or accidentally, which could potentially lead to the access and exposure of payment data.

2. PCI DSS Related to Universal Automation Center

Because we strongly believe that not all of the requirements are related to standard software suppliers like Stonebranch, the 12 PCI DSS requirements listed in the table below are also marked with their respective relevance in regards to Universal Automation Center. The following section describes in more detail how Universal Automation Center complies with the aforementioned relevant requirements.

2.1. Requirement Relevance & Compliance

Before examining the requirements in detail, we will look at the Universal Automation Center architecture to better understand how the communication between the various components operates, and how to protect them. The *figure 1* below illustrates the Universal Automation architecture at a glance.

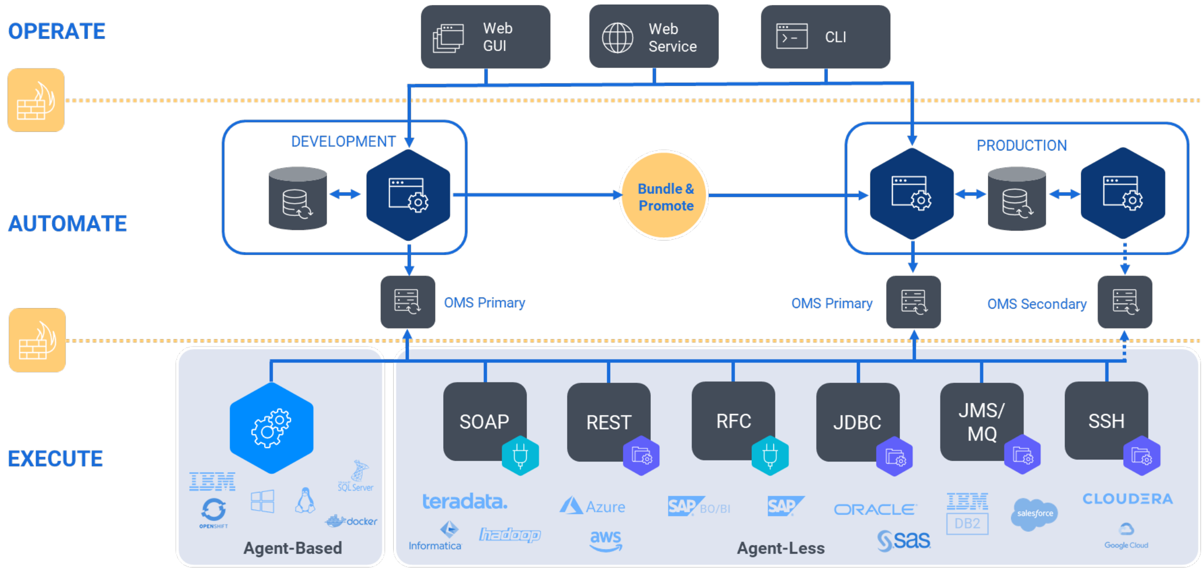

Figure 1: Universal Automation Center - Architectural Overview

Figure 1 shows a two instance Universal Automation Center System comprised of a test and a production instance. The production instance is set up in a high available mode, so that an interrupt free failover scenario can be applied in the case of failure of the primary instance. The test instance is setup as a single, non-high available system.

Category	Requirement	Relevant
Build and Maintain a Secure Network	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data	Yes

	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Yes
Protect Cardholder Data	**Requirement 3:** Protect stored cardholder data	Yes
	Requirement 4: Encrypt transmission of cardholder data across open, public networks	Yes
Maintain a Vulnerability Management Program	**Requirement 5:** Use and regularly update anti-virus software or programs	No
	Requirement 6: Develop and maintain secure systems and applications	No
Implement Strong Access Control Measures	**Requirement 7:** Restrict access to cardholder data by business need to know	Yes
	Requirement 8: Assign a unique ID to each person with computer access	Yes
	Requirement 9: Restrict physical access to cardholder data	No
Regularly Monitor Test Networks	**Requirement 10:** Track and monitor all access to network resources and cardholder data	Yes
	Requirement 11: Regularly test security systems and processes	Yes
Maintain an Information Security Policy	**Requirement 12:** Maintain a policy that addresses information for all personnel	No

Table 2: Requirements and Relevance for Compliance Overview

3. Building & Maintaining a Secure Network

3.1. Install and Maintain a Firewall Configuration to Protect Cardholder Data

Universal Automation Center operates with solely outgoing ports to be opened from any on-premise component into the internet. All port definitions are completely customizable by the end-user and access to core components can additionally be protected by internal measures like ACL (Access Control Lists) within the system configuration.

All communication between the system components is based on TCP/IP over SSL using TLS 1.2 and is additionally protected by using certificates that can be imbedded from any X 509 standard based certificate authority.

The OMS middleware messaging layer ensures that no direct communication is established between Universal Agent and Universal Controller components. Universal Agents register with the OMS server, as does the Universal Controller component. Any following communication for the processing of automation tasks and data transport is based on messages inserted into the OMS database and then processed by the receiver.

3.2. Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

The Universal Automation Center supports a very granular security and protection mechanism, down to the individual command level, if wanted and required.

We strongly recommend configuring Universal Controller with your LDAP, Active Directory, or SAML Single Sign-on tools. This allows the Universal Controller to inherit your corporate standards for password and password expiration rules.

For any local user definition, managed by the Universal Controller, we strongly recommend setting the number of allowed login attempts, as well as activating the account locking mechanism within the Universal Automation Center.

4. Protect Cardholder Data

4.1. Protecting Stored Cardholder Data

As shown in the requirements table above, we consider this requirement to have a medium relevance, as we do not directly deal with cardholder data. We might execute applications that do so, or we might transfer data with our unique Universal Data Mover (UDM) transfer protocol, (protected by SSL over TCP1.2), but we do not and will not store any card holder data within our own sources or databases.

Nevertheless, all data processed by Universal Automation Center is encrypted both at rest and in transit by using the appropriate cipher suites within our internal database as well as during transit of data in all types of transfer operations.

Database contend is currently encrypted with AES 128, while transfer encryption can be completely user defined with up to AES 256 and the appropriate hashing algorithm, as shown in the following extract of available ciphers:

- AES256-GCM-SHA384
- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA

All ciphers are accepted as secure until at least 2023 by the appropriate authorities. New ciphers will be added on a regular base to the system as required, while outdated ciphers will be deprecated as needed.

4.2. Encrypting Transmission of Cardholder Data Across Open Public Networks

The transfer encryption can be completely user defined with up to AES 256 and the appropriate hashing algorithm, as shown in the following extract of available ciphers:

- AES256-GCM-SHA384
- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA

All ciphers are accepted as secure until at least 2023 by the appropriate authorities.

5. Maintain a Vulnerability Management Program

5.1. Use and Regularly Update Anti-Virus Software or Programs

This requirement is not valid for standard automation software solutions but needs to be maintained on an OS level by the respective client organization.

Stonebranch maintains a vulnerability program for its own software components and regularly publishes any known vulnerabilities within their customer portal. Development processes have been established to ensure a regular review of known vulnerabilities and their impact, to ensure that available fixes are communicated properly to the customer base.

5.2. Develop and Maintain Secure Systems and Applications

Stonebranch follows the latest security standards within their development organization. The customer portal also contains informational documentation regarding how to secure Universal Automation Center implementation by using the available security features.

5.3. Restrict Access to Cardholder Data by Business Need to Know

As already pointed out within “*Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*” Universal Automation Center provides a very granular level of access control that allows organizations to protect relevant information within their CDE environment.

6. Implement Strong Access Control Measures

6.1. Assign a Unique ID to Each Person with Computer Access

Universal Automation Center supports a very granular access control on the user and job levels with the integration of LDAP/active directory or single sign on systems and in combination with the credential definitions on the job level that can be enforced by instance-wide property settings.

6.2. Restrict physical access to cardholder data

This requirement is not relevant for Universal Automation Center, as card holder data is not stored anywhere internal to the system.

7. Regularly Monitor Test Networks

7.1. Track and Monitor all Access to Network Resources and Cardholder Data

Universal Automation center has a detailed integrated audit trail that monitors actions against any object within the Universal Automation Center environment. Standard audit reporting is available through the embedded report generator along with many other standard report templates. Any change to a relevant object will create a new version of the object, as well as an audit record describing the change, and will keep the status before and after available.

7.2. Regularly Test Security Systems and Processes

Stonebranch regularly performs penetration tests on the components of the Universal Automation Center which are available upon request. In addition, Stonebranch provides a vulnerability tracking system in which known software vulnerabilities are listed and solutions are documented, where available.

8. Maintain an Information Security Policy

8.1. Maintain a Policy that Addresses Information for All Personnel

This requirement is not relevant, as it has more to do with the client holding the PCI data. Stonebranch does have an appropriate policy implemented that is available upon request.

9. Conclusion

Workload automation is a foundational IT management discipline that is an essential component of almost every IT infrastructure. In most environments supporting payment applications or the processing of card and payment data, batch workload services are so integral that they are directly involved in PCI DSS compliance.

Stonebranch Universal Automation Center delivers an enterprise workload automation solution that is fully compliant with the PCI DSS standard. Universal Automation Center users can confidently manage their PCI workload, together with all their other enterprise batch applications, without having to implement separate tools or segregated environments. This fully integrated and dynamic approach enables customers to realize the full benefits of Stonebranch's Universal Automation Center for their entire IT environment, including features such as:

- A single point of control that delivers an end-to-end view of all workload and IT processes
- Support for all platforms and applications that make up the IT or CDE environment.
- Predictive forecasting and change impact analysis, policy-based dynamic workload management, and automated incident management
- Full exploitation of dynamic resource management via virtualization and cloud technologies

Figures

Tables

stonebranch