EngageOne Converse

Version 2.3

Security White Paper

June 2020

This document describes the security of EngageOne Converse. It begins with a summary of the key security points. More information about these points is provided in the remainder of the document.

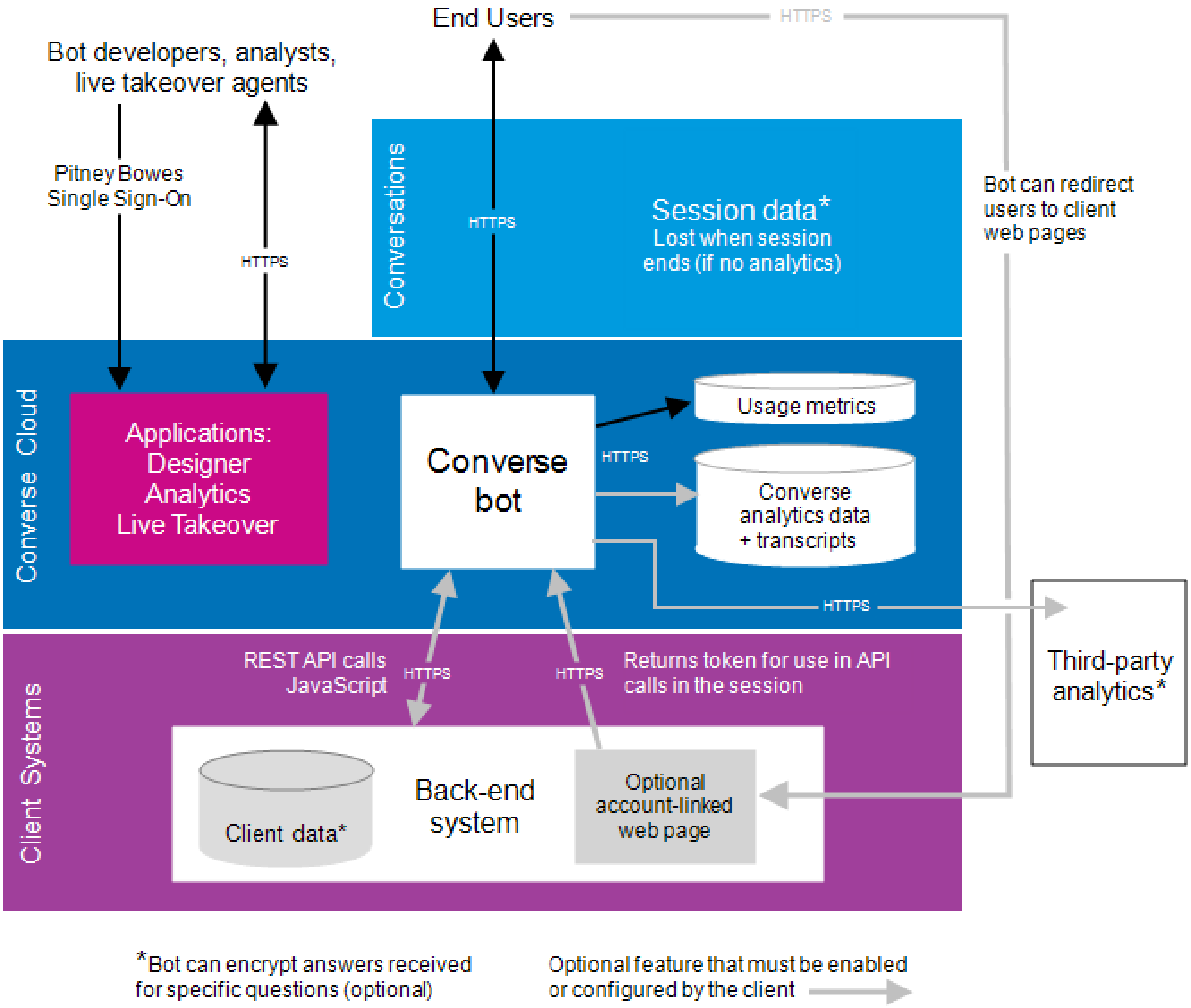
This document is intended for Precisely clients, partners and employees.

Contents:

Introduction

This document describes the security of EngageOne® Converse such as the Converse cloud infrastructure, how bot services are developed, and Converse handles the personal data received during live conversations. The main security considerations are shown in the following figure, with an overview in the **Converse security summary** on page 3. For more detail on any points, refer to the remainder of the document.

Figure: Converse – Main Security Considerations


End Users
HTTPS
Bot developers, analysts, live takeover agents
Pitney Bowes Single Sign-On
HTTPS
Conversations
HTTPS
Session data*
Lost when session ends (if no analytics)
Bot can redirect users to client web pages
Converse Cloud
Applications: Designer Analytics Live Takeover
Converse bot
Usage metrics
HTTPS
Converse analytics data + transcripts
HTTPS
Third-party analytics*
Client Systems
REST API calls JavaScript
HTTPS
HTTPS
Returns token for use in API calls in the session
Client data*
Back-end system
Optional account-linked web page
*Bot can encrypt answers received for specific questions (optional)
Optional feature that must be enabled or configured by the client

Converse security summary

This is an overview of the main security considerations for EngageOne Converse. You can find more information about these points in the remainder of this document.

Cloud-based tools and services

- Converse uses HTTPS (TLS 1.1 or higher) for all internet traffic.
- All Converse tools (Designer, Live Takeover, Converse Analytics) and bot services are hosted on **Amazon Web Services** (AWS). See **here** for what this means.
- Precisely has a global Single Sign On mechanism for all its online services.
- Clients only have access to their company account.
- Precisely run annual threat scan and penetration tests to examine the security of Converse software.

Handling of personal data

- Use of regional AWS servers ensures that data stays in the country of origin.
- Data used in a live conversation persists for the session, and is lost when the session times out.
- Data at rest is only stored if the client enables Converse Analytics.
- Answers to specific questions can be **encrypted** during live conversations, in analytics data and when sent to back-end systems.

> **Note:** Precisely counts the number of sessions in order to understand how clients are using Converse. For example we record that a conversation has taken place but not what it was about.

Converse Analytics and third-party analytics tools

Optionally clients can track conversations in order to measure the success of their bot:

- **For third-party analytics tools**, data (including any encrypted data) is sent to the analytics tool in real time. It is not stored by Converse.
- **For Converse Analytics**, analytics data includes, for example, numbers of users and conversations, most frequent user messages and the number of times users sent a message for which the bot had no answer. This data is stored by Converse. Clients can access a transcript of each conversation. Encrypted data is never displayed in Converse analytics data or transcripts.

> **Note:** Bots must be designed to minimize the amount of personal data that needs to be entered in live conversations. Encryption is also available.

Building bots and integrating with third-party services

- Bots are created in Designer, and the same tool is used for developing integrations with third-party services (such as Facebook, Amazon Alexa) and back-end systems.

- Converse is designed to validate all requests originating from the third-party to ensure that they are legitimate requests.
- Third-party data, such as personal information, usernames and passwords, will never be exposed to Precisely.

> **Note:** Third-party service providers capture the information that is processed by Converse bots, and utilize messaging data in accordance with their own security policies. Precisely therefore has no control over how these third parties will utilize this information. Please see their specific policies for more information.

Converse security in more detail

This section discusses the Converse security in more depth.

- **Converse Cloud infrastructure** on page 4
- **Building bots and integrating with third-parties** on page 9
- **Data handling and use of personal data** on page 7
- **Converse software** on page 11

Converse Cloud infrastructure

All bots run in the Converse Cloud, a cloud computing platform that is built on the highly-secure, physical infrastructure provided by Amazon Web Services (AWS).

Amazon Web Services (AWS)

The highly-secure, physical infrastructure provided by Amazon Web Services (AWS) enables Precisely to provide a world-class, scalable and affordable software solution that does not make any compromises concerning the security of client data. Precisely follows best practice in the configuration and management of its infrastructure in order to offer a secure and reliable platform that meets the requirements of the most security sensitive organizations.

> **Note:** You can find comprehensive documentation on AWS' security measures on the AWS website. For example AWS: Overview of Security Processes which is available from **https://aws.amazon.com/whitepapers/#security**.

Managing the cloud infrastructure

Precisely is responsible for configuring, managing and protecting its infrastructure in the AWS cloud. For example:

- Connections to the AWS cloud infrastructure are only allowed from specific IP addresses.
- Additional servers are automatically provisioned as demand for the client's service increases. The provisioning service ensures that servers are configured to the correct specification to meet both technical and security requirements.
- Proactively monitoring infrastructure configuration in AWS Trusted Advisor, and acting on any recommendations received.
- Logging all infrastructure changes in AWS CloudTrail. Server logs are recorded in AWS CloudWatch Logs.

All software, databases, database backups and snapshots for disaster recovery are stored on the cloud.

Configuration of the AWS security group(s)/firewalls

The virtual servers and network provisioned by Precisely run within a series of virtual private clouds. Routing of network traffic is explicitly controlled by the configuration of subnets and by AWS security groups which specify the inbound and outbound traffic allowed to connect to specific parts of the cloud infrastructure.

Configuration and management of AWS instances

Precisely provisions large numbers of Amazon EC2 instances to meet the service needs of its clients. Provisioning is automated by using AWS OpsWorks. This is an application management service that ensures that each instance is deployed with all the required software dependencies, applications and tools, and that they are correctly configured to avoid known security risks.

> **Note:** The AWS services are SOC1/ISAE 3402 (formerly known as SAS70), SOC 2, DIACAP and FISMA certified. The AWS services also have other certifications and accreditations.

Logical access controls

Precisely use AWS Identity and Access Management (IAM) to control user access to its AWS infrastructure. This means that:

- Staff access to the AWS cloud infrastructure is enforced by automated provisioning processes.
- Account creation follows the principle of least privilege.
- All users with access to the Converse Cloud infrastructure on AWS have separate user accounts for each server instance.
- AWS OpsWorks is used to configure the OpenSSH key pairs that are permitted to connect to each instance.
- AWS CloudTrail is used to log connections.
- There are no default user names and passwords for admin users.

> **Note:** Logical access to the Designer, which is used for creating and deploying bots, is managed separately. A user account with access to the Designer has no access to the cloud infrastructure.

Software patching and security updates

The servers in the Converse Cloud run Amazon Linux. The Amazon Linux Security Center continuously publishes security alerts, and provides a mechanism for deploying security patches and other updates. Precisely immediately reviews all patches and updates, and then tests the relevant patches for at least two business days on the servers in a staging environment before updating the live servers. There will be no disruption to the bot service because each environment has a minimum of two load balanced servers, and each server is updated separately.

Business continuity and disaster recovery tests

Converse has been developed to be fault tolerant across availability zones in AWS. Precisely reviews the Business Continuity and Disaster plan quarterly, and tests this annually. Precisely performs disaster recovery tests on a regular schedule. As part of the disaster and recovery procedure, full server backups are made on a daily and monthly cycle.

Anti-virus software

Anti-virus software is installed on employee machines that are used to connect to AWS infrastructure. Precisely uses McAfee as standard.

Logs

- Logs are stored on the application servers on an encrypted drive.
- Logs on the application servers are stored for 7 days.
- Application servers are inside a private subnet and do not have direct internet access.
- Access to all servers are restricted to particular addresses inside the Precisely network.
- Logs are moved in near-real time to the cloud using AWS Cloudwatch Logs.
- Logs being moved to the cloud are encrypted in transit.
- Logs can only be accessed via the AWS Console.
- The AWS Console requires username and password access along with a single-use code (MFA).
- Access to the logs are restricted only to AWS Console users who require it.

Databases

Converse uses MongoDB to store bot configurations set up in Designer. Session data is stored in the EngageOne Commerce Cloud. Analytics data for each bot is stored in a separate area from the Converse service usage data.

Database management

Depending on the storage type in use, some of the following may apply:

- Automatic, encrypted backup, facilitating point-in-time restore for a retention period of up to 8 days. (Backups are deleted after 8 days.)
- Patching – patches are applied to a standby database which is then promoted to the new primary so that the impact of the maintenance event is mitigated.

- Continuous data replication to an encrypted backup database.
- Failover – if a database becomes unavailable then the database automatically fails over to the standby database.
- Monitoring for database space, server load and failover events.
- Storing and rotating database transaction logs.

Data at rest

The databases (including the replicas made for backup and failover purposes) can be encrypted. However, due to the trivial nature of the data that is collected, this feature is not used by default.

Data in transit

All data is transmitted using a Secure Socket Layer (TLS 1.1 or higher). This is referred to as HTTPS.

Data handling and use of personal data

This section discusses the data used by a Converse bot service and how it is handled. The different types of data are:

- Personal data
- Session (conversation) data
- Converse Analytics data
- Service usage data
- Cookies

Personal data

Clients can configure their bots to ask for personal data as part of the conversation. This data is never stored in the **service usage data** collected by Precisely. If Converse Analytics is enabled then the data is stored in the **analytics data** for the bot.

It is the client's responsibility to design their bots in such a way that they minimize the amount of personal data entered by their customers when interacting with their bot. For example, if the client designs a bot that receives personal data during the conversation then it's the client's responsibility to handle that data appropriately. This includes:

- Enabling encryption for questions that request personally identifiable information (see **Encrypting user answers** on page 10).
- Considering whether it is appropriate to enable analytics where the captured data could include unencrypted, personally identifiable information. Enabling analytics whether Converse Analytics or any of the other third-party analytics tools will capture any data entered by customers during the conversation (excluding data entered on the account-linked web page).

Personal data and third-party platforms

Bots can be deployed across multiple third-party messaging platforms (such as Facebook, Amazon Alexa) and each platform has its own security responsibilities and policies. These third parties capture and utilize messaging data in accordance with their own policies.

EngageOne has no control over how these third parties will utilize the information that is processed by bots created using Converse. Please see their specific policies for more information.

Session data

Session data consists of the following:

The conversation

The messages sent to and from the user. This *excludes* anything entered on the account-linked web page as this is not part of the chat session.

To save the conversation, the client must enable Converse Analytics.

See **Converse Analytics data** on page 8.

Service usage metrics

This includes data such as session ID, date, channel. This is always saved for use by Precisely.

See **Service usage data** on page 8.

Session data is stored on the EngageOne Commerce Cloud. Converse Analytics (conversational) data and service usage data are stored separately.

Converse Analytics data

If a client chooses to enable Converse Analytics then everything that end users enter and receive in a conversation is captured and saved in the Converse Analytics data. This excludes anything entered on the account-linked web page because this web page is not part of the bot.

Aggregated and individual session data is displayed on the **Analytics** pages in Converse, and transcripts of conversations can be accessed on the **Conversations** page. Conversations are identified by session ID. Encrypted data remains encrypted. See **Encrypting user answers** on page 10.

Service usage data

So that Precisely can analyze service usage, Converse captures a small amount of data about all the sessions that occur. For example, in order to calculate the total number of conversations, Converse logs that a conversation has occurred but not what the conversation was about. The data is stored on the EngageOne Commerce Cloud.

Details of conversations, including personal information about users, is never stored in the service usage data.

Use of cookies

Session cookies are necessary to the running of a Converse service, for example to the operation of the load balancer that distributes network traffic evenly across all servers in order to maintain the responsiveness of the chat service. The session cookie has a randomly-generated ID that identifies the session. Session IDs have an expiry time and the ID does not contain any personal or sensitive information.

Building bots and integrating with third-parties

This section discusses the security considerations around building bots in the Designer and integrating with different messaging channels.

Integrating the bot with different channels

The client can integrate a bot with a range of channels. Precisely will validate all requests originating from the third-party to ensure that they are legitimate requests. Third-party data, such as personal information, usernames and passwords, will never be exposed to Precisely.

Using the web client channel

Converse Web Client is hosted on a secure connection with modern ciphers to reduce security vulnerabilities. This means that browsers that do not support TLS 1.1 or higher will not be able to use the Web Client. This isn’t a problem for most users. However for Microsoft Internet Explorer 10 and earlier, TLS 1.1 is not enabled by default (although users can configure this in Internet Explorer options).

> **Note:** Clients embedding the Web Client on their website may choose to provide user feedback when TLS 1.1 is not enabled.

Using the Facebook Messenger channel

You can integrate a bot with Facebook using the Facebook Messenger API. Facebook users can then log into Facebook and interact with the bot.

- Converse will validate all HTTP requests originating from Facebook to ensure they are legitimate requests.
- Facebook data such as Personal Information, usernames and passwords will never be exposed to Precisely.

Integrating the bot in the client's website

Clients can embed the Converse Web Client into their own website using a JavaScript code snippet that can be copied from Designer. The code will only access the specified bot using its Unique Bot ID. No data from the client's site will be exposed to Converse.

Integrating with back-end systems

Bot developers can integrate the bot with the client's own system by using REST API calls:

- Data that is encrypted by Converse remains encrypted when passed in API calls to the back-end system. The developer must explicitly decrypt it.
- The JavaScript integration can be written to handle authentication by the back-end system, and data encryption.
- Data received in API calls to the back-end system is forgotten when the session ends.
- If the client enables analytics then any data used in questions and messages will be saved in the analytics data or passed to the third-party analytics tool. It is therefore up to the designers and developers of the bot to ensure that the data is handled appropriately. For example by considering whether it is appropriate to enable analytics. See **Converse Analytics data** on page 8.

Account linking

Clients can configure a bot to link to an end-user's account in order to access or provide information that requires authentication. Account linking must be set up from the client's end to use the client's authentication method.

- Converse and Precisely will never have access to the end-users' credentials.
- Data returned from a client's web service persists for the duration of the session, and is deleted once the session expires. The session timeout can be configured by the bot designer.
- Data entered on the account-linked web page is *not* captured by Converse Analytics because this page is *not* part of the conversation with the bot.

Encrypting user answers

Clients can choose to protect sensitive data received from users during conversations by encrypting the answers to specific questions. Encryption is then used when the answers are:

- Stored for the duration of the conversation (session)
- Passed in REST API calls to other systems
- Saved in the transcript that is generated for each conversation (if Converse Analytics is enabled)
- Sent in real time to third-party analytics tools
- Shown in Live Takeover and in the Live Takeover history

Converse uses AES encryption. The encryption key is generated from a passcode entered as part of the bot configuration and stored securely in the EngageOne Cloud:

- The passcode can be up to 32 characters long.
- The same passcode, even if used multiple times in different bots, always provides a unique encryption key.
- The same value when encrypted by the encryption key will always result in a unique encrypted value.

The encryption key is not displayed anywhere in Converse.

Converse software

Precisely develops the software that is used to build and deploy bots to servers on the Converse Cloud. The software includes:

Runtime	The platform on which services run. The Runtime is deployed to each virtual server that hosts client services.
Designer	Web-based tools for creating bots.
Converse Analytics	Web-based tool for reporting on bots.
Live Takeover	Allows agents to take over live conversations.

EngageOne Converse software is updated on a regular cycle.

Access to the Converse tools

- All access is over an SSL encrypted connection.
- Access is granted based on roles, and clients can only see the bots that are created in their company account.
- A password policy is applied (minimum requirement is: 8 characters, with 1 uppercase character, 1 numeric character or 1 special character).
- Following industry best practice, stored passwords are hashed with a salt (a cryptographically-strong random value).
- Converse uses session IDs. The ID is a randomly-generated string that will be overwritten when the user logs out. The ID contains no personal or sensitive information. The session ID will expire if the user forgets to log out.

> **Note:** Access to the Converse tools is completely separate from staff access to the AWS cloud infrastructure on which the Converse Cloud runs.

Threat scan and penetration testing

Precisely runs a threat scan at every major release, and commissions a third-party to perform annual threat scan and penetration tests.

> **Note:** Penetration tests examine the security of the EngageOne Converse software. The tests try to discover any security weaknesses in the current release that would be useful to a hacker trying to gain access to the Designer or disrupt services.

The results of the test are dependent on individual client requirements as not all services are the same. The results will be shared with clients under a non-disclosure agreement. Using a screen share, a Precisely representative will show the report to the client and explain the results.

Development practice

Precisely has a change management policy which includes code review and testing:

- Detailed code reviews are performed for all updates to EngageOne Converse software. This includes a review of security. Code review is followed by testing.
- A suite of automated tests runs regularly after reviewed changes are submitted to the code base.
- All changes are tested before release.
- Regression testing is performed at every minor release (regression testing ensures that older parts of the software work with the new changes).

When deploying software updates, staff follow standard operating procedures. If an incident occurs, the circumstances are reviewed so that operating procedures can be updated if necessary.

All deployments are logged in AWS CloudTrail.

Converse terms

Bot Runner
Proprietary Converse software and libraries that are deployed to each server to create the platform on which chat services run.

Dependencies
Underlying Linux, Apache, and NodeJS server build and associated open-source software libraries required by the EngageOne Converse Runtime environment. This is deployed to each live production server.

EngageOne Converse Analytics
When enabled, gathers and saves data about conversations with the client's bots that is displayed on the Dashboard. The data is stored on the EngageOne Commerce Cloud.

EngageOne Converse Cloud
The infrastructure provisioned by Precisely from Amazon Web Services. Used to create and deliver EngageOne Converse chat services.

EngageOne Converse Designer
EngageOne Converse bots are created and configured in the Designer.

EngageOne Commerce Cloud
Clients who enable Converse Analytics store their analytics data on the EngageOne Commerce Cloud.

Document history

Version/date	what changed
12th August 2019	In Security Summary, changed HTTPS (SSL) to HTTPS (TLS 1.1 or higher), and added extra section on web client and TLS to Integration section. As requested by Harry Pynn and Chris Cummings in email.

Copyright