Hub and Interact 4.0

Security Reference Guide

Document Revision: 1.0

Blue Prism Interact Security

This document provides a functional and technical point of reference to help with customer concerns, compliance queries and incoming Request for Proposals (RFP) around security and covers the following:

Encryption

Blue Prism Interact uses the following encryption methods:

Algorithm	Description
Traffic encryption	Enable HTTPS only communication for production. Requires customers to provide TLS certificates for all web applications and all communication channels must be secured. For more information about configuring certificates, see the online help.
Data protection	The Hub installer generates a PFX certificate and saves it to Trusted Root Certificate Authorities. All applications use it to encrypt sensitive data, such as connection strings in the appsettings.json file. Data protection uses the following default algorithms: • Encryption Algorithm is AES-256-CBC • Validation Algorithm is HMACSHA256 The key size is 2048 bit.
JWT token signing	The Hub installer generates a PFX certificate and saves it to Trusted Root Certificate Authorities. The Identity Server uses it to encrypt the JWT token and to validate the license file. The JWT token is encrypted by the RSA-SHA-256 algorithm and the key size is 2048 bit.
Identity Management Server (IMS)	This is the authorization server - users login via the IMS which determines the components they have access to. The identity server uses SHA-256 to hash the client secret and client ID.
Password Storage	The AspNetIdentity library is used for password hashing and uses the following algorithms: • PBKDF2 with HMAC-SHA256 • 128-bit salt • 256-bit subkey • 10000 iterations

The license key is encrypted by the RSA-SHA-512 algorithm.

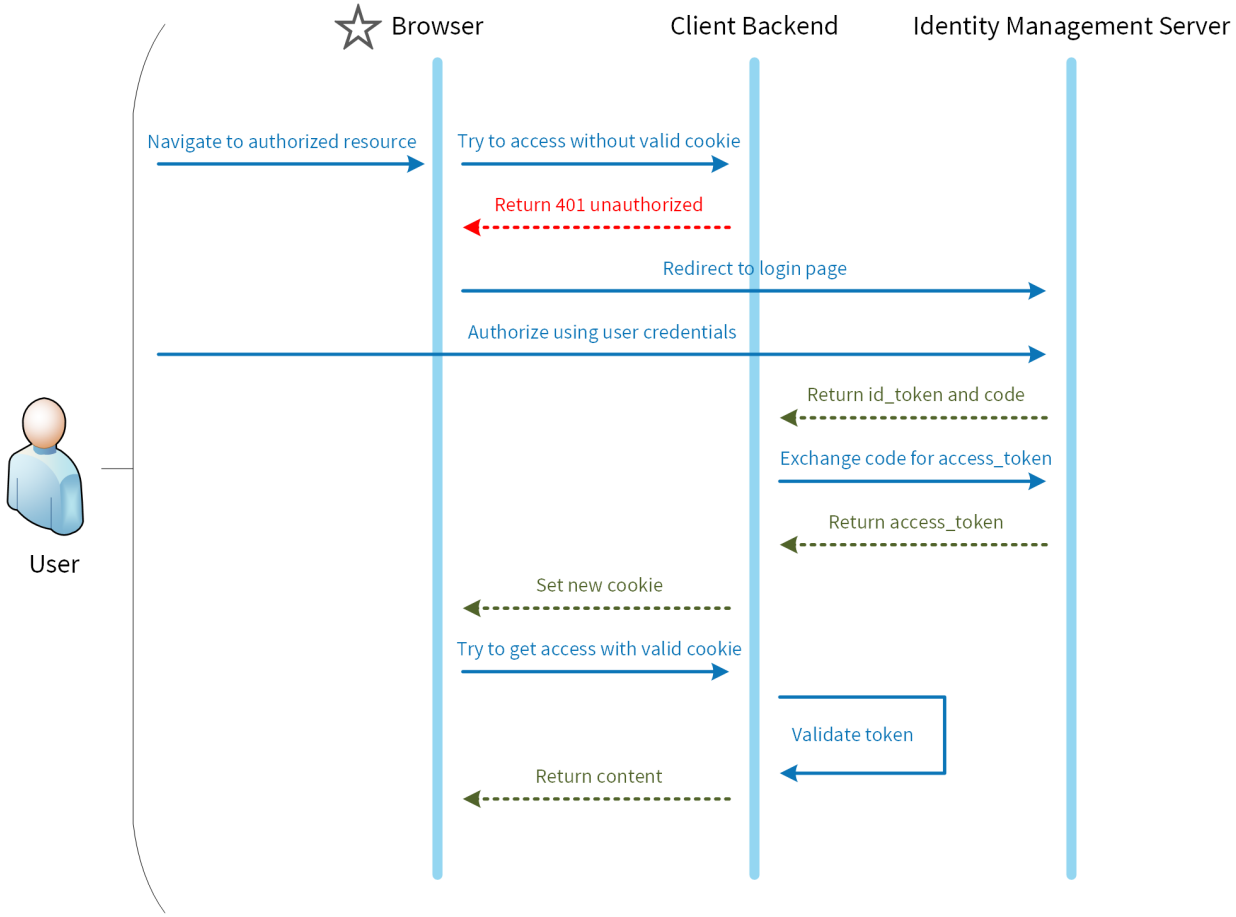
Database encryption can be provided by the default Microsoft encryption mechanism (Transparent Data Encryption - TDE) but must be implemented by the end user. For more info see: docs.microsoft.com.

TLS defaults to the host operating system configuration for both TCP and HTTP communications, selecting the best security protocol and version. Available protocols and ciphers are managed by the end user or automatically handled through Microsoft security updates.

Authentication

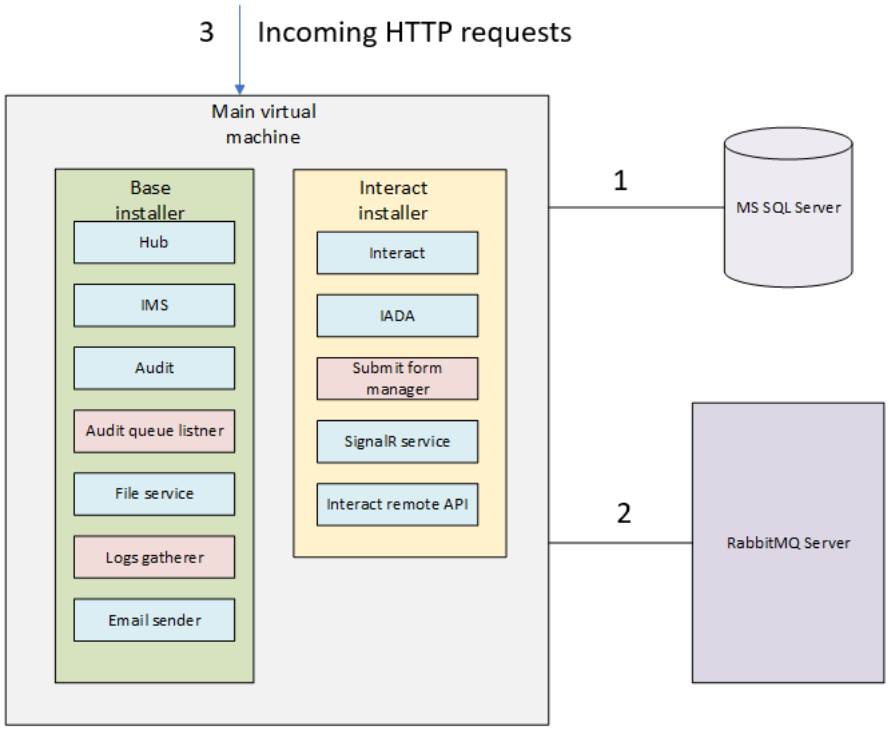
Authentication in Interact is outlined below:

- An Identity Server is provided which is implemented by the OpenId Connect protocol.
- All users' API calls are authorized.
- All API calls between applications are authorized.
- The access token is stored in HTTPS cookies only which cannot be intercepted or modified.



Network connectivity

The diagram provides an overview of the common communication that occurs with the Interact platform.



1. Secured by TLS - Certificate-based encryption is supported by leveraging SQL Server functionality which can auto-generate self-signed certificates or leverage an existing verifiable certificate
2. Using AMQP protocol secured by TLS
3. Connection is secured via HTTPS by default

Logging

Blue Prism Interact logging performed in Interact is outlined below:

- Logs are saved to TXT files in user configurable locations – the default location is the Application folder in the installation location but this can be configured by editing the value of the following line in the nlog.configfile, located in the Interact folder of the installation location:

  ```
  <variable name="logsFolder" value=".\Logs_Interact"/>
  ```

  Once updated, restart IIS.
- The default logging level can be configured in the appsettings.json file:
  - Default: Information
  - System: Warning
  - Microsoft: Warning

  The following logging levels can be applied: Critical, Debug, Error, Information, None, Trace, Warning. For more information about these logging levels, see docs.microsoft.com.

  The file is located in the Blue Prism > Interact folder within the installation directory – edit the file to change the logging levels. Following an update to the logging level, World Wide Web Publishing service must be restarted for the change to take effect.
- Logs are archived to zip files every month to reduce the file size volume.
- Logs do not contain any personal or sensitive information.