Web Application Overview for BrightPay Connect

What is BrightPay Connect?

BrightPay Connect is a web-based add-on service for the BrightPay and Thesaurus Payroll Manager applications. It enables users of these applications to backup their data to cloud-based storage and provide access to payroll information to their clients and employees via a web-based portal.

Hosting

BrightPay Connect is hosted in Microsoft Azure using Azure App Services. All server management and maintenance including security updates and patches are handled by Microsoft Azure. The service is deployed as a web farm with automatic failover to handle server outages and automatic scaling to handle periods of increased activity.

All external access to BrightPay Connect is via a secure endpoint using the Azure Front Door service with a web application firewall. Access via this endpoint is restricted to ports 80 and 443 for HTTP and HTTPS traffic. Access via HTTP is automatically redirected to an HTTPS address.

For information regarding Azure Hosting certification and compliance, see the the link below:
https://azure.microsoft.com/en-gb/support/trust-center/

Access to the Azure Portal

Access to the Azure Management portal for BrightPay Connect is restricted to senior development staff. Separate Azure subscriptions are used for Production and Test/Development environments. There are no shared data stores or resources between the development and production systems. Two-factor authentication is required when logging into the Azure portal.

Data Transmission

Web portal

All access to the BrightPay Connect web portal uses HTTPS/SSL. Any attempt to use HTTP is redirected to a HTTPS web address.

BrightPay/Thesaurus Client

Data sent to and from the payroll client software uses HTTPS/SSL. Payroll data is encrypted using AES with a 256 bit key before being uploaded. Each uploaded version of payroll file is encrypted with a unique one-time use key.

Data Storage

Each uploaded version of a payroll file is encrypted using AES with a unique 256 bit one-time use key. Encryption keys are stored in a separate data store from the uploaded payroll files to which they relate. The keys themselves are encrypted prior to being stored.

In addition to payroll data, documents created or uploaded to BrightPay Connect are encrypted using AES with a unique 256 bit employer specific key prior to being stored. The encryption key is stored in a separate data store from the document data. The key itself is encrypted prior to being stored.

Access Control

BrightPay Connect uses a role-based account system to control access via both the payroll client applications and web portal. All accounts require email verification at the point of creation. Email verification is also required to reset a forgotten password.

There are multiple levels of access:

Administrator

Administrators are typically the owner of the BrightPay Connect subscription. They can view all data within the subscription and have the ability to invite other users to have access to the subscription either as Administrators or Standard Users.

Standard User

Standard Users are typically employers, or payroll bureau staff who have been granted limited access to selected employer data within a subscription. Standard Users can be configured to have specific permissions to further control their access to data for selected employers.

Employee

Employees have access to view only their own payroll information, calendar and documents to which they have been granted access by their employer.

Connecting BrightPay or Thesaurus Payroll Manager to BrightPay Connect

Payroll application users connect their software to BrightPay Connect by entering their username and password. These are the same credentials that they use for logging into the web portal. When the client successfully authenticates with BrightPay Connect, a connection token is issued and this is then used to authenticate all communication between the payroll application and BrightPay Connect. Usernames and passwords are never stored on the user's machine.

Application Vulnerability

BrightPay Connect is resistant to common attack vectors including:

SQL Injection

Developers make use of frameworks, coding standards and review processes to prevent SQL Injection attacks. Application credentials for SQL databases are granted the minimum required permissions to read/modify application data.

Cross Site Scripting

Developers make use of frameworks, coding standards and review processes to ensure data submitted to the system is HTML encoded prior to being stored. All client side scripting makes use of modern browser features to prevent the execution of dynamically injected script references or tags.

URL Tampering

BrightPay Connect encrypts all data used in URLs making it impossible to tamper with URL parameters without breaking the URL. URL data is encrypted and decrypted on the web server. Key data elements used in forms are also encrypted.

Cookies

Cookies containing sensitive data are encrypted on the web server prior to being served to the web browser. They are marked as HTTP-only which prevents their access from browser based script. BrightPay Connect uses some non-sensitive cookies to control certain UI elements. These non-sensitive cookies are not encrypted and are accessible to client script.

Brute Force Password Attack

BrightPay Connect automatically locks out a user account after a number of consecutive failed login attempts . When an account is locked out, a message is displayed and the user can perform a password reset in order to gain access to the system.