Secure Connectivity Options for hc1 Solutions

hc1 is committed to providing robust and reliable connectivity options for your IT department that meet the highest security standards and work within your site's capabilities. This document describes the available methods for connecting your data to hc1.

Our Commitment to Security

As a HIPAA-regulated and HITRUST-certified company, hc1 prioritizes the security of your data. Our systems are designed with multiple layers of protection, and we continuously monitor and update our security protocols to address evolving threats. Once your data reaches our systems, it is maintained in an encrypted state. We will not accept data via an unencrypted means.

Connectivity Options

We offer various secure connection methods to ensure your organization can choose the option that best fits your security requirements and infrastructure. These options include both inbound connections to hc1 and outbound connectivity from hc1 to your customers' sites.

For most customers, we recommend using a TLS connection, which provides encryption from end to end using standard protocols and procedures. The following sections provide an overview of TLS and our other available connectivity options.

1. Transport Layer Security (TLS)

TLS is a cryptographic protocol that provides secure communication over a computer network. It encrypts data transmitted between your systems and hc1.

Pros:

- Is widely supported and easy to implement
- Provides strong encryption and data integrity
- Requires minimal configuration

Con:

- TLS v1.2 or higher may not be supported by older systems

To set up a TLS connection with you, we need this information:

- IP addresses that are sending traffic to hc1. We set our firewalls to allow traffic from the addresses you provide. Note that we will need IP addresses for both sandbox and production environments. In return, we will give you the names of the load balancers for sandbox and production environments that are the source of our traffic to you.

- Port numbers where you want to receive data.

2. Virtual Private Network (VPN)

A VPN establishes an encrypted tunnel between your network and hc1, providing a secure and private connection. If your source system is not able to create a TLS connection or otherwise encrypt the data, a VPN connection is a good option.

We use a FortiGate VPN appliance that allows us to connect using multiple encryption and authentication protocols. To ensure a secure connection, we also use Diffie-Hellman Groups from 1 to 32. This setup also allows us to make site-to-site connections with other FortiGate devices as needed.

Pros:

- Highly secure, providing end-to-end encryption.
- Isolates traffic from the public internet.
- Allows for secure access to other resources in the hc1 network.

Cons:

- Requires more complex setup and maintenance.
- Requires the most configuration options.

To set up a VPN connection with you, we need this information:

- VPN server address
- Authentication credentials (Pre-Shared-Key)

- VPN configuration settings
- Application server address(es)

3. Mutual Transport Layer Security (mTLS)

In mTLS, a more advanced form of TLS, both the client and server authenticate each other using certificates. Enabling mTLS takes several steps:

1. Your organization creates a private key.
2. Your organization creates a Certificate Signing Request (CSR) from the private key and emails the CSR file to hc1.
3. hc1 signs the CSR with the hc1 Certificate Authority (CA) and sends a certificate back to you with a copy of hc1's CA certificate.

   Note: Once hc1 generates the certificate and passes it to your organization, your organization is responsible for managing the certificate and requesting a new one before it expires.

4. You use your private key and the certificate from hc1 in your own system to securely connect to hc1.

Please consult with your application provider for proper installation and use of an mTLS certificate.

Pros:

- Most secure option, providing strong authentication and encryption.
- Ensures that both parties are who they claim to be.
- Reduces the risk of man-in-the-middle attacks.

Cons:

- Requires more complex setup and certificate management.
- May have compatibility issues with older systems.

To set up an mTLS connection with you, we need this information:

- Client certificate and private key
- Server certificate and private key
- Certificate Authority (CA) certificates

4. Secure File Transfer (SFTP)

SFTP leverages encryption and authentication mechanisms to ensure that your data remains confidential and protected during transit. SFTP is particularly well-suited for scenarios where you regularly exchange large files or batches of data with hc1.

hc1 prefers a public and private key SFTP environment. This replaces less secure password-based authentication, which is vulnerable to brute force attacks. Keys can be generated on a per-user basis or can be shared, but access to the private key is needed to encrypt and decrypt traffic. The public key is shared with hc1, and you will use your private key to authenticate to the SFTP server.

Connectivity and the Activation Process

Consult with your IT department to determine the best connectivity option for your organization. Based on what you choose, we will provide you with a connection information form that will have connectivity details about the production and test hc1 environments we have provisioned for your organization. This document is collaborative, requiring action and information from both the hc1 integration engineer and your IT resource to fill out the necessary information. Establishing connectivity is a key part of the hc1 activation process, so it is important to ensure that your IT resources will be available for this step so that it can be completed efficiently and successfully.