Connectivity & Transmission

Specification

Version 01
01.23.2024

Table of Contents

Overview

This specification is for provider organizations to send patient panel files containing patient demographic information and Health Provider data to establish an active care relationship (ACR) between an organization and their patients. Connie uses the patient panel to populate the patients care team, enable search for clinical information and populate Connie alerts.

1. Transmission Options

The estimated timeline to complete connectivity setups is 3-5 business days. During the implementation process, submitters must transmit electronic data using one of the following methods:

1.1. HTTPS

Provide the following information to your Implementation or Account Manager.

- Certificate signing request (CSR) . The following articles provide insights in to how generate a CSR CSR Creation | Create Certificate Signing Request | DigiCert. We do request 2048-bit signing and a separate certificate will be issued from both TEST and PROD domains. The same CSR can be used for both TEST and PROD from the same server, or one CSR each from separate servers depending on the requirements.
- Organization's OID
- Organization's physical address
- Contact information – Name, email and phone number, for the appropriate technical resource(s)
- Public/Peer IP address(es) from which the data is sent

Note: SSLv3, TLSv1 & TLSv1.1 are not supported protocols

1.2. SFTP (Secure File Transfer Protocol)

Requires a submitter to obtain credentials and folder set up with CRISP Shared Services. The preference is to have CRISP Shared Services/Connie to host the MFT/SFTP account.

Hostname: https://mft.conniect.org
Username: Will be provided securely to organization contact on file
Password: Will be provided securely to organization contact on file
Port: 22

Account credential policies:

- Just a Password - 1 year and needs to be changed.
- Just a Private key - 2 years and needs to be changed.
- Password OR Private key *and* Whitelisting - 3 years and needs to be changed.

The following information should be provided to your Implementation or Account Manager.

- Which credential policy for SFTP service account (see options above)
- Public IP's to be whitelisted? (if applicable)
- Technical POC name, phone number, and email address for the account. Connie recommends using a departmental email address.

First Time Login

The ***first time*** you login to the service account will ***require 2fa*** to be used and very complex passwords (which will be supplied). The interface is browser based. Once you login you can change the password. Your organization will then be able to automate SFTP file transmissions on your service account.

The initial password will expire in 90 days. An email will be sent 10 days prior to expiration, 7 days prior to expiration and after the account expires. You will be requested to reset your password that will be used in your automation and select a complex password with 12 or more characters.

SFTP FAQ

- **How will I know when my password is set to expire?** Email reminders will be sent 10 days before password is set to expire to the email address provided during onboarding.
- **How do I reset my password before it expires?** Please log into the MFT website and select "My Account" OR On the login page, there is a Forgot Password link
- **How do I reset my password after it expires?** Please send an email to support@crisphealth.org and cc your Connie Account manager.
- **How long is a file stored in MFT folder?** Files are stored for up to 72 hours before it is automatically deleted. If there are sweeps in place, it would be moved once placed into the folder and does not follow the 72-hour window.

1.3. VPN

Complete VPN form and return it to your Implementation or Account Manager. The information required to complete the VPN form are VPN device details, Peer IP and Host IPs, Phase 1 & 2 preferences, and technical contact name, phone and email address.

Upon completion of the VPN and load balancer setup we will schedule a meeting to bring up the tunnel and validate traffic is being successfully routed.

Note: SSLv3, TLSv1 & TLSv1.1 are not supported protocols

1.3.1. Device and IP Address Information

CSS/Connie Account Manager or Implementation Manager will provide the CRISP end point details as part of the onboarding process.

Client	::: NOTES :::	CRISP End Point
VPN Tunnel Description		**VPN Tunnel Description**
Customer Name		CRISP
Device & Version		**Device & Version**
Customer to complete		Palo Alto VM-300 - v9.0.3.xfr
Gateway		**Gateway**
	<= VPN PEERS =>	40.xx.xxx.xxx
Client Host IP's		**CRISP LB Public Host IP:PORT**
	<- Please NAT ips to public ranges if Req'd	
PROD -		**PROD – Contact CSS Acct Mgr**
TEST -		**TEST – Contact CSS Acct Mgr**

1.3.2. VPN Settings Phase 1 (IKE v 2 Preferred)

Client	::: NOTES :::	CRISP End Point
IKE Authentication Method	***To be agreed upon on the phone or by secure e-mail***	**IKE Authentication Method**
IKE using Preshared Secret		IKE using Preshared Secret
IKE Diffie-Hellman Group	***Must be the same at both ends***	**IKE Diffie-Hellman Group**
14	***DH Group2, 5, or 14 (preferred)***	14
IKE Encryption Algorithm	***Must be the same at both ends***	**IKE Encryption Algorithm**
AES-256	***AES-128, AES-192, or AES-256 (preferred)***	AES-256
IKE Hash Algorithm	***Must be the same at both ends***	**IKE Hash Algorithm**
SHA-256	***SHA-1 or SHA-256 (preferred)***	SHA-256
Lifetime in seconds	***Must be the same at both ends***	**Lifetime in seconds**
86,400	***Define in seconds please***	86,400

1.3.3. VPN Settings Phase 2 IPSEC

Client	::: NOTES :::	CRISP End Point
Perfect Forward Secrecy	***Must be the same at both ends***	**Perfect Forward Secrecy**
DH14	***OFF, DH2, DH5, or DH14 (preferred)***	DH14
IPSEC Encapsulation	***Must be the same at both ends***	**IPSEC Encapsulation**
ESP	***ESP only***	ESP
IPSEC Encryption Algorithm	***Must be the same at both ends***	**IPSEC Encryption Algorithm**
AES-256	***AES-128, AES-192, or AES-256 (preferred)***	AES-256
IPSEC Authentication Algorithm	***Must be the same at both ends***	**IPSEC Authentication Algorithm**
SHA-256	***SHA-1 or SHA-256 (preferred)***	SHA-256
Lifetime in seconds	***Must be the same at both ends***	**Lifetime in seconds**
28,800	***Define in seconds please***	28,800

1.3.4. Application Settings

Client	::: NOTES :::	CRISP End Point
Allowed Ports	*ICMP Allowed for testing purposes*	**Allowed Ports**
TEST/PROD		TEST/PROD
Traffic Type		**Traffic Type**
Any		Any

Revision History

Date	Version	Author	Comments
1/28/2024	1.0	Connie	Create initial document.