­

Sftp Connection Document

Sftp Customer Connection Testing Document for Kronos Private Cloud (KPC) Environments

This document will assist with details pertaining to testing your Kronos provided SFTP account connection(s) into your Kronos Private Cloud (KPC) environments along with some additional Sftp offerings supported in the Kronos Private Cloud

Table of Contents

[Introduction 2](#_Toc512344649)

[Document Purpose 2](#_Toc512344650)

[Overview 2](#_Toc512344651)

[Sftp Connection Methods 2](#_Toc512344652)

[Connection Methods Overview 2](#_Toc512344653)

[Sftp Account Credentials 3](#_Toc512344654)

[Sftp Client Connections for Sftp 3](#_Toc512344655)

[Sftp Web Browser HTTPS Connections for File Transfer 4](#_Toc512344656)

[Additional Information 6](#_Toc512344657)

[Sftp Standard Directory Structure/Interface Designer Details 6](#_Toc512344658)

[Sftp Offering Details 7](#_Toc512344659)

[Additional Sftp Offerings 8](#_Toc512344660)

[PGP Encryption/Decryption 8](#_Toc512344661)

[SSH Key Authentication 8](#_Toc512344662)

[Support 9](#_Toc512344663)

# 

# Introduction

## Document Purpose

This document will assist with details pertaining to testing your Kronos provided SFTP account connection(s) into your Kronos Private Cloud (KPC) environments along with some additional Sftp offerings supported in the Kronos Private Cloud.

## Overview

The Kronos Secure File Transfer server was architected to manage secure file transfers by directing inbound files as they enter the Kronos Private Cloud (KPC) environment directly to the corresponding customer(s) application server(s) into their dedicated environment.  In the same manner, when a customer “pulls” a file, the outbound files flow directly from the customer application server and is immediately directed back out of the KPC environment.  Through this design, multiple temporary mounts for all customers are continuously being created and dismantled in both inbound and outbound file transfers to ensure there is never a permanent connection enabled which would allow customer data to remain on the SFTP server.  This architectural design allows the SFTP environment to scale without significant management and mitigates significant security risks associated with having sensitive payroll data and PII “parked” on the SFTP server.   The Kronos Private Cloud supports three different authentication methods of managed file transfers listed below:

* Username with Password Authentication only (default)
* Username with SSH Key Authentication only (no password)
* Username with SSH Key and Password Authentication

**NOTE:** For customers requiring SSH key authentication for their SFTP Managed File Transfer Accounts, the customer would need to generate and provide a SSH Public Key for Kronos to attach to their SFTP Account as the customer would initiate the SFTP session(s).

# Sftp Connection Methods

## Connection Methods Overview

SFTP connections into your Kronos Private Cloud environments can be accessed by your preferred SFTP client or via a web browser HTTPs. Some functionality and features may not be available with Web Browser HTTPS connections and would require the use of a SFTP client application such as FileZilla. Some file transfer utilities such as FileZilla also support pause, reconnection, and resume functionality.

To Download the FileZilla FTP Client, go to <http://filezilla-project.org>

## 

## Sftp Account Credentials

You will receive the following information from your Cloud Services Representative. If you do not have these SFTP credentials, please contact your Kronos Project Manager or Kronos Cloud Services Representative:

**NOTE:** Port 22 may be required to be opened outbound on your firewall for (158.228.129.229 and 158.228.200.165) when using a Sftp Client. Web Browsers connections use port 443 for Sftp connections.

SFTP Client: Web Browser (HTTPS URL):

**Production SFTP Hostname:** <customer>-xfer.kronos.net https://<customer>-xfer.kronos.net

**Non-Prod SFTP Hostname:**  <customer>-dev-xfer.kronos.net https://<customer>-dev-xfer.kronos.net

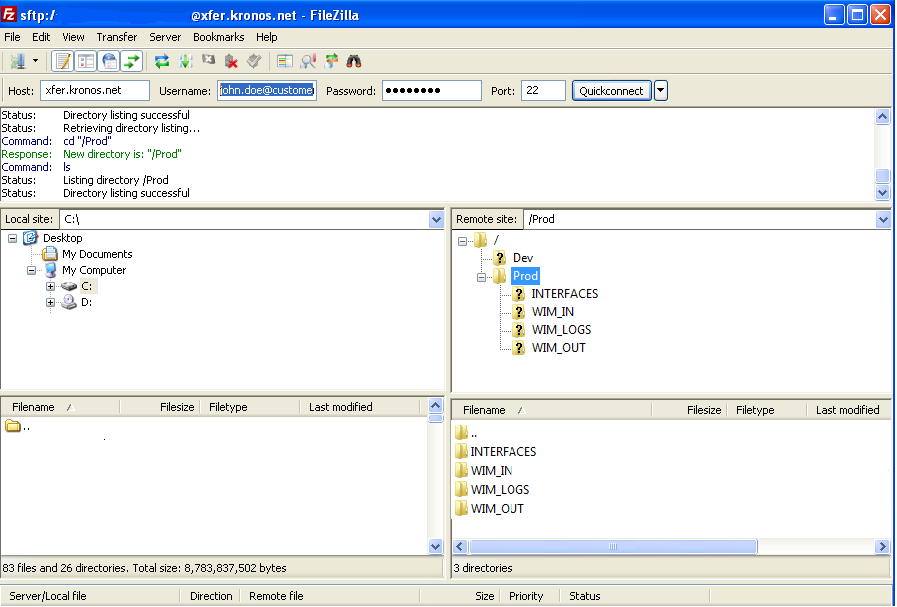
**SFTP Account:** *Username and Password Username and Password*

**Port:** 22 for SFTP Client 443 for Web Browser

## Sftp Client Connections for Sftp for File Transfer

The following steps and screen captures show the use of FileZilla SFTP Client and are used to provide general overview on how to connect using a SFTP client application. Port 22 must be open from your client device to the Kronos SFTP server public address. **Customers can choose to use their SFTP client of choice for connections and are not limited to FileZilla.**

1. Open your SFTP Client
   1. Host: <customer>-xfer.kronos.net provided by your Cloud Services Representative
   2. Username: SFTP account name provided by your Cloud Services Representative
   3. Password: SFTP account password provided by your Cloud Services Representative
   4. Port: 22
2. Click Connect (Quick Connect for FileZilla)
3. You should now be connected to the hosted environments via SFTP
4. You should now see two panels. The left side being the local computer and the other being the Hosted environments (Prod and Dev) with their respective sub folders.

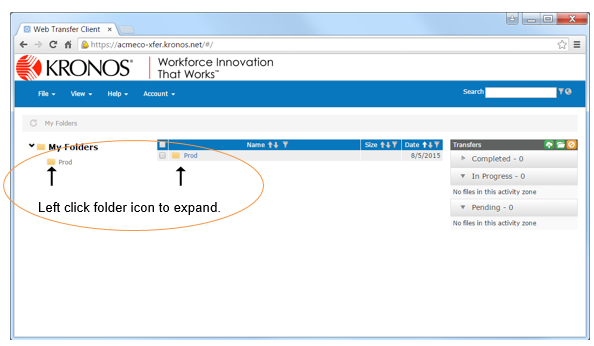


1. To upload files to the hosted environment, you will navigate within the left panel (Local Machine) and locate the file to transfer
2. To transfer (upload) a file, you can drag the file from the left panel into the right panel on top of the folder labeled “WIM\_IN” for the appropriate environment
3. To download files from the hosted environment, you will navigate within the right panel (Hosted Environment) and select the environment along with the sub-directory “WIM\_OUT”
4. To transfer (download) a file, you can drag the file from the right panel into the left panel to the specific directory of your choice for local machine access
5. When your SFTP session has completed, please log off the SFTP session with your SFTP client

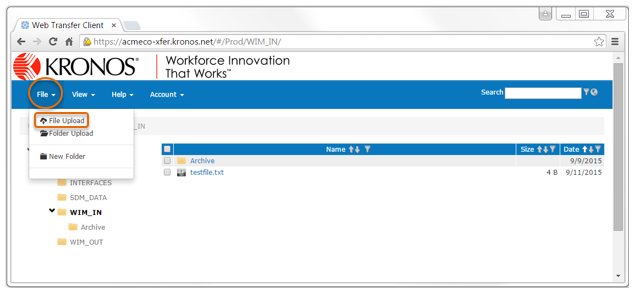
## Sftp Web Browser HTTPS Connections for File Transfer

The following steps and screen captures show the use of a Web Browser and are used to provide general overview on how to SFTP connect using HTTPS. Port 443 must be open from your client device to the Kronos SFTP server. **Browsers supported Internet Explorer v10 or later, Google Chrome v34 or later, Mozilla Firefox v29 or later, Safari v6 or later.**

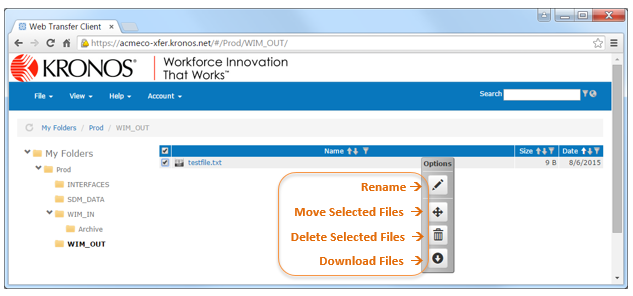
1. Open your Web Browser
2. Enter in your unique HTTPS URL to connect to the Kronos secure transfer page
3. Under the username you will enter the SFTP account name provided by your Cloud Services Representative
4. Under the password you will enter the SFTP account password provided by your Cloud Services Representative
5. Click “Log In” and then click “Accept” on the “Terms of Service” Popup
6. Expand the Environment Folder to see sub folders (WIM\_IN, WIM\_OUT, INTERACES, WIM\_LOGS)



1. To upload a file, enter in the WIM\_IN folder or subfolder and left click and drag the file you want to upload or click “File> File Upload” and browse your local machine for the file.



1. To download a file, enter in the WIM\_OUT folder or subfolder and check the box next to the file name and select the download icon. Browse your local machine for location to save the file.



1. When your SFTP session has completed, please log off the SFTP session with your SFTP client

# Sftp Additional Information

## Sftp Standard Directory Structure/Interface Designer Details

**Hosted Environment Sftp Standard Directory Structure Legend:**

Folders listed below may contain sub-folders designated for specific interfaces. Please work with your project resources to verify folder structure and locations of interface generated files for customer download and source file locations for customer uploads.

* **Non-Production (possibly including the following Development, UAT, Training, Stage, etc.)**
  + – **Interfaces** (Location of Interfaces deployed to Workforce Application)
  + – **WIM\_IN** (Source file upload directory for Interface file processing)
  + – **WIM\_OUT** (Target file download directory for Interface generated files)
  + – **WIM\_LOGS** (run summary, errors, disqualifications Interface Log Files Location)

Optional Folders for Custom Report Development provided with Kronos Citrix account setup

* + – **OtherReports** (Visual Studio 2005 or prior developed .rdl custom reports directory)
  + – **OtherReports2008** (Visual Studio 2008 or later developed .rdl custom reports directory)
  + – **Reports** (Crystal Reports developed .rpt/.rep custom reports directory)
* **Prod (Production environment)**
  + – **Interfaces** (Location of Interfaces deployed to Workforce Application)
  + – **WIM\_IN** (Source file upload directory for Interface file processing)
  + – **WIM\_OUT** (Target file download directory for Interface generated files)
  + – **WIM\_LOGS** (run summary, errors, disqualifications Interface Log Files Location)

Optional Folders for Custom Report Development provided with Kronos Citrix account setup

* + – **OtherReports** (Visual Studio 2005 or prior developed .rdl custom reports directory)
  + – **OtherReports2008** (Visual Studio 2008 or later developed .rdl custom reports directory)
  + – **Reports** (Crystal Reports developed .rpt/.rep custom reports directory)

## 

## Sftp Account Offering Details

* Accounts will be locked for 15 minutes following 3 invalid login attempts over a 5-minute period. An invalid login is defined as using the wrong login ID or password, or both.
* The source public IP from where an Account originates will be blocked after 5 invalid login attempts over a 1-minute period. If an IP address is blocked, contact Kronos Global Support (<https://community.kronos.com>) and provide your public IP address to have the Public IP removed from the blocked list.
* To obtain your public IP open a web browser and go to <https://google.com>
* Enter in the search “What is my ip” and your public IP address will be displayed
* The standard Sftp connection time out is 300 seconds.
* Accounts will be inactivated after 100 days of inactivity. If a Sftp account needs to be reactivated, contact Kronos Global Support (<https://community.kronos.com>).
* Accounts will be deactivated after 365 days of inactivity. If a Sftp account needs to be reactivated, contact Kronos Global Support (<https://community.kronos.com>).
* Accounts will have the following connection limits:
  + A maximum concurrent connection per user is 10.
  + A maximum concurrent connection from the same IP address is 10.
* Archival of source and target files should be archived on customer premise, as Kronos SFTP does not support file archiving on customer KPC environments
* Customers would be responsible for initiating Sftp sessions to push or pull files from their KPC Environments.

# Additional Sftp Offerings

## PGP Encryption/Decryption

Kronos, Inc. supports encryption algorithms that meet the OpenPGP Proposed Standard. The OpenPGP Proposed Standard is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) Proposed Standard RFC 4880. This document contains all the necessary information to develop interoperable applications based on the OpenPGP format. It describes the format and methods needed to read, check, generate, and write conforming encrypted messages, keys, and signatures. (<http://www.ietf.org/rfc/rfc4880.txt>).

1. PGP decryption of inbound files to Kronos are completed upon successful transmission of file
2. PGP keys must be type RSA and length must be a minimum of 2048.
3. PGP keys must be set to expire at 3 years or less.
4. Encrypted file names must end with one of the following suffixes:
5. .pgp
6. .gpg

\*PGP decryption of inbound files to your Kronos environment which are required to remain PGP encrypted until interface run time would require an engagement from your Kronos Professional Services Team and may incur billable hours if out of scope.

\*\*PGP encryption of outbound files from your Kronos environment would require an engagement from your Kronos Professional Services Team and may incur billable hours if out of scope.

## SSH Key Authentication

Kronos supports SSH key authentication for password-less logins. It is highly recommended to use SHH key authentication for any automated process. SSH keys must meet the following requirements:

1. Keys must be in the openSSH or ssh.com format.
2. Key length must be a minimum of 2048.
3. Customer would provide public SSH key due to customer initiating SFTP sessions

# Support

If you need Sftp account support and currently in the implementation phase of your Kronos Project (Not Live). Please contact your Kronos Project Manager for assistance or Kronos Cloud Services Representative for assistance.

If you need Sftp account support and are Live and/or have been transitioned to Kronos Global Support (KGS), please open a case with KGS and they will be able to assist with resolution.

**How to Open a Support Case with Kronos Global Support (KGS) in Community**

<https://community.kronos.com/s/article/How-To-Open-a-Support-Case-with-KGS-in-Communities>

**Kronos Global Support**

1-800-394-4357 (1-800-FYI-HELP)

<https://community.kronos.com>