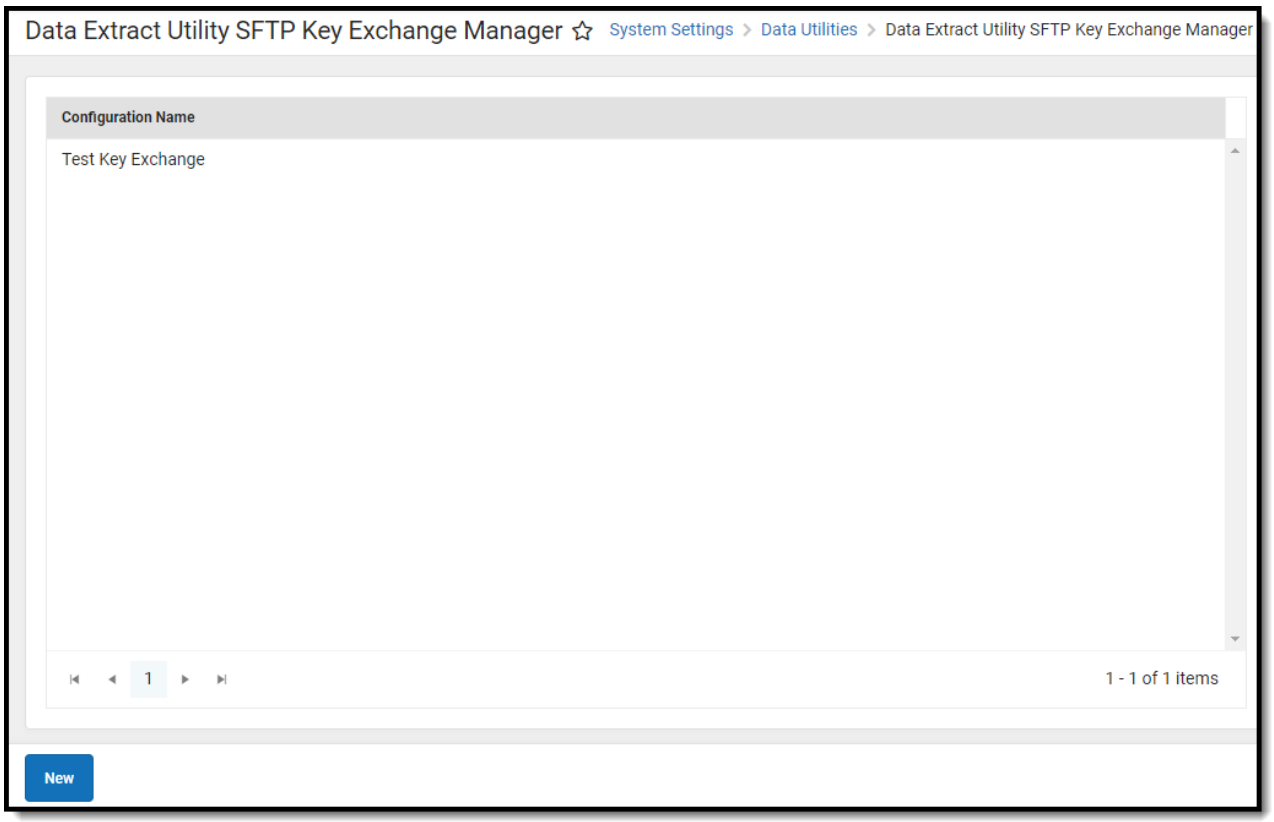
Data Extract Utility SFTP Key Exchange Manager

Last Modified on 06/01/2026 10:29 am CDT

Tool Search: Data Extract Utility SFTP Key Exchange Manager

The Data Extract Utility SFTP Key Exchange Manager allows SFTP configurations within the Data Extract Utility to utilize a keypair between Infinite Campus and a third-party server(s) to bolster security for the data transferring process. Users can use this tool to generate an Infinite Campus public key to be shared with a third-party system.

In order to use established SFTP keys, an extract within the Data Extract Utilities must be configured to use a Delivery Mode of SFTP.

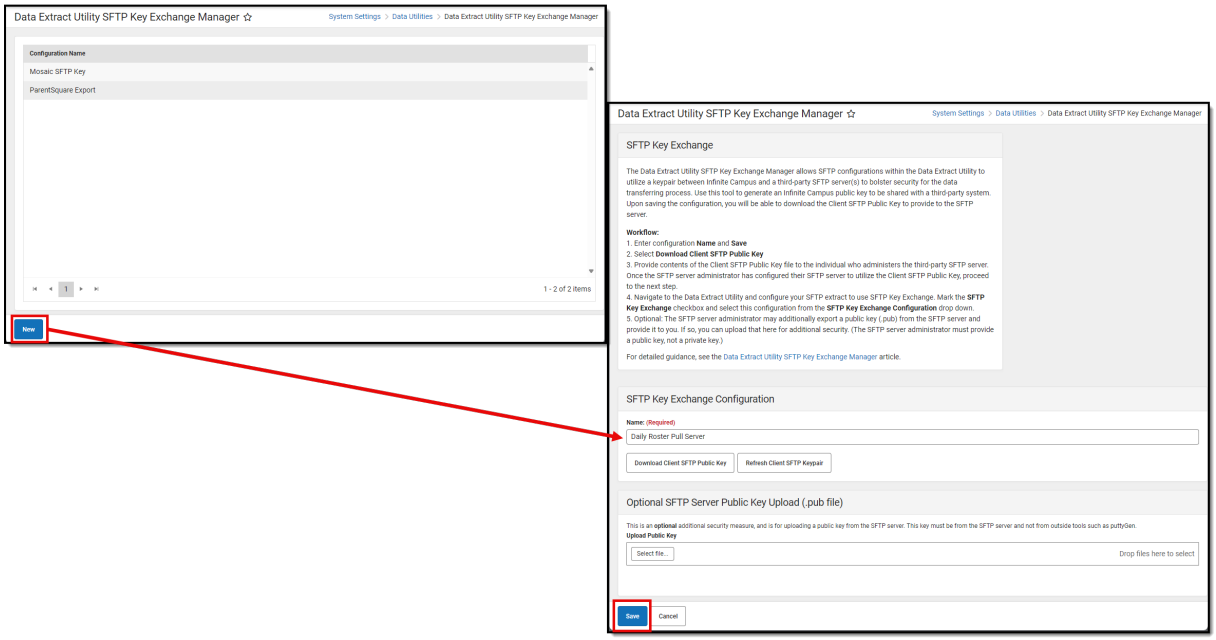


See the Data Extract Utilities Tool Rights article for available tool rights information.

Tool rights for this tool should only be granted to system administrators.

Create and Connect an Infinite Campus-Generated SFTP Key

1. Click the **New** button. The SFTP Key Exchange Configuration editor will appear.



2. Enter a **Name** for the key. Choose a name that is easily identifiable and differentiated from other keys.

> The **SFTP Server Public Key Upload (.pub file)** section is optional and should be ignored unless your vendor has supplied you with a .pub file from their server. **If you have not been supplied a .pub file from the individual who administers the SFTP server/your vendor, do not hit Select Files. Proceed to the next step.**
>
> If you do have a .pub file from your vendor/SFTP server and wish to use it, we will cover this later in the article.
>
> **NOTE:** Infinite Campus must have a private key stored on its server in order to successfully complete the SFTP Key Exchange. This means you must generate a key within the Data Extract Utility SFTP Key Exchange and enter the generated .pub file into your SFTP server/vendor. Skipping this step and only importing your server's .pub file into Infinite Campus will not complete the authentication and will not successfully connect your extract from Infinite Campus to your server/vendor.

3. Click **Save**. When the key successfully generates, a green notification box displays.

4. Click the **Download Client SFTP Public Key** button. This generates a private key within your Infinite Campus server as well as a public key (.pub file). Download and save this .pub file.



5. Once the key (.pub file) is downloaded, you must supply this file to whoever administers the SFTP server/your vendor and have them add it to their server, typically in the authorized_keys area of the server.

   Some vendors require you to provide them the key itself, which can be obtained by opening the .pub file within a text editor (or compatible program) and copying the entire key (see below for example).



6. Paste this key within your external SFTP system/server where you store your other authentication keys and save.

7. Once this Infinite Campus-generated key has been successfully added and saved in your system's/server's key store, a new extract can be configured using the SFTP protocol with an SSH key within the Data Extract Utility or you can modify an existing extract to begin using the SFTP protocol with an SSH key.

8. Navigate to the Data Extract Setup Screen.

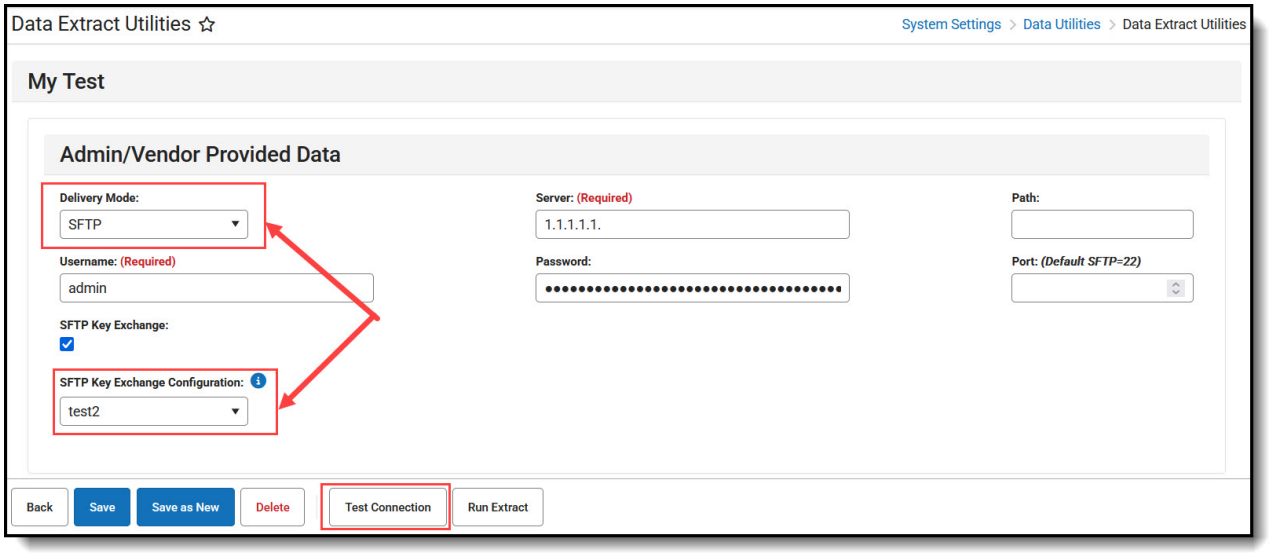
9. To utilize this new key for an existing or new Data Extract Utility configuration:
   1. Select the **SFTP** Delivery Mode
   2. Mark the **SFTP Key Exchange** checkbox
   3. Select the key you just set up in the **SFTP Key Exchange Configuration** dropdown list (see the image below for an example).

10. Once these are selected, **clear out the Password field** and select the **Test Connection** button (you do not have to click Save) to test and make sure the connection between Infinite Campus and your system is authenticating correctly.

11. If tested and working correctly:
    - If you want to use passwordless authentication, leave the Password field blank and click the **Save** icon.
    - If you want to use username/password authentication as a failover in the event there's an

issue with the public key exchange authentication (assuming the SFTP server supports this), leave the **Password** value in place (Ctrl+Z to fill it back in if you just deleted it) and click the **Save** icon.

NOTE: **Do NOT use SFTP Legacy (Being Deprecated)**. If you have previously set up the Data Extract Utility to use this Delivery Mode, you must update the configuration to use SFTP to avoid issues once the old SFTP mode is removed.



Import a Third-Party SFTP Key

To bolster security and create an even more secure connection between Infinite Campus and your SFTP server/vendor, you can import your server's .pub file and upload it within the Data Extract Utility SFTP Key Exchange tool. This is an optional layer of security and is not required in order to utilize SFTP Key Exchange functionality.

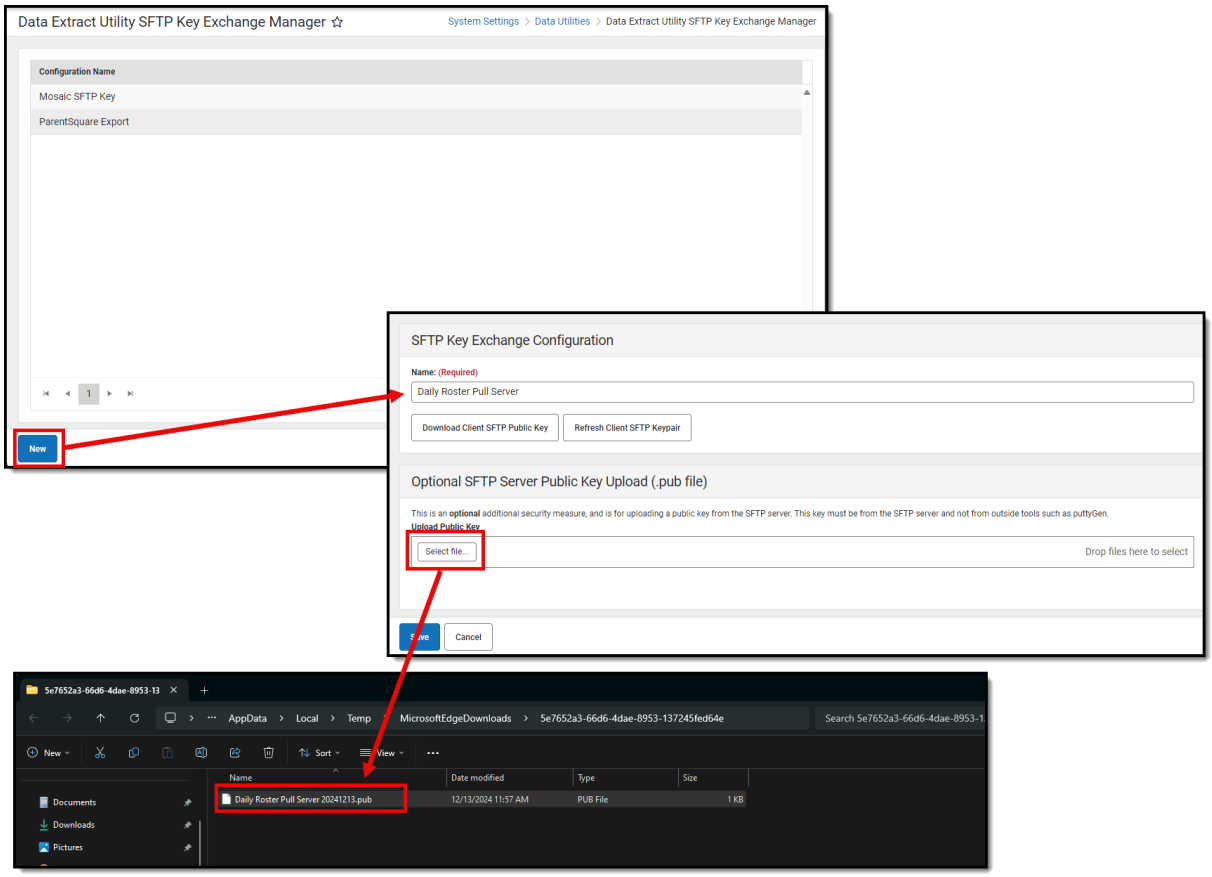
NOTE: Infinite Campus must have a private key stored on its server in order to successfully complete the SFTP Key Exchange. This means you must generate a key within the Data Extract Utility SFTP Key Exchange and enter the generated .pub file into your SFTP server/vendor. Skipping this step and only importing your server's .pub file into Infinite Campus will not complete the authentication and will not successfully connect your extract from Infinite Campus to your server/vendor.

To upload your server's/vendor's .pub file (public key):

1. Click the **New** button **OR** if you're reinforcing security for an existing key exchange configuration, select an existing configuration.

2. Enter a **Name** for the key. Choose a name that is easily identifiable and differentiated from other keys.

3. Click the **Select File** button and select the key file (.pub file) from your local hard drive or network. **NOTE: The key MUST be a .pub file**.



4. Once the key has been selected, it is uploaded into Infinite Campus and displays below the **Select files** button.



5. Click the **Save** button. The key is now successfully imported and saved into Infinite Campus

and extra layer of authentication security is now enabled.

Manage SFTP Keys

The key management options include:

Refresh the Client SFTP Keypair	This generates a new keypair (private and public key). This is useful in the event of a potential security breach or any scenario in which a brand new keypair between Infinite Campus and your SFTP server/vendor would be needed. NOTE: Refreshing the Client SFT Keypair means you will need to go through the process of placing the new .pub file on your SFTP server/vendor.
Download Client SFTP Public Key	This is useful if you need access to an Infinite Campus SSH key.
Delete Server SFTP Public Key	This is useful for deleting an expired, incorrect, or compromised key. Often this option will work in conjunction with the Refresh Client SFTP Keypair option where a user would first delete an old key, upload a new key and then refresh and repair the connection between Infinite Campus and your system.

