Titan MFT Server

DropZone

How-To/Sample Script for use with DropZone Video

- Welcome to this overview and demo of the DropZone functionality in Titan Server, which allows secure request and receipt of data
- Before Beginning, ensure that you have the HTTPS Service enabled and this functionality is working properly to allow users access through the built-in web interface for Titan Server. Configuration for HTTPS can be found in the Titan Administrator, under "Services" → HTTPS

DropZone from an Administrator's Perspective:

DropZone can be configured in the Titan Administrator under "Services" → HTTPS → File Sharing

NOTE: This option can be further configured at the Group and User level within Titan Server, allowing for full control over exactly which Users, or Groups of Users, can perform this action.

Secure File Sharing can be difficult to achieve in many file server environments. Titan MFT Server provides file sharing with top-level security, flexibility, and ease of use. In addition to Sharing data with others, Titan MFT Server allows for securely requesting data to be uploaded into your environment, including by external vendors and customers.

Content is shared through the use of secured links to a designated folder for upload. These links can be password-protected. The ability to assign specific permissions and expire the link to upload content provide additional security controls. Administrators can also define whether data can be requested only from other internal users, or if data can be requested and received from external parties/email addresses.

Administrators enjoy complete flexibility with the ability to set each of these options at the Server, Group, and Individual User levels in order to maintain full control over exactly ***WHICH*** users can and cannot request data, ***FROM WHOM*** the data can be uploaded, and ***WHAT*** to do with the data once received

DropZone from an End User Perspective:

From a user's perspective, requesting data to be uploaded can be accomplished through the Titan user web interface. The HTTPS Service in Titan allows providing a URL to which users can navigate and then authenticate for access. This specific functionality, called "DropZone", allows users to request and securely receive data from other users or, if permitted, external parties and vendors. Another common use case would be to generate a secured link that you choose to share with yourself via your own username or email address, and then embed this link in a website, email signature, or other location where perhaps you have public users upload data to your environment.

To begin, Users should log into the End User Web Interface using valid credentials. Users that have been granted permissions to use DropZone functionalities will be able to do so through this web browser.

Users can select a folder to be used for receipt of files, and then choose "DropZone"

Users then have some fields to fill in:

The "Share As" field creates a User-Friendly name for the shared link. This is additionally useful if wanting to find this share and manually revoke access at any time.

To, Subject, and Message are just like an email message.

- To can be usernames (for internal sharing) or email addresses for external sharing.
- Subject and Message will appear in the resulting email for the Recipient as the Subject and Message of the email.

The next screen allows Users to apply security controls.

- Permission allows either Upload, or Upload and List
  - LIST means the recipients would be able to View any content in the folder.
  - Upload ONLY would allow for blindly uploading files into the folder.
- Link Expiration allows the link to become inaccessible after specified criteria are met
  - Never: Link is valid indefinitely unless manually revoked
  - After Uses: Specify the number of times a link should be able to be accessed before the link will no longer be valid
    - For example, set to "1", the link can be clicked one time, and then it will no longer be accessible
  - After Date: Specify a Date and Time after which the link will no longer be valid

The final screen shows a confirmation of the content being shared. Choose "Send" to Share the link and request the data

DropZone from a Recipient's Perspective:

The recipient of the shared content will receive a secured link via email. The Subject and Message will match what the End User entered when Sharing the content.

The recipient can open and read the email, and then click on the Shared Link name in order to access the content through a branded web interface.

- If Password-Protection is enabled for the shared content, the user will be prompted to authenticate before accessing the data. Otherwise, the folder will simply display.
- The shared content is accessible according to the security controls configured (how long the link is valid, and what permissions the recipients have for the received content (Upload, List)