

# Viewpoint™ File Store Security Guide

Application Version: 7.0  
August 19, 2026

© 2021 Conduent, Inc. All rights reserved. Conduent and Conduent Agile Star are trademarks of Conduent, Inc. and/or its subsidiaries in the United States and/or other countries.

Other company trademarks are also acknowledged.

Document Version: 7.0 (October 2021).

## Document Conventions

| Convention                                                                        | Explanation                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bold</b>                                                                       | For file names, commands, fields, menus, options, and window names.                                                                                                           |
| <code>Courier New</code>                                                          | Commands as you should type them.                                                                                                                                             |
| <code>Lucida Console</code>                                                       | Example output generated by the system.                                                                                                                                       |
| <i>Italics</i>                                                                    | For configuration variables, including variable portions of file names and URLs. Also indicates a document name.                                                              |
| Note / Blue Callout                                                               | The Blue Callout text indicates information that is of special interest or importance, an idea that could be useful or additional information about a product or a feature.   |
|  | The Caution icon along with the text indicates actions that can lead to problems in system operation or configuration settings if the instructions are not followed properly. |

## Document Revision History

This section tracks the initial creation of the document after each major version thereafter.

| Ver: | Date         | Description                                                                                 | Reviewed / Approved By |
|------|--------------|---------------------------------------------------------------------------------------------|------------------------|
| 1.0  | Jan 20, 2014 | Initial Version                                                                             | Team                   |
| 1.1  | Oct 6, 2021  | Rebranded adhering to the latest Conduent brand central documentation standards/guidelines. | Technical Writer       |

# Table of Contents

- 1. File Store Security Guide..... 1-1
  - 1.1. Overview..... 1-1
  - 1.2. Selecting a Security Model..... 1-1
  - 1.3. Implementation..... 1-1
    - 1.3.1. Internal Users..... 1-1
    - 1.3.2. External Users..... 1-1
    - 1.3.3. External Users and Terminal Server..... 1-2
    - 1.3.4. Staging Folder Setup..... 1-2
    - 1.3.5. Anti-Virus..... 1-3

# 1. File Store Security Guide

## 1.1. Overview

This guide outlines the options for securing Viewpoint File Store. It is assumed that Viewpoint Review has already been installed and has been run at least once (the “First Run” steps of the Installation Guide have been completed). This guide makes reference to the VP\_Internal and VP\_External Active Directory groups.

Processing users (including Worker users) should be a member of the VP\_Internal Active Directory group, as outlined in the Viewpoint Installation Guide. No additional File Store setup is required for Processing users.

## 1.2. Selecting a Security Model

Review Users will access the Viewpoint File Store either directly (internal) or through file system impersonation (external). Determine which mode the Viewpoint implementation must support. Evaluation installations are generally internal only whereas production implementations which will support remote users will typically have a mix of both internal and external users.

Every Viewpoint User is a member of a single Company. File Store access identity (internal or external) is established at the Company level.

- **Internal Users** – Users directly access the File Store. Internal Users should be in the VP\_Internal Active Directory group and a member of a Company which has not been configured for file system impersonation.
- **External Users** – Users access the Viewpoint File Store through file system impersonation. External users may be in any Active Directory group (including none). The Company they are a member of must be configured to support file system impersonation.

## 1.3. Implementation

### 1.3.1. Internal Users

Internal Users should be a member of the VP\_Internal Active Directory group and be a member of a Viewpoint Company which has not been configured to use impersonation. By default, Viewpoint Companies do not use impersonation. No additional steps are required for internal Users.

### 1.3.2. External Users

External Viewpoint Review Users which should be made a member of a Viewpoint Company which supports file system impersonation. To configure a Viewpoint Company to use file system impersonation perform the following steps:

1. Determine the Active Directory user which will be used to perform impersonation. This Active Directory user will be either:
  - a. This is the most common approach. A domain user which has access to the section(s) of the File Store which the Company is permitted to access, and also has access to the user's file system, the if the user will access through an external application server (Terminal Server, etc.) the Active Directory user will need access to the application server's file system.
  - b. A domain user which has access to the section(s) of the File Store which the Company is permitted to access, and also have access to a “staging folder”. A staging folder is a folder which both the impersonation user and the Viewpoint user have access to. See the section titled Staging Folder setup to configure Viewpoint to use a Staging Folder. This approach is

only used when an extra level of security and isolation is desired – it is not necessary for most implementations.

2. Launch Viewpoint Review as an administrator.

3. Click the Security manager icon on the main toolbar.



4. Select the Companies tab. Select the Company you wish to configure for file system impersonation. The Properties pane (right side) displays information about the Company. Populate the Impersonated User field with the domain qualified username and password of the Active Directory impersonation user. The password will be encrypted.

| Properties            |                        |
|-----------------------|------------------------|
| Impersonated Password | *****                  |
| Impersonated User     | ImipolexG@RocketDomain |
| Name                  | Baltic International   |

5. Select a different Company to commit your change.
6. Test your configuration:
  - a. Select or create a Viewpoint Review User.
  - b. Assign this User to the Company.
  - c. Log into Viewpoint Review (or have someone else log in) as this User.
  - d. Click the “Review” button. The Review screen appears.
  - e. Select any Document. If there is not a document viewer pane (“Viewer” pane) then open one by selecting View | Panels | Viewer. The Document content should be visible in the viewer – the test has succeeded.

### 1.3.3. External Users and Terminal Server

When using Terminal Server with External Users these additional steps must be performed on the Terminal Server instances to facilitate impersonation:

1. Turn on the "Impersonate a Client After Authentication" User Right (SeImpersonatePrivilege). To turn on this privilege follow these steps:
  - a. Click **Start**, select Programs, select Administrative Tools, and then click **Local Security Policy**.
  - b. Expand Local Policies, and then click **User Rights Assignment**.
  - c. In the right pane, double-click Impersonate a client after authentication.
  - d. In the **Local Security Policy Setting** dialog box, click **Add**.
  - e. In the Select Users or Group dialog box, click the Active Directory account (the Active Directory user / group that will be running Viewpoint) and click **Add**, select the VP\_External and then click **OK**.
  - f. Click **OK**.
2. The Impersonation service account should be made administrators on the Terminal Server instance so that the user(s) may access user profile-specific file storage on the Terminal Server instance. (If you are using the Staging Folder this is not necessary).

### 1.3.4. Staging Folder Setup

If your implementation requires that you use a “staging folder” for external users, perform the following steps:

3. Determine the location / name of the Staging Folder. It will need to be in a location which is accessible by both the users running the Viewpoint application and by the file system impersonation user(s) (defined at the Company level). Create the Staging Folder.
4. Grant full access to all Review users (including the user(s) that Terminal Server, etc., run Viewpoint Review on behalf of).
5. Grant full access rights to the impersonation user.
6. Using the Viewpoint Installer application, open the Processing Settings window from under the Maintenance section.
7. With the Processing Settings open, find the Impersonalization Staging Area setting, and enter in the file path to the staging folder that was created in the first step.
8. Click OK to save the changes.

#### **1.3.5. Anti-Virus**

You may choose to install anti-virus software on the file store, however this has been known to greatly slow overall Viewpoint performance. It is considered a Viewpoint best practice to install anti-virus software on the Workers and Viewpoint Processing, not the file store.