Reactiv SUITE

WHITE PAPERS: Data Access

Data Access

Reactiv SUITE IWB provides users many different methods by which they can access their files securely. The software was designed around the goal of honouring your existing IT, data, and user policies. Reactiv SUITE does not require you to change your data repository architecture or existing user and data access privileges. Reactiv SUITE does not copy, host, move or upload your files to any online servers; it works and operates on your files where you store them.

There are a number of different strategies that can be used in order for your users to securely access their files in a public environment using Reactiv SUITE IWB. This white paper describes all of these methods and outlines the various pros and cons associated with each method.

Local\Network File Access

The simplest method is to allow the software to save files directly to the local hard drive. This allows the software to quickly access any content based on the credentials of the root windows user account. Mapped network drives and local drives could be used to store content and create presentations. In addition, Reactiv SUITE IWB also allows administrators to force users to use specific directories and restrict others such as desktop, program files, and windows system directories. Any drive that is visible to the Windows user can be configured for use in Reactiv SUITE IWB.

Administrators can use the System->Folder Settings to configure which directories and drives are visible to the user.

Please note that Reactiv SUITE PRO can only access files that are available locally to the user logged into Windows. As it is designed to operate on personal devices it does not allow users to login and change their privileges.

LOCAL DRIVES can be used when:

- Users are working locally and do not need to share content across multiple IWBs
- Users are working with generic content that is used regularly and security is not required (generic company, sales, and product presentations)
- Users are working in an environment where network connectivity is not guaranteed (on the road, mobile IWB devices that are being moved)
- A single user is exclusively using the software and can be relied to login to Windows using their credentials to unlock content
- Users are willing to login using Windows, and create a roaming profile on the IWB, in order to unlock their resources and data repositories

PROS	CONS
Simple – IT administrators can rely on Windows to authenticate, manage passwords, and unlock resources as per user and data policies	Inefficient – If multiple users were logging in and out of Windows, multiple roaming profiles would be created for each user requiring additional CPU resources and hard drive space which would compromise performance
File Access Speed – Large files can be easily loaded without network latency	Slow Startup – Login and logout time must be considered whenever users are switching back and forth between different Windows accounts

Active Directory

Reactiv SUITE IWB can authenticate users using existing Active Directory user policies, such that any individual in the organization can login, navigate the network, and access their private data using their existing privileges.

This method allows the IWB to login to Windows using a generic, restricted resource account that has no data or network privileges. Individual users can use the Reactiv SUITE network login button to connect to their AD server, authenticate themselves and create a temporary trusted connection to elevate the privileges of the software session. This allows users to quickly login, access data and logout without compromising security.

If the content is stored in a network directory, Reactiv SUITE IWB will not copy or move data to local directories thus ensuring security. Users would authenticate and access their network resource, work and save data back to these network resources and disconnect without leaving any traces behind on the local PC.

AD DRIVES can be used when:

- The IWB is a shared resource where multiple users can use the software and the security of their data is a concern
- Users would like to login to IWBs in any room and continue to work
- The IWB is in a public space where the base Windows account does not have any data access privileges
- It is not desirable for users to login to Windows and create multiple roaming profiles that have to be managed

PROS	CONS
Simple – Leverage existing AD domain architecture, user, and data policies	Network access - Requires the PC to be on the network and joined to the domain directly or through VPN
Easy to Manage – Administrators can control data access, create new folders, map drives, control access, and propagate changes using existing tools and policies	Latency – File access will be slower when accessing data through an authenticated tunnel

O365 Cloud Access

Reactiv SUITE IWB allows users to connect directly with their online OneDrive repository using Microsoft Graph API. This allows users to access, modify and save files directly to the cloud without synching or downloading any files to the local PC. Any individual in the organization can login, navigate the network, and access their cloud data using their login privileges.

This method allows administrators to grant access to files regardless of domain connectivity. This is ideal for organizations that are no longer supporting VPN or on-prem domain connectivity and have transitioned to complete cloud-based data storage using OneDrive. Using this method, the user can simply use the login button to connect to their OneDrive account. They can create presentations based on the content stored in their OneDrive folders, download\stream this data when presenting, ink and save these files back directly to their OneDrive account.

Reactiv SUITE IWB leverages the Microsoft Graph API to authenticate and access the user's data. As such there is no data copied or stored locally on the PC. Data security will be maintained and there is no opportunity for data leakage to occur once the meeting has been concluded.

OneDrive can be used when:

- Organizations that are moving to a cloud infrastructure for data storage
- The IWB is a shared resource where multiple users can use the software and the security of their data is a concern
- Users must be able to access their data and workspaces using any network and do not want to tunnel using VPN
- Cloud access to data is critical

PROS	CONS
Simple – Leverage existing OneDrive user and data policies	Latency – File access will be based on network speed, especially for large files, as data has to be downloaded and changes have to be uploaded
Easy to Manage – Administrators can control data access, create new folders, map drives, control access, and propagate changes using existing web console and management tools	

Online Repository Connectors

We recognize that there are many different types of online data repositories. We do plan to support many of them in the future natively, but at the present time several workarounds can be explored to connect Reactiv SUITE to them.

One of the most common workarounds is to install a virtual drive connector on the PC and allow Reactiv SUITE to connect with this drive. Many different online repositories offer an app that create a virtual drive that allows third party applications to seamlessly access and save data back without the need for a custom implementation. Google Drive and Box Drive are such examples. They both allow a user to login and access their data as if these online repositories were physically connected to the PC.

Online Connectors can be used when:

- Organization is using a repository that we currently do not support
- Users must be able to access their data and workspaces using any network and do not want to tunnel using VPN
- Cloud access to data is critical

PROS	CONS
Simple – Use existing off-the-shelf connector to map data into Reactiv SUITE IWB as a virtual drive with no changes required	Network access - Requires the PC to be on the network
Easy to Manage – Administrators can control data access, create new folders, map drives, control access, and propagate changes using existing web console and management tools	Security – Every connector operates differently, and we cannot guarantee that files are not copied locally and when they are deleted
	Multiple Logins – Users will have to login, through the connector app, separately in order to access their data requiring multiple steps