

WGS Administrator (IRF Specific) Session Notes

fireSpace Architecture

Overview

Explain the different concepts involved in the IRF Solution. Describe how mobile data capture component; fireSpace is used as key tool in the solution.

What is fireSpace?

What is WGS?

What is IRS/IRF?

What is...? (Any other SOPHTLOGIC terms not understood)

Global TUI

Explain the purpose of the global TUI vault, what it serves and how we've added redundancy to the model.

fireSpace utilizes SOPHTLOGIC's Trusted User Interface (TUI) framework.

The TUI enables SOPHTLOGIC applications to access user credentials from the Operating System; these are then looked up on a central TUI database.

Central TUI details are maintained by SOPHTLOGIC, referred to as SOPHT.Vault. TUI information returned from the vault includes license expiry, local database credentials and URL of the WGS server.

At present the process for updating TUI details is done manually via SOPHTLOGIC support.

Consequences of not having updated TUI details in the vault may include:

- User failing to check out or open record via activation (e.g. pharOS).
- User checking out invalid set of work if using post code logins and the TUI is out-of-date

<< Decide on process for managing TUI Accounts >>

<< TUI Console – Run through the window >>

Important to note that the TUI may still validate even if database credentials are invalid.

Once the TUI have been validated it cannot be overwritten unless revalidated by another successful TUI validation.

TUI credentials and other user preferences are cached locally in the Application Data system folder (%APPDATA%). It always has the name of WAND2.User.settings.

Local TUI

Describe how using SOPHTLOGIC's TUI model differs from the traditional post code usernames. Explain how the move to usernames being specific to individuals - not posts is implemented using the TUI and provide example of each method.

Local TUI accounts are used to attach local database accounts to personnel within the establishment.

Local TUI accounts are not mandatory if the system has been configured to use post code logins.

If the system uses user name logins and not post codes, local TUI accounts are needed to be attached to personnel via the PRC.

<< Demonstrate creation of TUI accounts and attaching them to personnel records >>

The local TUI accounts are maintained by each customer.

<< Discuss the strategy for migrating user accounts to the new username based credentials >>

Mobile Data

Describe the mobile data concepts of fireSpace including caching, form data, rules and solutions. Explain about how, where and why the data is stored locally. How records are managed by fireSpace and current techniques for managing such data when in a live environment.

fireSpace caches entire dataset to client. It behaves exactly the same in the Citrix environment, the data is always held in the users' Application Data Folder – specified by the environment variable %APPDATA%.

The local data store holds everything about a WAND form, including attributes and their calculations, rules and solutions. It also holds version and pagination details.

WAND Data Stores are stored as uncompressed XML data sets. They are named in the following convention: [tui_account].wand. They can be interchanged from one client to another - e.g. for training/debugging purposes.

<< Demonstrate being able to identify cache location and clear it using settings tab on WAND Browser >>

fireSpace supports migration from one version of a data store to another.

Check out and retrieval of single record via activation uses the same mechanism.

During data entry, the underlying data set is updated each time a field is validated.

It is only saved (persisted to hard disk) when the user checks in/out or closes the fireSpace client.

The checkout process involves building a template record based on the attribute structure and pre-populating it with default values. Then, WGS pre-populates the record with values from the logical last record. This is determined by the specific form.

Finally, the system overlays the bound values from the WGS bindings. In most cases the bindings are mutually exclusive of the data brought forward, but in some cases the data is overwritten. This is what we call a "forced binding" or "forced update".

<< Provide diagram of how the WGS builds the data sent to the client >>

Along with the records "checked-out" the WGS also sends the latest versions of the forms cached on the web server. This should be explained in more detail when discussing WGS.

Activation and Interoperability

fireSpace activation works on document association of the .wand file type.

Interop with pharOS is provided using a dynamically generated vbs scribt that create a script shell object and "runs" a dynamically generated .wand parameter files.

<< Demonstrate the creation of vbs and .wand file and explain the content >>

<< Discuss potential issues with privileges and security >>

Deployment

Describe the deployment method available to fireSpace.

ClickOnce, best used on system admin installations, tablet PCs or other remote workstation. Does not require admin permissions to run - although not options in installation path, etc.

MSI - fireSpace is only supported if the latest version of the application is being used. If MSI installation is used, onus is on IT depts to ensure deployment is up-to-date.

Organisation wide deployment is achieved via MSI installation through GP (active directory)

<< Demonstrate GP deployment >>

<< Demonstrate model for downloading a evaluating software from pre-production >>

Network Configuration

Web Proxy

Explain the impact of default proxy settings (set via IE) have on fireSpace. Describe how these settings can be used to ensure fireSpace utilises web proxy.

TUI Console shows the proxy settings that will be used by fireSpace when communicating with WGS and the SOPHTLOGIC vault.

<< Demonstrate the Network Configuration settings on the TUI Console >>

<< Demonstrate how changes to system internet settings via Internet Explorer affect the fireSpace network configuration >>

Note: Using the WAND Library (explained later) is a good test to ensure client has connectivity to SOPHTLOGIC and local WGS.

Other Considerations

WGS' CLG Interface required access to the CLG web services.

Public access to WGS for remote users (not using Citrix) requires publishing via firewall - or VPN client on remote users' workstations.

Form Deployment

Synchronisation of Forms

Describe the process for managing the transmission of new versions of forms to the site's database. Explain how the synch process works and subsequent actions needed to ensure system works as expected.

System allows forms to be deployed via WAND Library.

<< Demonstrate WAND Library via fireSpace >>

Once a new form has been synchronised system administrators should use the eQ Configuration Manager to ensure the underlying attribute tables are available.

<< Provide demonstration on using eQ Configuration Manager to run the DLL >>

<< Provide for specific information on which attribute groups are part of which form >>

Form Structure

Describe how the forms are created. Show examples in eQ Configuration, e.g. how inline help is generated.

Inline help is entered against each attribute.

Show the principals of how user defined attributes can be added to a form and how rules and solutions dictate the form's logic.

Customised Attributes

If well known (core) form attributes are modified on the local system, they are subject to being overwritten by the synch. However it is possible to make a change pending updates from SOPHTLOGIC.

<< Show examples of how fireSpace manages the lookup values from CLG taxonomies and how they could be replaced very quickly pending an update from CLG >>

WAND Gateway Services

What is WGS...?

Explain the purpose of WGS and how it sits in the overall picture

WGS – Wand Gateway Services provides data transformation services between SOPHTLOGIC systems and 3rd party systems such as IRS and MDTs.

Web Server Administration

Web server management done using the MMC snap-in.

<< Demonstrate ensuring the services is running and how to restart the process >>

<< Demonstrate basic check of WAND2.ASMX page to ensure WGS methods are available >>

Updating/reinstalling WGS done from published MSI on SOPHTLOGIC web site.
(<http://www.safeashouses.net/publishing/WAND.Gateway.services/>)

Configure logging via the global.asmx.

IRS the WGS' CLG Proxy Service

CLG Proxy service is a series of web based functions that take information from pharOS and populate IRS data structures. These structures are then sent to the CLG's IRS interface.

The result is recorded against the incident's IRF QA section.

Automatic alert can be setup to notify specific users when certain errors occur on the interface.

<< Give overview on how automatic query could be setup >>

Troubleshooting

Using the Windows Event Log

Using the WGS Log file

<< Demonstrate where to find the log file and display contents >>

IRS and pharOS

IRF Privilege Profiles

Explain the different levels we've proposed. Fire-fighter, District Manager (commander) and Administrator.

Explain the purpose of Team Scope and how it relates to Who Can see What (WCW).

Who Can see What (WCW) is a mechanism used to tell the system to limit a users view of locations and personnel to a particular team scope.

IRF Specific Privileges

Provide list of privileges used and what affect they have on usage.

Who Can see What (WCW) is a mechanism used to tell the system to limit a users view of locations and personnel to a particular team scope.

IRF Record Locks (2059SP9)

Viewing the locks using QueryBuster

Clearing one or more locks using basic SQL Script or individually using the IRF Browser

<< Demonstrate using query buster to view locks on a record >>

*Data will not be available until next WGS deployment