"The ICE Dataspace is a collection of Image FOCUS Inspection Findings, LPAR Configuration Profiles and a Journal of Controlled Actions and Events. The goal of ICEDirect is to provide broad-based Browser access to its content."

Getting Started with ICEDirect

A Set of *MY Applications
With Access to The Integrity Controls Environment (ICE)

ICE 17.0 Patch 5

NewEra Software Technical Support
800-421-5035 or 408-520-7100
support@newera.com

Rev: 2023-02-23

1. YouTube

This document contains many references to YouTube Videos – Google NEWERA SOFTWARE YOUTUBE. Each ICEDirect Video is referenced by a number that ties back directly to this document. We believe you will find them instructive and helpful to your understanding of the many features of both ICEDirect and the Integrity Controls Environment. Please avail yourself to them as you consider necessary.

https://www.youtube.com/channel/UCqmLWrvyn0n_49Fbpi-74uA

2. Table of Contents

3. What is ICEDirect?

ICEDirect is a collection of application interfaces that provide access to the Integrity Controls Environment (ICE). ICE is a z/OS-based system utility that may be accessed with TSO/ISPF, The Legacy Edition, or through the internet using a browser-based interface, The Web Edition.

The purpose of this document is to provide guidance in the setup and use of The Web Edition.

4. Setting Up ICEDirect

ICEDirect is included as part of the ICE download that contains both Image FOCUS and the Control Editor. Both components are installed using the SMP/E instructions found in the respective User Guides. Prior to starting two primary tasks, it is necessary to customize the environment using members found in the ICE Parmlib dataset.

4.1.1. Server Installation

NEZWEBxx is the ICE Parmlib member that controls the configuration of the integrated HTML Web Server. An explanation of this member and a detailed description of the Web Server is found in Appendix "A" – The Web Server Explained.

4.1.2. User Registry

Each ICEDirect user will be supported by a user-specific registry partitioned dataset. This dataset will be defined to the system with a name of:

```
userid.MYICEWEB.REGISTRY
```

where "userid" is the userid that was supplied for login.

These registry datasets are allocated whenever a user logs in. It is critical to the operation of ICEDirect that users are allowed to allocate and alter the content of these datasets.

4.1.3. Global Registry

In addition, during installation a Global Registry dataset is defined as follows:

```
DD WEBREG
DSN=install_hlq.WS.WEBREG
```

It is critical to the integrity of ICEDirect that users NOT be allowed access to this ICEDirect Global Registry dataset.

During installation a userid should be assigned to the ICE Primary Started Task (IFOM), to the individual TSO/ISPF (IFOS), to the Web Server and to the Interval Detector.

- RACF commands for setting up started task userids:

```
adduser ifom name('IFOM STARTED TASK') SPECIAL AUDITOR
adduser ifos name('IFOS STARTED TASK') SPECIAL AUDITOR
adduser ifomws name('IFOMWS STARTED TASK') SPECIAL AUDITOR
adduser ifodet name('IFODET STARTED TASK') SPECIAL AUDITOR

rdefine started ifom.* stdata(user(ifom) trusted(yes))
rdefine started ifos.* stdata(user(ifos) trusted(yes))
rdefine started ifomws.* stdata(user(ifomws) trusted(yes))
rdefine started ifodet.* stdata(user(ifodet) trusted(yes))

setropts raclist(started) refresh
```

The Global Registry Dataset should be protected with a UACC of NONE. When this is the case The IFOM userid must be permitted READ/UPDATE Access and Interval Detector userid must be permitted READ.

4.1.4. Server Security – YouTube #5

The Web Server component of ICE is *CLOSED* to all others. It supports and responds only to the ICEDirect application.

In addition to setting up the Web Server, it will be necessary to configure a secure socket (IPaddress and PORT) to be used as the login entry point into the Mainframe LPAR hosting z/OS and the ICEDirect Web Server. A proper, secure connection will be indicated by a "Security Lock" appearing in the browser location window during login and throughout the duration of a browser session connection. It is recommended that you do not attempt to connect to the server before socket security is enabled. The URL for a secure login point would look similar to this:

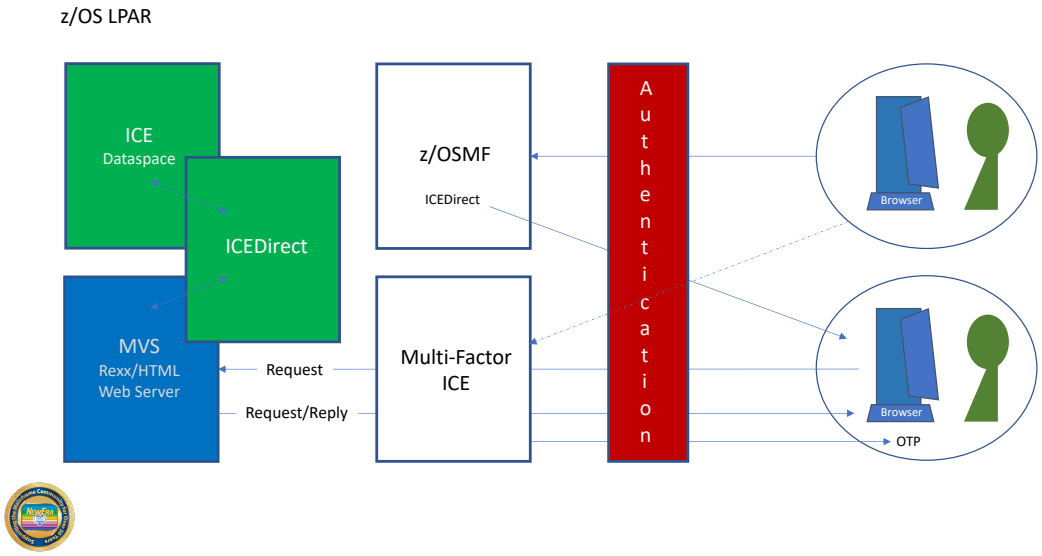
https://24.234.192.41:8200

Optionally, a step may be taken to select and register a unique IPaddress Domain Name. With a registered domain name, the login point might look similar to this:

https://www.myicedirect.com:8201

The port number is provided in these examples to denote the additional protections afforded by the use of a firewall.

Once selected, registered and secured, the login address may be integrated in the z/OSMF Framework as a Linked Application.



4.1.5. Content-Security-Policy (CSP)

Content-Security-Policy is the name of a HTTP response header that modern browsers use to enhance the security of the document (or web page). The Internet Explorer (IE) does not support CSP and is there not a recommend.

Pages shown by the browser will contain a Content Security Profile (CSP). The CSP will define "Valid Content" as only that content that comes from "Self", meaning only from the ICEDirect Server. The CSP is intended to prevent Cross Site Scripting (XSS) and data injection attacks. This will make such attacks very difficult or near-impossible when combining both AT-TLS and CSP in a single browser session. The default CSP is shown below:

- Content-Security-Policy:
- default-src 'none'; (the absolutely most restricted default setting see below)
- script-src 'self' 'nonce-@WEB_RANDOM@';
- img-src 'self';
- style-src 'self' 'unsafe-inline';
- base-uri 'self';
- form-action 'self';
- frame-ancestors 'self';
- frame-src 'self';
- child-src 'self';
- object-src 'self';
- font-src 'self';

While the design rule for ICEDirect is "NO Inline Scripting" dynamic objects like Chart.js require inline script. To accommodate these exceptions a unique random "NONCE" is injected by the server in the "script-src 'self'" policy which is intended to deny all inline scripting. The NONCE creates a random relationship between the server and HTML pages containing inline scripting that is unique and therefore not exploitable.

The starting point for this Policy is "default-src 'none'" which sets the value for all of the following to 'none', unless overridden by Policies shown above.

- child-src,
- connect-src,
- font-src,
- frame-src,
- img-src,
- manifest-src,
- media-src,
- object-src,
- prefetch-src,
- script-src,
- script-src-elem,
- script-src-attr,

- style-src,
- style-src-elem,
- style-src-attr,
- worker-src

4.1.6. Operating from a z/OSMF LINK – YouTube #10

Using a z/OSMF login, most likely on an internal TCP/IP intranet, will provide a very secure browser session.

- Why is a z/OSMF Connection Infrastructure Secure?

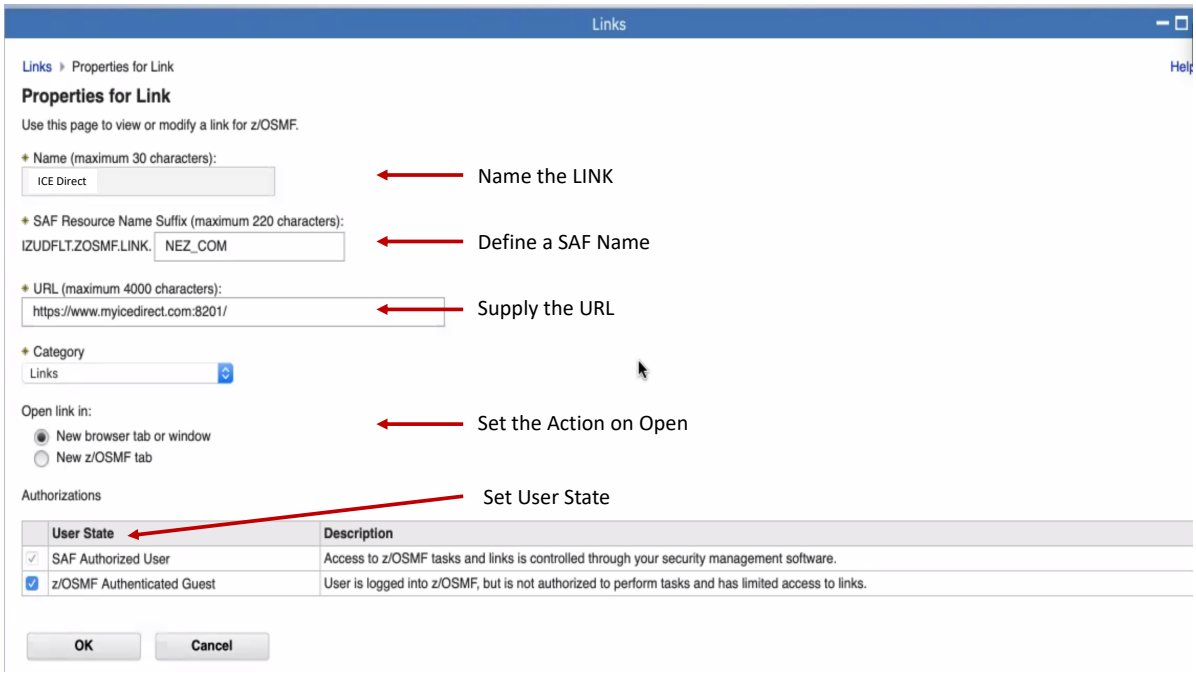
The configured connection to z/OS will have the RACF, ACF2, or TSS security prerequisites defined. Additionally, the port that z/OSMF attaches to will have been elevated, using PAGENT, for protection by AT-TLS. The browser will therefore show HTTPS (the lock) not HTTP and all traffic to/from z/OS will be encrypted. The TCP/IP PROFILE configuration of the port and the NETACCESS BLOCK in the PROFILE will both be protected by SERVAUTH profiles and any instance of a z/OSMF connection will need specific permission to attach to or access the port and the source IP address of the browser, then the TCP/IP stack, and then z/OS. Clearly, there are several access permission layers.

- How does ICEDirect benefit from this z/OSMF Infrastructure?

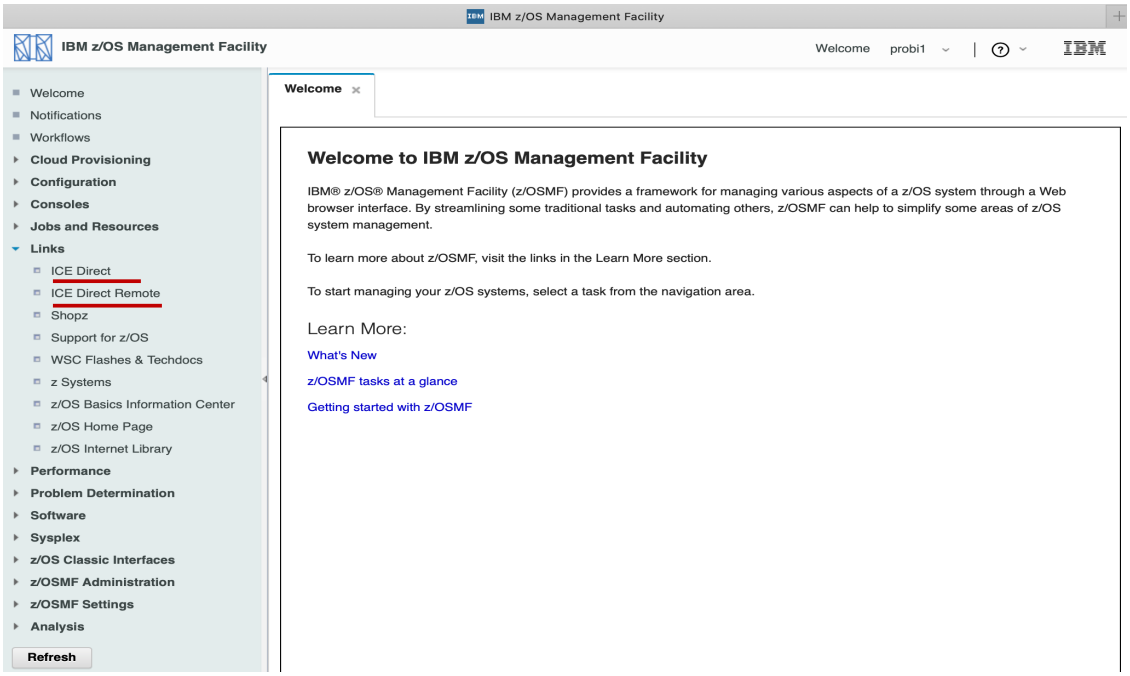
Once z/OSMF is configured to an organization's satisfaction, individual users will need to be permitted to use it and to authenticate with z/OS similar to a TSO logon. To integrate ICEDirect, such an authorized user would need to use the z/OSMF LINK configuration file (/samples/sampleLink.properties) or its browser tools to configure a link that will attach to the ICEDirect URL. A sample configuration definition is shown here.

```
LinkName=ICEDirect
LinkURL= https://www.myicedirect.com:8201
LinkNavigationCategory=3
LinkAuthorizedRoles=z/OSMF Guest, z/OSMF User
LinkSafSuffix=NEZ_COM
LinkLaunchWorkArea=false
```

Or use the authority of the z/OSMF Administrators, dynamically setup the Link once logged onto z/OSMF using the interface panel shown here.



Updates are dynamic so there is no need to restart z/OSMF. When The Integrity Controls Environment (ICE) is active on remote systems not associated with the running sysplex, setup Multiple LINKs to allow for the attachment of their specific ICEDirect URL. An example is shown here.



To be most secure, the ICEDirect HTML server should sit behind the same port as z/OSMF and must have LinkSafSuffix permitted to both PORT and NETACCESS SERVAUTH

profiles. This will achieve the same level of environmental security as z/OSMF. A login to ICEDirect is the next step.

- Logging In to ICEDirect from z/OSMF

To log into ICEDirect, the user will need to authenticate to z/OS and then make a request via ICE authentication for server access. This is done using the ICE Multi-Factor Interface (MFI) functionality. If these authentication challenges are successful, the ICEDirect "Welcome Page" will be displayed.

With Pages in the browser, it is important to note that these Pages will not contain inline java script, Cascading Style Sheets (CSS), or the use of Cookies. The server/browser interaction will use both scripts and CSS in the processing and delivery cycles. The design rules of ICEDirect specify such needs can only be satisfied by related files defined, stored/contained in the ICEDirect Server z/OS environment and delivered by "Self", the ICEDirect Server.

The primary containing structure of all ICEDirect Pages is a static, three-part Iframe Set. These frame containers are named Sidebar, Directs, and Results. Requested Pages can only be displayed by the browser in one of these three frames. Each of the three frames is protected CSP security settings that restrict the Iframe, allowing it to only display content that comes from "Self", the ICEDirect Server.

- Securing the z/OSMF LINK

Follow the model below to create a Profile that defines the ICEDirect Link.

```
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.LINK.NEZ_COM UACC(NONE)
```

Follow the model below to permit Administrators and Users to the ICEDirect Link.

```
PERMIT IZUDFLT.ZOSMF.LINK.NEZ_COM CLASS(ZMFAPLA)   ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.LINK.NEZ_COM CLASS(ZMFAPLA)   ID(IZUUSER) ACCESS(READ)
```

4.1.7. Operating from a Standalone Browser

ICEDirect supports the common family of HTML5 supporting browsers and, when operated standalone, can be configured to provide support to the ICE Dataspace from any Internet connected platform.

- Best Practice – Turn off Autofill

When operated either as a z/OSMF LINK or from a standalone browser always turn off the browser Autofill function. If you do not, Autofill will store and return your userid and password automatically allowing anyone that operates your computer to masquerade as you, gaining access as if they are you to z/OSMF and/or ICEDirect both running on z/OS.

The Integrity Controls Environment (ICE) offers Multi-Factor ICE to mitigate against the possibility of Autofill being used during ICEDirect authentication.

4.1.8. User Authentication – YouTube #5

To access the ICEDirect Interface a user must authenticate with two layers of security. The first layer authenticates the user with the z/OS External Security Manager (ESM) in use: RACF, AFC2, or Top Secret. The second layer authenticates the user with ICE.

Authentication with z/OS

ICEDirect uses standard RACROUTE calls to authenticate a user with the active security product.

If the authentication fails, the user will receive one of the following messages:

- Login failed using the credentials entered
- The Password/Passphrase has expired
- The new Password/Passphrase is invalid for this site

4.1.9. Authentication with ICE

ICE Authentication requires the user to be in possession of a One-Time-Token PassTicket (OTP). This token is eight characters in length but can be configured in two different ways:

- First, a full token may be delivered to a user email address.
- Second, a portion of the token (token material) is delivered to the user on-screen. This is the "NOEMAIL" option. The user next prefixes this material with a previously registered private PIN.

In either case, if the entered token authenticates the user, the ICEDirect Main Iframe Set is displayed.

If the authentication fails, the user will receive one of the following messages:

- No PassTicket generated. This userid may not be defined
- No ICE PassTicket was generated for this userid
- An ICE PassTicket has been emailed to you
- Enter your Private Prefix followed by the Token Material as the PassTicket

Upon ICE authentication failure, the user is returned to the first level of authentication.

With each permitted use, a record, as shown below, is written to the ICE Control Journal and optionally, an email alert sent.

```
01C|-SRC: MFIAUTH--------------THE CONTROL EDITOR---------------- MFIPermit -
02C|SYSPLX:ADCDPL SYSNM:ESSD6 USRID:ESSJDL1 TM:15:29:58 DT:09/25/20
03C|-MFIPERMIT: ESSJDL1-----------------------------------------------------
-----------------------------------EVENT DATA-------------------------------
Authentication request MFI token: OKFWJX0E
```

Similar messages are written to the Journal when authentication fails noting user, date and time and the reason for the failure

5.Patient Zero - First ICEDirect Administrator – YouTube #0

The first ICE Administrator to attempt login to ICEDirect (and all other ICEDirect Users) will need to pre-define an ICE authorization profile. To define such a profile, an Administrator must logon to TSO/ISPF on the z/OS LPAR where IFOM and the ICEDirect web server are running. Once at the TSO/ISPF Primary Menu the following command is entered:

```
TSO $CLI,*MYMFI,a_valid_userid
```

The system will reply with:

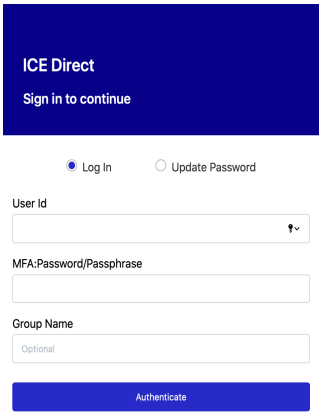
```
- NSIMRBX – MFI User Added, Prefix Set to 'INIT' & Activated. -
```

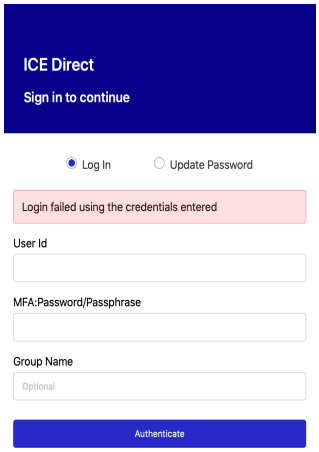
An action block entry is added to the NSEENSxx ICE Parmlib Member:

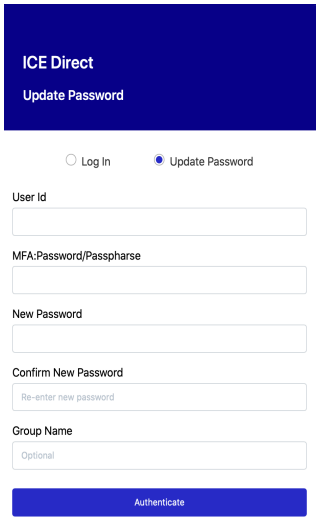
This command sequence may also be used by ICE Administrators to reset and activate a user-defined prefix, resetting it to its default initial value.

5.1.1. *Logging In – YouTube #5*

To login to ICEDirect, open a browser session and enter the defined URL of the Server. When the login page is presented, enter a TSO UserId and Password in the textbox fields and "Click" Log In. These actions will begin the z/OS authorization process with the External Security Manager.







If the authentication fails, one of the following messages will be displayed:

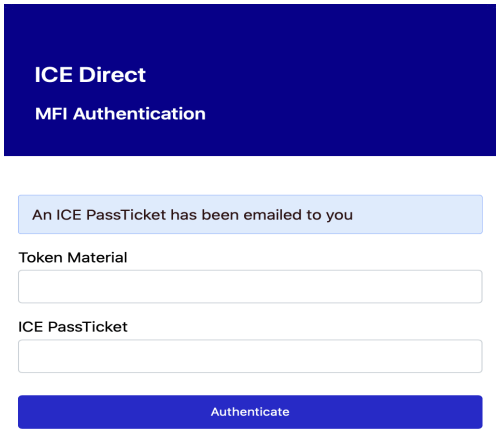
- Login failed using the credentials entered
- The Password/Passphrase has expired
- The new Password/Passphrase is invalid for this site

When the use of the optional Group Name is used, failure responses include:

- Group is invalid
- User is not authorized to Group

5.1.2. Using the Prefix

With the authentication into z/OS completed successfully, the ICE authentication process is initiated. See the panel shown below:



As shown, Token Material "MFSH" has been generated by the z/OS ESM for specific one-time use in authenticating into ICE. Using your Initial Prefix, enter the following into the ICE PassTicket text-box field.

```
INITMFSH
The Field is Masked
```

"Click" Authenticate to validate the ICEDirect PassTicket token. If successful, the ICEDirect Main Iframe will be displayed.

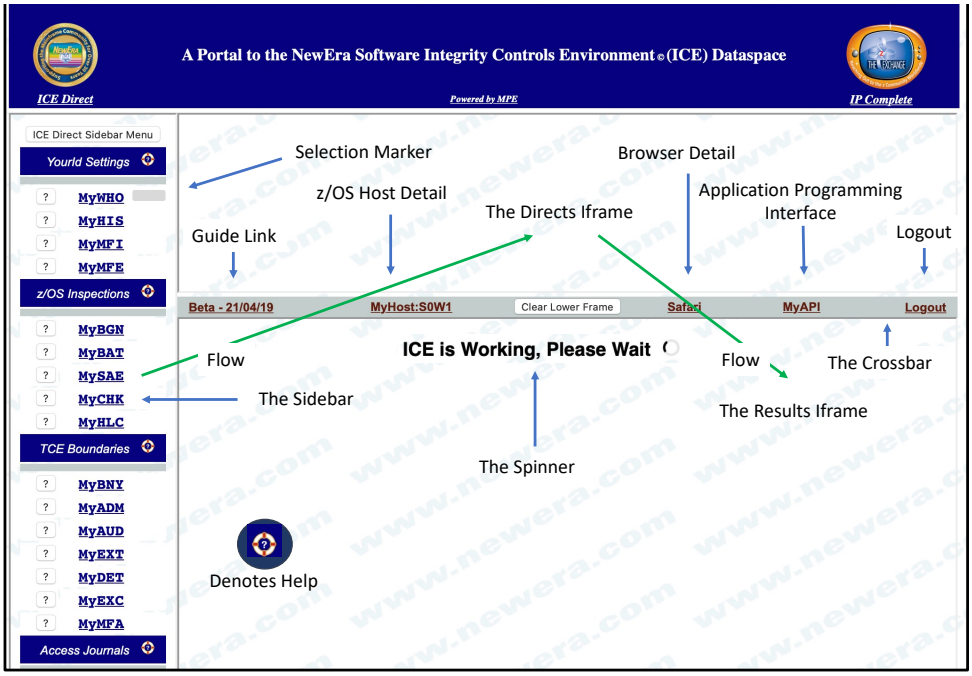
If authentication fails, one of the following messages will be displayed.

- No PassTicket generated. This userid may not be defined
- No ICE PassTicket was generated for this userid
- An ICE PassTicket has been emailed to you
- Enter your Private Prefix followed by the Token Material as the PassTicket

Users that encounter the first of these messages have not yet had their Prefix Accounts initialized by an ICE Administrator.

5.1.3. ICEDirect Main Iframe Set– YouTube #5

The ICEDirect Main Iframe Set is a series of browser windows set within a single HTML page. Each serves a specific purpose acting independently or in harmony with other windows.



5.1.4. Sidebar

The Iframe to the immediate left is called the Sidebar. Its purpose is to present application options. To select an application, cursor under it and click on it. This action will present a supporting application specific interface in the upper window called Directs.

The Sidebar offers two types of Help. First, Mini-Help is found when "Clicking" the Question Mark submit button that precedes each application name. Second, Group-Help is shown when the "Life-Ring" following the group name is "Clicked". In either case, related Help Text will "Float" above the Main Iframe, to continue "Click" Close.

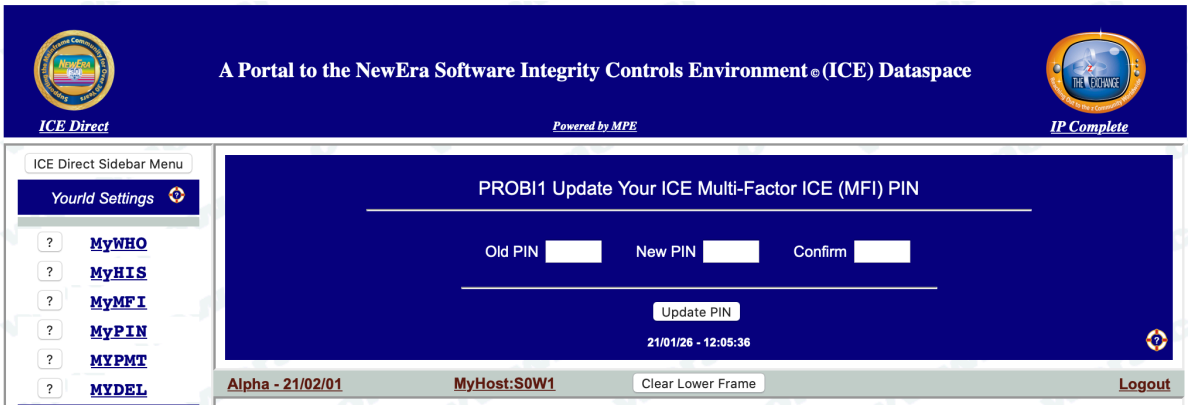
5.1.5. Selection Marker

As selections are made from the Sidebar the area adjacent to them is marked with small gray rectangle that will persist in that location until an additional selection is made in which case the marker will move to the area adjacent to the new selection.

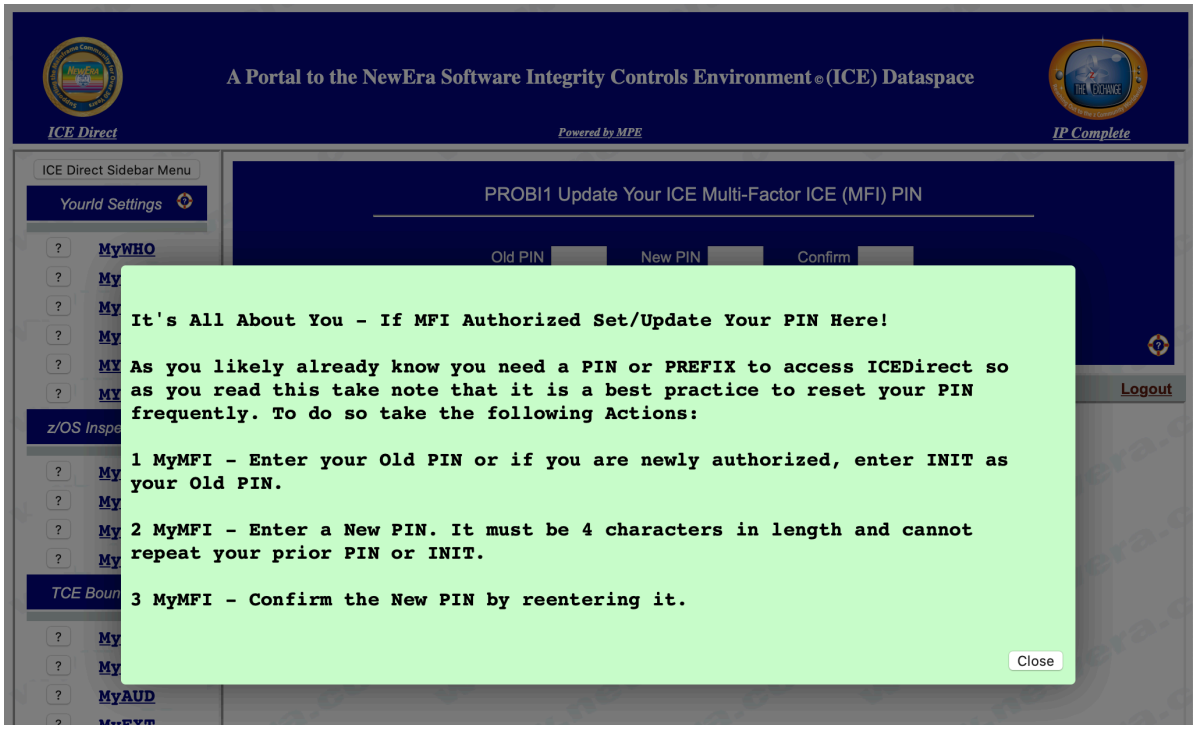
5.1.6. Directs IFrame

When an application is selected from the Sidebar, its related interface is displayed in the Directs Iframe window. As it is being fully resolved, a "Spinner" will appear in the lower window and will disappear when request resolution is complete.

When resolution of the selected request is complete, an Application Directs Panel, similar to the one shown, will appear.



This specific panel is the Interface Panel for the "MyMFI". Use this panel to update the Prefix/PIN used to authenticate with ICE and Login to ICEDirect. Selecting the "Life-Ring" in the lower right will display the Help Panel Floater shown in part below:

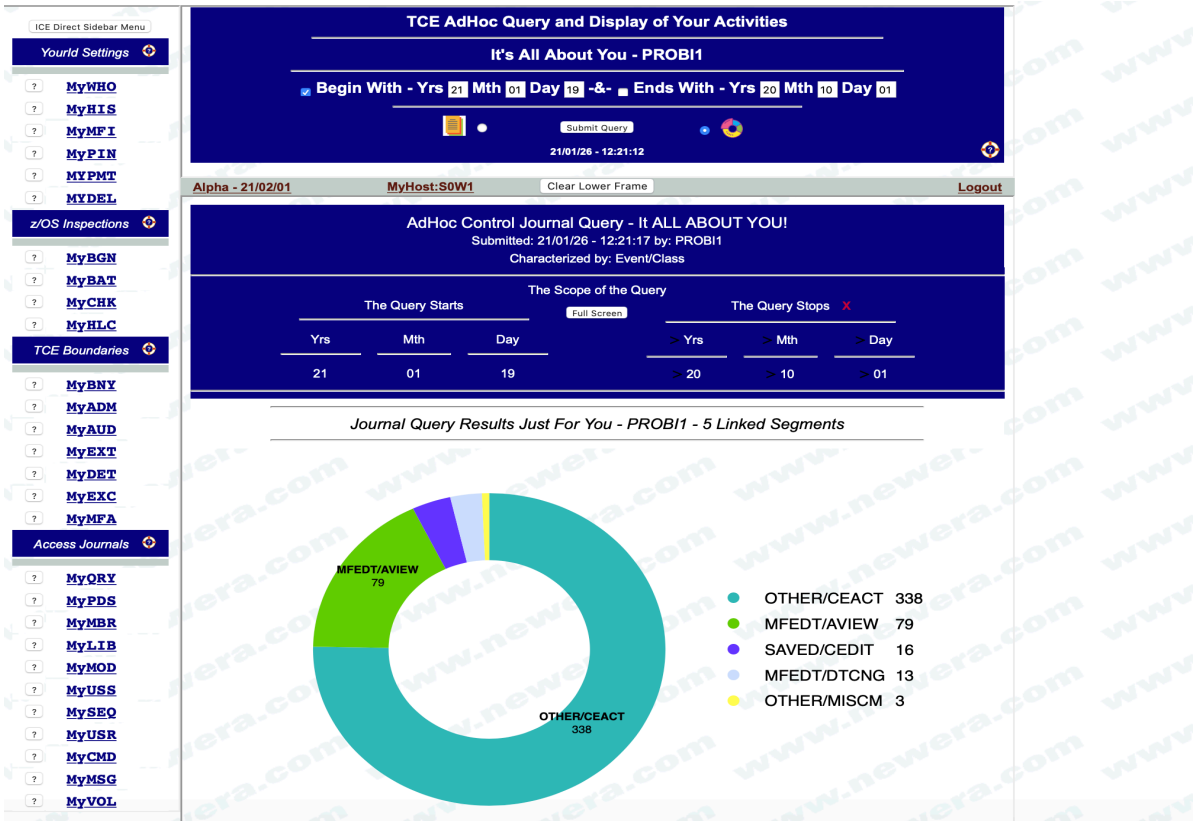


To close the help panel, "Click" Close.

This process of selecting from the Sidebar display of the Interface Panel in the Directs Iframe will continue for all *My Applications.

5.1.7. Results IFrame

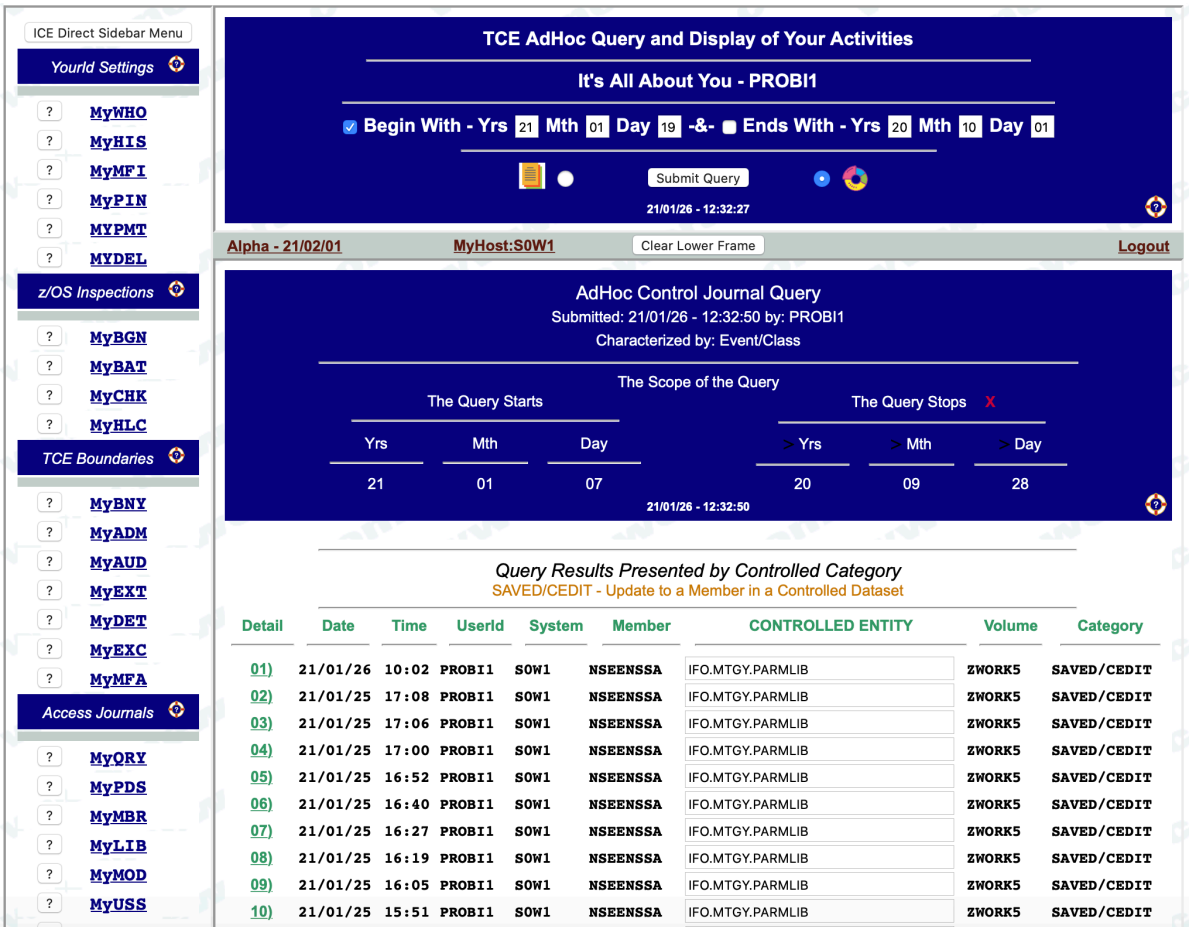
In general, each Application Interface will present a number of options. Review the related help panel for each option before submitting a request for results. An example of a results page is shown below:



This graph presentation was derived by selecting "MyHIS" from the Sidebar and then completing Query Scope, defined by start and end date, presented by the Application Interface shown in the Directs Iframe. Most results can be presented in either a Report or a Graph and that selection is made prior to request submission. To make an additional request, repopulate the Application Interface with a new set of options and resubmit the updated/new request.

As the presentation suggests, segments in this case are linked to underlying source detail. "Clicking" a segment or its related legend will display it and additional selection options.

To generate the example shown below, the segment legend labeled “SAVED/CEDIT” was selected. Saved Edit is a term related to The Control Editor (TCE) and reflects an action taken by a user to modify a member in a Controlled Dataset that was recognized, captured and recorded in the ICE Control Journal. The ICE Control Journal is the base source of the information shown in these examples.



In this example, the Application Interface is a constant while the results Iframe is updated with each additional request. This has the advantage of allowing for a redefinition of options without having to start over again. However, should a new selection be made from the Sidebar, the Results Iframe will be cleared and the current Application replaced with that of the requested update.

Take note of the “Row Numbers”. They are additional selection points that when “Clicked”, will display the underlying Control Journal Detail, a sample of which is shown on the following page.

5.1.8. The Crossbar

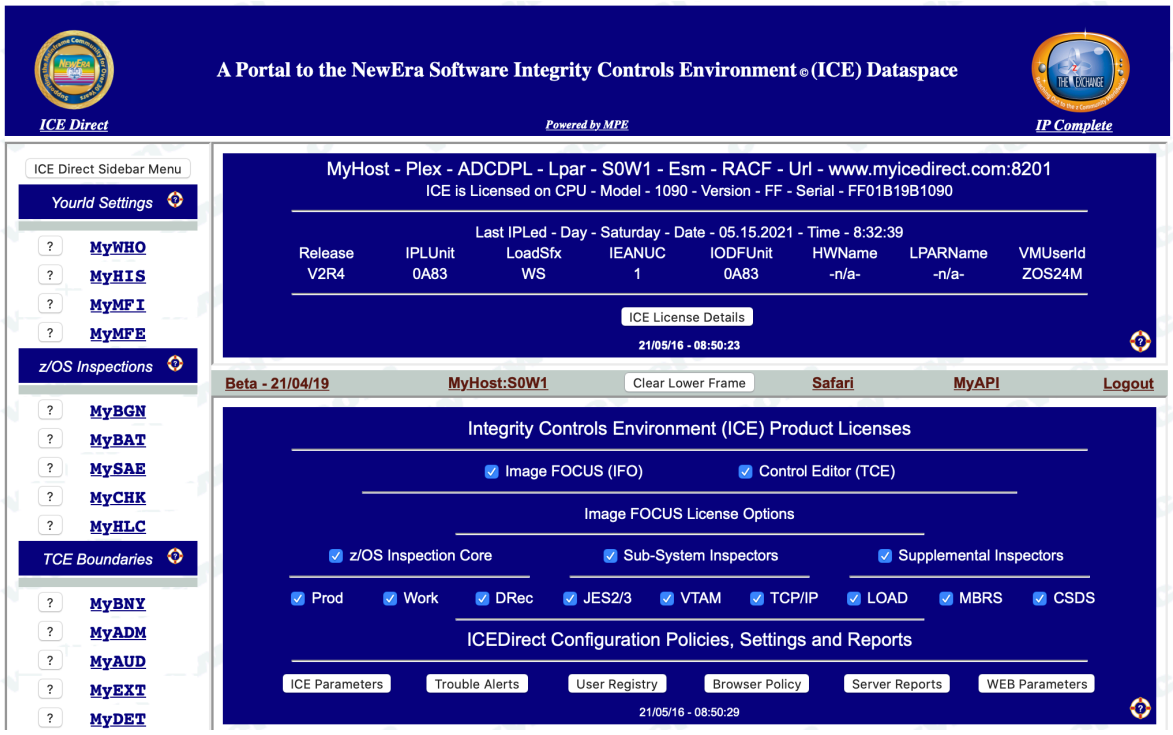
The upper and lower Iframes are separated by the "IFrame Crossbar". This bar contains additional options. They include:

Current Release Information

To the very left is shown the release identifier of the version of ICEDirect that is running. "Click" this to show the accompanying documentation for the release in the lower Results Iframe. This release information will be important when technical assistance is needed.

MyHOST

"Click" MyHOST to view a description of the z/OS system that is Hosting ICEDirect. Options along this path show – ICE Licensing details, ICE Server Outages, ICE Server and Web Server configuration details. In addition users may sign up for real-time notification of ICEDirect returning to service following an outage.



Clear Lower IFrame

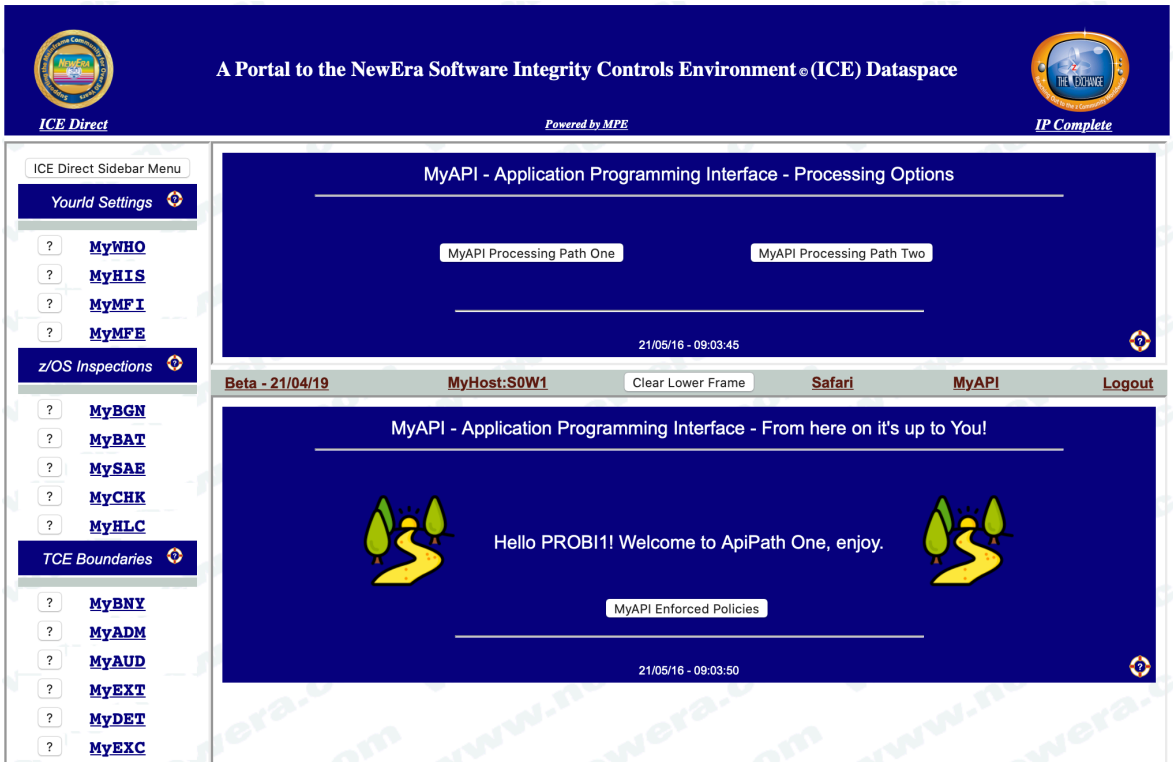
Results will populate the lower Iframe and be cleared automatically by subsequent selections. However, this option may come in handy for "Hiding Results" and revealing them using the browser backup button.

Browser Details

The name of the displaying browser is shown on the Crossbar, "Click" it to show the browser specifics, release level etc. This information may be helpful to technical support when problems occur.

MyAPI

Select this option to access the Rexx Script member NSIMAPI that resides in the your_hlq.WS.WEBREXX dataset. This single member may be used to house custom functions that are contained therein.



Logout

Although the REXX processing addresses spaces will timeout automatically as defined during initialization of the Web Server, it is a "Best Practice" to always Logout.

6. ICEDirect Applications – Each Briefly Explained

6.1.1. YourID Settings

It's All About You! Select an Option to find out more.

MyWHO – Your ICE User Scope – YouTube #6

Your assigned identity Prime, Admin, Auditor, ROAuditor/General User determines what ICEDirect functions and applications you may access. Selecting MyWHO will show you all your current identities.

MyHIS – Your ICE Event History – YouTube #6

ICE is at its best when tracking and capturing system activities. These include - configuration updates, operator commands, system messages - some of which may be linked back to you. Select MyHIS to see your activity.

MyMFI – Your Multi-Factor ICE Prefix – YouTube #0

Multi-Factor ICE (MFI) controls the final step in ICE Direct authentication. Similar to MFE, it also requires a private PIN to meet a challenge during a web logon. Select MyMFI to register or update your PIN.

MyPIN – Your Multi-Factor Edit Prefix

Multi-Factor Edit (MFE) is a novel form of MFA that challenges you as you attempt to make "Controlled Edits." To meet this challenge, you need to create a private PIN. Select MyPIN to register or update your PIN.

6.1.2. z/OS Inspections

z/OS Inspections - Sysplex/ICEBATA/IPLCheck Inspections and IBM HealthChecks.

MyBGN – Image FOCUS Sysplex Background Inspections – YouTube #1

Background Inspection configurations are defined from the ICE/VTAM Primary Menu. Once defined, the inspections run at intervals defined to IFO or a job scheduler. If defined to a scheduler, they may be started directly from the panel that will follow when MyBGN is selected.

MyBAT – ICEBATA Inspection Logs and Analysis – YouTube #2

This option is used for the inspection of Images inside/outside of a given Sysplex. Each inspection is started independently using a supplied batch procedure. Results are written to a named log dataset. The panel that follows the selection of MyBAT will support common naming, ad hoc naming, or unique naming in a dynamic worksheet.

MySAE – SAEBATA Inspection Logs and Analysis – YouTube #3

This procedure creates inspection logs and configuration baselines which focus on specifically defined LPARs and are used in real-time from the HMC or an SAE Console to spot configuration changes that may have resulted in an IPL failure. This function parallels the HMC application supporting on-demand creation of baseline and comparative analytics that identify configuration changes.

MyCHK – IPLCheck Inspection Logs and Analysis – YouTube #4

IPLCheck will initiate an inspection, under control of the HealthChecker, that evaluates various elements of a running system configuration. The selection of MyCHK supports multiple log access conventions.

MyHLC – IBM z/OS Health Checker Reporting – YouTube #7

Selecting MyHLC will display a panel that allows for the naming of up to 18 LPARS. Once named, the status of the checks associated with an LPAR are displayed with links to the underlying Check Finding and Policy. Multiple LPARS may be selected. This results in a side-by-side comparative analysis presentation.

6.1.3. Control Boundaries

Control Boundary Intercept Points, Admin, Audit and Global Functions!

MyBNY – Access or Update ICE Intercept Point and Boundaries

ICE supports five "Intercept Boundaries" that both define and report on impactful events. These events include - datasets, library, and file updates and system command and message issuance. MyBGN presents these events and access to their configurations.

MyADM – Assign/Unassign ICE Adminstration Credentials

ICE will recognize two levels of Administration: Prime and Other. Only one Prime is allowed with access to all ICE functions. Up to six other userids have limited access. MyADM presents Administrator settings.

MyAUD – Assign/Unassign ICE Auditor Credentials

Both a Senior Auditor and six ReadOnlyAuditors may be recognized. They differ in the degree to which they may access and update ICE Reports, Displays and Settings. MyAUD shows Auditor settings.

MyEXT – Global Control over External Notifications Settings – YouTube #8

ICE supports External Notification from all control boundaries. This option will provide access to global notification "ON|OFF", the status of WAEMAIL, and a list of all possible recipients with scheduled deliveries.

MyDET – Global Control over Interval Detector Settings – YouTube #8

Automated interval reporting is configured to support notification to concerned users of events impacting control boundaries. MyDET shows Global ON|OFF, Alternate HLQ, STC PROC and "Lists All" active Detectors.

MyEXC – Global Control over Journal Event Exclusions – YouTube #8

Certain auto-collected ICE Events - Heartbeat, TCE Activation, Email Debug, STC Interval, Email Notify, Logon Success, Privileged Logon Success, Expiring Password Notification - may be seen as unneccessary. MyEXC presents their recording status with an ON|OFF toggle for each.

MyMFA – Overview/Control over of ICE MFA – MFI/MFE – YouTube #9

ICE supports two novel forms of Multi-Factor Authentication (MFA) - Multi-Factor Edit (MFE) and Multi-Factor ICE (MFI). Each is uniquely configured to support individual users. MyMFA provides access to settings.

MyREG – User Registry Access and Management

ICEDirect maintains two Registries; The Master Registry, named during installation, which includes encrypted user records and an individual user registries, Partitioned Datasets, prefixed with the users, userid. This function allows ICE Administrators management access.

6.1.4. Journal Access

The ICE Journal Captures Controlled Events; these options bring them to You!

MyQRY – Ad Hoc Queries/Reports to/from the Control Journal

Global in scope, this Ad Hoc Query supports query ranges bounded by date and time, characterized by category or event type and presented as groups or charts. An interval detector is provided for automated report creation and optional notification. Select MyQRY to display your settings.

MyXXX – Directed Queries/Reports to/from the Control Journal

ICEDirect offers the additional specific query interfaces:

MyPDS, MyMBR, MyLIB, MyMOD, MyUSS,
MySEQ, MyUSR, MyCMD, MyMSG and MyVOL

These query interfaces are focused to deliver events directly related to - Partitioned Datasets, Members in a PDS, Load Libraries, Modules in a Library, Unix Files, Sequential Datasets and Activities or Events related to Users, Commands, Messages and Volumes.

Queries may be bounded by date and time, target specific entities - a user, a member, a command - for example, or generically for all events. Query results are optionally shown as groups or charts. A group's selection will reveal an ever-increasing level of "Journal Recorded" event detail.

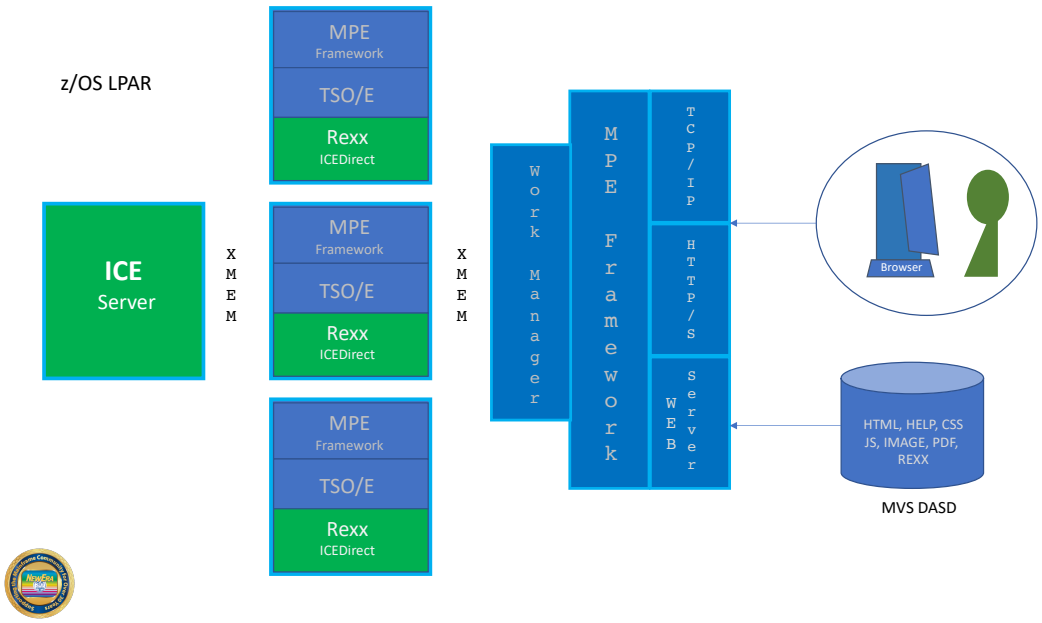
7. The Web Server Explained

The integrated ICEDirect Web Server on the MPE Framework provides an interface between "one too many" browser sessions and the IFOM started task. The Work Manager monitors the incoming browser request and will spawn, as needed, TSO/E REXX address spaces to support the request. These tasks interpret the request and, as necessary, makes requests to IFOM. Data returned from IFOM is formatted into complete HTML documents by the REXX sub task using a combination of static templates and/or dynamically generated HTML structures.

This release of ICE requires z/OS 2.2

7.1.1. Server Overview – YouTube

The Web Server runs as a z/OS started task and supports HTTP/HTTPS connections from common web browsers such as Safari, Microsoft Edge, Chrome and Firefox. The content html, javascript, css, images, etc. are served up from PDSE datasets. The server-side processing is supported by REXX scripts running under a TSO/E environment, accessing the data and functions of ICE.



There are two main components to the ICE Web Server environment:

The first component is a standard Web Server capable of managing multiple browser-connected users and serving up standard web content. The Web Server validates users via RACF, ACF2, or TSS and supports passwords, passphrases, and IBM's multi-factor tokens. It also supports the ICE Multi-Factor Authentication facility (MFI).

The second component of the ICE Web Server environment provides support for the execution of REXX scripts running under a TSO/E environment. This includes connectivity to the ICE Server and access to the ICE data and functions.

The TSO/E REXX processing runs in a multi-address space mode. The TSO/E REXX processing environment runs in one or more separate started task address spaces. In multi-address space mode, requests to execute REXX scripts are distributed to a pool of started tasks running the TSO/E REXX processing environment.

When a browser user completes authentication, the Web Server spawns an instance of the TSO/E Rexx started task. That task runs under the authority of the user, and processes all requests from the user's browser session. If multiple users are logged in, then each user will have their own dedicated started task instance to process their requests. When the user logs out or their session times out, their instance of the started task is shut down. These TSO/E Rexx started tasks are started and stopped as needed by the Web Server started task.

7.1.2. Server Datasets

The Web Server task uses a set of PDSE datasets to store web content. These are referenced by the following DD statements included in the started task JCL:

- WEBHTML - Contains html source that can be referenced by *member-name.htm* or *member-name.html.*
- WEBHELP - Contains html source for help pages. These can be referenced by REXX scripts using a web server interface command. WEBHELP is used primarily to organize help pages separately from the regular content pages.
- WEBCSS - Contains web style sheets. It is referenced by *member-name.css.*
- WEBJS - Contains client side javascript. It is referenced by *member-name.js.*
- WEBIMAGE - Contains images. It is referenced by *member-name.jpg, member-name.jpeg, member-name.ico, member-name.gif,* or *member-name.png.*
- WEBPDF - Contains pdf files. It is referenced by *member-name.pdf.*

Dataset Attributes

```
IFO.MTGY.WS.WEBCSS                      PO-E  VB       4092  32740
IFO.MTGY.WS.WEBHELP                     PO-E  VB       4092  32740
IFO.MTGY.WS.WEBHTML                     PO-E  VB       4092  32740
IFO.MTGY.WS.WEBIMAGE                    PO-E  VB      32654  32658
IFO.MTGY.WS.WEBJS                       PO-E  VB       4092  32740
IFO.MTGY.WS.WEBPDF                      PO-E  VB      32654  32658
IFO.MTGY.WS.WEBREXX                     PO-E  VB        255  32760
```

7.1.3. User sessions

Users are validated at initial connection time using RACF, ACF2, or TSS. ICE Multi-Factor Authentication is also used to provide an additional level of security before access to ICE data and functionality is available.

Each session is maintained until the user logs out or until the idle timeout limit is reached.

Once the user session is established, the main page is displayed. The user may select from the list of available functions (Sidebar). When a function is selected, a related request to execute a REXX script is sent to the Web Server. The Web Server, in turn, selects an available TSO/E server address space and forwards the request, along with input data from the web page and any user session data.

The TSO/E server address space processes the request and returns its response data and updated user session data to the Web Server. The Web Server will return the response to the user.

The response may consist of HTML generated directly by the REXX script, or the response may use an HTML member (a template) from WEBHTML with server resolved symbolic substitution of values generated by the REXX script.

Each time the user initiates a function that requests the execution of a REXX script, the script execution process repeats itself. There is no fixed relationship between the user and the TSO/E server address space. Each user request can run in whichever TSO/E server address is available at the time.

7.1.4. Server Management

The TSO/E server runs as a started task and is started and stopped by the Web Server. When the Web Server starts, it will start at least one of these TSO/E servers based on configuration values. When the Web Server is stopped, it will stop all existing TSO/REXX servers that are still active. There are a number of configuration values related to the TSO/E servers that determine how each server is managed.

- srid – specifies the Web Server id (and also the cross-memory pipe name).
- stcname – specifies the name of the TSO/E server started task.
- stcmin – specifies the minimum number of TSO/E servers that should be running.
- stcmax – specifies the maximum number of TSO/E servers that should be running.
- stcidle – specifies how long (in seconds) an extra TSO/E server above the minimum can be idle before it is stopped.
- stcuser – specifies the STC userid to be used by the TSO/E server started task. This is used to validate the cross-memory connection from the TSO/E server to the Web Server.

At Web Server start, it will start the minimum number of TSO/E server address spaces. The format of the start command is:

S *stcname.sridnn*,TSID=*sridnn*

where “stcname” is derived the configuration values, “srid” is the id of the Web Server, and “nn” is a server id number starting from 01.

7.1.5. Server ParmLib Member

A sample NEZWEBxx Parmlib member is distributed in install PARMLIB(NEZWEB00). See the sample contents below:

```
*--------------------------------------------------------------------*
*
* ICE WEB SERVER PARMS
*
* THIS PARM MEMBER IS READ BY BOTH THE ICEDIRECT WEB SERVER TASK
* AND ANY TSO/E STARTED TASKS.
*
*--------------------------------------------------------------------*
*
SERVER-ID=??????            WEB SERVER ID (REQUIRED, MAX 6)
*
DS-PREFIX=????.??           WORKING DATASET PREFIX (REQUIRED MAX 12)
LOG-RETAIN=1                DAYS TO RETAIN LOG DATASETS (DEFAULT 1)
*
TCP-NAME=TCPIP              TCP/IP STACK NAME (DEFAULT TCPIP)
WEB-PORT=8200               WEB SERVER CONNECTION PORT (REQUIRED)
HTTPS-ONLY=N                FORCE HTTPS CONNECTIONS (DEFAULT N)
WEB-TIMEOUT=10              IDLE WEB USER TIMEOUT (DEFAULT 10 MINUTES)
*
WEB-ERROR-LIMIT=10          ERRORS BEFORE IP ADDRESS QUARANTINED
*                           (DEFAULT 10)
WEB-QUARANTINE=30           TIME AN IP ADDRESS IS IN QUARANTINE
*                           (DEFAULT 30 MINUTES)
*
STC-NAME=??????             TSO/E STC NAME (REQUIRED MAX 8)
STC-TIMEOUT=3               IDLE TSO/E STC TIMEOUT (DEFAULT 3 MUNUTES)
*
TSO-VBUFSIZE=256            REXX VARIABLE POOL SIZE (DEFAULT 256K)
TSO-HTMLSIZE=4096           REXX HTML BUFFER SIZE (DEFAULT 4096K)
*
IFO-NAME=IFOM               SPECIFY THE IFOM NAME (DEFAULT IFOM)
IFO-DEBUG=N                 IFO DEBUG OPTION (DEFAULT N)
*
STOP-ON-LOGOUT=Y            STOP USER'S TSO STC AT LOGOUT (DEFAULT Y)
*
DEBUG=N                     DEBUG OPTION (DEFAULT N)
TSO-VERBOSE=Y               TSO VERBOSE OPTION (DEFAULT Y)
TSO-DEBUG=N                 TSO DEBUG OPTION (DEFAULT N)
*
CODEPAGE=1047               Z/OS CODE PAGE (DEFAULT=1047)
```

7.1.6. CSP Violation Report Options

By default CSP Violation Reports are written to a file defined by the report-uri CSP Directive. It is anticipated that in the future (it had been in the planning stages for a long time) browsers will support both it and the CSP report-to Directive. The configuration option CSP-REPORT-TO is in anticipation of this future update. Currently (4/21) browsers generally do not support report-to, therefore a decision to use CSP-REPORT-TO should not be taken without considering the number of CSP errors that may result from browsers that do not provide FULL support for both.

7.1.7. Audit Log File

The Web Server and TSO STC's will generate audit log files recording information about the server activities. The audit log datasets are created using the dataset prefix defined by the DS-PREFIX parameter in the PARMLIB member. A new log dataset is created each time the Web Server or TSO STC is started. They are automatically cleaned up based on value of the LOG-RETAIN parameter in the PARMLIB member.

7.1.8. Error Report

The Web Server and TSO STC's can also generate error reports when an unexpected error occurs. The error report (EREP) datasets contain diagnostic information related to the detected error. These datasets are created using the dataset prefix defined by the DS-PREFIX parameter in the PARMLIB member. These datasets are not automatically cleaned up. If these datasets are being created, contact NewEra Technical Support for assistance. Please do not delete the file prior to necessary problem resolution.

The Web Server will automatically suppresses generating error reports if the errors are happening fast and furious. If the server is under attack, it will not generate thousands of report files. The error report generation is automatically restored after a period of time when the error rate subsides and no new errors of a similar type are encountered.

Web Error Report are generated under your_hlq.WS.WSRV.WEBREP.*

7.1.9. Error Examples

An error can be generate by using the url line in the browser and typing in some bogus request like:

https://www.myicedirect.com:8201/xxx.rexx

Do that 10 times in a row and get both 10 reports, and quarantined from the web server. The quarantine time is 3 minutes by default or as specified during installation.

Web Error Reports are also generated when:

- Run a script without being logged on.
- Try to access non-existent web content (pdf, images, css, js, etc)
- Violate CSP policy
- Mismatch CSRF
- Run a script, while one is already running
- Attempts to modify a <a href:// link

Certain integrity errors may generate the follow message display and log the user off the system.

- Web server related Audit/Error datasets are named as follows:

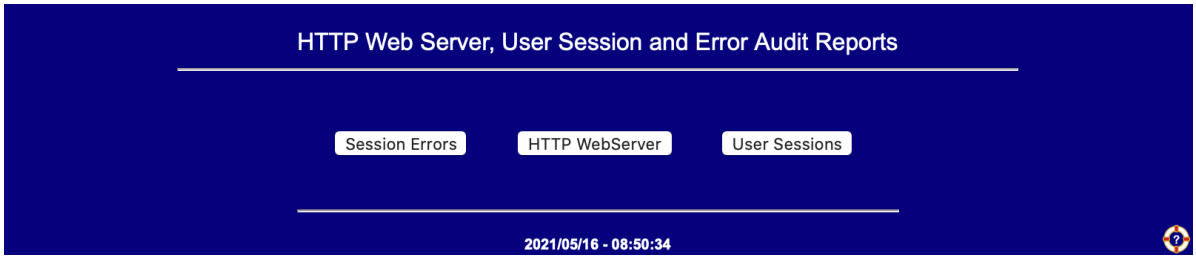
  DS-PREFIX. SERVER-ID.LOG.Dyymmdd.Thhmmss
  DS-PREFIX. SERVER-ID.EREP.Dyymmdd.Thhmmss

- TSO task related Audit/Error datasets are named as follows:

  DS-PREFIX. SERVER-IDnn.LOG.Dyymmdd.Thhmmss
  DS-PREFIX. SERVER-IDnn.EREP.Dyymmdd.Thhmmss
  "nn" is a sequence assigned to each TSO STC started, i.e. 01,02,03,...

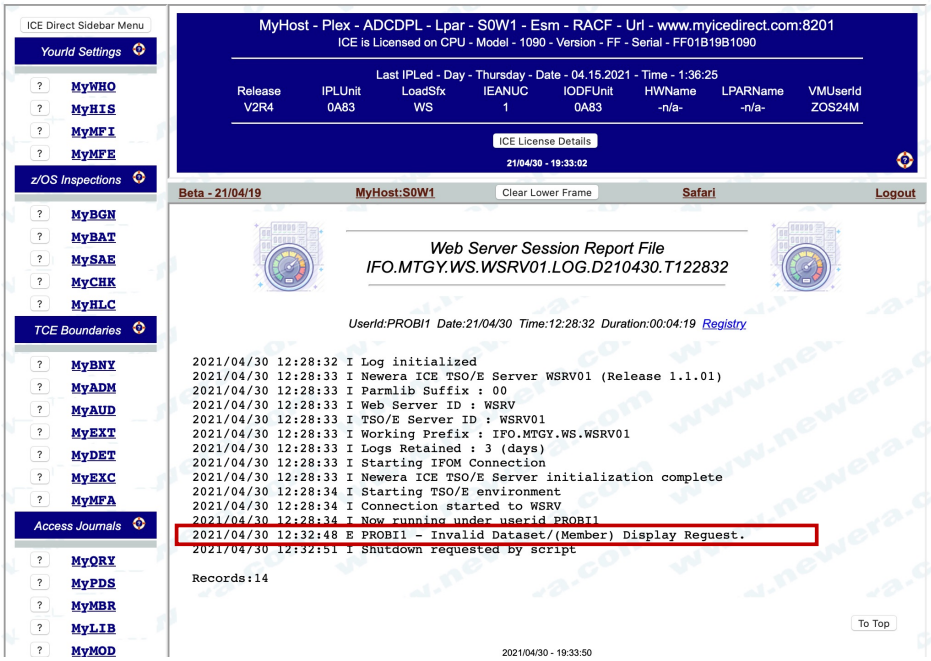
7.1.10. Accessing Error Reports

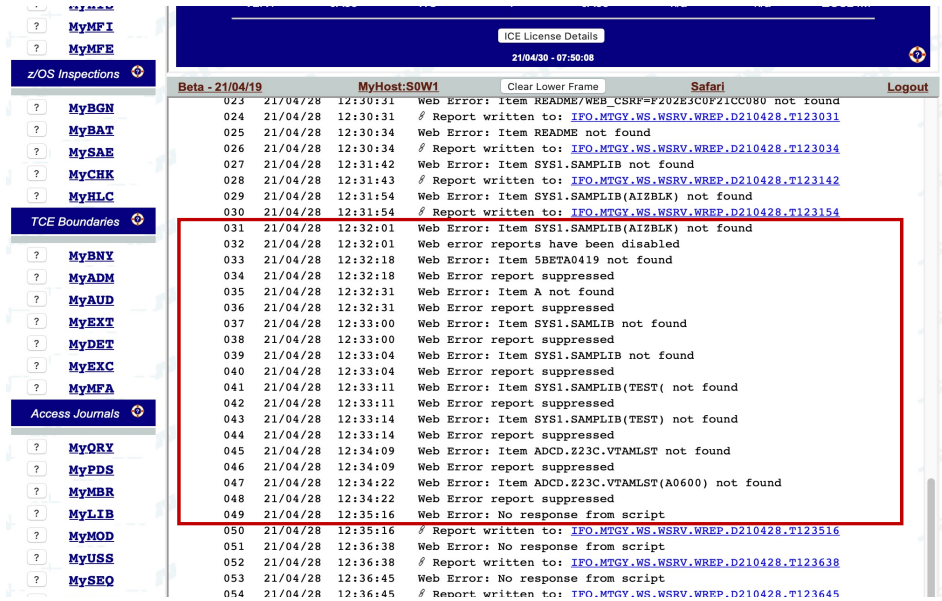
Error and Audit Reports are accessed from the following panel:



To reach the panel select ‘MyHOST’ from the crossbar then ‘click’ ICE License Details. Next ‘click’ Server Reports.

7.1.1. Sample Server and Error Reports





7.1.2. SMP/E Installation

SMP/E install is required for both the ICE Primary Task (IFO) and the Web Server. In addition to the $NOTESMP Dataset you will find these JOBs in IFOHLQ.INSTLIB. These must all be executed. See the Image FOCUS User Guide for Detailed Installation Instruction.

Primary Task Includes:

$SM10AL1
$SM10AL2
$SM10AL3
$SM10BLD
$SM20CSI
$SM30INI
$SM40DDF
$SM50REC
$SM60APL
$SM70ACC

Web Server Includes:

$SM80AL1
$SM80BLD
$SM80DDF
$SM80REC
$SM82APL
$SM82CPY
$SM84ACC

8.Installation Quick Reference Guide

To install the ICEDirect option to the Integrity Controls Environment (ICE), for access to the Inspection logs created by Image Focus (IFO) and the Journal records created by The Control Editor (TCE), these steps need to be completed in addition to a complete install of the ICE products.

ICEDirect also can provide 2 additional options at this time. They are located under the Visual Stack link. They do require additional license keys. They are z/OS Visual and RACF Visual. All option will be installed following the steps detailed in the document, but each option will be allowed access to with a separate license key.

These Datasets for the ICE products must have been created.

```
ICE Datasets:
$SM10AL1
$SM10AL2
$SM10AL3
$SM10BLD
$SM20CSI
$SM30INI
$SM40DDF
$SM50REC
$SM60APL
$SM70ACC

These additional datasets are required for ICEDirect.
Web Server Datasets:
$SM80AL1
$SM80BLD
$SM80DDF
$SM80REC
$SM82APL
$SM82CPY
$SM84ACC
```

After running all the above jobs, and successfully installing the ICE products continue with these steps.

In addition to the normal IFOM and IFOS address spaces, ICEDirect will require 2 new address spaces, IFOWEBM and IFOWEBS. Initially these should be configured the same as the IFOM and IFOS within the ESM (RACF, ACF2 or TSS) definitions.

The security for each ICEDirect USER is determined by that individual's security setting within the ESM on the LPAR that is hosting ICEDirect. This requires each user to logon to ICEDirect with a valid TSO USERID and PASSWORD, validated by the ESM at logon.

Create a member in your IFOHLQ.REGISTRY Dataset named LICENSE.

Placed the attached license cards into your IFOHLQ.REGISTRY Dataset with a Member name of LICENSE.

Next Edit your IFOHLQ.PARMLIB dataset member as described below.

Configuring NEZWEBxx MEMBER.

Update the Member NEZWEB00 in the IFOHLQ.PARMLIB Dataset with a valid WEB-PORT for the Web Server.
WEB-PORT=???? WEB SERVER CONNECTION PORT (REQUIRED)

.

Update the NSEJRNxx Member in your IFOHLQ.PARMLIB and make sure users are set up as TCEPRIME and TCEADMIN.

```
TCEPRIME tsouserid
TCEADMIN (tsouserid,tsouserid,tsouserid)
```

These TSOUSERIDs will be the PRIMARY users of ICEDirect. Other user maybe allowed access to the ICEDirect application with restrictions.

Add the following in your NSEENSxx Member in your IFOHLQ.PARMLIB Dataset for each user who will be signing onto the ICE Webserver:

```
ACTION MFIPERMT(tsouserid) METHOD(NOEMAIL) OBJ(ALL) SCOPE(REPORT)
*MFIPREFIX TST1
MFIPREFIX %T%2
ACTION .END
```

The *MFIPREFIX TST1 is note that present the personal PIN value for each user in clear text. It is a representation of the encrypted MFIPREFIX %T%2 value. The MFIPREFIX will be required at logon to ICEDirect as a second confirmation of the user's identity. The 4-digit value serves as a prefix and must be combined with a 4-digit token generated by the ESM and displayed to the user to serve as a valid value and allow the logon request to be completed.

Each user can set their own value for this PIN once signed into ICEDirect. That new PIN value will be encrypted and updated into this

member. The *MFEPREFIX value will not be updated by ICEDirect.

Move over to your SYSTEM Proclib

IFOM
IFOS
IFOWEBM
IFOWEBS

Then follow the instructions below:

Issue the following setprog command for the new IFOHLQ.WS.LOAD dataset before starting IFOM & IFOWEBM.

SETPROG APF,ADD,DSNAME=IFOHLQ.WS.LOAD,volume=xxxxxx

Start IFOM and then start IFOWEBM

Log onto the Web Server using the PORT you set up in your NEZWEB00 Member: **WEB-PORT=???? WEB SERVER CONNECTION PORT**

http://XX.XXX.XXX.XX:???? or https://XX.XXX.XXX.XX:????

As with IFOS starting when a user has successfully logged on to ICE, a IFOWEBS address will be created for each user who successfully logs into ICEDirect.

Appendix "A" – Server Certificates

Secure servers require the ability to retrieve the certificate that is associated with a particular server, along with the ability to perform operations with the private key of the server, such as establishing an SSL session.

This LINK is to presentations on Certificates hosted by Mr. Charles Mills, a known authority, they will prove helpful to those needing a tutorial on certificates and their installation:

https://www.newera-info.com/CM1.html

This LINK is to a presentation "What Keyring? What certificates? All I know is TLS doesn't work!" hosed by Wai Choi CISSP, Senior Software Engineer, IBM Poughkeepsie.

https://www.newera-info.com/WC1.html

In addition, this narrative from IBM on step by step specifics of setting up certificates using RACF should also prove to be enlightening:

- Assume that you have a secure server which has a distinguished name of `OU=Inventory,O=XYZZY,C=US`
- and a domain name of `xyzzy.com`
- and the server executes on z/OS with the user ID INVSERV.

The steps to implement a server certificate are:

1. Generate a self-signed certificate for the server. This certificate is associated with the user ID that is associated with the secure server.

```
RACDCERT ID(INVSERV)
         GENCERT
         SUBJECTSDN(CN('xyzzy.com')
                    OU('Inventory')
                    O('XYZZY')
                    C('US'))
         WITHLABEL('Inventory Server')
```

   Note: Some SSL applications require that the common name (CN) be equal to the domain name.

2. Create a certificate request to send to your chosen certificate authority. The certificate request that is being created is based on the certificate that was created in the previous step. Place this certificate into the data set `'MARKN.INVSERV.GENREQ'`.

```
RACDCERT ID(INVSERV)
```

```
                GENREQ(LABEL('Inventory Server'))
        DSN('MARKN.INVSERV.GENREQ')
```

3. Send the certificate request to the certificate authority. The certificate request is in base64-encoded text. Typically, the request is sent to the certificate authority by using "cut and paste" to place the certificate request into an e-mail that is sent to the certificate authority.

4. The certificate authority validates the certificate. If the certificate is approved by the certificate authority, it is signed by the certificate authority, and returned to the requestor.

5. Receive the returned certificate into a data set (for example,`'MARKN.INVSERV.CERT'`). The returned certificate is in base64-encoded text. This can be done with "cut and paste", FTP, or other techniques that might be available.

6. Replace the self-signed certificate with the certificate signed by the certificate authority. Note that the certificate is only replaced if the user ID that is specified as the ID value on the RACDCERT ADD command is the same user ID that was specified when the certificate was created. If the ID is not the same, then the certificate is added anew.

```
RACDCERT ID(INVSERV)
       ADD('MARKN.INVSERV.CERT')
       WITHLABEL('Inventory Server')
```

7. Connect the certificate to INVSERV's existing key ring and mark it as the default certificate.

```
RACDCERT ID(INVSERV)
              CONNECT(LABEL('Inventory Server')
       RING(RING01)
       DEFAULT)
```

8. Assuming the chosen certificate authority certificate has already been added to RACF under CERTAUTH with the label of `'External Inventory CA'`, connect it to the key ring as well. This completes the certificate hierarchy from root to inventory server.

```
RACDCERT ID(INVSERV)
      CONNECT(CERTAUTH LABEL('External Inventory CA')
      RING(RING01))
```

9. Give user INVSERV permission to read its own key ring by administering a profile in either the FACILITY or the RDATALIB class.

- When using the FACILITY class:

- ```
  RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
  PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(INVSERV)
  ACCESS(READ)
  ```
  - If the FACILITY class is not already active, activate and RACLIST it:
    `SETROPTS CLASSACT(FACILITY) RACLIST(FACILITY)`
  - If the FACILITY class is already active and RACLISTed, refresh it:
    `SETROPTS RACLIST(FACILITY) REFRESH`

- When using the RDATALIB class:

- ```
  RDEFINE RDATALIB INVSERV.RING01.LST UACC(NONE)
  PERMIT INVSERV.RING01.LST CLASS(RDATALIB) ID(INVSERV)
  ACCESS(READ)
  ```
  - If the RDATALIB class is not already active, activate and RACLIST it:
    `SETROPTS CLASSACT(RDATALIB) RACLIST(RDATALIB)`
  - If the RDATALIB class is already active and RACLISTed, refresh it:
    `SETROPTS RACLIST(RDATALIB) REFRESH`

10. Configure INVSERV's software to use `RING01` for SSL. For example, for z/OS HTTP Server, set the `keyFile`directive to `KeyFile RING01 SAF`.

Appendix "B" – Common Browser Insecurities

All z/OS access points require maximum security. In addition to the 'Best Practice' recommendations – z/OSMF, AT-TLS, ESM, and MFI – described herein, The ICEDirect Server supports the following methods of mitigation against Common Browser vulnerabilities.

Cross Site Request Forgery (CSRF)

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy defined in the site CSP, which is designed to prevent different websites from interfering with each other.

Mitigation

ICEDirect mitigates this threat using both session and anti-CSRF tokens generated by the server. The session token is known and stored in the browser while the anti-CSRF token is known to the each unique HTML page returned to the browser and therefore the Document Object Model. Each is validated with each request and remains valid for the duration of the users session. While these defenses are considered adequate they are made more so from a shorter user session time-out. User session "Time-Out" is a settable value at installation.

Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Mitigation

The Content Security Policy used in ICEDirect, described in the Security Section, is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware. The specific policy delivered by the Server to the browser with each returned request is shown here.

```
Content-Security-Policy: default-src 'none';  script-src 'self' 'nonce-@WEB_RANDOM@'; img-src 'self'; style-src 'self';  base-uri 'self';  form-action 'self';  frame-ancestors 'self';  frame-src 'self';  child-src 'self'; object-src: 'self'
```

Cookie Misuse Management

In addition to direct injections into the request stream session cookies that link the server to a specific user session instant may be compromised or stolen. If successful, the cookie is then used by the attacker to impersonate the user at the original site.

Mitigation

Since it is not necessary for a browser supporting ICEDirect to read javascript inline the following processing model has been adopted. With each request the server returns the Security String shown below where "Secure;" is an installation option. When the option is NOT set the browser will honor both HTTP and HTTPS replies. When the option is set the browser will only honor HTTPS replies.

Set-Cookie: sessToken=@token@; SameSite=Strict; **`HttpOnly`**; **`Secure`**;

- sessToken

The session token is randomized dynamically generated value inserted directly by the server and sent to the browser remaining valid for the duration of the user session.

- Secure Attribute

The **`Secure`** cookie attribute instructs web browsers to only send the cookie through an encrypted HTTPS (SSL/TLS) connection. This session protection mechanism is mandatory to prevent the disclosure of the session ID through MitM (Man-in-the-Middle) attacks. It ensures that an attacker cannot simply capture the session ID from web browser traffic. Forcing the web application to only use HTTPS for its communication (even when port TCP/80, HTTP, is closed in the web application host) does not protect against session ID disclosure if the **`Secure`** cookie has not been set - the web browser can be deceived to disclose the session ID over an unencrypted HTTP connection. The attacker can intercept and manipulate the victim user traffic and inject an HTTP unencrypted reference to the web application that will force the web browser to submit the session ID in the clear.

- HttpOnly Attribute

The **`HttpOnly`** cookie attribute instructs web browsers not to allow scripts (e.g. JavaScript or VBscript) an ability to access the cookies via the DOM document.cookie object. This session ID protection is mandatory to prevent session ID stealing through XSS attacks. However, if an XSS attack is combined with a CSRF attack, the requests sent to the web application will include the session cookie, as the browser always includes the cookies when sending requests. The **`HttpOnly`** cookie only protects the confidentiality of the cookie; the attacker cannot use it offline, outside of the context of an XSS attack

- SameSite Attribute

`SameSite` allows a server to define a cookie attribute making it impossible for the browser to send a cookie along with cross-site requests. The main goal is to mitigate the risk of cross-origin information leakage, and provides some protection against cross-site request forgery attacks.

Denials-Of-Service (DoS)

An attack meant to shut down a Web Server or Network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Mitigation

Auto-Quarantine of Web Server IP Address is provided for a user defined maximum consecutive recognized errors. Once the maximum is reached two actions are take. First, the recording of error events is suspended following the writing of a final message indication that the suspension (for the offending URL only) is imminent. Second, the offending URL is placed on a temporary "Black List" and in-turn automatically denied service until automatically removed from the "Black List". Duration of these action is controlled by a the Web Server parmlib setting - WEB_QUARANTINE.

Man-in-the-Middle attacks - protocol downgrade attacks and cookie hijacking

Websites that prefer HTTPS will generally still listen for connections over HTTP in order to redirect the user to the HTTPS URL. Left unchecked this redirect may be exploited and the user redirected with malicious intent.

Mitigation

HTTP Strict-Transport-Security (HSTS) directs the browser never connect to ICEDirect using HTTP and automatically convert all attempts using HTTP to HTTPS requests instead. This primary and subdomain translation is activated, in the browser, with the first access to an ICEDirect site, remaining effective for 2 years a default term reset to 2 years with each subsequent site access.

Browser and Content Delivery Networks (CDN) caching

HTML pages and objects (images, scripts, etc.) may be cached in the browser and/or a content delivery network (CDN) server. While this caching facilitates performance it also may expose information remaining in local/remote cache.

Mitigation

A Cache-Control Directive is used to protect both HTML Pages and Other Objects. For HTML pages it is set "no-cache". For all Other Objects it is set "private, max-age=7200; (2 hours)". The latter (private) to indicate that the cache is only shareable between the directly communicating server and browser and no other network node for limited period, 2 hours, after which it is removed.

Use of Autofill

Commonly used Autofill can create and exposure when it "Remember" a user's logon credential this allowing an imposter to assume an identity in the absence of its owner.

Mitigation

Multi-Factor ICE (MFI) presents an additional, multi-factor, challenge to users as they attempt to login and authenticate with ICEDirect. The challenge may be presented in configurable forms including one that allows the user to registrar a private PIN to be concatenated with real-time token material generated at presented at the point of the challenge.

Failure to Logout

A users failure to formally logout will create an exposure when an imposter "takes their seat" and "authenticated identity" and continues an active session.

Mitigation

User Session and Started Task "time outs", configurable duration options, are used to automatically log OFF inactive user and/or automatically CANCEL an inactive session Started Task. Short durations are considered a Best Practice.

Direct Script Injection

This occurs when users enter into an otherwise assigned TEXT field HTML/JAVA character syntax and submit it embedded with a normal request. The server not being able to distinguish this Injection from a normal request would without mitigation process the request and reply accordingly.

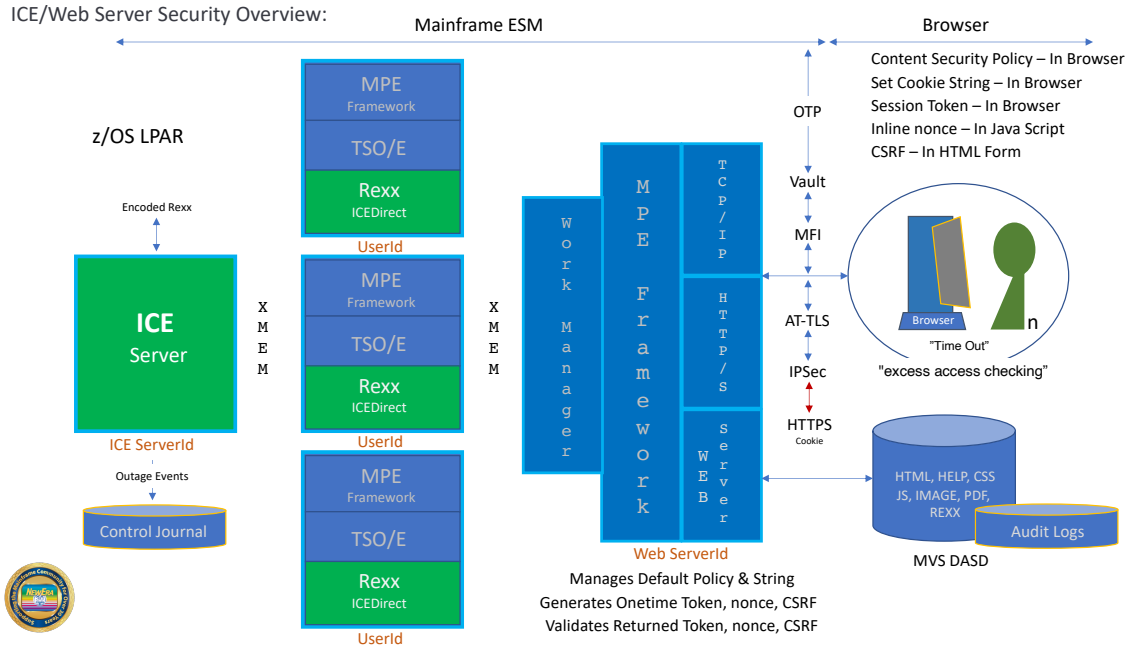
Mitigation

The ICEDirect Server supports a filter/checklist of common HTML/JAVA activation characters – currently set - '< & %'. It filters each request string received against the list. If an offending character is discovered, the request is denied, an appropriate message displayed, an Error Message written to the Server Log and the user is logged off.

APPENDIX "C" – Security Attributes - An Overview

- Environment

The Integrity Controls Environment (ICE) is a purpose-built, proprietary z/OS software utility, developed and maintained by NewEra Software. It contains NO public domain source code, supports only two primary applications: Image FOCUS and The Control Editor. Its installation package is digitally signed with an encoded HASH. This "Digital Key" is asynchronously delivered electronically and is used to verity that the package was not tampered with prior to installation. All components of an ICE install, including its integrated and uniquely adapted version of the MainTegrity Processing Environment (MPE) Web Server, are programmatically *Closed* to all others.



- Network

Domain: Uniquely defined Socket (ipaddress:port)
Firewall: Open to Domain from listed URLs
Security: HTTPS/AT-TLS (PAGENT) specific to a Domain
PROFILE SAF: PORTACCESS, NETACCESS - Permitted to PORT and Domain

- z/OS Login

z/OSMF – External Security Manager, Authentication of User Credentials
ICEDirect Welcome - Identification prior to Authentication with z/OS & ICE
Support HTTP or HTTPS only depending on "Set-Cookie" option selection
Native – External Security Manager, Authentication of User Credentials

- Tokens

Session – JS_Script Nonce, Session Cookie, HTML Token
CSP*: Content Security Policy
Security String*: HttpOnly; Secure; (where Secure is optional assuring HTTPS exchange)

- ICEDirect Login

Multi-Factor ICE (MFI), Authentication User - Master Registry/Encrypted PIN Vault
Passticket (OTP) Generation: ESM
OTP Delivery: By Email or Inline

- NSIMxxx – A Rexx Application

Use of Nonce:
<script nonce="some_random_value”>
*For example, <script nonce="B2F43454A7B34640">
Use of Hidden Input:
<input type="hidden" id="WEB_CSRF" name="WEB_CSRF" value=" @WEB_CSRF@">
*For example, <input type="hidden" id="WEB_CSRF" name="WEB_CSRF" value="X1C69041W6UI8451">
Encoded: All “Rexx Text” is delivered digitally encoded and dynamically decoded during called for processes.

- Web Host – Web Server Address Space

External Security Manager, Authentication of the User
System Authorization Facility - SAF
Derives, Returns and Authenticates:

1. JS_Script Nonce = @WEB_RANDOM@
2. Cookie sessToken= *unique-token*
3. HTML Token = @WEB_CSRF@"

- Web Host – Rexx Address Spaces

External Security Manager, Re-Authentication of the User Credential
System Authorization Facility – SAF

- Idle Timeout of user sessions

Customer defined (default of 10 minutes)
New login forced after timeout

- Auto-Quarantine of Client IP Address

Customer defined maximum consecutive errors before quarantine
Customer defined duration in quarantine

- Content-Security-Policy

default-src 'none'; script-src 'self' 'nonce-@WEB_RANDOM@'; img-src 'self'; style-src 'self'; base-uri 'self'; form-action 'self'; frame-ancestors 'self'; frame-src 'self'; child-src 'self'; object-src: 'self'

- Security String

Set-Cookie: httpsCheck=”random-number”; SameSite=Strict; HttpOnly; Secure; (Optional)

- Cache Control Directives

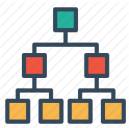
A server provided default HTTP header that holds directives for caching both browser requests and server responses. For HTML objects this directive is set: no-cache. For all others, this directive is set: private, max-age=7200; (2 hours). Will prevent/limit Content Delivery Networks (CDN) caching.

- HTTP Strict-Transport Security (HSTS) Directive

This default directive informs the browser that it should never connect to ICEDirect using HTTP & should automatically convert all attempts using HTTP to HTTPS requests instead. HTTP connections are set: max-age=0. HTTPS connections are set: max-age=63072000; (730 days) includeSubDomains. Prevents Man-in-the-middle (MITM) attacts.

Appendix "D" – Application Icons

ICEDirect uses a number of Graphical Icons to direct attention to functions and denote various analytic findings and related severity. They include the following:

	Link to an Image FOCUS Inspection Log/Report
	Link to a Chart showing linked segments to Inspection Detail
	Link to a Chart showing linked bars to Inspection Detail
	Link to a Chart showing linked segments to Inspection Detail
	Image FOCUS Background Sysplex Inspection and Analysis
	Image FOCUS ICEBATA Inspection and Analysis
	Image FOCUS IPLCheck Inspection and Analysis
	SAEBATA Inspection and Analysis

	Launch a Started Task
	IBM HealthChecker for z/OS
	Interval Detector Settings
	Email Recipient List
	Inspection Baseline Analysis
	Compare and Contrast Configuration Elements
	Inspector Link to Control Journal

	CERTVFY – Warns of Uncertified Dataset Versions.
	Used to indicate a Control Category Definition
	Used to indicate the Addition of a Control Structure
	Used to indicate the Deletion of a Control Structure
	AUTHVFY – Provides supplemental in an LPAR MFA Protections
	ICE and z/OS Configuration Datasets and Members
	Event of Serious Concern Detected - Error
	Event of Serious Concern Detected - Warnings
	Event of Moderate Concern Detected - Notice

	Informational Event Detected
	Indicates Email Delivery of MFI or MFE OTP (Token)
	Indicates NoEmail of OTP (Token) instead Inline Token Suffix
	Link to an uninspected Image Configuration Element
N/A	Indicates that a named function/service is Not Available
	Link to ICEBATA/SAEBATA Inspection and Blueprints
	Indicates Image FOCUS Message or Control Editor Event Filters
	Used to Denotes Web Server Reports and Log Files

	Used to Denote Content Security Policy (CSP)
	Used to indicate Compliance Interface and Reports
	Denotes default event detection and alert notification
	Denotes IODF – IOCP, SWCP and OSCP
	Denotes IODF/IOCP Channel Path IDs (CHPID)
	RACF SETROPTS Analytics

	Indicates Roles and Access Rights

Technical Support Contact Information

NewEra Software, Inc.

Mailing Address:

18625 Sutter Boulevard, Suite 950
Morgan Hill, CA 95037

Phone:

(408) 520-7100
(800) 421-5035

FAX:

(888) 939-7099

Email Address:

support@newera.com

Web Site:

https://www.newera.com

Technical Support:

24 hours a day, 7 days a week
1-800-421-5035
support@newera.com