

A Simple, Straightforward Way to Get What You need from ICE

“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: 2023-07-01

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. These videos are instructive and helpful to understanding the many features of both ICEDirect and the Integrity Controls Environment.

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

2. Table of Contents

Contents

1. YOUTUBE	2
2. TABLE OF CONTENTS	3
3. WHAT IS ICEDIRECT?	5
4. SETTING UP ICEDIRECT	5
4.1.1. SERVER INSTALLATION	5
4.1.2. USER REGISTRY	5
4.1.3. GLOBAL REGISTRY.....	5
4.1.4. SERVER SECURITY – YouTube #5.....	6
4.1.5. CONTENT-SECURITY-POLICY (CSP).....	8
4.1.6. OPERATING FROM A z/OSMF LINK – YouTube #10	9
4.1.7. OPERATING FROM A STANDALONE BROWSER.....	11
4.1.8. USER AUTHENTICATION – YouTube #5.....	12
<i>Authentication with z/OS.....</i>	<i>12</i>
4.1.9. AUTHENTICATION WITH ICE.....	12
5. PATIENT ZERO - FIRST ICEDIRECT ADMINISTRATOR – YOUTUBE #0	15
5.1.1. LOGGING IN – YouTube #5	16
5.1.2. USING THE PREFIX	17
5.1.3. ICEDIRECT MAIN IFRAME SET– YouTube #5	18
5.1.4. SIDEBAR	18
5.1.5. SELECTION MARKER.....	18
5.1.6. DIRECTS IFRAME.....	19
5.1.7. RESULTS IFRAME	20
5.1.8. THE CROSSBAR	22
<i>Current Release Information</i>	<i>22</i>
<i>MyHOST.....</i>	<i>22</i>
<i>Clear Lower IFrame</i>	<i>22</i>
<i>Browser Details.....</i>	<i>23</i>
<i>MyAPI.....</i>	<i>23</i>
<i>Logout.....</i>	<i>23</i>
6. ICEDIRECT APPLICATIONS – EACH BRIEFLY EXPLAINED.....	24
6.1.1. YOURID SETTINGS.....	24
<i>MyWHO – Your ICE User Scope – YouTube #6.....</i>	<i>24</i>
<i>MyHIS – Your ICE Event History – YouTube #6.....</i>	<i>24</i>
<i>MyMFI – Your Multi-Factor ICE Prefix – YouTube #0.....</i>	<i>24</i>
<i>MyPIN – Your Multi-Factor Edit Prefix</i>	<i>24</i>
6.1.2. z/OS INSPECTIONS	25
<i>MyBGN – Image FOCUS Sysplex Background Inspections – YouTube #1.....</i>	<i>25</i>
<i>MyBAT – ICEBATA Inspection Logs and Analysis – YouTube #2</i>	<i>25</i>
<i>MySAE – SAEBATA Inspection Logs and Analysis – YouTube #3.....</i>	<i>25</i>
<i>MyCHK – IPLCheck Inspection Logs and Analysis – YouTube #4.....</i>	<i>25</i>
<i>MyHLC – IBM z/OS Health Checker Reporting – YouTube #7.....</i>	<i>25</i>
6.1.3. CONTROL BOUNDARIES.....	26
<i>MyBNY – Access or Update ICE Intercept Point and Boundaries.....</i>	<i>26</i>
<i>MyADM – Assign/Unassign ICE Administration Credentials.....</i>	<i>26</i>
<i>MyAUD – Assign/Unassign ICE Auditor Credentials.....</i>	<i>26</i>
<i>MyEXT – Global Control over External Notifications Settings – YouTube #8</i>	<i>26</i>

<i>MyDET – Global Control over Interval Detector Settings – YouTube #8</i>	26
<i>MyEXC – Global Control over Journal Event Exclusions – YouTube #8</i>	26
<i>MyMFA – Overview/Control over of ICE MFA – MFI/MFE – YouTube #9</i>	26
<i>MyREG – User Registry Access and Management</i>	27
6.1.4. JOURNAL ACCESS.....	28
<i>MyQRY – Ad Hoc Queries/Reports to/from the Control Journal</i>	28
<i>MyXXX – Directed Queries/Reports to/from the Control Journal</i>	28
7. THE WEB SERVER EXPLAINED	29
7.1.1. SERVER OVERVIEW – YOUTUBE	29
7.1.2. SERVER DATASETS.....	31
<i>Dataset Attributes</i>	31
7.1.3. USER SESSIONS.....	31
7.1.4. SERVER MANAGEMENT	32
7.1.5. SERVER PARMLIB MEMBER.....	33
7.1.6. CSP VIOLATION REPORT OPTIONS.....	33
7.1.7. AUDIT LOG FILE.....	33
7.1.8. ERROR REPORT.....	34
7.1.9. ERROR EXAMPLES	34
7.1.10. ACCESSING ERROR REPORTS	35
7.1.1. SAMPLE SERVER AND ERROR REPORTS.....	36
7.1.2. SMP/E INSTALLATION	37
<i>Primary Task Includes:</i>	37
<i>Web Server Includes:</i>	37
8. INSTALLATION QUICK REFERENCE GUIDE	38
APPENDIX “A” – COMMON SECURITY REQUIREMENTS	41
APPENDIX “B” – SERVER CERTIFICATES	42
APPENDIX “C” – COMMON BROWSER INSECURITIES	45
<i>Cross Site Request Forgery (CSRF)</i>	45
<i>Cross Site Scripting (XSS)</i>	45
<i>Cookie Misuse Management</i>	46
<i>Denials-Of-Service (DoS)</i>	47
<i>Man-in-the-Middle attacks - protocol downgrade attacks and cookie hijacking</i>	47
<i>Browser and Content Delivery Networks (CDN) caching</i>	48
<i>Use of Autofill</i>	48
<i>Failure to Logout</i>	48
<i>Direct Script Injection</i>	49
APPENDIX “D” – SECURITY ATTRIBUTES - AN OVERVIEW	50
APPENDIX “E” – APPLICATION ICONS	53
TECHNICAL SUPPORT CONTACT INFORMATION	59

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. To begin, 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 “B” – 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

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 are prevented from accessing the 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. Review the Appendix “A” - Common Security Requirements, for userid set up.

The Global Registry Dataset should be protected with a security product profile that has a UACC of NONE. Additional security product set up recommendations will follow.

4.1.4. *Server Security – YouTube #5*

The Web Server component of ICEDirect is closed to external contact. 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 no attempt be made to connect to the server before socket security is enabled. The URL for a secure login point would look similar to this:

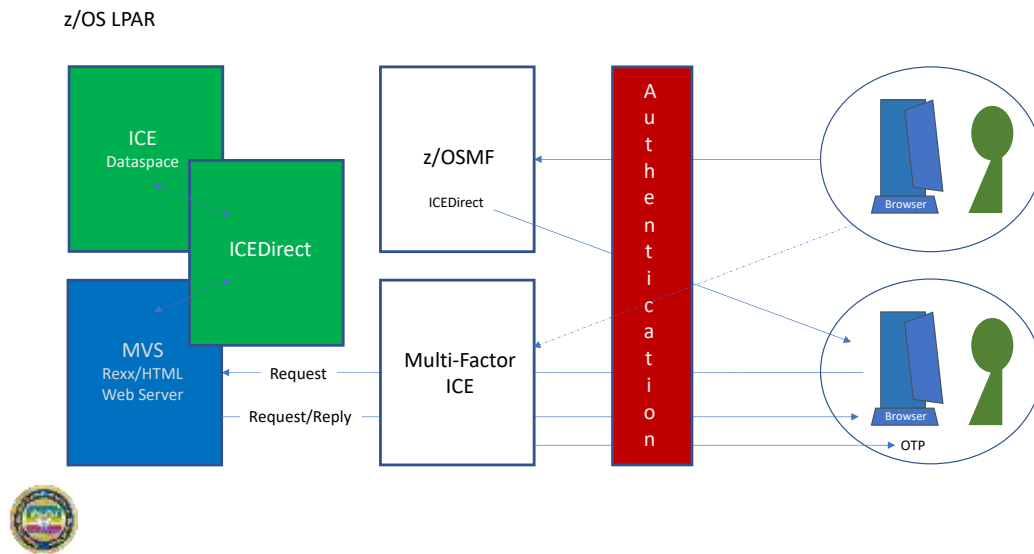
<https://24.234.192.41:8200>

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>

A registered and secured login address may be integrated into the z/OSMF Framework as a Linked Application.

A Simple, Straightforward Way to Get What You need from ICE



4.1.5. *Content-Security-Policy (CSP)*

Content-Security-Policy is the name of an HTTP response header that modern browsers use to enhance the security of documents (or web pages). Internet Explorer (IE) does not support CSP and is therefore not a recommended browser for ICEDirect.

Pages shown by the browser will contain a Content Security Profile (CSP). The CSP will define “Valid Content” as only the 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';

The design rule for ICEDirect is “no inline scripting” however, dynamic objects like Chart.js require inline scripts. To accommodate these exceptions; a unique random “NONCE” is injected by the server into 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 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 elevated protection provided by PAGENT and 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, the TCP/IP stack, and z/OS. There are several access permission layers.

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

Upon proper z/OSMF configuration, individual users will need to be permitted to use z/OSMF and to authenticate with z/OS similar to a TSO logon. To integrate ICEDirect, 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 below.

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

An authorized z/OSMF Administrator can dynamically set up the link once logged onto z/OSMF using the interface panel shown below.

Properties for Link
Use this page to view or modify a link for z/OSMF.

+ Name (maximum 30 characters):
ICE Direct

+ SAF Resource Name Suffix (maximum 220 characters):
IZUOFLT.ZOSMF.LINK, NEZ.COM

+ URL (maximum 4000 characters):
https://www.myicedirect.com:3201/

+ Category
Links

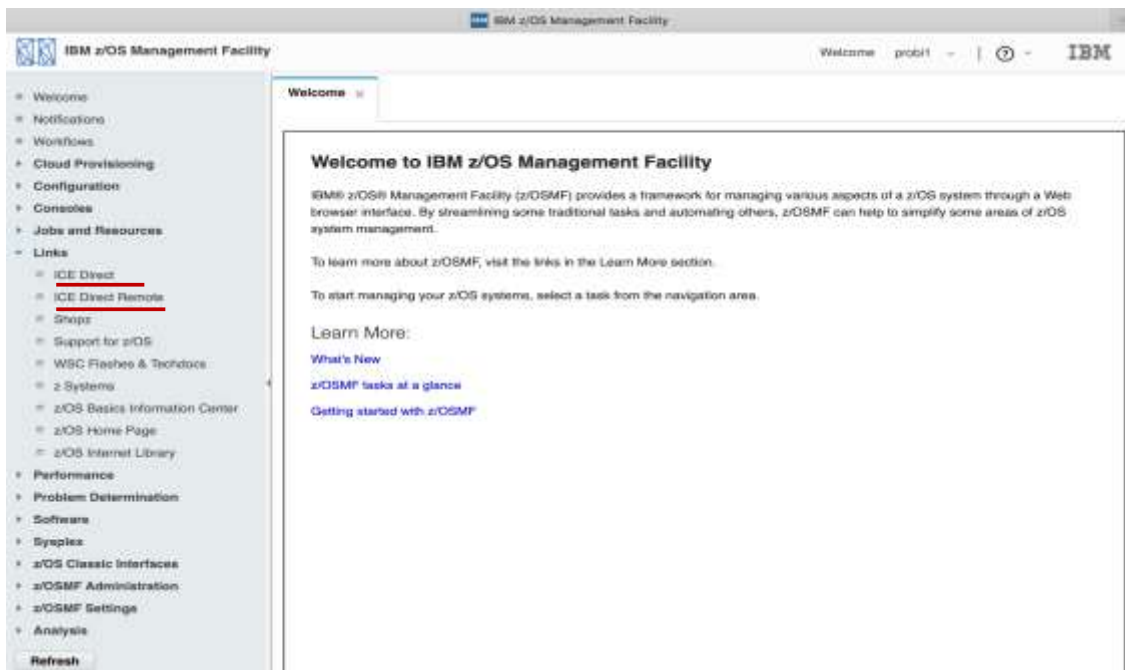
Open link in:
☒ New browser tab or window
☐ New z/OSMF tab

Authorizations

User State	Description
<input checked="" type="checkbox"/> SAF Authorized User	Access to z/OSMF tasks and links is controlled through your security management software.
<input checked="" type="checkbox"/> z/OSMF Authenticated Guest	User is logged into z/OSMF, but is not authorized to perform tasks and has limited access to links.

OK Cancel

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, set up multiple links to allow for the attachment of specific ICEDirect URLs. An example is shown here:



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

profiles. This will achieve the same level of 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 ICEDirect authentication for server access. This is done using the ICE Multi-Factor Interface (MFI) functionality. If this authentication challenge is successful, the ICEDirect “Welcome page” will be displayed.

Browser pages will not contain inline java script, Cascading Style Sheets (CSS), or use 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 and stored/contained in the ICEDirect Server z/OS environment and delivered by “Self”, the ICEDirect Server.

The primary 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 by 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 ICEDirect dataspace from any Internet connected platform.

- Best Practice – Turn off Autofill

When operated as either a z/OSMF LINK or from a standalone browser, it is recommended that browser Autofill function be turned off. If browser Autofill is not disabled, Autofill will store and return userid and password values automatically. This will allow anyone who

operates that computer to masquerade as the last user who logged into z/OSMF and/or ICEDirect both running as z/OS applications.

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
- Environment error while generating a PassTicket

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. This is the “EMAIL” option.
- 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

An ICE authentication failure returns the user to the first level of authentication.

A Simple, Straightforward Way to Get What You need from ICE

An entry is made to the ICE Control Journal for any successful ICEDirect login. An optional email notification can also be sent. Journal entries for successful login would look similar to the following:

```
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. Those entries indicate the user, the date and time of the access attempt, and the reason for the failure.

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

Any user who will be accessing ICEDirect will need a pre-defined ICE authorization profile. To define these profiles, an ICE Administrator must logon to TSO/ISPF on the z/OS LPAR where IFOM and the ICEDirect web server are running. From a TSO/ISPF panel, on the primary command line, the following command is entered:

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

where “a valid userid” is a security product defined userid that is to have ICEDirect access.

The following response indicates success:

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

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

Repeat this command for all userids who should have ICEDirect access.

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, select either “Log In” or “Update Password”. If “Log In” is selected, (or defaulted) enter the security product userid and password that is to be used and then select “Authenticate”.

If “Update Password” is selected, a new display is presented that allows for the entry of the existing password/phrase value as well as entry areas for a new password/phrase value and its value confirmation area. When the necessary information has been entered, select “Authenticate”.

These actions will begin the z/OS authorization process with the External Security Manager.

The image displays three sequential screenshots of the ICE Direct web application interface. Each screenshot has a dark blue header with the text 'ICE Direct' and 'Sign in to continue'.
1. The first screenshot shows the 'Log In' tab selected (indicated by a blue star icon). Below the header are three input fields: 'User Id', 'MFA Password/Passphrase', and 'Group Name'. At the bottom is a blue 'Authenticate' button.
2. The second screenshot shows the same 'Log In' tab, but a red error message box is displayed above the input fields, stating 'Login failed using the credentials entered'.
3. The third screenshot shows the 'Update Password' tab selected (indicated by a blue star icon). The input fields are: 'User Id', 'MFA Password/Passphrase', 'New Password', 'Confirm New Password' (with a 'Show/Hide' link), and 'Group Name'. A blue 'Authenticate' button is at the bottom.

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
- Environment error while generating a PassTicket

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

- Group is invalid
- User is not authorized to Group

5.1.2. *Using the Prefix*

When the authentication into z/OS completes, the ICE authentication process is initiated. See the panel shown below:

The image shows a web-based authentication panel titled "ICEDirect MFI Authentication". It has a dark blue header with the text "ICEDirect" and "MFI Authentication" in white. Below the header, there is a light blue instruction box that says "Enter your Private Prefix followed by the Token Material as the PassTicket". Underneath this, there are two input fields: "Token Material" with the value "IKFQ" entered, and "ICE PassTicket" which is empty. At the bottom of the form is a large blue button labeled "Authenticate". In the bottom right corner, there is a timestamp "05/11/2018 11:08:57".

As shown, Token Material “IKFQ” has been generated by the z/OS ESM for specific one-time use in authenticating into ICE. Using the user’s MFI prefix, enter the following into the ICE PassTicket entry field.

MFAZIKFQ
The Field is Masked

Select “Authenticate” to validate the ICEDirect PassTicket token. If successful, the ICEDirect main Iframe will be displayed.

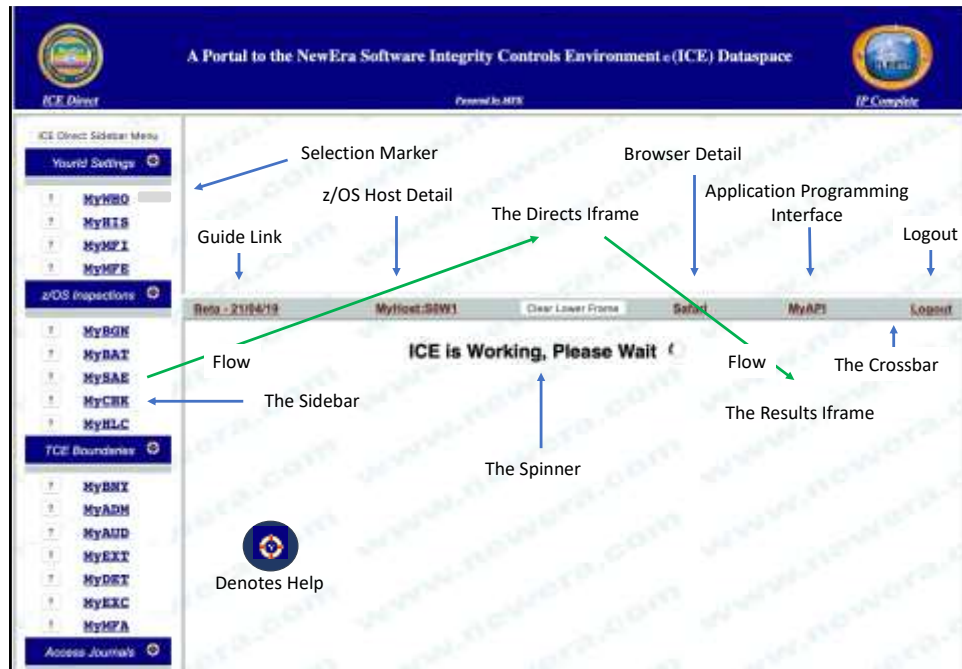
If authentication fails, one of the following messages will be displayed.

- 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 who receive the first message have not yet had their userid and prefix 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 to the desired application name and select 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 selecting the Question Mark submit button that precedes each application name. Second, Group-Help is shown when the “Life-Ring” following the group name is selected. In either case, related help text will “Float” above the Main Iframe. To continue, select Close.

5.1.5. *Selection Marker*

As selections are made from the Sidebar, the area adjacent to the selected option is marked with a small gray rectangle that will persist in that location until a new selection is made. When that new selection is made, the gray marker will move to the area adjacent to the new selection.

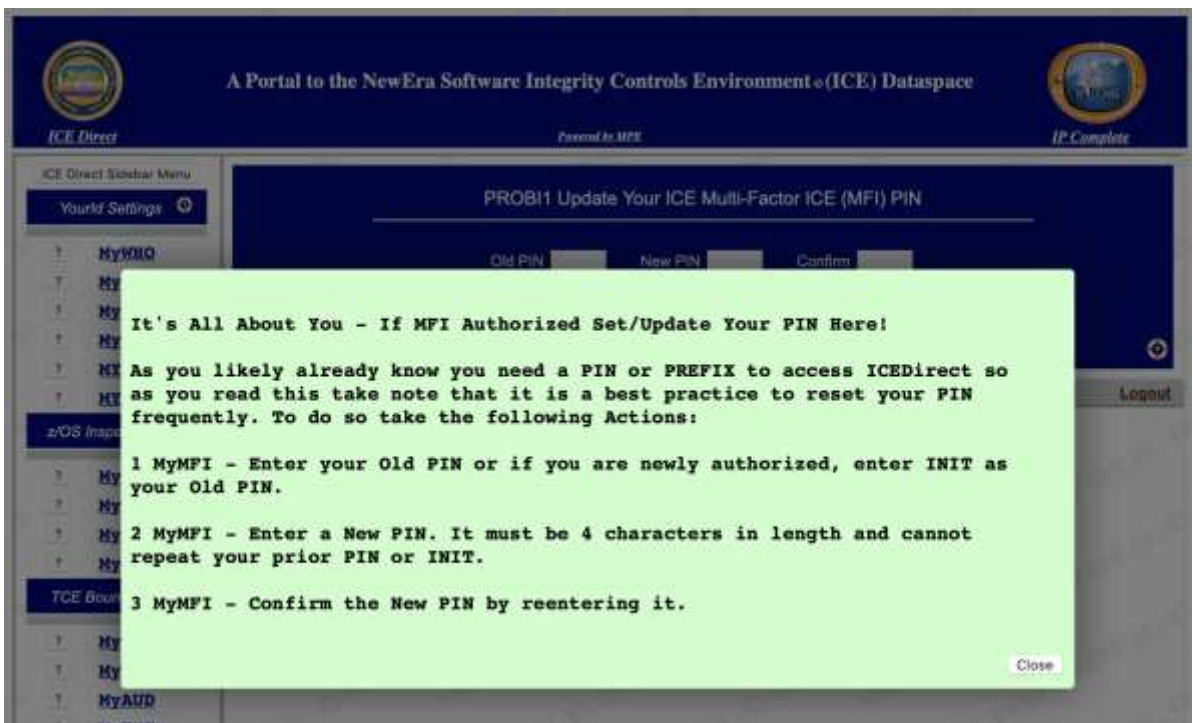
5.1.6. *Directs IFrame*

When an application is selected from the Sidebar, its related interface is displayed in the Directs IFrame window. During resolution, a “Spinner” will appear in the lower window and will disappear when the requested operation is complete.

A successful request will result in the display of an Application Directs panel similar to the one shown below.



This specific panel is the Interface Panel for the “MyMFI” selection. 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:

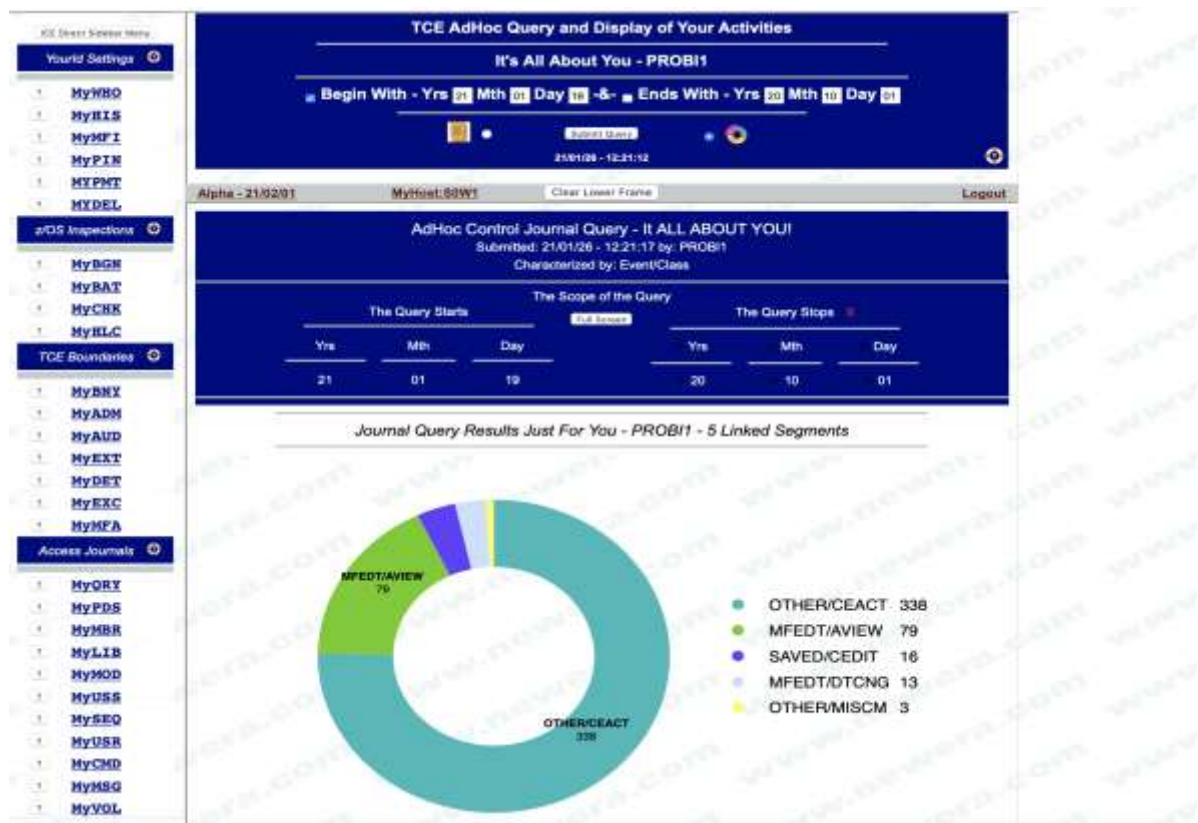


To close the help panel, select “Close”.

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.

Segments are linked to underlying source detail. Selecting 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/CEDIT 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.

TCE AdHoc Query and Display of Your Activities

It's All About You - PROBI1

Begin With - Yrs 21 Mth 01 Day 19 -&- Ends With - Yrs 20 Mth 10 Day 01

Submit Query

21/01/26 - 12:32:27

Alpha - 21/02/01 MyHost: SOW1 Clear Lower Frame Logout

AdHoc Control Journal Query

Submitted: 21/01/26 - 12:32:50 by: PROBI1

Characterized by: Event/Class

The Query Starts The Scope of the Query The Query Stops

Yrs Mth Day Yrs Mth Day

21 01 07 20 09 28

21/01/26 - 12:32:50

Query Results Presented by Controlled Category

SAVED/CEDIT - Update to a Member in a Controlled Dataset

Detail	Date	Time	Userid	System	Member	CONTROLLED ENTITY	Volume	Category
01)	21/01/26	10:02	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
02)	21/01/25	17:08	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
03)	21/01/25	17:06	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
04)	21/01/25	17:00	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
05)	21/01/25	16:52	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
06)	21/01/25	16:40	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
07)	21/01/25	16:27	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
08)	21/01/25	16:19	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
09)	21/01/25	16:05	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT
10)	21/01/25	15:51	PROBI1	SOW1	NSEENSSA	IFO.MTGY.PARMLIB	ZWOKS5	SAVED/CEDIT

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 will be replaced with that of the requested update.

Take note of the “Row Numbers”. They are additional selection points that when selected, the underlying Control Journal detail will be displayed. A sample of is shown below.

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. Select this to show the accompanying documentation for the release in the lower Results Iframe. This release information will be important if technical assistance is needed.

MyHOST

Select 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.

The screenshot displays the ICEDirect web application interface. At the top, a blue header bar contains the "ICE Direct" logo on the left, the title "A Portal to the NewEra Software Integrity Controls Environment (ICE) Dataspace" in the center, and the "IP Complete" logo on the right. Below the header, a sidebar on the left lists navigation options under "ICE Direct Sidebar Menu", including "YourId Settings", "MyWHO", "MyHIS", "MyMFI", "MyMFE", "z/OS Inspections", "MyBGN", "MyBAT", "MySAE", "MyCHK", "MyHLC", "TCE Boundaries", "MyBNY", "MyADM", "MyAUD", "MyEXT", and "MyDET". The main content area is titled "MyHost - Plex - ADCDPL - Lpar - S0W1 - Esm - RACF - Uri - www.myicedirect.com:8201" and shows "ICE is Licensed on CPU - Model - 1090 - Version - FF - Serial - FF01B19B1090". It includes a table with system details: Release (V2R4), IPLUnit (0A83), LoadSfx (WS), IEANUC (1), IODFUnit (0A83), HWName (-n/a-), LPARName (-n/a-), and VMUserid (ZOS24M). Below the table is a button for "ICE License Details" and a timestamp "21/05/18 - 08:50:23". A secondary bar contains "Beta - 21/04/19", "MyHost:S0W1", "Clear Lower Frame", "Safari", "MyAPI", and "Logout". The main section is titled "Integrity Controls Environment (ICE) Product Licenses" and lists "Image FOCUS (IFO)" and "Control Editor (TCE)". Under "Image FOCUS License Options", it shows "z/OS Inspection Core" and "Sub-System Inspectors". The "Sub-System Inspectors" section includes checkboxes for "Prod", "Work", "DRec", "JES2/3", "VTAM", "TCP/IP", "LOAD", "MBRS", and "CSDS". At the bottom, a section titled "ICEDirect Configuration Policies, Settings and Reports" contains buttons for "ICE Parameters", "Trouble Alerts", "User Registry", "Browser Policy", "Server Reports", and "WEB Parameters". A timestamp "21/05/18 - 08:50:29" is at the bottom right.

Clear Lower IFrame

Results will populate the lower Iframe and be cleared automatically by subsequent selections. This option is useful for hiding results and revealing them using the browser back button.

Browser Details

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

MyAPI

Select “MyAPI” 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 address 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

MyWHO shows the assigned identity Prime, Admin, Auditor, ROAuditor/General User of the logged in user. This identity determines what ICEDirect functions and applications that may be accessed.

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 the loggedin user. Select MyHIS to see the logged in user's activity.

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

Multi-Factor ICE (MFI) controls the final step in ICEDirect authentication. Similar to MFE, it also requires a private PIN to meet a challenge during a web logon. Select MyMFI to register or update a 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, a private PIN is required. Select MyPIN to register or update a 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, the inspectors 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 the scope 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 identify 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 as well as system command and message issuance. MyBGN presents these events and access to their configurations.

MyADM – Assign/Unassign ICE Administration 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 unnecessary. 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 individual user registries, The Master Registry and individual user registries are partitioned datasets. The Master Registry is uniquely named based on existing high level qualifiers used for Image FOCUS. The user registry datasets are prefixed by the user's userid.

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 the settings for the logged in user.

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 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.

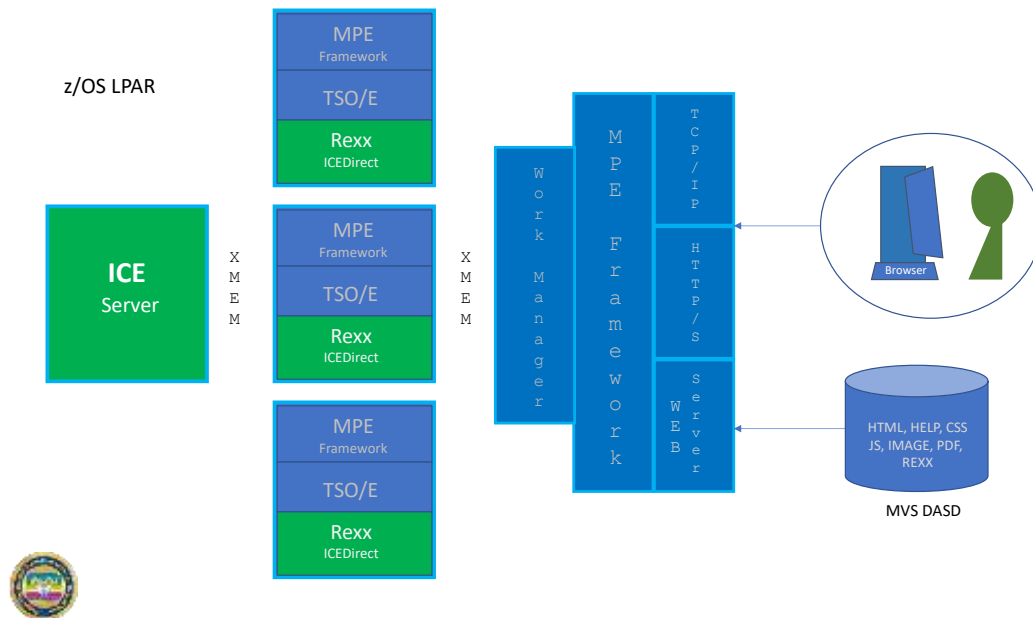
7. The Web Server Explained

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 make 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 a minimum of z/OS 2.2 release level.

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 logged in user and processes all requests from the user's browser session. If multiple users are logged in, then each user will have a dedicated started task instance to process 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 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 requires 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/E 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, a minimum number of TSO/E server address spaces will be started. 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 member is distributed in install dataset .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-MFA=Y               MFA LOGON ENABLED (DEFAULT Y)
*
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*

CSP Violation Reports are written to a file defined by the report-uri CSP Directive as default behavior. It is anticipated that in the future, browsers will support both the CSP report-uri directive and the CSP report-to Directive. The configuration option CSP-REPORT-TO is in anticipation of this future update. Currently, browsers generally do not support report-to, therefore a decision to use CSP-REPORT-TO should be taken only after consideration of 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/E started tasks will generate audit log files that record 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/E started task is triggered. The log datasets are automatically cleaned up based on the value of the LOG-RETAIN parameter in the PARMLIB member.

7.1.8. *Error Report*

The Web Server and TSO/E started tasks can also generate error reports when errors occur. 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 EREP datasets are being created, contact NewEra Technical Support for assistance. Please do not delete error report datasets prior to necessary problem resolution.

The Web Server will automatically suppress generation of error report datasets if the errors are happening at a high rate. 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 generated by using the url line in the browser and typing in some bogus request such as:

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

Repeating that request 10 times will result in 10 error reports and the offending IP address being quarantined from accessing the web server. The quarantine time is 30 minutes by default but can be set to a different value using the WEB-QUARANTINE parameter in NEZWEB00.

Web Error Reports are also generated when:

- A script is run without a user being logged on.
- Trying to access non-existent web content (pdf, images, css, js, etc).
- CSP policy has been violated.
- CSRF mismatches occur.
- Running a script, while another one is already running.
- Attempts are made to modify a <a href:// link.

Certain detected conditions are treated as integrity errors. In those cases, the offending user will be notified and the logged in session will be terminated.

- 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/E 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 number assigned to each TSO/E started task, 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 select ICE License Details. Next select Server Reports.

7.1.1. Sample Server and Error Reports

ICE Direct Sidebar Menu

MyHost - Flex - ADCDPL - Lpar - S0W1 - Esm - RACF - Url - www.myicedirect.com:8201
ICE is Licensed on CPU - Model - 1090 - Version - PF - Serial - FFO1B1001000

Release V2R4 IPLUnit OAB3 LoadSh WS IEANUC 1 XCDUnit OAB3 HWName -N- LPARName -N- VMUserid ZDS24M

ICE License Details
210430 - 12:32:48

Beta - 21/04/19 MyHost: S0W1 Clear Lower Frame Safari Logout

Web Server Session Report File
IFO.MTGY.WS.WSRV01.LOG.D210430.T122832

Userid: PROBIT Date: 21/04/30 Time: 12:25:32 Duration: 00:04:19 Registry

2021/04/30 12:28:32 I Log initialized
2021/04/30 12:28:33 I Newera ICE TSO/E Server NSRV01 (Release 1.1.01)
2021/04/30 12:28:33 I Parnlib Suffix : 00
2021/04/30 12:28:33 I Web Server ID : NSRV
2021/04/30 12:28:33 I TSO/E Server ID : NSRV01
2021/04/30 12:28:33 I Working Prefix : IFO.MTGY.WS.WSRV01
2021/04/30 12:28:33 I Logs Retained : 3 (days)
2021/04/30 12:28:33 I Starting IFOM Connection
2021/04/30 12:28:33 I Newera ICE TSO/E Server initialization complete
2021/04/30 12:28:34 I Starting TSO/E environment
2021/04/30 12:28:34 I Connection started to NSRV
2021/04/30 12:28:34 I Now running under userid PROBIT
2021/04/30 12:32:48 E PROBIT - Invalid Dataset/(Member) Display Request.
2021/04/30 12:32:51 I Shutdown requested by script

Records: 14

20210430 - 19:33:06

ICE License Details
210430 - 12:32:48

Beta - 21/04/19 MyHost: S0W1 Clear Lower Frame Safari Logout

023 21/04/28 12:10:11 Web Error: Item HEADREQ.WEB CURF=F2Z2JCOP2ICL00 not found
024 21/04/28 12:10:11 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123011
025 21/04/28 12:10:14 Web Error: Item HEADREQ not found
026 21/04/28 12:10:14 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123019
027 21/04/28 12:11:42 Web Error: Item SYSL.SAMPLIB not found
028 21/04/28 12:11:43 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123142
029 21/04/28 12:11:54 Web Error: Item SYSL.SAMPLIB(ATRBLF) not found
030 21/04/28 12:11:54 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123158
031 21/04/28 12:12:01 Web Error: Item SYSL.SAMPLIB(ATRBLF) not found
032 21/04/28 12:12:01 Web error reports have been disabled
033 21/04/28 12:12:18 Web Error: Item SMETA0419 not found
034 21/04/28 12:12:18 Web Error report suppressed
035 21/04/28 12:12:31 Web Error: Item A not found
036 21/04/28 12:12:31 Web Error report suppressed
037 21/04/28 12:13:00 Web Error: Item SYSL.SAMPLIB not found
038 21/04/28 12:13:00 Web Error report suppressed
039 21/04/28 12:13:04 Web Error: Item SYSL.SAMPLIB not found
040 21/04/28 12:13:04 Web Error report suppressed
041 21/04/28 12:13:11 Web Error: Item SYSL.SAMPLIB(TST) not found
042 21/04/28 12:13:11 Web Error report suppressed
043 21/04/28 12:13:14 Web Error: Item SYSL.SAMPLIB(TST) not found
044 21/04/28 12:13:14 Web Error report suppressed
045 21/04/28 12:14:09 Web Error: Item ADCD.221C.VTANLET not found
046 21/04/28 12:14:09 Web Error report suppressed
047 21/04/28 12:14:22 Web Error: Item ADCD.221C.VTANLET(A0600) not found
048 21/04/28 12:14:22 Web Error report suppressed
049 21/04/28 12:15:16 Web Error: No response from script
050 21/04/28 12:15:16 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123519
051 21/04/28 12:16:18 Web Error: No response from script
052 21/04/28 12:16:18 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123638
053 21/04/28 12:16:49 Web Error: No response from script
054 21/04/28 12:16:49 / Report written to: IFO.MTGY.WS.WSRV.NREP.D210428.T123645

7.1.2. *SMP/E Installation*

SMP/E installation is required for both the ICE Primary Task (IFO) and the Web Server. In addition to the \$NOTESMP member, you will find these jobs in IFOHLQ.INSTLIB. All jobs must 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

Additional jobs must be run 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 members for the ICE products must have been created.

ICE Members:

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

These additional members are required for ICEDirect.

Web Server Members:

\$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 two 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 the IFOHLQ.REGISTRY dataset named LICENSE. The supplied license data should be put into this member.

Next, edit the 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 the IFOHLQ.PARMLIB, be sure users are set up as TCEPRIME and TCEADMIN.

```
TCEPRIME tsuserid  
TCEADMIN (tsuserid,tsuserid,tsuserid)
```

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

Update the NSEENSxx Member

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

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

The *MFIPREFIX TST1 is a comment that indicates the personal PIN value for this user in clear text. It is shown here simply for documentation purposes and should not exist in the active NSEENSxx member. 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-character value serves as a prefix and must be combined with a 4-character 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. The new PIN value will be encrypted and updated into this member. The *MFEPREFIX value will not be updated by ICEDirect.

Copy to system PROCLIB Members

```
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=xxxxxxx
```

Start IFOM and IFOWEBM

Log on to 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:????
```

An IFOWEBS address space will be created for each user who successfully logs into ICEDirect.

Appendix “A” – Common Security Requirements

Image FOCUS and ICEDirect have setup requirements for proper functioning with the installed security product. These requirements are outlined below from a RACF perspective.

Started task userids for the Image FOCUS primary started task (IFOM), for the VTAM application started task (IFOS), for the ICEDirect web server started task, and for the interval detector started task should be set up as follows:

```
ADDUSER IFOM    NAME('IFOM STARTED TASK') SPECIAL AUDITOR OMVS(AUTOUID)
ADDUSER IFOS    NAME('IFOS STARTED TASK') SPECIAL AUDITOR OMVS(AUTOUID)
ADDUSER IFOMWS  NAME('IFOMWS STARTED TASK') SPECIAL AUDITOR OMVS(UTOUID)
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 token generation process that is used by Multi Factor ICE (MFI) authentication requires security product access for PassTicket generation. Authority to use the PassTicket generator is required for IFOM as follows:

```
SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA)
RDEFINE PTKTDATA IFOM UACC(NONE) SSIGNON(KEYMASKED(0123456789abcdef))
SETROPTS RACLIST(PTKTDATA) REFRESH
```

The KEYMASKED value is a 16 hexadecimal character value that is chosen by the site.

To collect information and to activate functional processes, ICEDirect, on behalf of a logged in user, will occasionally be required to issue commands to the MVS console. Access to issue commands is required only for ICEDirect users who will be performing administrative functions. The setup of the OPERCMDS class profile and the access permission is done as follows:

```
RDEFINE OPERCMDS NEZ.CMD.* UACC(NONE)
PERMIT NEZ.CMD.* CLASS(OPERCMDS) ACCESS(READ) ID(userid)
SETROPTS RACLIST(OPERCMDS) REFRESH
```

Appendix “B” – 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.

Access the link below to get information on installing and using certificates.

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

“What Keyring? What certificates? All I know is TLS doesn’t work!” is an insightful presentation. It can be accessed at:

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

Here is a step-by-step narrative for setting up certificates using RACF

- Assume that you have a secure server which has a distinguished name of
OU=Inventory,O=XYZZY,C=US
- and a domain name of
xyzzzy.com
- and the server executes on z/OS with the userid 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('xyzzzy.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 'userid.INVSERV.GENREQ'.

```
RACDCERT ID(INVSERV)
  GENREQ(LABEL('Inventory Server'))
  DSN('userid.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, 'userid.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('userid.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 RDATA LIB 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 RDATA LIB class:

- RDEFINE RDATA LIB INVSERV.RING01.LST UACC(NONE)
PERMIT INVSERV.RING01.LST CLASS(RDATA LIB) ID(INVSERV)
ACCESS(READ)

- If the RDATA LIB class is not already active, activate and RACLIST it:
SETROPTS CLASSACT(RDATA LIB) RACLIST(RDATA LIB)
- If the RDATA LIB class is already active and RACLISTed, refresh it:
SETROPTS RACLIST(RDATA LIB) 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 “C” – 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 to and stored in the browser, while the anti-CSRF token is known to each unique HTML page returned to the browser and therefore the Document Object Model. Each request is validated, and that validation is in effect for the duration of the user’s 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 configurable 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 attacks, including Cross Site Scripting ([XSS](#)) and data injection attacks. These attacks are used in many ways 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 instance 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 a randomized dynamically generated value, inserted directly by the server and sent to the browser. It remains valid for the duration of the user session.

- Secure Attribute

The **Secure** cookie attribute instructs web browsers to send only 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 use only HTTPS for its communication (even when TCP/IP port 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’s 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 to not 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 theft through XSS attacks. If an XSS attack is combined with a CSRF attack, the requests sent to the web application will include the session cookie, since the browser always includes the cookies when sending requests. The **HttpOnly** cookie protects only the confidentiality of the cookie; the attacker cannot use it offline, outside 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. This provides some protection against CSRF attacks.

Denials-Of-Service (DoS)

A Denial-of-Service attack is 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 can trigger a crash.

Mitigation

Auto-Quarantine of Web Server IP Address is provided for a user defined maximum consecutive recognized error limit. When the maximum is reached two actions are taken. First, the recording of error events is suspended following the writing of a final message indicating that the suspension (for the offending URL only) is imminent. Second, the offending URL is placed on a temporary “Black List” and, in-turn, is automatically denied service until a later time when it is automatically removed from the “Black List”. The duration of these actions is controlled by 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 to never connect to ICEDirect using HTTP and to automatically convert all attempts to use HTTP into HTTPS requests. This primary and subdomain translation is activated with the first access to an ICEDirect site. It remains in effect for two years. This default term is reset to two 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 better performance, it may also expose information that remains 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 to “no-cache”. For all other objects, it is set to “private, max-age=7200; (2 hours)”. The latter (private) indicates that the cache is only shareable between the directly communicating server and browser and no other network node. This control has a time limit of two hours, after which it is removed.

Use of Autofill

Commonly used Autofill can create an exposure when it remembers a user’s logon credential. This allows 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 an option that allows the user to registrar a private PIN that is to be concatenated with real-time token material presented at the point of the challenge.

Failure to Logout

A user’s failure to formally logout from ICEDirect 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 have configurable duration options. These are used to automatically logoff an inactive user and/or automatically cancel an inactive session started task. Short durations are considered a best practice.

Direct Script Injection

Direct Script Injection occurs when users enter into an otherwise assigned text field HTML/JAVA character syntax and then submit it, embedded with a normal request. The server not being able to distinguish this injection from a normal request would process the request and reply accordingly.

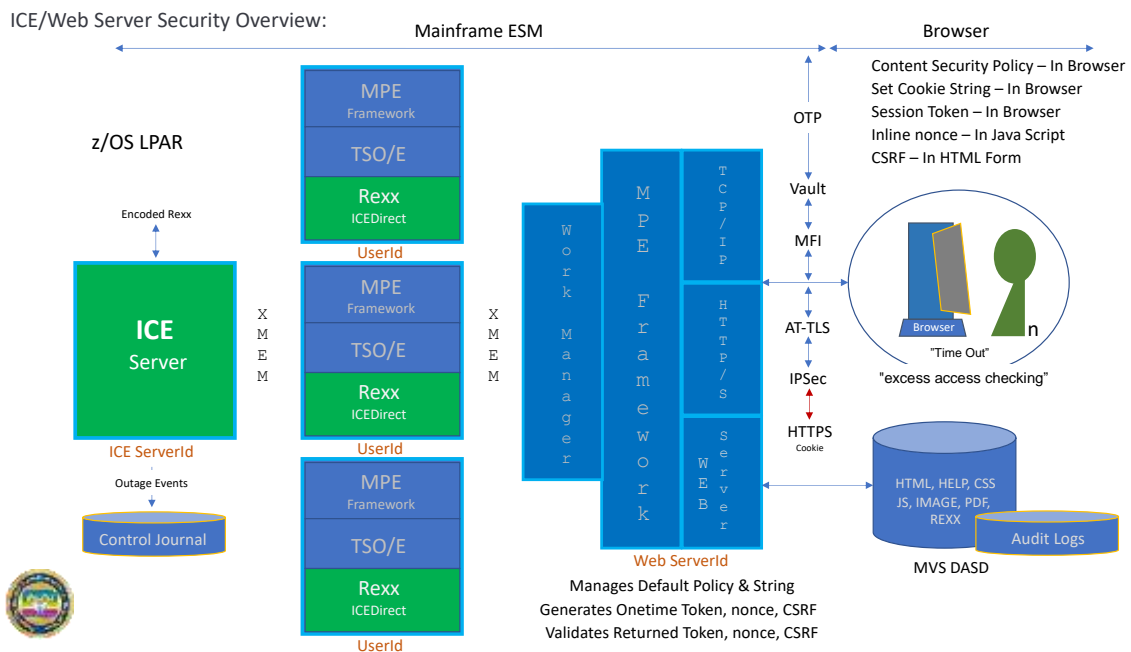
Mitigation

The ICEDirect Server supports a filter/checklist of common HTML/JAVA activation characters – the current filter /checklist is set at - '< & %'. Each request string received is filtered 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 “D” – 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 and 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 verify 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 when called for processing.

- 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









Cache Control Directives provide the server with a 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). This will prevent/limit Content Delivery Networks (CDN) caching.






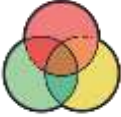

- HTTP Strict-Transport Security (HSTS) Directive










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









Appendix “E” – 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 |

| | |
|---|---|
|  | CERTVIFY – 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 |
|  | AUTHVIFY – 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 |
|  | 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 |

| | |
|--|-----------------------------------|
|  An illustration of a woman with brown hair wearing a yellow top, and a man with brown hair wearing a dark blue suit, white shirt, and red tie. | Indicates Roles and Access Rights |
| | |

Technical Support Contact Information

NewEra Software, Inc.

Mailing Address:

8070 Santa Teresa Blvd, Suite 240
Gilroy, CA 95020

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

