

This is a Simple, Straightforward way to Get what You need from ICE on the WWW

“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 3



NewEra Software Technical Support

800-421-5035 or 408-520-7100

support@newera.com

Rev: 2022-05-01



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 (ICE). Please avail yourself to them as you consider necessary.

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

Table of Contents

1. WHAT IS ICEDIRECT?	6
2. SETTING UP ICEDIRECT	6
2.1. SERVER INSTALLATION	6
2.2. USER REGISTRY	6
2.3. GLOBAL REGISTRY	6
2.4. SERVER IDENTIFICATION	7
2.5. SERVER SECURITY – YouTube #5	7
2.6. CONTENT-SECURITY-POLICY (CSP)	9
2.7. OPERATING FROM A z/OSMF LINK – YouTube #10	10
2.8. A LOGIN TO ICEDIRECT IS THE NEXT STEP	12
2.9. OPERATING FROM A STANDALONE BROWSER	12
2.10. SETTING UP THE OTP TOKEN GENERATOR	13
2.11. USER AUTHENTICATION – YouTube #5	13
2.11.1. Authentication with z/OS	13
2.11.2. Authentication with ICE	13
3. PATIENT ZERO - FIRST ADMINISTRATOR – YOUTUBE #0	15
3.1. USE THE ICE 3270 PANELS TO SET THE PIN	15
3.2. UPDATE THE NSEENSxx DIRECTLY TO SET THE PIN	15
3.3. LOGGING IN – YouTube #5	16
3.4. USING THE PREFIX	17
4. ICEDIRECT PLATFORM HEADER	18
4.1. UPPER LEFT “D”	18
4.2. UPPER RIGHT “G”	18
4.3. LOWER CENTER “POWERED BY GATEWAY z/OS”	18
4.4. LOWER LEFT ICEDIRECT	18
4.5. LOWER RIGHT IPCOMPLETE	18
5. ICEDIRECT MAIN IFRAME SET – YOUTUBE #5	19
5.1. SIDEBAR	19
5.2. SELECTION MARKER	20
5.3. DIRECTS IFRAME	20
5.4. RESULTS FRAME	21
5.5. THE CROSSBAR	24
5.5.1. Current Release Information	24
5.5.2. MyHOST	24
5.5.3. Clear Lower (Results) IFrame	24
5.5.4. Browser Details	25
5.5.5. z/OS Visual	25
5.5.6. RACF Visual	25
5.5.7. Logout	25
6. ICEDIRECT APPLICATIONS – EACH BRIEFLY EXPLAINED	26
6.1. YOURID SETTINGS	26
6.1.1. MyWHO – Your ICE User Scope – YouTube #6	26
6.1.2. MyHIS – Your ICE Event History – YouTube #6	26
6.1.3. MyMFI – Your Multi-Factor ICE Prefix – YouTube #0	26
6.1.4. MyZTA – Your Multi-Factor Edit Prefix	26
6.2. z/OS INSPECTIONS	26

6.2.1.	MyBGN – Image FOCUS Sysplex Inspection – YouTube #1.....	26
6.2.2.	MyBAT – ICEBATA Logs and Analysis – YouTube #2	26
6.2.3.	MySAE – SAEBATA Logs and Analysis – YouTube #3.....	27
6.2.4.	MyCHK – IPLCheck Logs and Analysis – YouTube #4.....	27
6.3.	CONTROL BOUNDARIES	28
6.3.1.	MyBNY – ICE Intercept Point and Boundaries	28
6.3.2.	MyADM – ICE Administration Credentials.....	28
6.3.3.	MyAUD – ICE Auditor Credentials.....	28
6.3.4.	MyEXT – External Notifications Settings – YouTube #8.....	28
6.3.5.	MyDET – Interval Detector Settings – YouTube #8.....	28
6.3.6.	MyEXC – Journal Event Exclusions – YouTube #8.....	28
6.3.7.	MyMFA – Overview of ICE MFA – MFI/MFE – YouTube #9	28
6.4.	JOURNAL ACCESS	29
6.4.1.	MyQRY – Ad Hoc Queries to the ICE Control Journal.....	29
6.4.2.	MyXXX – Directed Queries to the ICE Control Journal.....	29
6.5.	NEWERA SUPPORT.....	30
6.5.1.	MyLIC – Application Licensing Updates and Activation.....	30
6.5.2.	MyBug – From Time to Time Bugs may Creep-In.....	30
7.	THE WEB SERVER EXPLAINED	31
7.1.	SERVER OVERVIEW	31
7.2.	SERVER DATASETS	33
7.2.1.	Dataset Attributes.....	33
7.3.	USER SESSIONS.....	33
7.4.	SERVER MANAGEMENT.....	34
7.5.	SERVER PARMLIB MEMBER.....	35
7.6.	SERVER REPORTS AND LOGS	35
7.6.1.	CSP Violation Report Options.....	35
7.6.2.	Audit Log File	36
7.6.3.	Error Report	36
7.6.4.	Error Examples.....	36
7.7.	ACCESSING ERROR REPORTS	38
7.7.1.	Sample Server and Error Reports	39
7.8.	SMP/E INSTALLATION	40
7.8.1.	Primary Task Includes:	40
7.8.2.	Web Server Includes:.....	40
8.	ADDITIONAL LICENSED APPLICATION	41
8.1.	RACF VISUAL.....	41
8.1.1.	RACF Settings & Practices	42
8.1.2.	Certificate Intelligence (CI).....	43
8.1.3.	Community Service & Action	44
8.1.4.	RACF Command Logs & Query.....	45
8.1.5.	Access Requirements.....	46
8.2.	z/OS VISUAL.....	47
8.2.1.	CMD = "D XCF"	47
8.2.2.	Supervisor Calls.....	48
8.2.3.	Display Commands.....	49
8.2.4.	Show the Jobs List.....	50
8.2.5.	Health Checker(s).....	51
8.2.6.	Gskkyman db(s).....	52
8.2.7.	IODF Configuration	53
8.2.8.	View Datasets/Files.....	54
8.2.9.	Parmlib Analysis.....	55

9.	APPLICATION LICENSE INSTALLATION AND ACTIVATION	56
9.1.	XML LICENSE DOCUMENT	56
10.	APPENDIX “A” – SERVER CERTIFICATES	58
11.	APPENDIX “B” – COMMON BROWSER INSECURITIES	61
11.1.	CROSS SITE REQUEST FORGERY (CSRF)	61
11.2.	CROSS SITE SCRIPTING (XSS)	61
11.3.	COOKIE MISUSE MANAGEMENT	62
11.4.	JAVASCRIPTS	62
11.5.	DENIALS-OF-SERVICE (DoS)	63
11.6.	MAN-IN-THE-MIDDLE - PROTOCOL DOWNGRADES AND HIJACKING.....	63
11.7.	BROWSER AND CONTENT DELIVERY NETWORKS (CDN) CACHING.....	64
11.8.	USE OF AUTOFILL	64
11.9.	FAILURE TO LOGOUT	64
11.10.	DIRECT SCRIPT INJECTION	65
12.	APPENDIX “C” – SECURITY ATTRIBUTES - AN OVERVIEW	66
12.1.	ENVIRONMENT	66
12.2.	NETWORK	66
12.3.	z/OS LOGIN.....	66
12.4.	TOKENS	67
12.5.	ICEDIRECT LOGIN	67
12.6.	NSIMxxx – A REXX APPLICATION	67
12.7.	WEB HOST – WEB SERVER ADDRESS SPACE.....	67
12.8.	WEB HOST – REXX ADDRESS SPACES	67
12.9.	IDLE TIMEOUT OF USER SESSIONS.....	67
12.10.	AUTO-QUARANTINE OF CLIENT IP ADDRESS	68
12.11.	CONTENT-SECURITY-POLICY.....	68
12.12.	SECURITY STRING	68
12.13.	CACHE CONTROL DIRECTIVES	68
12.14.	HTTP STRICT-TRANSPORT SECURITY (HSTS) DIRECTIVE	68
13.	APPENDIX “D” – APPLICATION ICONS	69
14.	TECHNICAL SUPPORT CONTACT INFORMATION.....	75

1. What is ICEDirect?

ICEDirect is a collection of application interfaces that provide access to the Integrity Controls Environment (ICE), z/OS and RACF. 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.

2. Setting Up ICEDirect

ICEDirect is included as part of the ICE download that contains both Image FOCUS (IFO) and The Control Editor (TCE). Additional ICEDirect applications, z/OS Visual and RACF Visual may be licensed separately. All components are installed using the SMP/E. Installation instructions can be found in their respective User Guides. Prior to starting the two primary tasks, IFOM and IFOMWS, it is necessary to customize the environment using members found in the ICE Parmlib dataset.

2.1. Server Installation

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

2.2. User Registry

Each ICEDirect user will be supported by a user-specific registry, a partitioned dataset. This dataset will be automatically 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.

2.3. 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.

2.4. Server Identification

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

- 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.

2.5. 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:

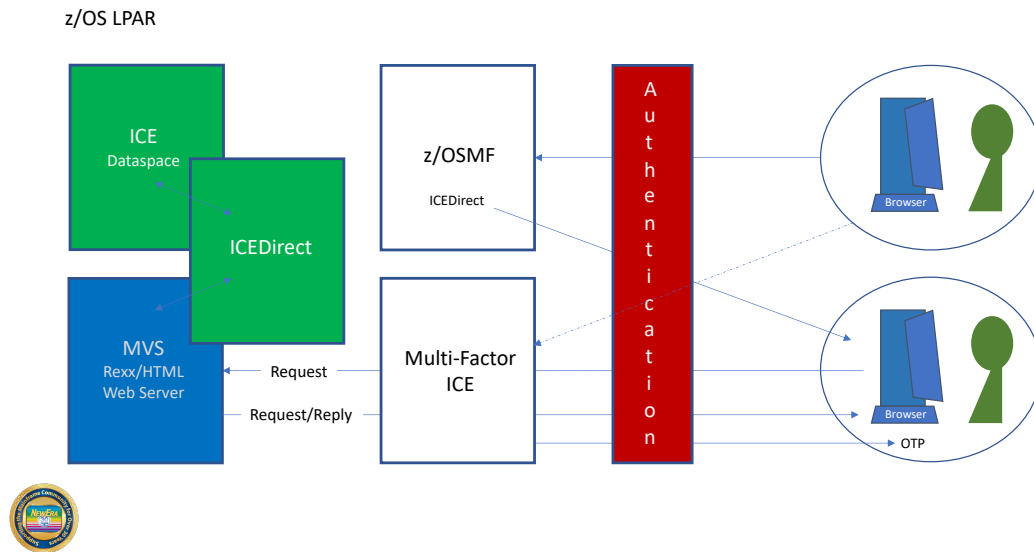
<https://24.234.192.41:8200>

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.



2.6. 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 therefore not a recommend web browser.

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 with an assigned entry PORT, 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

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

Using a z/OSMF login, most likely on an internal TCP/IP intranet, will provide an even more 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 using the authority of the z/OSMF Administrators, dynamically setup the Link once logged onto z/OSMF via the interface panel shown here.

Links 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): IZUDFLT.ZOSMF.LINK, NEZ_COM

* URL (maximum 4000 characters): https://www.myicedirect.com:8201/

* Category: Links

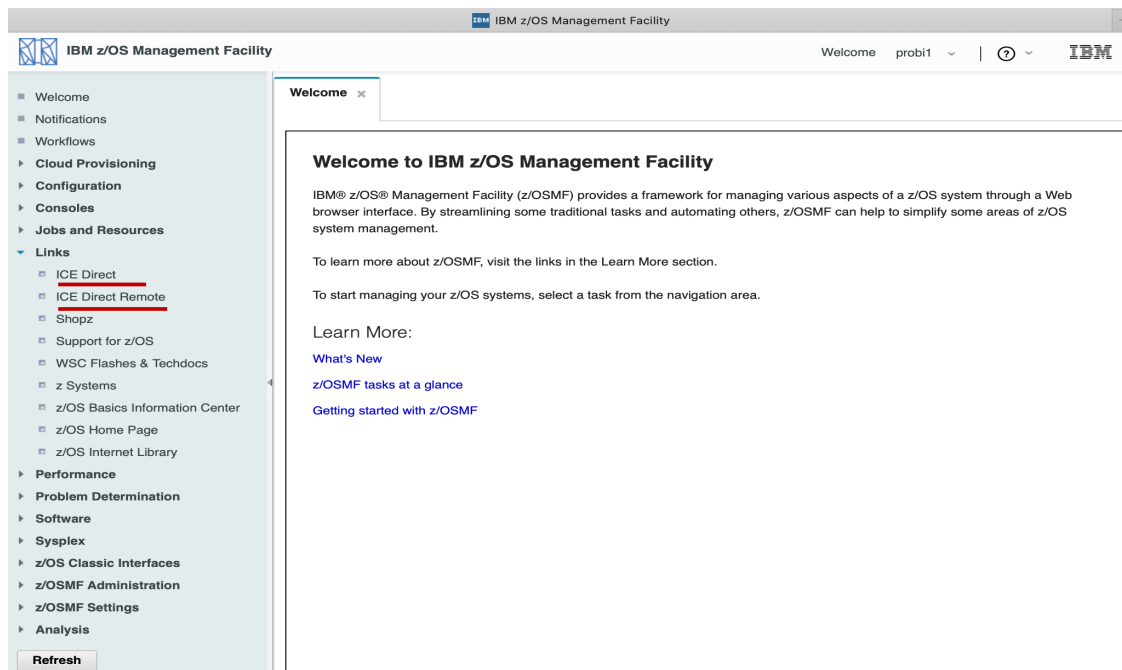
Open link in:
☒ New browser tab or window
☐ New z/OSMF tab

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, 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.

2.8. *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 Frame-Set” 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)
```

2.9. *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 if client address is recognized by the receiving server PORT.

- 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.

2.10. *Setting up the OTP Token Generator*

The External Security Manager (ESM) controls the generation of a One-Time Pass Ticket/Token used by MFI. If the ESM generation process has not been configured, use the job shown below customized to match site standards.

```
/RACFPKT JOB ' ', 'PERMIT ACCESS', MSGCLASS=H, MSGLEVEL=(1,1),  
// REGION=4M, TIME=1440, NOTIFY=&SYSUID, CLASS=A  
//*****  
//PERMIT EXEC PGM=IKJEFT01, DYNAMNBR=75, TIME=100, REGION=6M  
//SYSPRINT DD SYSOUT=*  
//SYSTSPRT DD SYSOUT=*  
//SYSTEM DD DUMMY  
//SYSUADS DD DSN=SYS1.UADS, DISP=SHR  
//SYSLBC DD DSN=SYS1.BROADCAST, DISP=SHR  
//SYSTSIN DD *  
SETROPTS CLASSACT(PTKTDATA)  
SETROPTS RACLIST(PTKTDATA)  
RDEFINE PTKTDATA IFOM UACC(NONE) SSIGNON(KEYMASKED(0123456789ABCDEF))  
SETROPTS REFRESH RACLIST(PTKTDATA)
```

If the generated pass ticket/token is not configured a warning message will appear in the authentication dialog stating that the MFI process has failed.

2.11. *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.

2.11.1. *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

2.11.2. *Authentication with ICE*

ICE Authentication requires the user to be in possession of a One-Time-PassTicket (OTP). This token is eight characters in length and 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 Welcome 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 the option to try again.

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.

3. *Patient Zero - First 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 may select one of two methods:

3.1. *Use the ICE 3270 Panels to Set the PIN*

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.

3.2. *Update the NSEENSxx Directly to Set the PIN*

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

Using this as a model the derived PIN will be set to TST1. It is best practice to change this default PIN as soon as possible using the MyMFI option found listed on the ICEDirect Sidebar.

3.3. 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.

The image displays three sequential screenshots of the ICE Direct web application interface, illustrating the login and password update process.

- Left Screenshot:** The 'Log In' radio button is selected. The form includes fields for 'User Id', 'MFA:Password/Passphrase', and 'Group Name' (marked as 'Optional'). An 'Authenticate' button is at the bottom.
- Middle Screenshot:** A red error message 'Login failed using the credentials entered' is displayed above the 'User Id' field. The 'Log In' radio button remains selected.
- Right Screenshot:** The 'Update Password' radio button is selected. The form includes fields for 'User Id', 'MFA:Password/Passphrase', 'New Password', 'Confirm New Password' (with the subtext 'Re-enter new password'), and 'Group Name' (marked as 'Optional'). An 'Authenticate' button is at the bottom.

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

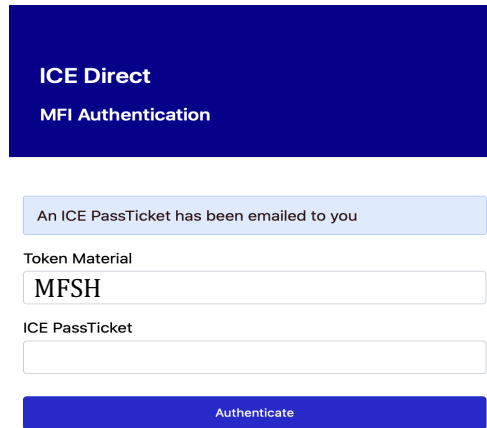
- Login failed using the credentials entered
- The Password/Passphrase has expired
- The new Password/Passphrase is invalid for this site

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

- Group is invalid
- User is not authorized to Group

3.4. Using the Prefix

With the authentication into z/OS completed successfully, the ICE MFI authentication process is initiated and displays the panel shown below:



The panel is titled "ICE Direct" and "MFI Authentication". It contains a message box stating "An ICE PassTicket has been emailed to you". Below this, there are two input fields: "Token Material" with the value "MFSH" and "ICE PassTicket" which is empty. At the bottom is a blue button labeled "Authenticate".

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 “**INIT**”, enter the following into the ICE PassTicket text-box field.

INITMFSH
The Field is Masked

“Click” Authenticate to validate the ICEDirect PassTicket. If successful, the ICEDirect welcome Iframe set 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.

4. ICEDirect Platform Header

At the very top of the Iframe set you will find the ICEDirect Platform Header. It contains five selectable options.



4.1. Upper Left “D”

Click the “D” in the upper left to open a new browser TAB and display the ICEDirect Platform - Getting Starting Guide.

4.2. Upper Right “G”

Click the “G” in the upper right to open a new browser TAB and display the GOOGLE Search Interface.

4.3. Lower Center “Powered by GateWAY z/OS”

Click “Powered By MPE” to review a brief document explaining the MainTegrity Processing Environment. The ICEDirect Web Server is derivative work of MPE innovation.

4.4. Lower Left ICEDirect

Click “ICEDirect” as shown, lower left, to open a new browser TAB and show an additional welcome Iframe set. This secondary set can be used in conjunction with the first when a user would like to work with more than one ICEDirect application at the same time.

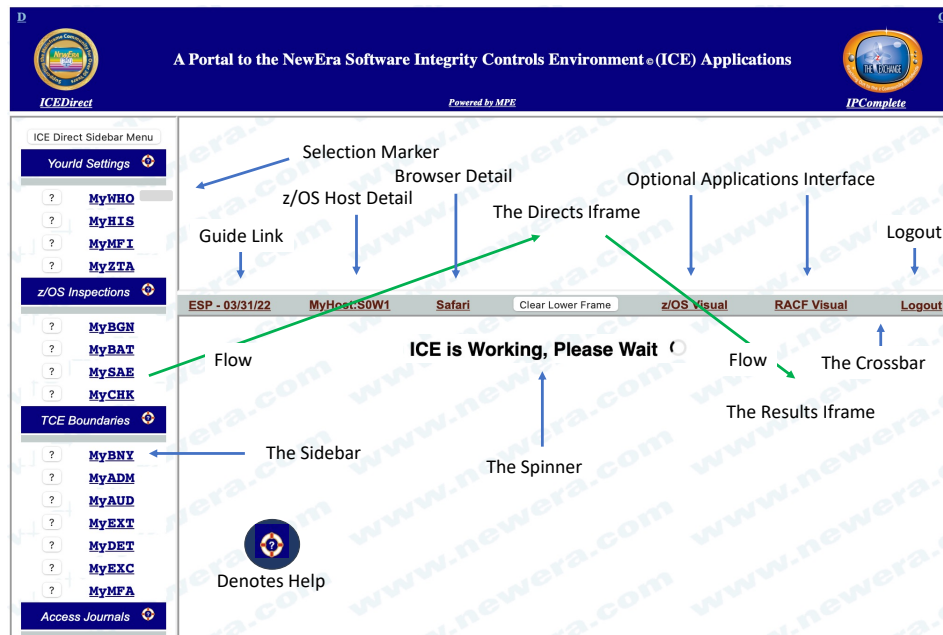
4.5. Lower Right IPComplete

Click “IPComplete” as shown, lower right, to open a new browser TAB showing the IPComplete application sidebar.

5. 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 Iframes in the same TAB or with any number of additional TABs that may have been open.

Note that no matter how many Iframe sets are open/active the user will only have one active z/OS session and only one network connection. All requests will be queued in a FIFO work stack. Logging out of any one TAB or quitting the browser altogether will terminate the z/OS session but closing a TAB will have no effect on the z/OS session or network connection.



5.1. Sidebar

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

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 Set. In either case “Click” Close to continue.

5.2. 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 Sidebar selection is made in which case the marker will move to the area adjacent to the new selection.

5.3. Directs IFrame

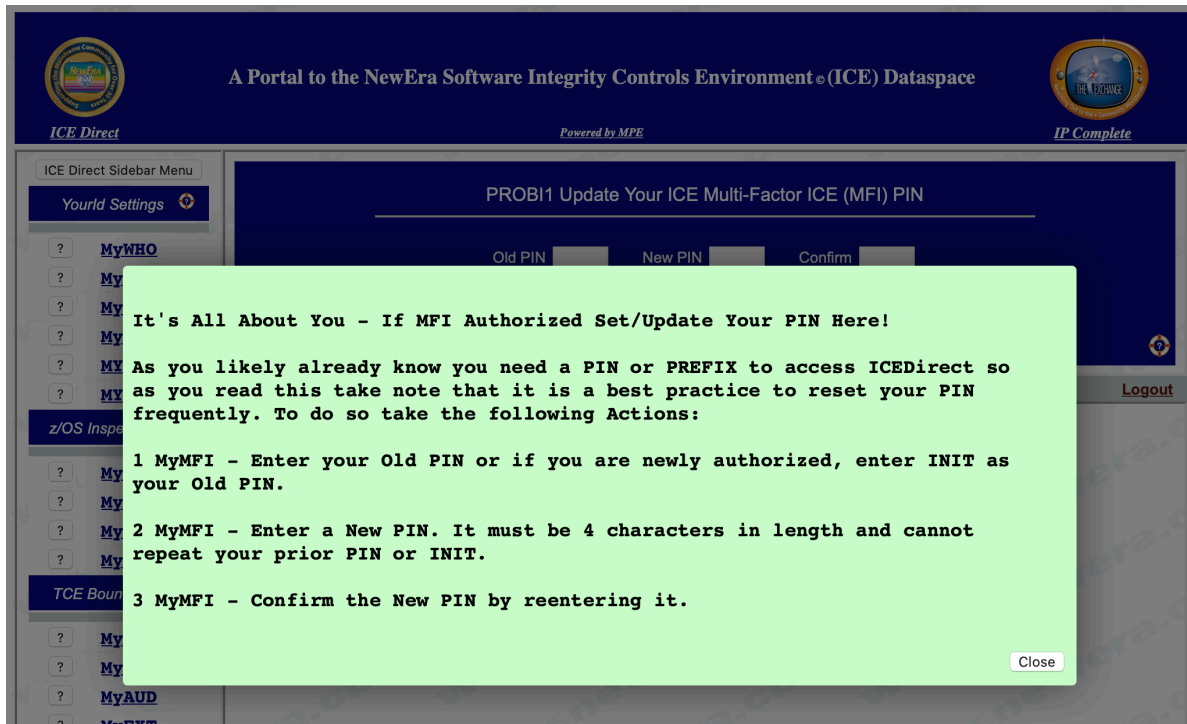
When an application is selected from the Sidebar, its related interface is displayed in the Directs frame window. As it is being fully resolved, a “Spinner” will appear in the lower window and will disappear when request resolution is complete. Making a selection while the “Spinner” is spinning will display the message, “Request already active for user”. It is best to wait for the spinning to stop before making a second selection.

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

The screenshot displays the ICE Directs web application interface. At the top, a dark blue header contains the ICE logo on the left, the text "A Portal to the NewEra Software Integrity Controls Environment (ICE) Dataspace" in the center, and another logo on the right. Below the header, the main content area is divided into a sidebar and a main frame. The sidebar, titled "ICE Direct Sidebar Menu", lists several options: "YourId Settings", "MyWHO", "MyHIS", "MyMFI", "MyPIN", "MYPMT", and "MYDEL". The main frame displays the "PROB1 Update Your ICE Multi-Factor ICE (MFI) PIN" form. This form includes input fields for "Old PIN", "New PIN", and "Confirm", followed by an "Update PIN" button. A timestamp "21/01/26 - 12:05:36" is shown below the button. At the bottom of the interface, a status bar displays "Alpha - 21/02/01", "MyHost:S0W1", a "Clear Lower Frame" button, and a "Logout" link.

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:

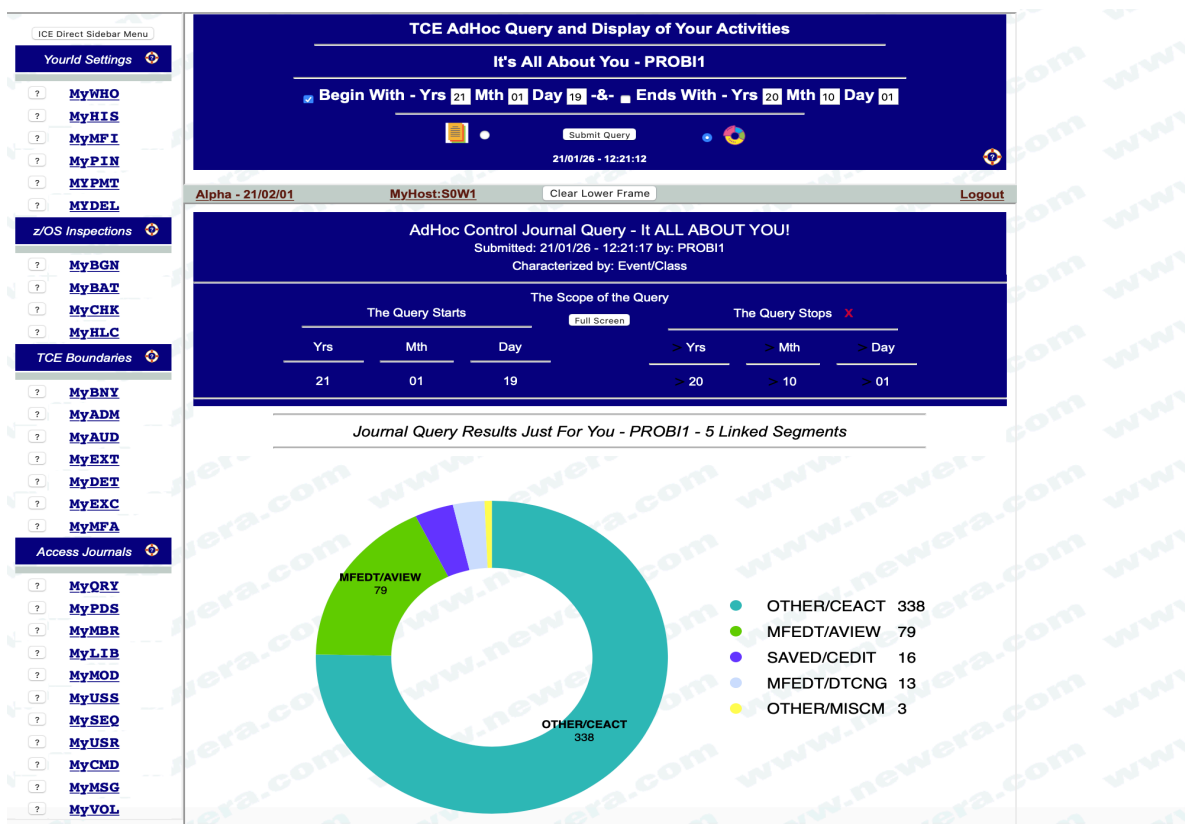
This is a Simple, Straightforward way to Get what You need from ICE on the WWW



To close the help panel, “Click” Close.

5.4. Results Frame

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 frame. 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 defined in the Control List, then an update was made, recognized, captured and recorded in the ICE Control Journal. The ICE Control Journal is the base source of the information shown in these examples.

ICE Direct Sidebar Menu

YourId Settings

MyWHO

MyHIS

MyMFI

MyPIN

MyPMT

MyDEL

z/OS Inspections

MyBGN

MyBAT

MyCHK

MyHLC

TCE Boundaries

MyBNY

MyADM

MyAUD

MyEXT

MyDET

MyEXC

MyMFA

Access Journals

MyORY

MyPDS

MyMBR

MyLIB

MyMOD

MyUSS

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:S0W1

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 X

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	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
02)	21/01/25	17:08	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
03)	21/01/25	17:06	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
04)	21/01/25	17:00	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
05)	21/01/25	16:52	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
06)	21/01/25	16:40	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
07)	21/01/25	16:27	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
08)	21/01/25	16:19	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
09)	21/01/25	16:05	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT
10)	21/01/25	15:51	PROBI1	S0W1	NSEENSSA	IFO.MTGY.PARMLIB	ZWORK5	SAVED/CEDIT

In this example, the Application Interface is a constant while the Results frame 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 frame will be cleared and the current Application replaced with that of the requested Application update.

Take note of the “Row Numbers”. They are additional selection points that when “Clicked”, will display the underlying Control Journal Detail.

5.5. The Crossbar

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

5.5.1. Current Release Information

To the very left is shown the release identifier of the version of ICEDirect that is running. When “clicked” it will display the Getting Started Guide in the Results IFrame.

5.5.2. 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 into service following an outage and other events.

The screenshot displays the ICEDirect web platform interface. At the top, a blue header bar contains the ICEDirect logo on the left, the title "A Portal to the NewEra Software Integrity Controls Environment (ICE) Applications" in the center, and the IPComplete logo on the right. Below the header, a sidebar on the left lists various menu items under "ICE Direct Sidebar Menu", including "YourId Settings", "MyWHO", "MyHIS", "MyMFI", "MyZTA", "z/OS Inspections", "MyBGN", "MyBAT", "MySAE", "MyCHK", "TCE Boundaries", "MyBNY", "MyADM", "MyAUD", "MyEXT", "MyDET", "MyEXC", and "MyMFA". The main content area is titled "MyHost - Plex - ADCDPL - Lpar - S0W1 - Esm - RACF - Url - www.myicedirect.com:8201" and displays licensing information: "ICE is Licensed on CPU - Model - 1090 - Version - FF - Serial - FF01B19B1090". It also shows the last IPLed date and time, and a table of system details including Release (V2R4), IPLUnit (0A83), LoadSfx (WS), IEANUC (1), IODFUnit (0A83), HWName (-n/a-), LPARName (-n/a-), and VMUserid (ZOS24M). Below this, there's a section for "ICEDirect Platform Detail" showing the platform version (ICE:17.0, NSIMDIR:03.11) and a timestamp (22/04/18 - 10:47:12). A navigation bar includes links for "ESP - 05/01/22", "MyHost:S0W1", "Safari", "Clear Lower Frame", "z/OS Visual", "RACF Visual", and "Logout". The main content area is titled "Integrity Controls Environment (ICE) Product Licenses" and shows a list of licenses with checkboxes: Image FOCUS (IFO), Control Editor (TCE), z/OS Inspection Core, Sub-System Inspectors, and Supplemental Inspectors. Below this, there's a section for "Image FOCUS License Options" with checkboxes for Prod, Work, DRec, JES2/3, VTAM, TCP/IP, LOAD, MBRS, and CSDS. At the bottom, there's a section for "ICEDirect Platform - Configuration, Policies, Settings and Reports" with links for ICE Parameters, Trouble Alerts, User Registry, Browser Policy, Server Reports, and WEB Parameters.

5.5.3. Clear Lower (Results) 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.

5.5.4. 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.

5.5.5. z/OS Visual

z/OS Visual, a licensed option supports access, actions and the display of certain z/OS system states and settings.

5.5.6. RACF Visual

RACF Visual, a licensed option supports access, actions and the display of certain RACF system states and settings in support of RACF Administration.

5.5.7. Logout

Although the REXX processing address spaces will time out 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. YourID Settings

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

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. MyZTA – 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 MyZTA to register or update your PIN.

6.2. z/OS Inspections

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

6.2.1. MyBGN – Image FOCUS Sysplex Inspection – 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.

6.2.2. MyBAT – ICEBATA 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.

6.2.3. *MySAE – SAEBATA 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.

6.2.4. *MyCHK – IPLCheck 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.

6.3. Control Boundaries

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

6.3.1. MyBNY – 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.

6.3.2. MyADM – 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.

6.3.3. MyAUD – 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.

6.3.4. MyEXT – 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.

6.3.5. MyDET – 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.

6.3.6. MyEXC – 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.

6.3.7. MyMFA – Overview 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.

6.4. Journal Access

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

6.4.1. MyQRY – Ad Hoc Queries to the ICE 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.

6.4.2. MyXXX – Directed Queries to the ICE Control Journal

ICEDirect offers the additional specific query interfaces:

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

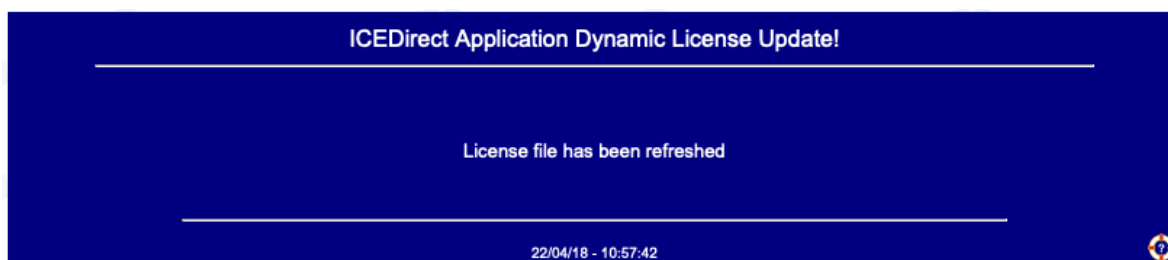
These query interfaces are focused to deliver events directly related to - Partitioned Datasets, Members in a PDS, Load Libraries, Modules in a Library, Unix Files, Sequential Datasets and Activities or Events related to Users, Commands, Messages and Volumes.

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.

6.5. NewEra Support

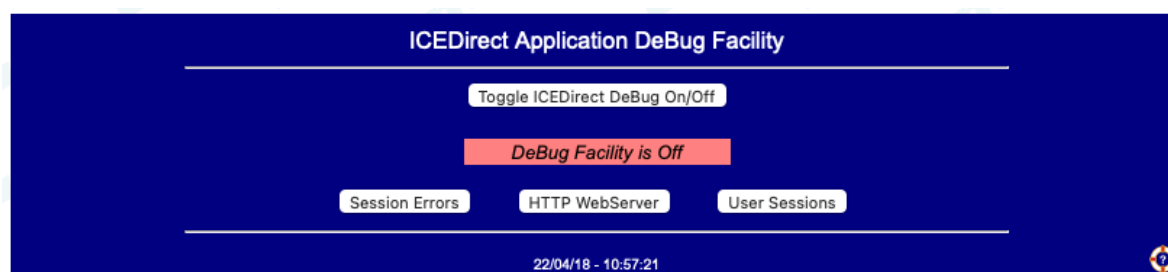
6.5.1. MyLIC – Application Licensing Updates and Activation

The licensing of ICEDirect applications – z/OS Visual and RACF Visual is controlled by the XML license file provided by NewEra Technical Support. From time to time it may be necessary/desirable to renew this license file. Once the new/updated file member has been placed in the ICE Parmlib dataset, it may be activated by simply selecting MyLIC. The message shown below will appear in the Directs frame.



6.5.2. MyBug – From Time to Time Bugs may Creep-In

When problems arise report them directly to NewEra Technical Support by email at this address - support@newera.com. ICEDirect incorporates an internal DeBug Facility that may be helpful in diagnosing problems. To access these functions – turning it ON/OFF or reviewing its various reports select MyBug. Doing so will display the panel shown below in the Directs Frame.



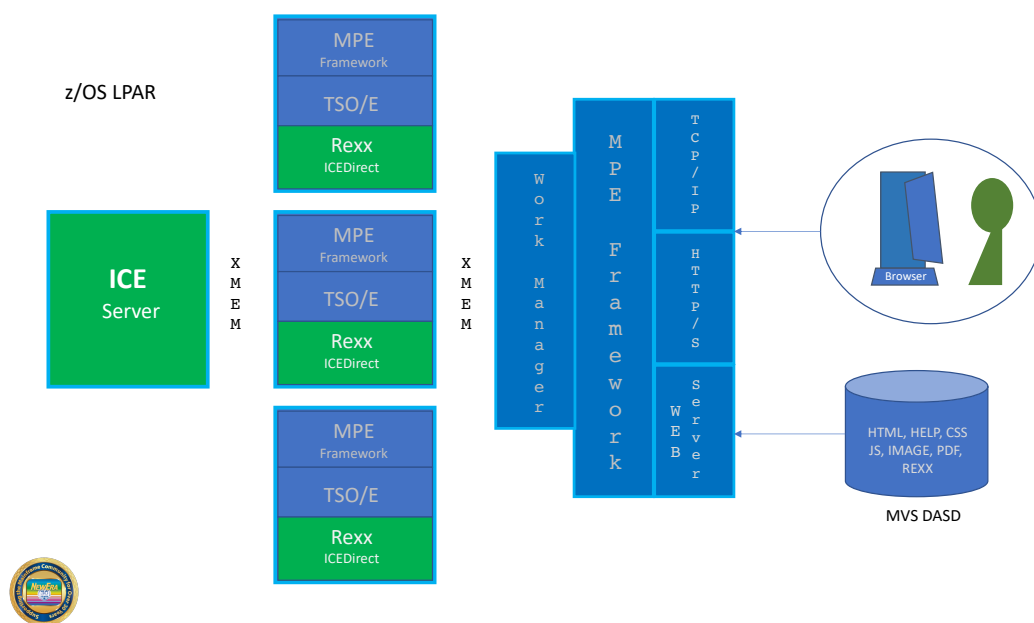
7. The Web Server Explained

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 2.3 or higher

7.1. Server Overview

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.

7.2. 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*.

7.2.1. 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

7.3. 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.

7.4. *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.

7.5. 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)
```

7.6. Server Reports and Logs

7.6.1. 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 (4/22) 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.

7.6.2. 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.

7.6.3. 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 suppress 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.*

7.6.4. Error Examples

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

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

Do that ten times in a row and get both ten 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

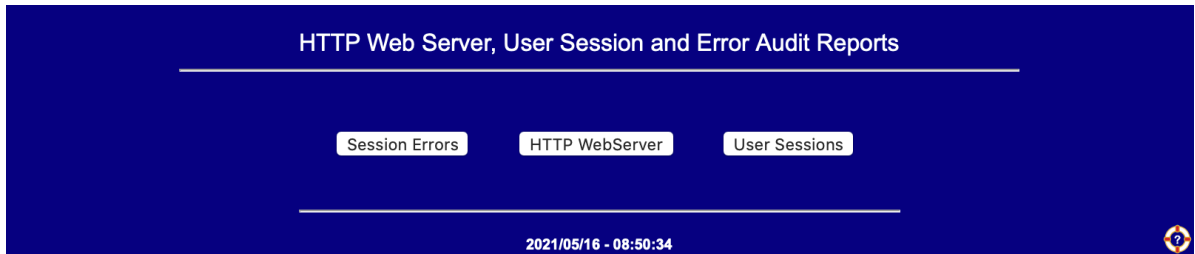
Certain integrity errors may generate the follow message display and log the user off the system.



- 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,...

7.7. 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.

7.7.1. Sample Server and Error Reports

ICE Direct Sidebar Menu
YourID Settings
MyWHO
MyHIS
MyMFI
MyMFE
z/OS Inspections
MyBGN
MyBAT
MySAE
MyCHK
MyHLC
TCE Boundaries
MyBNI
MyADM
MyAUD
MyEXT
MyDET
MyEXC
MyMFA
Access Journals
MyQRY
MyPDS
MyMBR
MyLIB
MyMOD

MyHost - Plex - ADCDPL - Lpar - S0W1 - Esm - RACF - Url - www.myicedirect.com:8201
ICE is Licensed on CPU - Model - 1090 - Version - FF - Serial - FF01B19B1090

Last IPLed - Day - Thursday - Date - 04.15.2021 - Time - 1:36:25
Release V2R4 IPLUnit 0A83 LoadSfx WS IEANUC 1 IODFUnit 0A83 HWName -n/a- LPARName -n/a- VMUserid ZOS24M

ICE License Details
21/04/20 - 19:33:02

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

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

Userid:PROB11 Date:21/04/30 Time:12:28:32 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 WSRV01 (Release 1.1.01)
2021/04/30 12:28:33 I Parmlib Suffix : 00
2021/04/30 12:28:33 I Web Server ID : WSRV
2021/04/30 12:28:33 I TSO/E Server ID : WSRV01
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 WSRV
2021/04/30 12:28:34 I Now running under userid PROB11
2021/04/30 12:32:48 E PROB11 - Invalid Dataset/(Member) Display Request.
2021/04/30 12:32:51 I Shutdown requested by script

Records:14

To Top

2021/04/30 - 19:33:50

MyMFI
MyMFE
z/OS Inspections
MyBGN
MyBAT
MySAE
MyCHK
MyHLC
TCE Boundaries
MyBNI
MyADM
MyAUD
MyEXT
MyDET
MyEXC
MyMFA
Access Journals
MyQRY
MyPDS
MyMBR
MyLIB
MyMOD
MyUSS
MySEQ

ICE License Details
21/04/20 - 07:50:08

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

023 21/04/28 12:30:31 Web Error: Item README/WEB CSRF=F202E3C0F21CC080 not found
024 21/04/28 12:30:31 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123031
025 21/04/28 12:30:34 Web Error: Item README not found
026 21/04/28 12:30:34 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123034
027 21/04/28 12:31:42 Web Error: Item SYS1.SAMPLIB not found
028 21/04/28 12:31:43 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123142
029 21/04/28 12:31:54 Web Error: Item SYS1.SAMPLIB(ALZBLK) not found
030 21/04/28 12:31:54 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123154
031 21/04/28 12:32:01 Web Error: Item SYS1.SAMPLIB(ALZBLK) not found
032 21/04/28 12:32:01 Web error reports have been disabled
033 21/04/28 12:32:18 Web Error: Item 5BETA0419 not found
034 21/04/28 12:32:18 Web Error report suppressed
035 21/04/28 12:32:31 Web Error: Item A not found
036 21/04/28 12:32:31 Web Error report suppressed
037 21/04/28 12:33:00 Web Error: Item SYS1.SAMPLIB not found
038 21/04/28 12:33:00 Web Error report suppressed
039 21/04/28 12:33:04 Web Error: Item SYS1.SAMPLIB not found
040 21/04/28 12:33:04 Web Error report suppressed
041 21/04/28 12:33:11 Web Error: Item SYS1.SAMPLIB(TEST) not found
042 21/04/28 12:33:11 Web Error report suppressed
043 21/04/28 12:33:14 Web Error: Item SYS1.SAMPLIB(TEST) not found
044 21/04/28 12:33:14 Web Error report suppressed
045 21/04/28 12:34:09 Web Error: Item ADCD.Z23C.VTAMLST not found
046 21/04/28 12:34:09 Web Error report suppressed
047 21/04/28 12:34:22 Web Error: Item ADCD.Z23C.VTAMLST(A0600) not found
048 21/04/28 12:34:22 Web Error report suppressed
049 21/04/28 12:35:16 Web Error: No response from script
050 21/04/28 12:35:16 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123516
051 21/04/28 12:36:38 Web Error: No response from script
052 21/04/28 12:36:38 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123638
053 21/04/28 12:36:45 Web Error: No response from script
054 21/04/28 12:36:45 / Report written to: IFO.MTGY.WS.WSRV.WREP.D210428.T123645

The Integrity Controls Environment (ICE) Application – ICEDirect Web Platform

39

7.8. 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.

7.8.1. Primary Task Includes:

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

7.8.2. Web Server Includes:

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

8. Additional Licensed Application

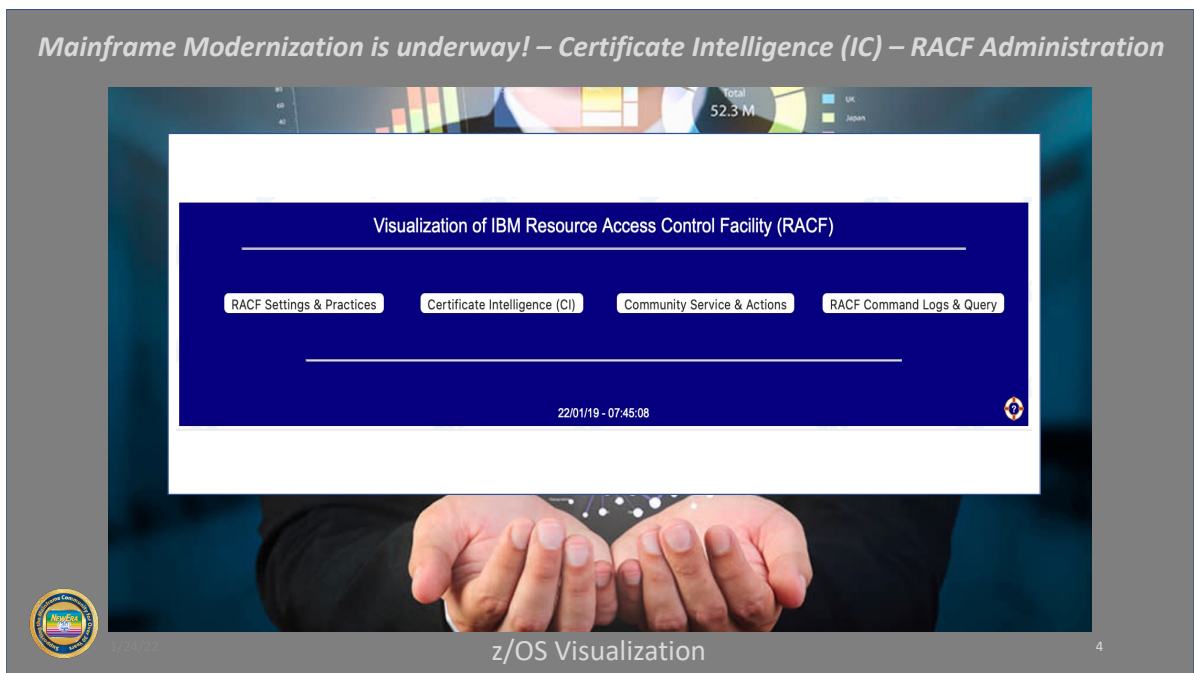
If you are licensed for z/OS Visual or RACF Visual or both, you will find their “Access Points” on the ICEDirect “Crossbar”. Select them to display their respective interfaces and function as described below.

If you are not licensed but would like to begin an evaluation of either/both send an email to NewEra Technical Support, address support@newera.com requesting a temporary license key.

8.1. RACF Visual

The RACF Dataspace and the function of RACF Visual related to it and their major features. They include:

1. RACF Settings & Practices
2. Certificate Intelligence (CI)
3. Community Service & Action
4. RACF Command Logs & Query



8.1.1. RACF Settings & Practices

SETROPTS is the core of RACF; its settings reflect and enforce organizational policy. The source data used by this function is extracted in real-time from the running systems and presented in three major groupings:

Control Class Descriptors - Event SMF Logging - Attributes and Options

These functions help to:

Identify and Audits Classes by Descriptor

Isolate Profiles with ACLs permitting Orphan UserIds

Pinpoint Non-Compliance with Generally Accepted Security Practices (GASP).

Mainframe Modernization is underway! – RACF Visual - RACF Settings & Practices

The screenshot displays the RACF Visual interface. At the top, it shows system information: IBM Resource Access Control Facility (RACF) - Release:7791, RACF Special: Yes, RACF Operations: ---, Last IPL: Saturday 01.22.2022 1:57:76, RACF Auditor: Yes, RACF ROAuditor: ---. Below this, it lists the running system details: SmfID: S0W1, IPLUnit: 0A83, LoadSfx: WS Nucleus: 1, System: S0W1, Dataset: SYS1.IPLPARM, HWName: -n/a-, Sysplex: ADCDPL, IODFUnit: 0A83, LPAR: -n/a-, z/OSVer: V2R4, Dataset: SYS1.IODF99, VM: ZOS24M. The interface also shows SYS1.RACFDS, None, and None. A button labeled 'Show SETROPTS Source Records' is visible. The bottom of the screenshot shows a person's hands holding a small globe, with the text 'z/OS Visualization' below it.

Linked SETROPTS Class Audit
ACTIVE CLASSES = 77/246 - Profiles = 1012

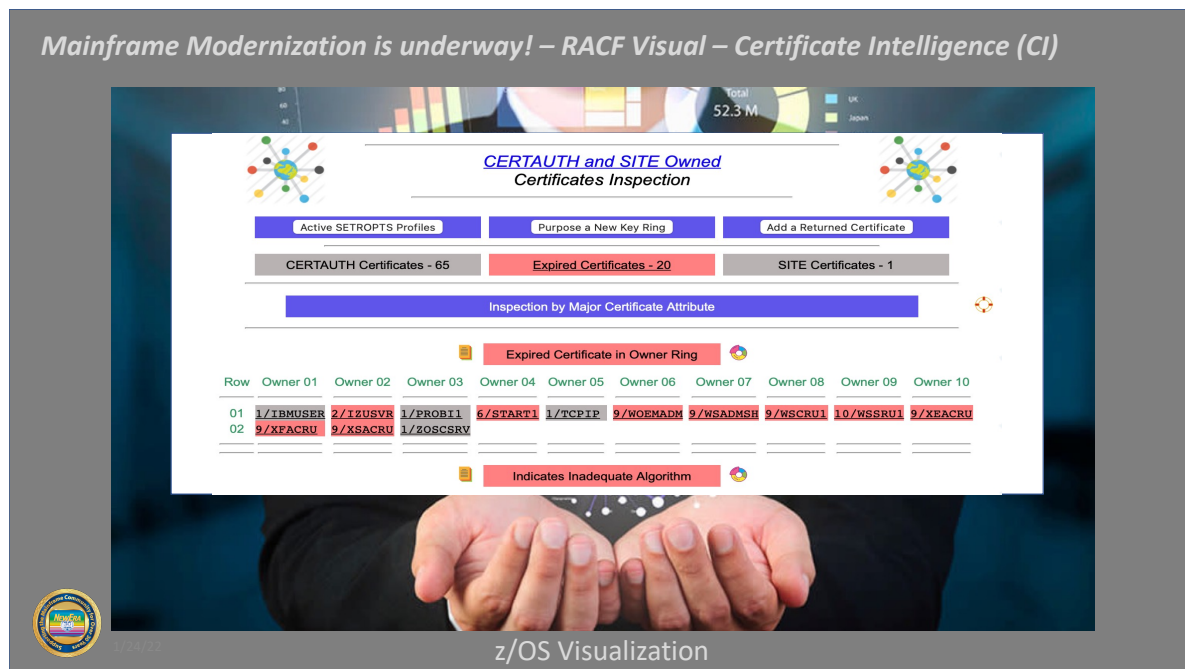
Row	Name 01	Name 02	Name 03	Name 04	Name 05	Name 06	Name 07	Name 08	Name 09	Name 10
01	DATASET	USER	GROUP	ACCTNUM	ACICSPCT	AIMS	APPL	BCICSPCT	CBIND	CCICSCMD
02	CDT	CIMS	CONSOLE	CSFKEYS	CSFSERV	DCICSDCT	DIGTCERT	DIGTCRIT	DIGTNMAP	DIGTRING
03	DIMS	DSNADM	DSNR	ECICSDCT	EJBROLE	FACILITY	FCICSFCT	GCICSTRN	GCSFKEYS	GEJBROLE
04	GIMS	GMOADMIN	GSDSF	GXCFSKEY	GXFACILI	GZMFAPLA	HCICSFCT	IDIDMAP	IIMS	JCICSJCT
05	JIMS	KCICSJCT	LIMS	LOGSTRM	MCICSPPT	MIMS	MOADMIN	NCICSPPT	OPERCMDS	PCICSPSB
06	PTKTDATA	PTKTVAL	QCICSPSB	RCICSPSB	RDATALIB	RIMS	SCICSTST	SDSF	SERVAUTH	SERVER
07	STARTED	SURROGAT	TAPEVOL	TCICSTRN	TEMPDSN	TIMS	TSOAUTH	TSOPROC	UCICSTST	UNIXPRIV
08	VCICSCMD	WBEM	WCICSPSB	XCSFKEY	XFACILIT	ZMFAPLA	ZMFCLOUD			

8.1.2. Certificate Intelligence (CI)

Certificate Intelligence (CI) inspects the certificate content of the RACF/RACDCERT Database and presents its findings in “Groups” on its introduction screen.

Inspection Points Include:

Key Rings, by Ring Owner, containing Expired Certificates (STIG ID:RACF-CE000020)
Signing Algorithms, Key Types, Key Sizes, Trust Status, Private Keys, Ring Connections



Digital Ring Information for UserId - START1



RACDCERT CERTAUTH/SITE LIST - Filtered by Owner/Ring - START1

Row	Owner	Certificate Labels Within UserId Owned Ring(s)	Expire	Usage	Default
Ring: >ICEDirectServer.Ring<					
001	CERTAUTH	GoDaddy Global Root CA	2031/05/02	CERTAUTH	NO
002	CERTAUTH	GoDaddy Global Inter 1	2031/05/29	CERTAUTH	NO
003	CERTAUTH	GoDaddy Global Inter 2	2034/06/29	CERTAUTH	NO
004	ID(START1)	ICEDirect Server	2022/11/21	PERSONAL	YES
Ring: >JES2EDS<					
005	ID(START1)	JES2 CLIENT EDS	2019/03/20	PERSONAL	YES
006	CERTAUTH	ZOSMFCA	2021/08/20	CERTAUTH	NO

8.1.3. Community Service & Action

Using the functions provided, administrators can answer questions for and take action on the behalf of users, for example:

What Certificates do I own? What is their Status? What Key Rings? What ACLs?
Can you Reset my Password, Resume/Revoke my UserId, Connect me to a Group?

In addition, new users can be added by using constructed or selected UserId Models.

Mainframe Modernization is underway! – RACF Visual – Community Service & Actions

z/OS Community
RACF Services and Actions

AdHoc Target UserId: **PROB1**

Buttons: Show Certificates, Show Key Rings, Show Access (ACL), Show RACF Profile, Show Connections, Revoke UserId, Resume UserId, Delete the UserId, Reset Password, Connect UserId

Models of Userids that may be used to Add New UserId to RACF

Indicates Model is not Defined

Model 01	Model 02	Model 03	Model 04	Model 05	Model 06	Model 07	Model 08	Model 09	Model 10
MODUSR01	MODUSR02	MODUSR03	MODUSR04	MODUSR05	MODUSR06	MODUSR07	MODUSR08	MODUSR09	MODUSR10
Model 11	Model 12	Model 13	Model 14	Model 15	Model 16	Model 17	Model 18	Model 19	Model 20
ACCOUNT: OBAGS1	Model User's	Model User's	Model User's	Model User's	Model User's	Model User's	Model User's	Model User's	Model User's
Cloneld	Cloneld	Cloneld	Cloneld	Cloneld	Cloneld	Cloneld	Cloneld	Cloneld	Cloneld

Alter Existing UserId Profile

z/OS Visualization

*UserId **PROB1** is Connected to 3 of the 31 Available Community Groups*

31 - Unique Community Groups

Row	Group 01	Group 02	Group 03	Group 04	Group 05	Group 06	Group 07	Group 08	Group 09	Group 10
01	CEAGP	CFZADMGP	CFZSRVGP	CFZUSRGP	CIMGP	IYU	IYU0	IYU0RPAN	IYU0RPAW	IYU000
02	IZUADMIN	IZUSECAD	IZUUSER	OMVSGRP	STCGROUP	SYS1	UNVGRP1	WEBGRP	WSCFG1	WSSR1
03	XACFG	XASRVG	XECFG	XESRVG	XFCFG	XFSRVG	XSCFG	XSGUESTG	KSSRVG	ZOSCGRP
04	ZWEADMIN									

8.1.4. RACF Command Logs & Query

The RACF Database of Settings and Certificates is modified using RACF and RACDCERT Commands. Knowledge of these commands, their real-time use and history is critical to maintaining the overall integrity of RACF and z/OS.

This function can dynamically change the logging profile, adding and/or deleting command targets. Generate, in real-time, reports and graphics showing command usage and control interval monitoring and alerts of command usage.

Mainframe Modernization is underway! – RACF Visual – RACF Commands & Logs

RACF Command History - LPAR S0W1

RACF Command Capture is now On

Row	Select	Column 1	Select	Column 2	Select	Column 3	Select	Column 4	Select	Column 5
01	<input type="checkbox"/>	SETROPTS	<input checked="" type="checkbox"/>	ADDSD	<input type="checkbox"/>	ADDUSER	<input checked="" type="checkbox"/>	ADDGROUP	<input checked="" type="checkbox"/>	CONNECT
02	<input checked="" type="checkbox"/>	PERMIT	<input checked="" type="checkbox"/>	RALTER	<input checked="" type="checkbox"/>	RDEFINE	<input type="checkbox"/>	DELDSD	<input type="checkbox"/>	DELGROUP
03	<input type="checkbox"/>	DELUSER	<input checked="" type="checkbox"/>	RDELETE	<input type="checkbox"/>	REMOVE	<input checked="" type="checkbox"/>	ALTDSD	<input type="checkbox"/>	ALTGROUP
04	<input checked="" type="checkbox"/>	ALUSER	<input type="checkbox"/>	LISTDD	<input type="checkbox"/>	LISTGRP	<input checked="" type="checkbox"/>	LISTUSER	<input type="checkbox"/>	PASSWORD
05	<input type="checkbox"/>	RLIST	<input type="checkbox"/>	SEARCH	<input type="checkbox"/>	RESTART	<input type="checkbox"/>	SIGNOFF	<input type="checkbox"/>	SETR
06	<input type="checkbox"/>	TARGET	<input type="checkbox"/>	RACDCERT	<input type="checkbox"/>					

☒ Denotes Recommended Default ☒ Denotes Current Defined Commands

Update the RACF Command Capture List

z/OS Visualization

Through RACF Visual those issuing commands may document the purpose of their work by providing Authority, Reference and Descriptive text. Information provided (or not) is, along with the issued command string and system reply, recorded in the ICE Control Journal.

Submit to Validate & Confirm Certificate Deletion

01) ☒ RACDCERT CERTAUTH DELETE (LABEL('ADCDCA')) FORCE

Authorization ☒ Reference

Event Descriptor

8.1.5. Access Requirements

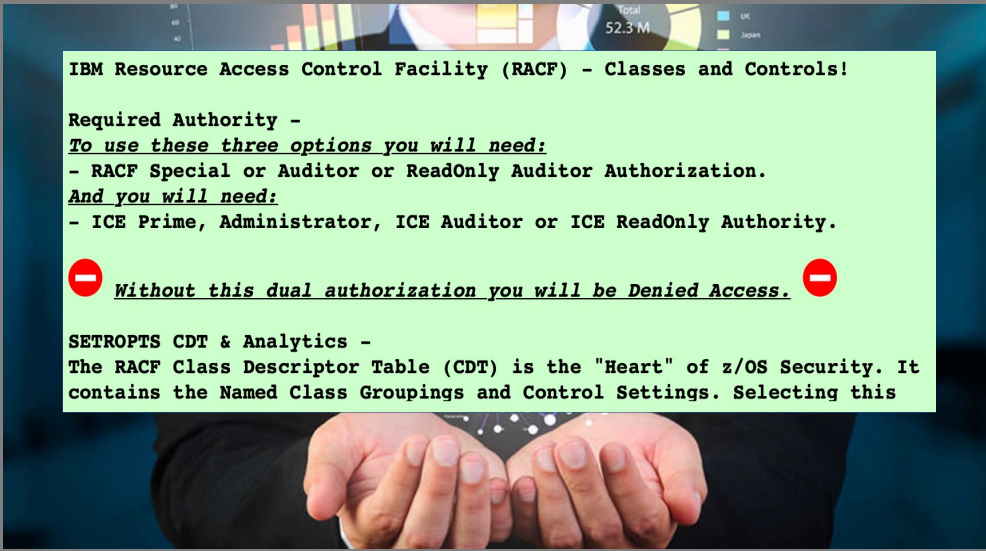
To access RACF Visual as hosted on your ICEDirect Platform, you will need the following Permissions and Authority:

From RACF – Special, Auditor and/or ROAuditor

From ICEDirect – TCEPrime, Admin, Auditor and/or ROAuditor

To execute commands – Update access to the NewEra nez. Profile in the Facility Class

Mainframe Modernization is underway! – RACF Visual – Access Requirements



IBM Resource Access Control Facility (RACF) - Classes and Controls!

Required Authority -
To use these three options you will need:

- RACF Special or Auditor or ReadOnly Auditor Authorization.
- And you will need:
- ICE Prime, Administrator, ICE Auditor or ICE ReadOnly Authority.

Without this dual authorization you will be Denied Access.

SETROPTS CDT & Analytics -
The RACF Class Descriptor Table (CDT) is the "Heart" of z/OS Security. It contains the Named Class Groupings and Control Settings. Selecting this

z/OS Visualization

Hello PROBI1! Your ICE Direct Access Status & IPAddress - 147.160.149.185

☐ General User ☒ TCEPrimeAdmin ☐ TCEAdmin ☒ MFEAuditor ☐ MFEROAuditor

What Can I Do?

22/01/24 - 08:12:15

PROBI1 - Your ICEDirect Role(s) is/are Privileged to these Activities

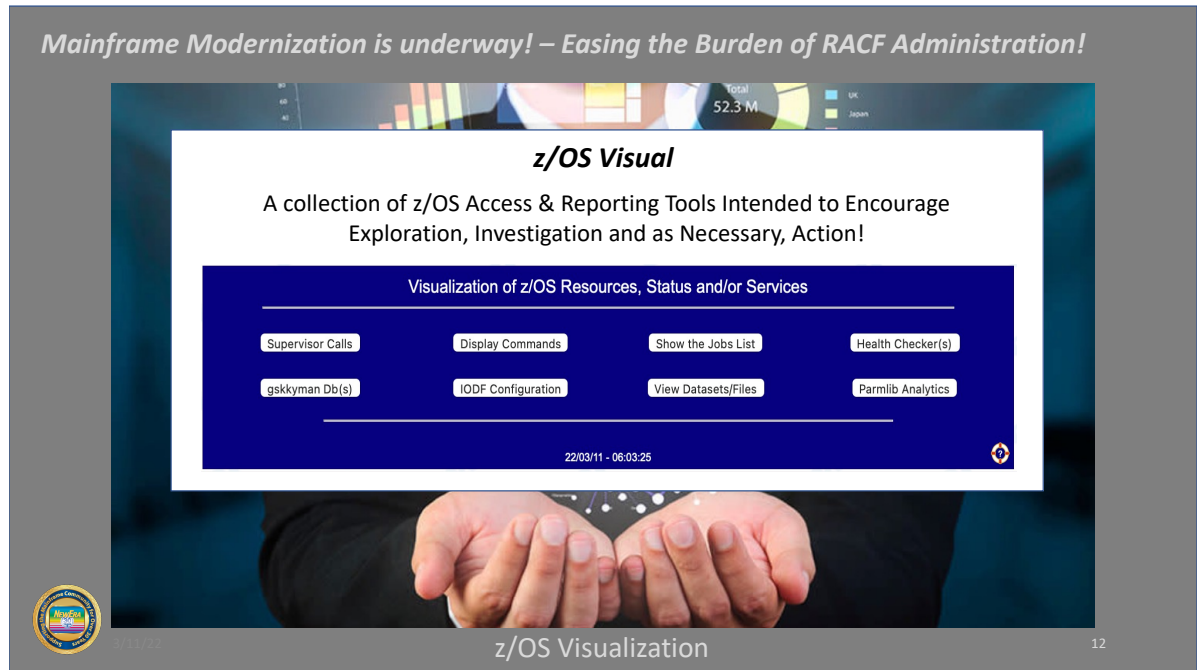
Working • Analytic • Controls • Security •

2022/01/24 - 08:13:25

8.2. z/OS Visual

The z/OS Dataspace and the function of z/OS Visual related to it and their major features. They include:

Supervisor Calls, Display Commands, Show the Jobs List, Health Checker
Gskkyman Db(s), IODF Configuration, View Dataset/Files, Parmlib Analytics



In order to access these applications you will need READ access to the ICE Facility Class profile. This Profile is used to control access to the TSO/ICE command execution module NSIMOCM. In addition, each command issued is LPAR specific and will be ROUTED to a named LPAR for execution. A sample command is shown below:

```
LPARNAME = 'LPAR123'  
COMMAND = 'IOS,CONFIG'  
CMD = " 'ROUTE "LPARNAME",D "COMMAND" ' "  
ADDRESS TSO ; "NSISOCM "CMD
```

8.2.1. CMD = "D XCF"

Access rights to the Display XCF command is of particular importance as it provides the names of the LPARs that make up the sysplex that ICEDirect is operating within and therefore the scope of the z/OS Visual Application.

8.2.2. Supervisor Calls

An SVC Instruction is used to generate a Supervisor Call. The table presented is generated by a bespoke version of SVCLOOK and displays, in two tables those SVCs from IBM and those Site specific. Each table shows - Module Name, Type, Location and other identifiers.

ESP - 05/01/22

MyHost:S0W1


XMLEditor

Clear Lower Frame


z/OS Visual

RACF Visual

Logout



Full List of Supervisor Call (SVC) Modules



From the Nucleus

From the LPAList

SVC is Unused

Duplicate

IBM Defined SVC Modules

Row	Type:SVCNum	Location	Values	Lib	Module	Type	Authorization	ASC	Locks
001	SVCMOD:IBM000	80FF39B0	00008000	NUC	IGC000	1	-----	---	LOCAL
002	SVCMOD:IBM001	80FF1358	00008000	NUC	IGC001	1	-----	---	LOCAL
003	SVCMOD:IBM002	81445628	00008000	NUC	IGC002	1	-----	---	LOCAL
004	SVCMOD:IBM003	81092590	00808000	NUC	IGC003	1	-----	Yes	LOCAL
005	SVCMOD:IBM004	814D8B6A	00008000	NUC	IGC004	1	-----	---	LOCAL
006	SVCMOD:IBM005	814D8B6A	00008000	NUC	IGC005	1	-----	---	LOCAL
007	SVCMOD:IBM006	813D1B68	80008000	NUC	IGC006	2	-----	---	LOCAL
008	SVCMOD:IBM007	813D89B8	80008000	NUC	IGC007	2	-----	---	LOCAL
009	SVCMOD:IBM008	813D1E40	80008000	NUC	IGC008	2	-----	---	LOCAL
010	SVCMOD:IBM009	813BDCC0	80008000	NUC	IGC009	2	-----	---	LOCAL
011	SVCMOD:IBM010	814D9EC6	00008000	NUC	IGC010	1	-----	---	LOCAL
012	SVCMOD:IBM011	842FFC60	C0000000	LPA	IGC00011	3/4	-----	---	---
013	SVCMOD:IBM012	813D5758	80808000	NUC	IGC012	2	-----	Yes	LOCAL
014	SVCMOD:IBM013	849C1000	C0808000	LPA	IGC00013	3/4	-----	Yes	LOCAL

8.2.3. Display Commands

The table at the top of the panel shows the name of all LPARs within the sysplex (D XCF) Discovery. Each can be selected by System Name by checking the radio-button that precedes it. This will set the ROUTE parameter for each Display command that follows. Once a System is selected (Local System is the Default) click the numeric value that precedes the Display command of interest. Target a new System by name at any time.

Eligible z/OS LPARS - Discoverd Targets/Selection - by Display XCF

System

S0W1

☒
☐
☐

Local

Remote

System

☐
☐
☐

System

☐
☐
☐

System

☐
☐
☐

System

☐
☐
☐

System

☐
☐
☐

Activate a New System Target

22/04/18 - 11:33:56

Display Command Selection List

Target LPAR - S0W1

View	Commands	SubParms	Command Description
01	A	-	System activity
02	ALLOC	GRPLOCKS	MVS device allocation group locks
03	ALLOC	OPTIONS	MVS
04	APPC	-	APPC/MVS information
05	ASCH	-	ASCH configuration
06	ASM	-	Auxiliary storage
07	AUTOR	-	Auto-reply policy and WTORs
08	CEE	-	System-level Language Environment options
09	CF	-	Attached coupling facility
10	CNGRP	-	Console group definitions
11	CONSOLES	-	Console status information
12	DIAG	-	DIAG parmlib information
13	DFL	-	Data lookaside facility
14	DUMP	-	Dump options or dump data set status
15	EMCS	-	Extended MCS information
16	ETR	-	Timer synchronization mode and ETR ports
17	FXE	-	Function enablement state information
18	GRS	-	Global resource serialization

The Integrity Controls Environment (ICE) Application – ICEDirect Web Platform

49

8.2.4. Show the Jobs List


To generate the records necessary to create the panel the following commands are issued:

- ADDRESS TSO ; "NSIRAJI "
- ADDRESS TSO ; "NETSTAT"
- CMD = "'D A,L'"; ADDRESS TSO ; "NSISOCM "CMD


NSIRAJI is a proprietary ICE command that returns all JOBS by name, active or waiting. This is modeled after SDSF option ST.

NETSTAT, a standard system utility returns, by JOB by name, Network Status. Of importance is the name of the PORT the JOB is listening on or connected to.

'D A,L', is a standard system Display command. It provides the real-time status of active JOBS.



AdHoc Criteria to Start a Job or Display Status



Route: Issue:

Submit AdHoc Command

Active Job Status - S0W1

Modify a Selected Job

Indicates a Job has ESM Profile

Indicates Established Connection

Row	Pop	Command	JobName	StepName	ProcStep	JobId	Owner	ASCB	ASID	PORT
001	<input type="radio"/>		LLA	LLA	LLA	----	----	00FB5000	001A	----
002	<input type="radio"/>		JES2	JES2	IEFPROC	----	----	00FCA680	001C	----
003	<input type="radio"/>		VLF	VLF	VLF	----	----	00FCA500	001D	----
004	<input type="radio"/>		HZR	HZR	IEFPROC	----	----	00FCA380	001E	----
005	<input type="radio"/>		VTAM	VTAM	VTAM	STC08990	START1	00FCA200	001F	----
006	<input type="radio"/>		DLF	DLF	DLF	----	----	00F52400	0021	----
007	<input type="radio"/>		RACF	RACF	RACF	STC09003	START1	00FB4500	0022	----
008	<input type="radio"/>		RRS	RRS	RRS	----	----	00F96700	002E	----
009	<input type="radio"/>		TSO	TSO	STEP1	STC08999	START1	00F96580	002F	----
010	<input type="radio"/>		SDSF	SDSF	SDSF	STC09000	START1	00F96400	0030	----
011	<input type="radio"/>		TN3270	TN3270	TN3270	STC09004	TCPIP	00F96280	0031	23
012	<input type="radio"/>		SDSFAUX	SDSFAUX	SDSFAUX	STC09005	START1	00FC8B80	0035	----

Selecting a highlighted PORT will display additional information about both Local and Remote connections – IPAddress, Domain Name and Status. If SAF controls are enabled for a JOB, the name will be highlighted in blue.

8.2.5. Health Checker(s)

As with other z/OS Visual functions, display XCF is executed in order to derive the names of all systems in the sysplex ICEDirect is running in. Any of the names may be selected as a target. This will be followed by a display of Health Check findings on the Target System.

Results are presented both by Severity and by Check Owner. Check Owner results can be further grouped by a selected Owner, for example RACF.

Cursor under a Check to show the detail being reported. Note that such detail is for the Local system only.

IBM HealthChecker for z/OS - LPAR S0W1 Findings
 Last IPL: Sunday 03.13.2022 15:9:92
 This is the Running System

SmfID: S0W1 IPLUnit: 0A83 LoadSfx: WS Nucleus: 1	System: S0W1 Dataset: SYS1.IPLPARM HWName: -n/a-	Sysplex: ADCDPL IODFUnit: 0A83 LPAR: -n/a-	z/OSVer: V2R4 Dataset: SYS1.IODF99 VM: ZOS24M
--	--	--	---

Exc/High: 0
 Exc/Med: 4
 Exc/Low: 1
 Success: 11
 Env/Ina: 6

22/04/18 - 14:16:02

HealthCheck Finding Grouped by Selected Owner

Check Owner is IBMRACF

EXCEPTION-HIGH	EXCEPTION-MEDIUM	EXCEPTION-LOW
INACTIVE	SUCCESS	ENVIRONMENT N/A

Click the Owner Name to Filter by Owner

001 IBMRACF has 22 Checks:

001	RACF_BATCHALLRACF	ACTIVE,ENABLED,EXCEPTION-MED
002	RACF_RRSF_RESOURCES	ACTIVE,ENABLED,SUCCESSFUL
003	RACF_ENCRYPTION_ALGORITHM	ACTIVE,ENABLED,SUCCESSFUL
004	RACF_AUDIT_CONTROLS	INACTIVE,ENABLED,INACTIVE
005	RACF_PASSWORD_CONTROLS	ACTIVE,ENABLED,EXCEPTION-LOW
006	RACF_CERTIFICATE_EXPIRATION	ACTIVE,ENABLED,EXCEPTION-MED

If Multiple selections are made a differential analysis of findings on the selected Systems will show similarities and differences in check findings across systems.


8.2.6. Gskkyman db(s)

This UNIX type Digital Certificate Database will often serve as the equivalent of a RACF Key Ring. After a preliminary decision is made between Searching for All such Databases or just those with a specific file extension, .kdb being the default, a scan of the UNIX file system (zHFS) on the Local is made.

Findings are reported in a table that details the state of the Database(s) discovered. To show the Certificates in a Database check the box adjacent to its name and Select the List option. The resulting worksheet will show the certificate name and expiration status.


It is considered a best practice to delete expired certificates as soon as possible.

Select a certificate from the worksheet to show its content and additional processing options.



[Dynamically Extracted gskkyman Key Database Files](#)

File Permission - General Accepted Practice "-rw-r-----"









List Certificates in Selected Key Database

Password in Stash File

Password has Expired

Password has Failed

Permissions Problematic

Row	Chk	Full Qualified Key Database File Path	Password	FIPS	Permits	Key
01	<input type="checkbox"/>	/u/paul/paul1.kdb	<input type="text"/>	No	-rw-r-----	
02	<input type="checkbox"/>	/u/paul/paul2.kdb	<input type="text"/>	No	-rw-r-----	
03	<input type="checkbox"/>	/u/paul/paul	<input type="text"/>	No	-rw-r-----	
04	<input type="checkbox"/>	/u/paul/paul3.kdb	<input type="text"/>	No	-rw-r-----	
05	<input type="checkbox"/>	/u/paul/paultestone.kdb	<input type="text"/>	No	-rw-r-----	
06	<input type="checkbox"/>	/Z24B/usr/lpp/ihpa_zos/plugin/etc/plugin-key.kdb	<input type="text"/>	No	-rwxr-xr-x	

Elapsed Seconds:45.98

ICE:96%

TCP:4%

To Top


2022/04/18 - 11:38:29

8.2.7. IODF Configuration


When this option is selected, Display XCF is run to determine the names of the systems in the sysplex that ICEDirect is running in. The discovered names are displayed in matrix. Selecting a system from the matrix results in running/routing the Display command IPLINFO and extracting its return values in order to discover the name of the selected systems IODF Dataset.

In the panel that follows the Real IODF becomes selectable as does a user provided Work IODF. Selecting either will result in the Dataset being passed to the standard system utility “CBDMGHCP”. If the Dataset is shared across the sysplex the process continues. If not a message is displayed.

The first panel displayed shows a break-down of all defined processors by LCSS with Partitions within LCSS. Click a partition by name to show additional configuration detail beginning with CHIPDs.





IODF/IOCP Analytics - Central Processor Complex (CPC)
SYS1.IODF22 - 2020-10-15 11:35:03



Indicates a Defined Partition

Indicates an Undefined Partition

Row	Name	Unit	Model	Description	Serial	SNAAddr	Mode	Level
1/2	CPA	8561	T01	IBM z15 at NL	03CBB88561	IBM390PS,CPA	LPAR	H191114
1/6	LCSS:0	MAXDEV=65280,65535,65535,65535						
	Partition:1	Partition:2	Partition:3	Partition:4	Partition:5			
	CPA01	CPAUS102	CPA03	CPA04	CPA05			
	Partition:6	Partition:7	Partition:8	Partition:9	Partition:A			
	CPAUS106	CPA07	CPA08	CPA09	CPAUS10A			
	Partition:B	Partition:C	Partition:D	Partition:E	Partition:F			
	CPA0B	CPA0C	CPA0D	CPA0E	CPA0F			
2/6	LCSS:1	MAXDEV=65280,65535,65535,65535						
	Partition:1	Partition:2	Partition:3	Partition:4	Partition:5			
	CPA11	CPA12	CPA13	CPAUS114	CPA15			


8.2.8. View Datasets/Files

Somewhat similar to ISPF 3.4 this single panel supports the display of both MVS Datasets and UNIX Files (zHFS).


To access Datasets enter a fully qualified dataset name or “Wildcard” name similar to that shown in the panel below and then click “Submit Dataset Query”. The results that follow will list all locally Cataloged Datasets that match the criteria showing, in addition to the full name, their Control List standing, ESM UACC, VOLUME, ESM Profile, Alloc type and member count, if any.

If the Dataset is a “Controlled Dataset” clicking the ICON will list members in Dataset as known to The Control Editor. Selecting a member from the list will show all Journaled member events. To list the “Real Dataset” cursor under the name and press enter to display the “Member List”. Selecting a member from the list will show its content.

To query UNIX (zHFS) files enter the file system Root, in the example “/u”, a word that is in the file path or for any path the “Wildcard Word PATH”, a file extension i.e. “.kdb” or the “Wildcard Word FILE”. PATH and FILE are not allowed in the same query, case is not sensitive.



Enter Criteria for a Dataset and/or File Query



Dataset Actions

USER.Z24B.*

Submit Dataset Query

UNIX File Actions

Root /u
Path PAUL
File FILE

Submit UNIX File Query

Resulting Records from Dataset Query

Row	CtL	UACC	Volume	Profile	Fully Qualified Dataset - Click to Show Contents	Alloc	Count
001		-----	B4CFG1	NONE	USER.Z24B.CIDTABL	PDS	0
002		-----	B4CFG1	NONE	USER.Z24B.CLIST	PDS	0
003		-----	B4CFG1	NONE	USER.Z24B.HELP	PDS	0
004		-----	B4CFG1	NONE	USER.Z24B.ISPLLIB	PDS/U	0
005		-----	B4CFG1	NONE	USER.Z24B.ISPMLIB	PDS	0
006		-----	B4CFG1	NONE	USER.Z24B.ISPPLIB	PDS	0
007		-----	B4CFG1	NONE	USER.Z24B.ISPSLIB	PDS	0
008		-----	B4CFG1	NONE	USER.Z24B.ISPTLIB	PDS	0
009		-----	B4CFG1	NONE	USER.Z24B.LINKLIB	PDS/U	0
010		-----	B4CFG1	NONE	USER.Z24B.LPALIB	PDS/U	5
011		-----	B4CFG1	NONE	USER.Z24B.MSGENU	PDS	0
012	⚠	-----	B4CFG1	NONE	USER.Z24B.PARMLIB	PDS	35
013		-----	B4CFG1	NONE	USER.Z24B.PROCLIB	PDS	28
014		-----	B4CFG1	NONE	USER.Z24B.STCJOBS	PDS	0
015		-----	B4CFG1	NONE	USER.Z24B.SYSEXEC	PDS	0

8.2.9. Parmlib Analysis

Like others, this function uses XCF to identify all LPARs in the sysplex associated with ICEDirect and uses that information to display a matrix of system names from which a system Target can be selected for Parmlib Analysis. When a target system is selected its name is used as the ROUTE Parm of two DISPLAY commands, IPLINFO and PARMLIB. The records returned from these are processed for information, IEASYS members are identified, content consolidated and Parmlib member usage determined. The results are mapped against a comprehensive list of all possible Parmlib members by name; the end result is the analysis shown below.

The analysis answers the questions, is the possible member in the Parmlib concatenation? If the member is not in Parmlib it is marked – Not in Parmlib Concatenation. If the member is in Parmlib the question is - it called out in the IEASYS concatenation – Activated or Not Active? The member may possibly be in Parmlib BUT not be a valid z/OS Parmlib member – Not a Defined z/OS Member. If the member is Activated a further question answered – is there a SET command that may be used to reset any named in IEASYS members – access permissions may limit command execution/access.

Eligible z/OS LPARS - Discovered Targets & Selection - Display XCF

System

S0W1

System

System

System

System

System

Local

Remote

Activate a New System Target

22/04/18 - 11:48:26

PARMLIB Member State and Selection List - S0W1

View	Members	Keyword	SetCmd	Parmlib Member Description
001	ADYSETxx	-	-	Dump suppression
002	ALLOCxx	ALLOC	ALLOC	Allocation system
003	ANTMIN00	-	-	ANTMAIN control parameters
004	ANTXIN00	-	-	XRC services
005	APPCPMxx	-	APPC	Define APPC/MVS configuration
006	ASCHPMxx	-	ASCH	APPC/MVS transaction scheduler
007	AUTORxx	AUTOR	AUTOR	Auto-reply policy specifications
008	AXRxx	AXR	-	System REXX options
009	BLSCECT	-	-	Formatting exits for dump and trace
010	BLSCUSER	-	-	Installation customization for dump/trace
011	BPXPRMxx	OMVS	-	z/OS UNIX System Services parameters
012	CEAPRMxx	CEA	-	Common event adapter parameters
013	CEEPRMxx	CEE	CEE	Runtime option parameters
014	CLOCKxx	CLOCK	-	Time of day parameters
015	CNGRPxx	-	CNGRP	Specify console groups
016	CNLcccxx	-	MMS	Time/date format for translated messages
017	COFDLFxx	-	-	Hiperbatch parameters

The Integrity Controls Environment (ICE) Application – ICEDirect Web Platform

55

9. Application License Installation and Activation

9.1. XML License Document

```
<customer>
  <id>@DOCIDNUM@</id>
  <docdate>@DOCIDNUM@</docdate>
  <docuser>@TUSER@</docuser>
  <name>@CUSTNAME</name>
  <contacts>
    <contact type="main" >
      <name>@MAINCONTACT</name>
      <email>@MAINCONEMAIL@</email>
    </contact>
    <contact type="technical" >
      <name>@TECHCONTACT@</name>
      <email>@TECHCONEMAIL</email>
    </contact>
  </contacts>
</customer>
<licenses>
  <product name="ICEDirect" code="ICE01" >
    <permission code="NE000" name="XMLSOURCE" >
      <expiry-date>2031/12/31</expiry-date>
      <grace-days>100</grace-days>
    </permission>
    <permission code="NE001" name="ZOSVIRTUAL" >
      <expiry-date>2031/12/31</expiry-date>
      <grace-days>100</grace-days>
    </permission>
    <permission code="NE002" name="RACFVIRTUAL" >
      <expiry-date>2031/12/31</expiry-date>
      <grace-days>100</grace-days>
    </permission>
  </product>
</licenses>
</bundle>
```

9.2. Functional XML License

A fully functional License provided by NewEra Technical Support will contain additional XML entries similar to the snippet shown below:

```
</licenses>
<generation>Generated on 2022/03/10</generation>
<validation>11A5C3297FBDA9598F41AFD79D72F53989E6A42ACBACA3...
</bundle>
```

9.3. Installing the XML License

Copy the XML License file into an MVS Datasets with attributes as shown below:

Data Set Information

Data Set Name : IFO.MTGY.WS.WSRV.LICENSE

```

General Data
Management class . . : **None**
Storage class . . . : **None**
Volume serial . . . : ZWORK5
Device type . . . . : 3390
Data class . . . . . : **None**
Organization . . . : PS
Record format . . . : VB
Record length . . . : 255
Block size . . . . : 32760
1st extent tracks . : 1
Secondary tracks . : 1
Data set name type :
Data set encryption : NO

Current Allocation
Allocated tracks . : 1
Allocated extents . : 1

Current Utilization
Used tracks . . . . : 1
Used extents . . . : 1

Dates
Creation date . . . : 2022/03/10
Referenced date . . : 2022/04/30
Expiration date . . : ***None***

SMS Compressible . : NO

```

9.4. Update the Web Server PROC

Reference the XML License Dataset in the Web Server PROC as shown below:

```

// *-----*
// *                NEWERA IMAGE FOCUS ENVIRONMENT                *
// *                STARTED TASK PROCEDURE                        *
// *
// *
// * MPE WEB SERVER PRIMARY ADDRESS SPACE                        *
// *
// * NSSPRFX - PREFIX FOR IMAGE FOCUS DATASETS                  *
// *
// *
// *-----*
// *
// * MTGYWS      PROC NSSPRFX='IFO.MTGY',PRM='00'
// *
// * WEBSVR      EXEC PGM=NEZMWSRV,REGION=0M,PARM='PRM=&PRM'
// * STEPLIB     DD DISP=SHR,DSN=&NSSPRFX..WS.LOAD
// * NSEPARM     DD DISP=SHR,DSN=&NSSPRFX..PARMLIB
// * LICENSE     DD DISP=SHR,DSN=&NSSPRFX..WS.WSRV.LICENSE
// * DEBUG      DD DISP=SHR,DSN=&NSSPRFX..WS.WSRV.DEBUG
// * WEBHTML     DD DISP=SHR,DSN=&NSSPRFX..WS.WEBHTML

```

9.5. Restart the Web Server

10. 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!” presented 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=XZZY, 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('XZZY')
                    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 RDATA LIB class.

- When using the FACILITY class:
 - RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(INV SERV)
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 INV SERV.RING01.LST UACC(NONE)
PERMIT INV SERV.RING01.LST CLASS(RDATALIB) ID(INV SERV)
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 INV SERV's software to use RING01 for SSL. For example, for z/OS HTTP Server, set the keyFile directive to KeyFile RING01 SAF.

11. 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.

11.1. 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.

11.2. 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'
```

11.3. 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

The ICEDirect Web Server generates CSRF Tokens that are unique to each browser tab. A Session Token could be stolen from one tab and used in any other during the browser session but a CSRF Token cannot and if moved into another session tab any request would fail.

11.4. Javascripts

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 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’s 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.

11.5. 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 of consecutive recognized errors. Once the maximum is reached two actions are taken. 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 actions is controlled by the Web Server parmlib setting - WEB_QUARANTINE.

11.6. Man-in-the-Middle - protocol downgrades and 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 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.

11.7. 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.

11.8. Use of Autofill

Commonly used Autofill can create an exposure when it “Remembers” a user’s logon credential thus 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 register a private PIN to be concatenated with real-time token material generated and presented at the point of the challenge.

11.9. Failure to Logout

A user’s 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 users and/or automatically CANCEL an inactive session Started Task. Short durations are considered a Best Practice.

11.10. 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.

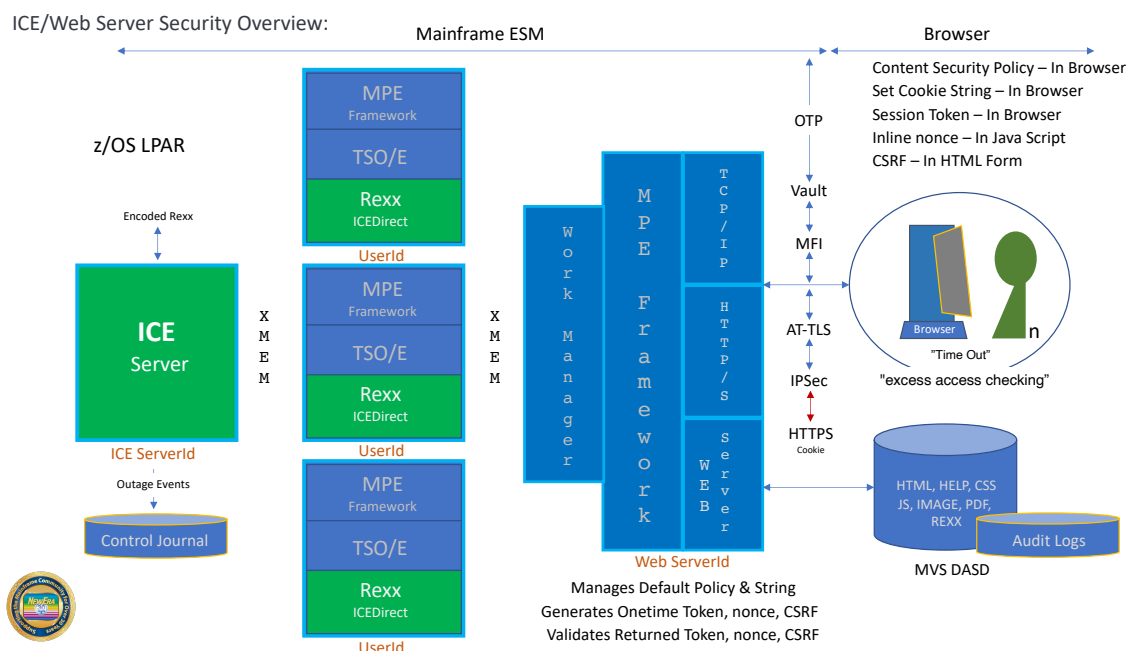
- Mitigation

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.

12.APPENDIX “C” – Security Attributes - An Overview

12.1. 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 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.



12.2. 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

12.3. 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

12.4. Tokens

Session – JS_Script Nonce, Session Cookie, HTML Token

CSP*: Content Security Policy

Security String*: HttpOnly; Secure; (where Secure is optional assuring HTTPS exchange)

12.5. ICEDirect Login

Multi-Factor ICE (MFI), Authentication User - Master Registry/Encrypted PIN Vault

Passticket (OTP) Generation: ESM

OTP Delivery: By Email or Inline

12.6. 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.

12.7. 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@"

12.8. Web Host – Rexx Address Spaces

External Security Manager, Re-Authentication of the User Credential

System Authorization Facility – SAF

12.9. Idle Timeout of user sessions

Customer defined (default of 10 minutes)

New login forced after timeout

12.10. Auto-Quarantine of Client IP Address

Customer defined maximum consecutive errors before quarantine

Customer defined duration in quarantine

12.11. 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'

12.12. Security String

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

12.13. 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.








12.14. 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) attacks.









13. 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 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

	<p>Indicates the span of ICEDirect Roles and Access Attributes</p>
	<p>Indicates the Discovery of one or more gskkyman Data Base(s)</p>
	<p>Indicates access the Inspection Log “UnPack” processing</p>
	<p>Indicates STASH File Password to gskkyman Data Base</p>
	<p>Indicates the Local z/OS System IPCS Report</p>
	<p>Indicates the Dataset and/or File Query Criteria</p>

14. Technical Support Contact Information

NewEra Software, Inc.

Mailing Address:

8070 Santa Teresa Blvd., Ste. 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



This is a Simple, Straightforward way to Get what You need from ICE on the WWW