
DJMS CAC Enablement User Guide

V 1.4.2

Prepared By: ESS



DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.

ABOUT THIS DOCUMENT1

1. SET-UP ACTIVITIES1

 1.1 CAC REGISTRATION1

 1.2 CLEARING YOUR CACHE2

2. DAILY LOGIN FLOW: END TO END.....5

 2.1 ACTIVATING YOUR SUPERSESSIONS8

3. TROUBLESHOOTING.....9

 3.1 MACRO TIMED OUT9

 3.2 MIAP TIME OUTS AND “BLACK SCREENS”.....10

 3.2.1 *PIN Requested*.....10

 3.2.2 *Black Screen, TLS Alert, Host Connection failed*10

4. CONTACTING THE DISA HELP DESK.....11

FREQUENTLY ASKED QUESTIONS (FAQ).....11

APPENDIX A: ACRONYMS12

ABOUT THIS DOCUMENT

This guide was updated April 2015

1. SET-UP ACTIVITIES

1.1 CAC REGISTRATION

The following are instructions on how to register your certificate to the z/OS LPAR or Guest using the zPAT tool.

First, CLOSE any MIAP portal instances you have open.

This process **should** be repeated for each region where **you have** access. Each region is **identified by** the first three characters of the URL. For instance:

MZO <https://mzo.csd.disa.mil/zpat>

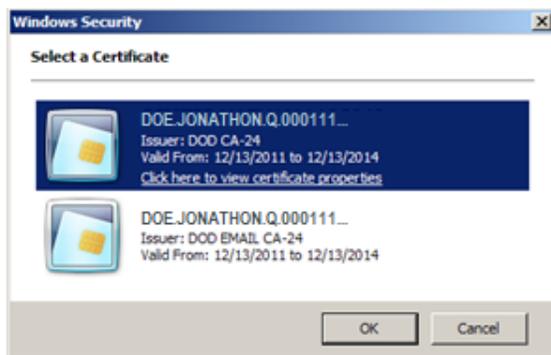
MMA <https://mma.csd.disa.mil/zpat>

MXC <https://mxc.csd.disa.mil/zpat>

The following text refers to registration for the MMA region. **Repeat these** steps necessary to register your CAC for each of the regions you access.

Using your Internet Browser, navigate to the URL <https://mma.csd.disa.mil/zpat>. (IE 11 can be used and has been tested successfully.) Upon entry to the zPAT URL, you **may** be presented with the DoD banner page and asked to **select** a certificate.

For CAC Enablement, you must choose the DOD CA ID certificate showing "Issuer: DOD CA-xx". The email certificate will not work for this process ("Issuer: DOD EMAIL CA-xx").



Highlight your DoD certificate and select OK, you will then receive the DoD warning banner:

NOTE: A certificate selection does not always happen if you have already been in a MIAP session the day you register.

If you did not have any issues, please continue to the next page and the DoD Warning Banner.

- NOTE:**
- 1 - If you are **not asked** to choose a certificate, or
 - 2 - you have any issues registering your CAC

It is recommended you logout of any online sessions and completely close the MIAP portal. Then clear your cache and restart the process.

Clearing your cache is effective with most certificate issues.

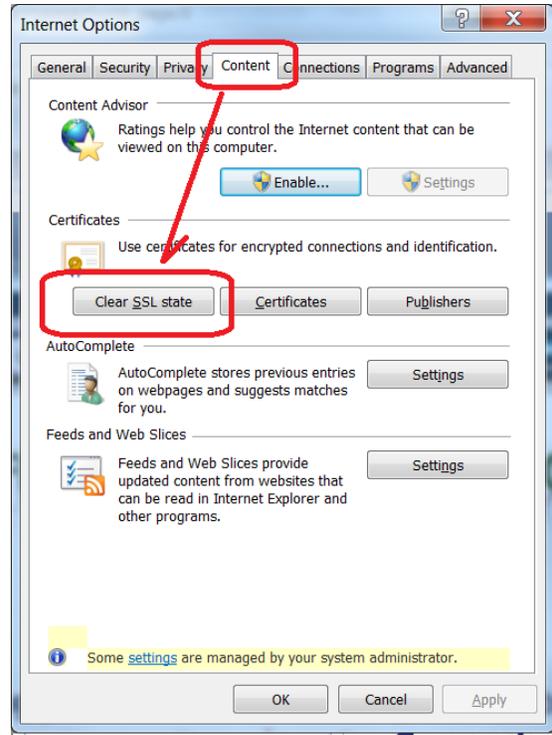
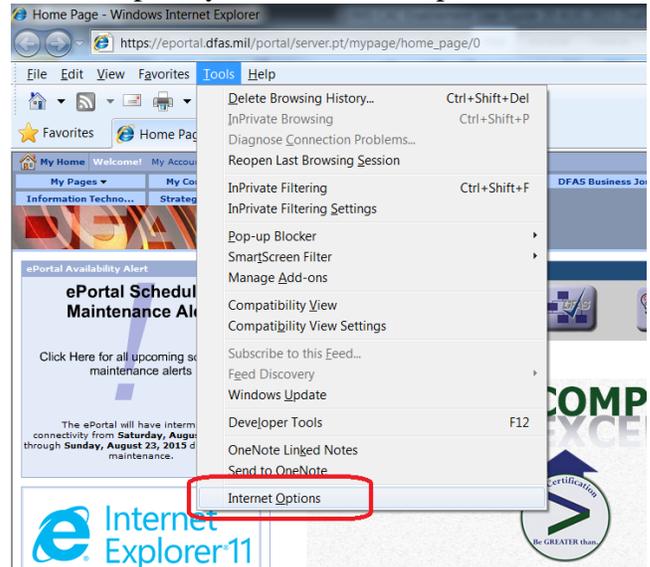
1.2 CLEARING YOUR CACHE

Open your internet explorer and clear your cache using the following steps.

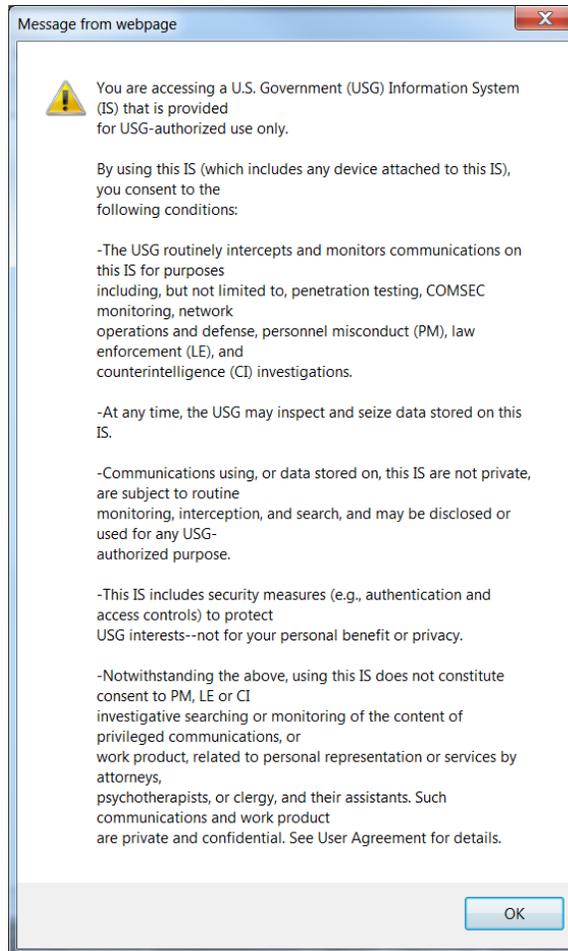
1. Open an instance of internet explorer.
2. Open the “Tools” tab
3. Choose “Internet Options”
4. Go to the “Content” tab on the internet options window that comes up and choose “Clear SSL state”. This will clear your cache.
5. Choose OK to complete, and close internet explorer.
6. Return to the first step

“1. SET-UP ACTIVITIES”

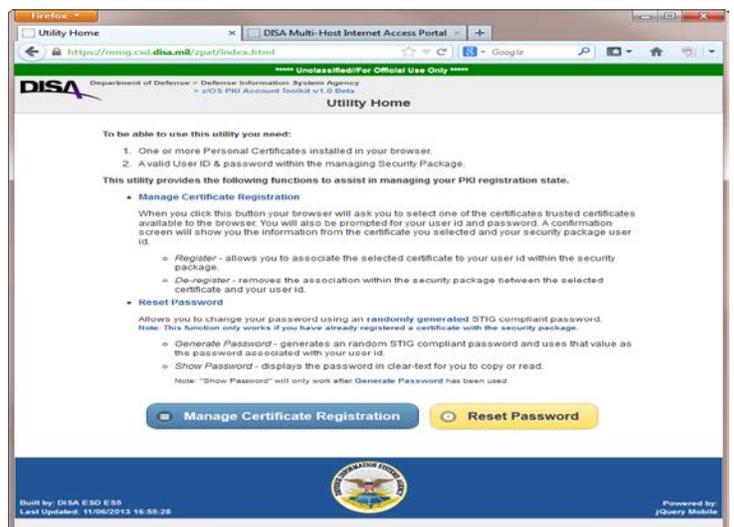
and restart the registration process.



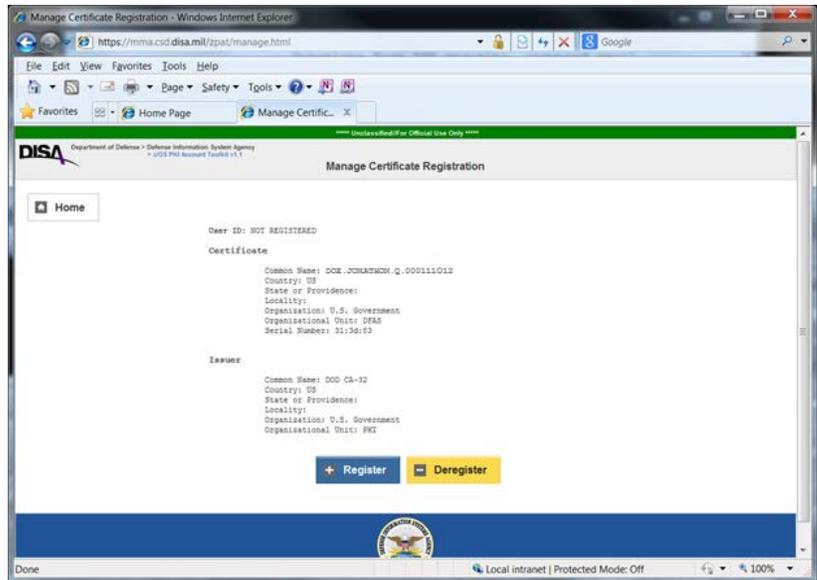
Click “OK” on the DoD warning banner to continue.



This is the zap Home page. From here, you are given the choices **Manage Certificate Registration** or **Reset Password**. For CAC Registrations, choose the “Manage Certificate Registration” button to register your CAC certificate to the host LPAR. Note that a CAC registration or deregistration can only be successful for users with a current user ID and password. If you do not have a current password, **refer to the zap User Guide**.

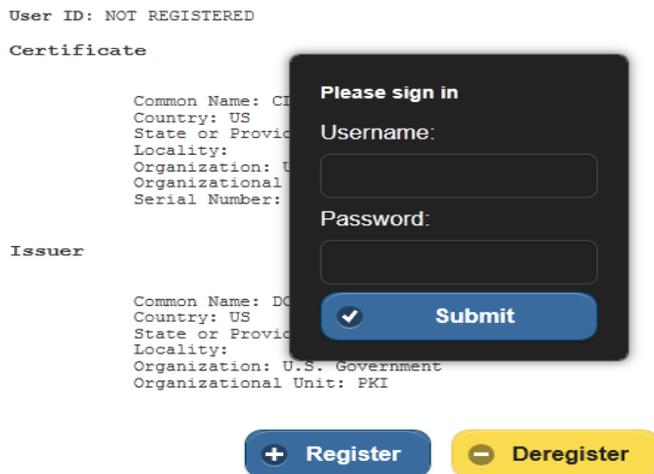


The Manage Certificate Registration screen will display the certificate for your verification and give you the option of either registering or deregistering your CAC. To register your certificate, choose “Register” as shown below.



Once you have selected “Register”, you will be prompted for username and password. Here you will fill in your username and password for the **region** you are registering your certificate and **submit**.

*NOTE: You will need to register separately for each **region** you use.*



Upon successful registration, the “Status” line at the top will change to:

Status: success Response: success

2. DAILY LOGIN FLOW: END TO END

NOTE: zPAT password resets provide temporary passwords only and users will be prompted to reset their password to a permanent password the first time they logon. The CAC/PKI sessions will not function properly if the user has not performed this function.

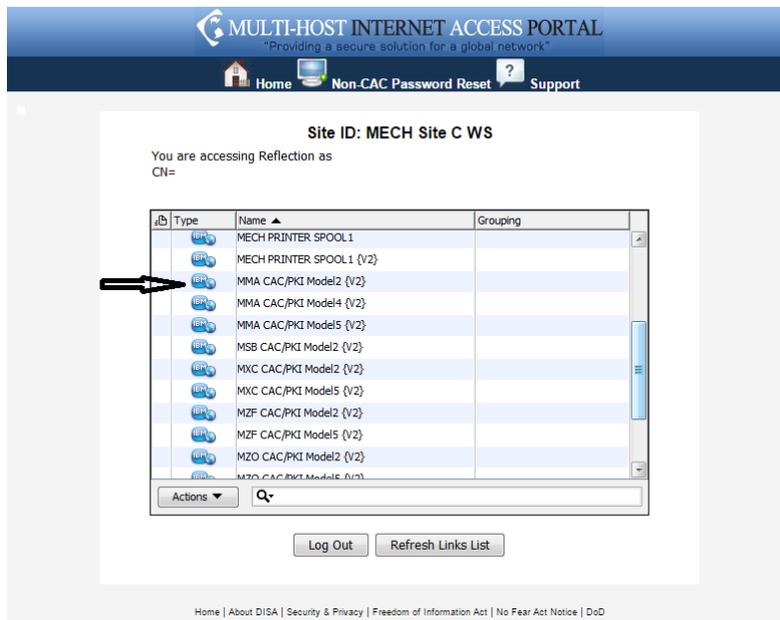
If you have performed a password reset via zPAT since the last time you used the CAC/PKI sessions, please logon via the non-CAC/PKI sessions (i.e., MECH Model 2 {V2}) to perform this function (to update the temporary password with a new password).

You must do this prior to using your CAC/PKI to login to your session.

Establish a web browser session to MIAP: <https://miap.csd.disa.mil> and perform normal login process to MIAP. The list of sessions presented is based on individual user profiles.

Launch the **CAC-Enabled login** to the target LPAR by double-clicking the “**MMA CAC/PKI Model2 {V2}**” selection as illustrated below. If you do not have the appropriate CAC/PKI selection, contact the helpdesk at:

Toll Free: 1-844-347-2457 (1-844-DISA HLP) or DSN: 850-0032
press 1 for Applications,
press 4 for the Mechanicsburg menu,
then press 6 for MIAP.



After launching the session, you will be presented with the DISA banner screen as illustrated below:

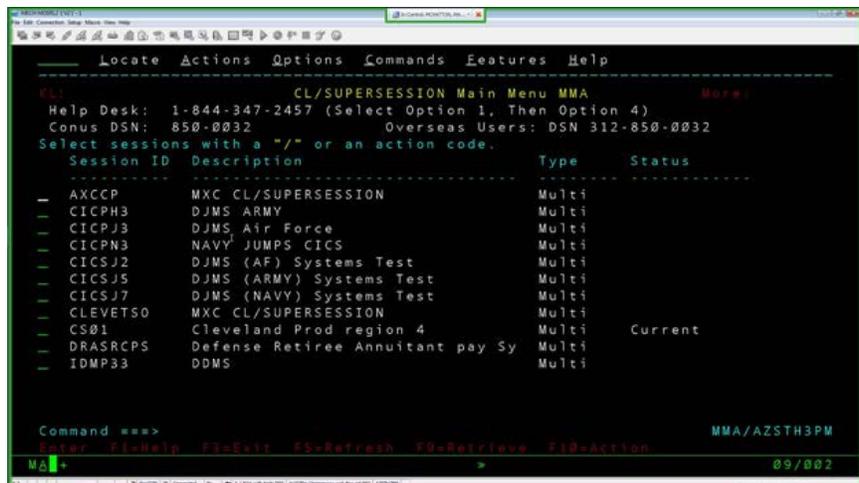
```
KLSLG011 Defense Information Systems Agency - DECC Mechanicsburg
  You are accessing a U.S. Government (USG) Information System (IS) that
  is provided for USG authorized use only. By using this IS (which
  includes any device attached to this IS), you consent to the following
  conditions:
  -The USG routinely intercepts and monitors communications on this IS for
  purposes including, but not limited to, penetration testing, COMSEC
  monitoring, network operations and defense, personnel misconduct (PM),
  law enforcement (LE), and counterintelligence (CI) investigations.
  -At any time, the USG may inspect and seize data stored on this IS.
  -Communications using, or data stored on, this IS are not private, are
  subject to routine monitoring, interception, and search, and may be
  disclosed or used for any USGauthorized purpose.
  -This IS includes security measures (e.g., authentication and access
  controls) to protect USG interests--not for your personal benefit or
  privacy.
  -Notwithstanding the above, using this IS does not constitute consent to
  PM, LE or CI investigative searching or monitoring of the content of
  privileged communications, or work product, related to personal
  representation or services by attorneys, psychotherapists, or clergy,
  and their assistants. Such communications and work product are private
  and confidential. See User Agreement for details.
  Press ENTER key to continue.
MMA+ >> 24/002
```

Press <Enter>.

At this point, the CAC/PKI Express Login Macro will automatically enter your authorization credentials. You will be prompted with a one-time pop-up requesting your CAC pin. Note: You would use CAC Pin to unlock screen in the event of a CL/Supersession timeout.

Once the session has connected to the mainframe, users should see the DJMS screens they are accustomed to seeing, as illustrated.

Select your session and press <Enter>.



```
CL/CL/SUPERSESSION Main Menu MMA
Help Desk: 1-844-347-2457 (Select Option 1, Then Option 4)
Conus DSN: 850-0032 Overseas Users: DSN 312-850-0032
Select sessions with a "/" or an action code.
-----
Session ID Description Type Status
-----
- AXCCP MXC CL/SUPERSESSION Multi
- CICPH3 DJMS ARMY Multi
- CICPJ3 DJMS Air Force Multi
- CICPN3 NAVY JUMPS CICS Multi
- CICSJ2 DJMS (AF) Systems Test Multi
- CICSJ5 DJMS (ARMY) Systems Test Multi
- CICSJ7 DJMS (NAVY) Systems Test Multi
- CLEVETSO MXC CL/SUPERSESSION Multi
- CS01 Cleveland Prod region 4 Multi Current
- DRASRCPS Defense Retiree Annuitant pay Sy Multi
- IDMP33 DDMS Multi
-----
Command ==> MMA/AZSTH3PM
Enter F1=Help F2=Exit F3=Refresh F9=Retrieve F10=Action
MMA+ >> 09/002
```

At this point, if you have other LPAR regions (MMA, MXC, MMF etc.) to register for CAC access; disconnect normally from the current session and go through the registration process for the next LPAR.

NOTE:

- You must use the MIAP MMA CAC/PKI sessions for CAC Enablement to work (*Do not use MECH Model 2 {V2} sessions unless you want to logon with your User ID and password*).
- The CAC/PKI session utilizes a time sensitive one time **passticket** to authenticate to the mainframe. In the event that the mainframe session is disconnected to non-use (approximately 30 minutes, however, it can go to sleep after 15 minutes requiring you to enter your CAC Pin again), close the MMA CAC/PKI window. Then restart your MMA CAC/PKI session from the MIAP Portal selection screen as illustrated below:

Site ID: MECH Site C WS

You are accessing Reflection as
CN=

Type	Name	Grouping
IBM	MECH PRINTER SPOOL 1	
IBM	MECH PRINTER SPOOL 1 {V2}	
IBM	MMA CAC/PKI Model2 {V2}	
IBM	MMA CAC/PKI Model4 {V2}	
IBM	MMA CAC/PKI Model5 {V2}	
IBM	MSB CAC/PKI Model2 {V2}	
IBM	MXC CAC/PKI Model2 {V2}	
IBM	MXC CAC/PKI Model5 {V2}	
IBM	MZF CAC/PKI Model2 {V2}	
IBM	MZF CAC/PKI Model5 {V2}	
IBM	MZO CAC/PKI Model2 {V2}	
IBM	MZO CAC/PKI Model5 {V2}	

Actions

Log Out Refresh Links List

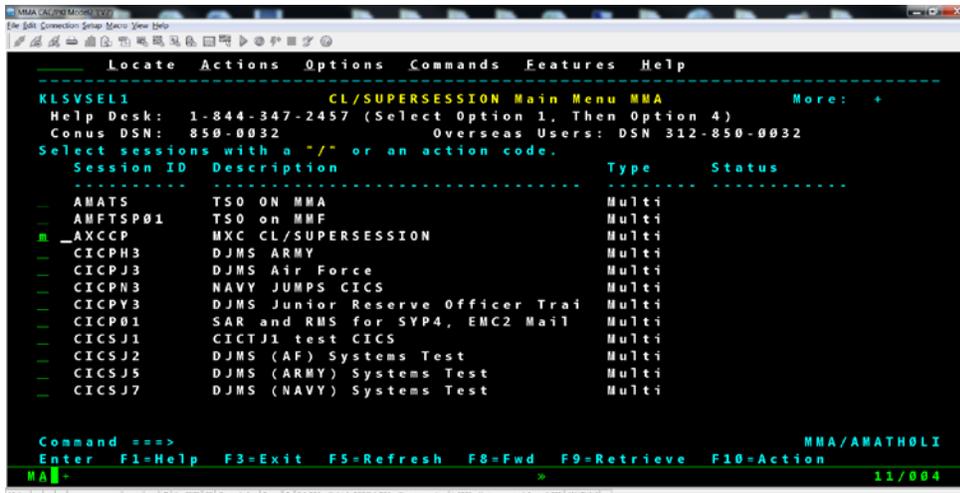
Home | About DISA | Security & Privacy | Freedom of Information Act | No Fear Act Notice | DoD

2.1 ACTIVATING YOUR SUPERSESSIONS

ONLY if you have multiple accesses, and utilize supersessions, you may need to modify your supersession with the CAC/PKI TSP login.

Open your MIAP portal using your CAC/PKI and login.

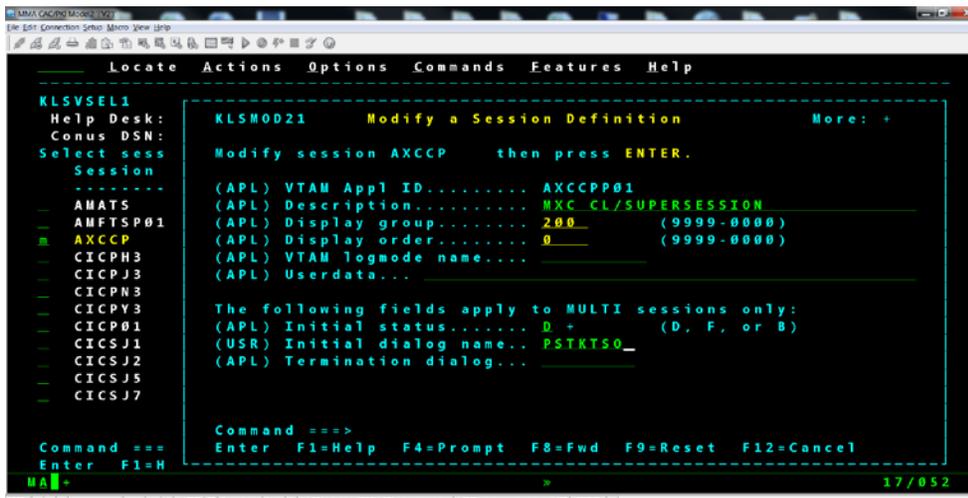
When you get to your first screen, type “m” (for modify) on the line of your supersession and hit the <Enter> key.



```
MMA CL/SUPERSESSION Main Menu MMA More: +
Help Desk: 1-844-347-2457 (Select Option 1, Then Option 4)
Conus DSN: 850-0032 Overseas Users: DSN 312-850-0032
Select sessions with a "/" or an action code.
-----
Session ID Description Type Status
-----
AMATS TSO ON MMA Multi
AMFTSP01 TSO on MMF Multi
AXCCP MXC CL/SUPERSESSION Multi
CICPH3 DJMS ARMY Multi
CICPJ3 DJMS Air Force Multi
CICPN3 NAVY JUMPS CICS Multi
CICPY3 DJMS Junior Reserve Officer Trai Multi
CICP01 SAR and RMS for SYP4, EMC2 Mail Multi
CICSJ1 CIGTJ1 test CICS Multi
CICSJ2 DJMS (AF) Systems Test Multi
CICSJ5 DJMS (ARMY) Systems Test Multi
CICSJ7 DJMS (NAVY) Systems Test Multi

Command ==>
Enter F1=Help F3=Exit F5=Refresh F8=Fwd F9=Retrieve F10=Action
MMA/AMATH0LI 11/004
```

In the USR Initial Dialog name, verify that PSTKTSO is in the field as seen below. If not, enter the PSTKTSO as below and hit the <Enter> key to update.



```
MMA CL/SUPERSESSION Main Menu MMA More: +
Help Desk: 1-844-347-2457 (Select Option 1, Then Option 4)
Conus DSN: 850-0032 Overseas Users: DSN 312-850-0032
Select sessions with a "/" or an action code.
-----
Session ID Description Type Status
-----
AMATS TSO ON MMA Multi
AMFTSP01 TSO on MMF Multi
AXCCP MXC CL/SUPERSESSION Multi
CICPH3 DJMS ARMY Multi
CICPJ3 DJMS Air Force Multi
CICPN3 NAVY JUMPS CICS Multi
CICPY3 DJMS Junior Reserve Officer Trai Multi
CICP01 SAR and RMS for SYP4, EMC2 Mail Multi
CICSJ1 CIGTJ1 test CICS Multi
CICSJ2 DJMS (AF) Systems Test Multi
CICSJ5 DJMS (ARMY) Systems Test Multi
CICSJ7 DJMS (NAVY) Systems Test Multi

Command ==>
Enter F1=Help F3=Exit F5=Refresh F8=Fwd F9=Retrieve F10=Action
MMA/AMATH0LI 11/004

KLSMOD21 Modify a Session Definition More: +
Modify session AXCCP then press ENTER.
-----
(APL) VTAM Appl ID..... AXCCPP01
(APL) Description..... MXC CL/SUPERSESSION
(APL) Display group..... 200 (9999-0000)
(APL) Display order..... 0 (9999-0000)
(APL) VTAM logmode name...
(APL) Userdata...

The following fields apply to MULTI sessions only:
(APL) Initial status..... D+ (D, F, or B)
(USR) Initial dialog name.. PSTKTSO_
(APL) Termination dialog...

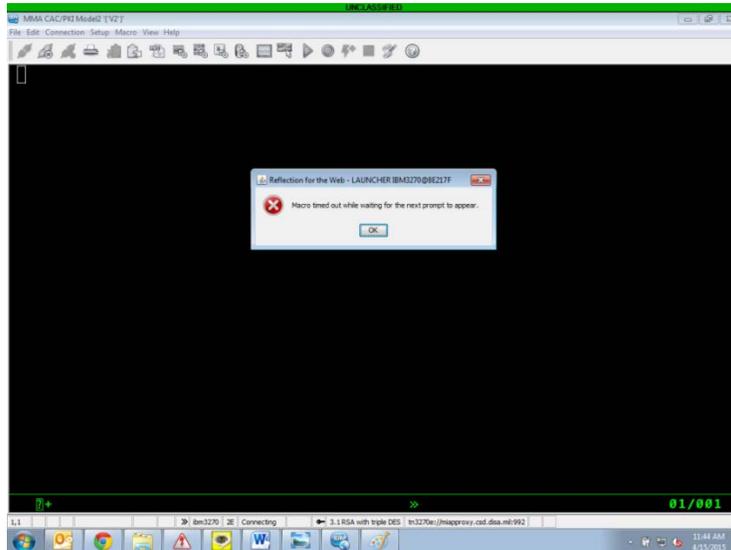
Command ==>
Enter F1=Help F4=Prompt F8=Fwd F9=Reset F12=Cancel
MMA/AMATH0LI 17/052
```

You will need to go out of your session and come back in for the supersession to be activated.

3. TROUBLESHOOTING

3.1 MACRO TIMED OUT

In the event of an issue when launching a CAC/PKI session, the user will receive a “Macro timed out” message as illustrated below:



There are two main reasons a user may receive this error:

1. The user’s Identity certificate has not been registered to their user ID on the mainframe.

Resolution: Launch the zPAT tool to register your Identity certificate to your mainframe user ID **following** section 1.1. Remember, registering with the email certificate will not work.

2. The user has performed a password reset via zap; the mainframe is prompting for update of their password. The password reset screen is not recognized by the CAC/E macro and is causing the timeout.

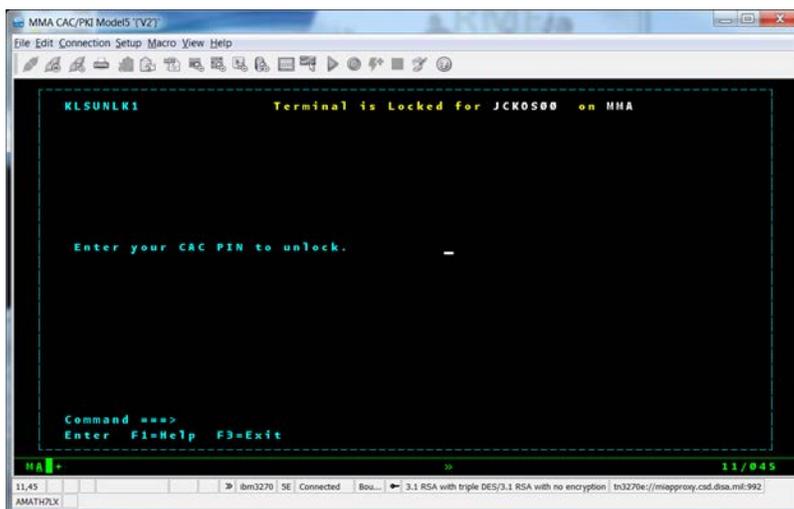
Resolution: Logon via a non-CAC/PKI session (i.e., MECH Model 2 {V2}). You will be prompted to update your password, **enter the same password that was used in zPAT**. Once this has been completed, you will be able to launch the CAC/PKI sessions successfully.

3.2 MIAP TIME OUTS AND “BLACK SCREENS”

MIAP drops, or time outs occur from non-use. *These are covered under DISA STIG requirements and are mandatory for online systems.* Generally speaking, you may experience a time out anywhere after 15 to 30 minutes of non-use.

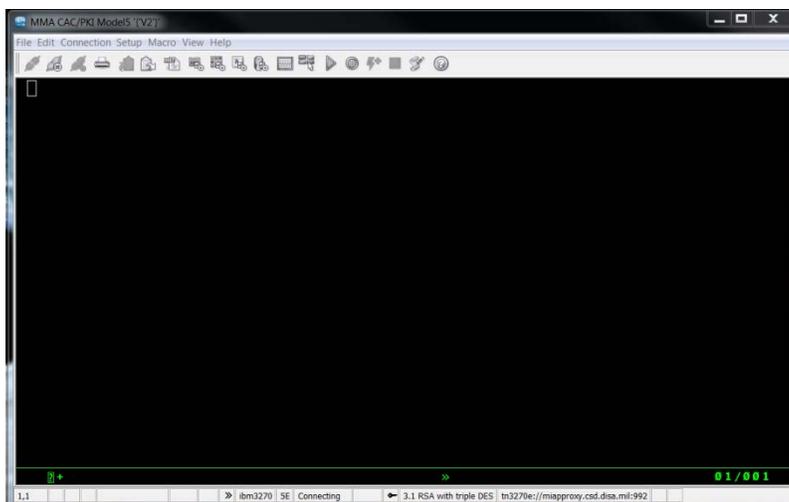
3.2.1 PIN Requested

The first case will be that you will be asked for your PIN. Enter your CAC PIN, and then OK. Check to see if you are still connected to the session. If you have been disconnected, you will need to close out of the portal and reconnect through the MIAP access portal.



3.2.2 Black Screen, TLS Alert, Host Connection failed

The second case is where the time out allotment has been exceeded. You may receive a total black screen. You may also receive a message that the “Connection to Host Failed” or a TLS Alert message. In this case, you have been disconnected, you will need to close out of the portal and reconnect through the MIAP access portal.



4. CONTACTING THE DISA HELP DESK

Issues requiring further assistance, contact your local **TASO/AIAO** or the **DISA Help Desk**

Toll Free: 1-844-347-2457 (1-844-DISA HLP) or DSN: 850-0032

press 1 for Applications,
press 4 for the Mechanicsburg menu,
press 6 for MIAP.

FREQUENTLY ASKED QUESTIONS (FAQ)

In what situations are CAC/PKI logins not available?

FTP Users and **DJMS** privileged users will still need to use their User ID and Password for access.

If you have an LPAR region that is not CAC enabled, please contact your local TASO/AIAO. For example, as of September 2015, the CICP01 region "SAR and RMS for SYP\$, EMC2 Mail" is not CAC enabled.

Will my password expire anymore?

Yes. However, as long as you are accessing the system using your CAC/PKI you will still be treated as an active user. When you go to use the user ID password and you have not used it in the past 60 days, you will be required to update your password before access.

What happens if my CAC is expiring?

If your CAC is expiring, you should confirm your logon using the Userid/Password (using a MECH Model 2 {V2} session) and if necessary, update your password. Then unregister your current CAC card before getting your new CAC. After you get your new CAC, follow the same process in section 1.1 to re-register your region(s) (MMA, MXC, etc.). As **before**, if you have access to multiple regions, you need to register your new CAC for each of those regions.

DISA Help Desk or contact local TASO/AIAO

Toll Free: 1-844-347-2457 (1-844-DISA HLP) or DSN: 850-0032

press 1 for Applications,
press 4 for the Mechanicsburg menu,
press 6 for MIAP.

APPENDIX A: ACRONYMS

ACP – Access Control Product. On zOS LPARs, this will be either CA ACF2, IBM RACF, or CA Top Secret.

CAC – Common Access Card

CL/SS – IBM’s CL Supersession Session Manager

DISA – Defense Information Systems Agency

LPAR – Logical Partition – region

MIAP – Multihost Internet Access Portal

PKI – Public Key Infrastructure

STIG – Security Technical Implementation Guidelines

UID – User Identification

URL – Universal Resource Locator

zPAT – zOS PKI Account Toolkit