Configuring IBM Case Manager 5.2 to support SSO via ISAM (IBM Security Access Manager 7.x)
Terminology

- ICM – IBM Case Manager
- ICN – IBM Content Navigator
- ISAM – IBM Security Access Manager
- WAS – WebSphere Application Server
- JAAS - Java Authentication and Authorization Service
- TAI – Trust Association Interceptor
- GSKit = IBM Global Security Kit
- TDS = Tivoli Directory Server
- CPE = Content Platform Engine (In Version 5.2.0, the Content Engine and Process Engine have been combined and now run as a single deployed application. The combined engine is called Content Platform Engine. Individually Content Engine is now referred as IBM FileNet Content Manager and Process Engine is referred as IBM Content Foundation)
- CMUI -Configuration Manager User Interface.
Presentation Overview

- **Section 1:**
  - P8 supported single sign-on (SSO) solutions,
  - Authentication review.
  - Basic ISAM components overview.

- **Section 2:**
  - Planning and Preparation.
  - ISAM 7 Installation and Configuration
  - Establishing trust between WebSphere Application Server and ISAM WebSEAL
  - Configuring ICN for SSO
  - Configuring ICM for SSO
  - Known Issues

- **Section 3:**
  - Trace/Logging and Troubleshooting

- **Section 4:**
  - Q&A session

**Target Audience:**
- Support engineers and customers dealing with ISAM integration solutions with P8.

**Prerequisites:**
- Basic understanding of P8 Security
Preface

- Performing a single sign-on (SSO) integration with IBM FileNet P8 using ISAM (IBM Security Access Manager) and a supported J2EE application server can be a very complex undertaking.

- In today's presentation we will introduce ISAM SSO into a existing / working an P8 ICN (IBM Content Navigator) and ICM (IBM Case Manager) environment.

- At the end of this presentation you should be able to:
  - Understand the Authentication flow with and without ISAM SSO.
  - Identify the ISAM components involved in configuring with IBM Content Navigator and IBM Case Manager.
  - Perform an ISAM installation and configuration.
  - Configuration and deployment of ICN and ICM application for ISAM SSO.
  - Have a better scope of where to begin your troubleshooting effort.

- Additional issues encountered beyond the scope of this presentation may require you to open a PMR with the appropriate support group, Access manager, WebSphere and P8.
Section 1

- P8 supported single sign-on (SSO) solutions
- Authentication review
- Basic ISAM components overview
### P8 supported single sign-on (SSO) solutions

- For Content Platform Engine with applications based on the server APIs, IBM supports the enablement of any SSO solution that is supported by a P8-supported application server and SSO vendor.

<table>
<thead>
<tr>
<th>SSO Provider</th>
<th>IBM Content Navigator (Web Client)</th>
<th>IBM Case Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Access Manager for e-business</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Security Access Manager for e-business (ISAM 7.0.x)</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Security Assertion Markup Language (SAML)</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>SPNEGO /Kerberos</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>CA SiteMinder</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>


- Client applications, such as IBM Content Navigator and Case Manager, can impose additional requirements on any SSO solution. Supported SSO solution for ICM link:
  www-01.ibm.com/support/knowledgecenter/SSCTJ4_5.2.1/com.ibm.casemgmt.design.doc/acmcf010.htm
Single Sign-On

- Single Sign-on is a method, which allows the user to access a resource, regardless of the resource's location, using only one initial login. Used to avoid multiple logins and avoid the overhead of administering and maintaining multiple login identities.

- When a protected resource is located on a back-end Web application server, a client requesting that resource can be required to perform multiple logins — one for the WebSEAL server and one for the back-end server. Each login likely requires different login identities.

- A client authenticates to the first SSO-protected service that they use and does not have to log into any other. Before a user request is handled, a third-party application, called an SSO provider, intercepts the request and authenticates the user.

- Web application SSO protection systems, such as secure reverse proxy like WebSEAL, will provide its own login page instead of using that of the underlying services.

- A common mechanism for SSO is Kerberos, which is the underlying technology that is used in Windows Integrated Login, and uses the same method when passing Kerberos tokens to applications.
Section 1

- P8 supported single sign-on (SSO) solutions
- Authentication review
- Basic ISAM components overview
Authentication review

Authentication

- Authentication is the act of verifying a user's identity based on credentials that the user provides.
- The application server uses the Java Authentication and Authorization Service (JAAS) to authenticate users.

How JAAS Login module authenticate users?

- Makes an authentication check and creates the subject for the client in which user information are stored.
- Interacts with User Registry or Repository to validate a user with username and password.

- There are two ways that can be used to obtain this JAAS Subject: Application-managed authentication and Container-managed authentication.
  - **Application-managed authentication**: the application is responsible for session management and Authentication. Application can prompt the user for different credentials when the user accesses different repositories.
  - **Container-managed authentication** – the application server is responsible for the initial user authentication. User's credentials are authenticated by the J2EE application server where application is deployed.

- **Container-managed authentication**
  - Container-managed authentication is referred to as “Application server authentication” by ICN.
  - This Authentication type is selected during ICN deployment within the CMUI if you are configuring your web application server to use SSO.
  - P8 repositories use Container –managed authentication.

- IBM Case Manager client runs as plug-in for ICN and uses ICN Authentication and Connection code.
User A passed into JAAS Login module

http://oclcsoce52vmm2.css:9080/navigator/?desktop=icm

User A /Username and PW passed to LDAP registry

User and group information retrieved for User A

Validate User A and password in LDAP Registry

User A /Username and PW passed to LDAP registry

EJB Call with subject +LTPA

LTPA Keys need to be Shared/Sync’d

JAAS Subject creation

WebSphere Application server
Section 1

- P8 supported single sign-on (SSO) solutions
- Authentication review
- Basic ISAM components overview
Basic ISAM components overview

The major components of Security Access Manager for Web are:

- WebSEAL: ISAM Reverse Proxy Server.
- User registry: LDAP repository, TDS, MSAD
- Policy Server
- Authorization server
- Web Portal Manager (optional)
- Junctions
- TAI (Trust Association Interceptor)
Basic ISAM components overview

**WebSEAL** – Security Access Manager/WebSEAL (a reverse proxy server) that intercepts any incoming HTTP/HTTPS requests. This ensures that end users accessing applications are authenticated and authorized for the request. The request can then continue on to the necessary applications deployed in the trusted zone.

- WebSEAL is a high-performance, multi-threaded *reverse proxy* that sits in front of back-end Web applications. It applies a security policy to a protected object space.
- WebSEAL can provide single sign-on solutions and incorporate back-end Web application server resources into its security policy. Because it is implemented on an HTTP server foundation, it is limited to enforcing policy for applications communicating with HTTP and HTTPS protocols.
Basic ISAM components overview

User registry

- The default user registry is LDAP-based, and Access Manager consolidates its registry support around a number of LDAP directory products:
  - IBM Tivoli Directory Server
  - Novell eDirectory
  - Sun™ Java™ System Directory Server
  - Microsoft® Active Directory
  - IBM Lotus® Domino Server

- During the ISAM installation is where additional ISAM schema added to the existing TDS user registry within the “SecAuthority=default” portion of the TDS tree.
Basic ISAM components overview

Policy Server

- The Access Manager Policy Server maintains the master authorization database for the secure domain. This server is primarily used for the following administrative activities:
  - Modifying the registry to define which objects participate in the secure domain.
  - Updating the authorization database with policy definitions.
  - Manages the master authorization database, which, in addition to resource policies, contains location information about other Access Manager servers in the secure domain.

- Authorization database
  - Separate from the user registry, Access Manager uses it for its authorization functions.
  - A special database containing a virtual representation of resources it protects, called the Security Access Manager policy database.
  - UNIX :/var/PolicyDirector/db/master_authzn.db
  - The master authorization database is controlled by the policy server, “pdmgrd” command

Authorization server:

- Authorization Server is a client side replica of Policy Server. It needs to be installed with Access Manager Java Runtime environment. It caches policy server data and synchronizes it on a regular basis. Even though Policy Server goes down, Authorization server still serves your requests.
Basic ISAM components overview

Web Portal Manager

- Security Access Manager has both command-line and graphical user interfaces for managing domains, users, groups, permissions, policies, and other resources in your enterprise.

- Security Access Manager includes the following user interfaces:
  - **pdadmin** is a command-line interface that is installed as part of the Security Access Manager runtime package.
  - **Web Portal Manager** is a management console for tasks that are like the commands provided by the pdadmin commands.
  - The Web Portal Manager is a plug-in to the WebSphere Application Server Integrated Solutions Console
Basic ISAM components overview

Junction:

- IBM Security Access Manager for Web uses junctions to identify web servers. The client's browser uses one set of URL links and the back-end web server.
- A WebSEAL junction is an HTTP or HTTPS connection between a front-end WebSEAL server and a back-end Web application server.
- A junction allows WebSEAL to provide protective services on behalf of the back-end server. WebSEAL performs authentication and authorization checks on all requests for resources before passing those requests across a junction to the back-end server.
- Junctions also allow a variety of single signon solutions between a client and the junctioned back-end applications; example junctions we will be creating:
  - /WorkplaceXT
  - /navigator
  - /CaseForms
  - /CaseBuilder
  - /CaseManager
  - /ICMClient
Basic ISAM components overview

**TAI (Trust Association Interceptor):**
- TAI++ - is the embedded Trust Association Interceptor++ (tai++) accepts an iv-creds HTTP request header from IBM Security Access Manager for Web and a trust password in a Basic Authentication header. The embedded tai++ authenticates the trust password and dismantles the iv-creds HTTP request header to build the credential of the original user.
  - Supported by WAS L2 team

**eTAI** - The extended version of the Trust Association Interceptor++ (ETAI) includes additional capabilities:
- Removes the need for any Security Access Manager configuration on WebSphere Application Server.
- Map the credential attributes of the original user to different registry formats or adds no credentials at all.
- Supported by Access Manager L2 team

Client

http://oclcsocpe52vmm4.css/navigator/?desktop=icm

User A

WebSEAL

Validation of user in ISAM and retrieve ISAM specific registry information

Registry returns user name and password for requested application resource.

Access Control info Replica

TDS LDAP registry

Verify "User A" Credential

BA [Basic Auth] Header info UserA+dummypassword "iv-creds" info junction=navigator/?desktop=icm

LoginID=WebSEALUse r Configuration Property

WebSphere Application server

ICM Client
ICM Admin Client
ICM Case Manager

CPE (Content Platform Engine)

EJB Call with subject +LTPA

LTPA Keys need to be Shared/Sync'd

LTPA
Section 2

- Planning and Preparation
- ISAM 7 Installation and Configuration
- Establishing trust between WebSphere Application Server and ISAM WebSEAL
- Configuring ICN for SSO
- Configuring ICM for SSO
- Known Issues
Section 2

- Planning and Preparation
  - ISAM 7 Installation and Configuration
    - Establishing trust between WebSphere Application Server and ISAM WebSEAL
  - Configuring ICN for SSO
  - Configuring ICM for SSO
  - Known Issues
Review documentation and version dependencies between components (1/2)

- Review ICM and ICN documentations for configuring SSO with ISAM
  

- Review planning documentation for ISAM 7.0
  

- Check for detailed system requirements for all products
  
  http://www-969.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html

- IBM Case Manager 5.2.1
  - Requires a minimum Content Platform Engine (CPE) level of 5.2.0.3-P8CPE-IF003 and IBM Content Navigator (ICN) 2.0.3.
  - Supports WebSphere Application Server 7.0, 8.0, 8.5, and 8.5.5. For WAS 8.5, minimum required is 8.5.0.2
  - Supports the IBM Case Manager supports the same databases that ICN, and CPE , except for DB2 V9.5 (any edition), IBM DB2 for z/OS (any edition), Oracle V11g R1, Oracle RAC V11g R1
  - Supports the same LDAP servers that CPE support.
  - Software Product Compatibility Reports for ICM 5.2.1:
    

- IBM FileNet Content Manager 5.2.0.3
  
Review documentation and version dependencies between components (2/2)

- Check for detailed system requirements for all products (continued)
  http://www-969.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html

- WAS 8.5.0.2

- IBM Security Access Manager 7.0.0.2 (minimum fix pack level to support WAS 8.5.0.2)

- DB2 Enterprise Server Edition 10.1
Lab Environment

- Three servers configuration

**Server #1**
(oclcsocpe52vmm2/ 9.39.39.21)
- Windows Server 2012 R2
- WAS ND 8.5.0.2
- 5.2.0.3-P8CPE-IF003
- DB2 10.1
- ICN 2.0.3
- ICM 5.2.1
- WorkplaceXT 1.1.5.2
- GSKit
- ISAM 7.0.0.2:
  - License
  - Runtime for Java
  - Web Portal Manager (WPM)

**Server #2**
(oclcsocpe52vmm3/ 9.39.39.43)
- Windows Server 2008 R2
- DB2 9.7 (used by TDS only)
- TDS 6.3

**Server #3**
(oclcsocpe52vmm3/ 9.39.39.75)
- Windows Server 2008 R2
- ISAM 7.0.0.x pre-requisites:
  - IBM Global Security Kit (GSKit)
  - IBM Security Utilities
  - ISAM License
- ISAM 7.0.0.2 components:
  - License
  - Runtime
  - Policy Server
  - Authorization Server
  - Web Security Runtime
  - WebSEAL
Configuring IBM Case Manager to support SSO through IBM Security Access Manager for Web - Overview

- Installation and Configuration Overview
  - Install and configure P8CPE, ICN, ICM, XT, and WAS Default application without SSO
    - Pre-installation checkpoint – Verify you have a working environment before proceeding
  - Install and configure ISAM V7.0.0
  - Create a trusted user account in WebSEAL user registry
  - Import an existing P8 user into WebSEAL user registry
  - Create junctions for snoop servlet, ICN, ICM, and WorkplaceXT
  - Edit WebSEAL configuration file
  - Configure Security Access Manager Runtime for Java component on the application server
  - Create PDPerm.properties file by running SvrSslCf utility
  - Configure single sign-on using trust association interceptor ++
    - Checkpoint - Verify Snoop servlet SSO
  - Re-deploy ICN
    - Checkpoint – Verify ICN SSO
  - Configure Permission for IBM Case Manager users
    - Checkpoint – Verify ICM SSO
Section 2

- Planning and Preparation
- **ISAM 7 Installation and Configuration**
  - Establishing trust between WebSphere Application Server and ISAM WebSEAL
  - Configuring ICN for SSO
  - Configuring ICM for SSO
- Known Issues
ISAM 7.0 Installation & Configuration – Overview (1/2)

- Step 1 - Install and configure Policy Server
- Step 2 - Install and configure Authorization Server
- Step 3 - Install and configure WebSEAL
- Step 4 - Configure Runtime for Java (done as pre-requisite for Web Portal Manager)
- Step 5 - Install and configure Web Portal Manager
- Step 6 - Install ISAM 7.0.0.2 Fix Pack

Note: In our environment, Steps 1 thru 3 are performed on the Server #3 - oclcsocpe52vmm2 and steps 4 and 5 are performed on server #1 oclcsocpe52vmm2. Step 6 is performed on both servers by updating the respective component.
ISAM 7.0 Installation & Configuration – Overview (2/2)

- New GUI interface on Windows, launchpad64.exe
- Allow installer to pick and choose multiple components
- Launchpad steps the user through the required installation steps and launches configuration at the end of the installation of components
- You can still install each component individually, on Windows platform this can be done by executing the following setup.exe.
  - Policy Server: windows\PolicyDirector\Disk Images\Disk1\setup.exe
  - Runtime for Java: windows\PolicyDirector\Disk Images\Disk1\PDJRT\setup.exe
  - Web Portal Manager: windows\PolicyDirector\Disk Images\Disk1\PDWPM\setup.exe
  - Authorization Server: windows\PolicyDirector\Disk Images\Disk1\PDAcl\Disk Images\Disk1\setup.exe
- Scripts available on all platforms for automation
Install Policy Server, select Policy server on the list of components

Pre-requisite components will be installed which include: IBM Global Security Kit (GSKit), Directory Server Client, Security Utilities, License and Runtime
ISAM 7.0 Installation & Configuration – Policy Server (2/7)

- **Installation path on Windows:**
  - GSKit (version 8.0.14.38): C:\Program Files\ibm\gsk8
  - Tivoli Directory Server Client 6.3: C:\Program Files\ibm\LDAP\V6.3
  - Security Utilities: C:\Program Files\Tivoli\TivSecUtil
  - Run time and Policy Server component: C:\Program Files\Tivoli\Policy Director\license:

- After pre-requisites software and Policy Server component have been installed, configuration consist of configuring the runtime and the Policy Server.

![Configuration for IBM Security Access Manager](image)
Configure Runtime

- Select the Registry type
- Provide the LDAP server information, host name and port number
- Select option whether to enable SSL with registry server or not.
Configure Runtime (continued)
- Choose logging option, by default Tivoli Common Directory for Logging is not enabled.
- Review configuration options and click Finish
- Runtime is configured
Configure Policy Server

- Provide TDS management domain name and domain location DN
- Provide the TDS administrator name and password and click OK
- If connection to TDS is successful, provide the password for ISAM Administrator.
Configure Policy Server (continued)

- Choose minimal or user standard group tracking.
- Specify SSL connection parameters
- Policy Server configured
- ISAM CA certificate is created in C:\Program Files\Tivoli\Policy Director\keytab\pdcacert.b64
On the TDS side, the secAuthority=Default is created and the ISAM Admin user is created.
Install Authorization Server

- Run launchpad64.exe again and select Authorization server from the list of components. Notice that Policy Server and Runtime components are no longer listed since they have been installed in previous steps.
- Clicking Next will launch Installshield wizard, follow the prompts to accept license agreement and to copy the executables to the server.
Configure Authorization Server

- Specify the domain information, from previous step we are using Default
- Provide Policy Server’s host name and port number that were configured in previous steps.
- Provide Policy Server’s Administrative ID and password that were configured in previous steps.
Configure Authorization Server (continued)

- Provide Instance Name and host name (optional), accept the default Administration and Authorization request ports: 7137 and 7136 respectively.
- Authorization Server is configured
Install WebSEAL

- Run launchpad64.exe again and select WebSEAL from the list of components and click Next. Notice that Policy Server, Runtime and Authorization Server components are no longer listed since they have been installed in previous steps.

- The pre-requisite Web Security Runtime will be installed as well. Clicking Next will launch Installshield wizard, follow the prompts to accept license agreement and installation path to copy the executables to the server.

- On Windows, the default path for Web Security Runtime installation is: C:\Program Files\Tivoli\PDWebRTE
  The default path for the WebSEAL installation is: C:\Program Files\Tivoli\PDWeb
Configure WebSEAL

- Click the Configure button
- Provide host name and listening port, accept the default 7234 port.
Configure WebSEAL (continued)

– Provide the domain name, Administrative ID and password needed for WebSEAL to connect to the Policy Server
– Once the credential is verified, specify SSL option for LDAP communication
– Specify both the HTTP and HTTPS access ports
  • WebSEAL root directory is C:/Program Files/Tivoli/PDWeb/www-default/docs
– WebSEAL is configured
Install Web Portal Manager

- Run launchpad64.exe again and select Web Portal Manager from the list of components.
- Pre-requisite components will be installed which include: Installation Manager and WebSphere (can be skipped if already installed), License, and Runtime for Java.
- License installed to C:\Program Files\Tivoli\Policy Director\
Configure Runtime for Java,
- Specify WebSphere JRE path
- Select Full for configuration type
- Choose whether the enable Tivoli Common Directory
Configure Web Portal Manager

- Specify the full path for WAS, host name and port number.
- In our environment, security is enabled for WAS Console thus SSL needs to be enabled. Specify WAS Admin credential and locations for trust store and key store files.

Note: If WAS JRE is not configured yet, error is thrown
Configure Web Portal Manager (continued)

- Specify Policy Server information, host name and port number.
- Specify Authorization Server information, host name and port number.
- Specify ISAM Admin, sec_master, credential
- The Web Portal Manager is deployed and be accessed from WAS Console
ISAM 7.0 Installation & Configuration – Apply Fix Pack 2

- **A. On oclcsocpe52vmm4 (9.39.39.75)**
  1. Upgrade GSKit to from Version 6.01.000 to Version 8.0.50.3 - GSKit installer downloaded separately (not included with ISAM 7.0 FP2)
  2. Upgrade the IBM Security Utilities from 6.01.000 to 7.0.0.2 (TivSecUtl)
  3. Upgrade the Security Access Manager Runtime (PDRTE) from 7.0.0.0 to 7.0.0.2
  4. Upgrade the Security Access Manager Policy Server (PDMGR) from 7.0.0.0 to 7.0.0.2
  5. Upgrade the Security Access Manager Authorization Server (PDAcld) from 7.0.0.0 to 7.0.0.02

- **B. On oclcsocpe52vmm2 (9.39.39.21)**
  1. Upgrade GSKit from Version 8.0.14.43) to Version 8.0.50.3
  2. Upgrade IBM Security Utilities from 6.01.000 to 7.0.0.2
  3. Unconfigure Web Portal using "amwpmcfg -action unconfig -interactive" command failed
  5. Upgrade Security Access Manager Runtime for Java to 7.0.0.2
  6. Upgrade Web Portal Manager to 7.0.0.2 (Lesson learned: For fix pack installation, the Web Portal Manager needs to be redeployed, thus for a new environment, first install Web Portal Manager 7.0 base and install Web Portal Manager FP2 then configure it to avoid deploying WPM twice. Refer to Technotes 1261117 and 1625232 if you run into problems with redeployment).
Section 2

- Planning and Preparation
- ISAM 7 Installation and Configuration
- Establishing trust between WebSphere Application Server and ISAM WebSEAL
  - Configuring ICN for SSO
  - Configuring ICM for SSO
- Known Issues
Create a trusted user account in WebSEAL user registry

- Use either Web Portal Manager or ISAM pdadmin command-line utility to create the trusted user.
- This account includes the ID and password that WebSEAL uses to identify itself to WebSphere Application Server.
Import an existing P8 user into WebSEAL user registry

- This is done to verify snoop servlet later
Create a junction for snoop servlet

- Create a junction between WebSEAL and WebSphere Application Server using the `-c iv_creds` option for TAI++
- In WAS Console -> IBM Security Access Manager -> Web Portal Manager -> Create Juncions (need to login as sec_master)

Or use command line option: TAI++
server task WebSEALd-server create -t tcp -b supply -c iv_creds -h host_name -p WebSphere_app_port_number junction_name
Create additional junctions

- Use same procedure and options in Web Portal Manager to create additional junctions with the following paths:
  - /WorkplaceXT
  - /navigator
  - /CaseForms
  - /CaseBuilder
  - /CaseManagerHelp
  - /CaseManager
  - /ICMClient

- NOTE: In the Client Identify Header section, we only need “User Credential” for iv_creds header. The “User Name (Short)” and “User Name (Full DN)” options will generate the iv-user and iv-user-l headers respectively.
Edit WebSEAL configuration file

- Edit the WebSEAL configuration file `WebSEAL_install_directory/etc/WebSEALd-default.conf` (oclcsoce52vmm4 in our env)
- Set the following parameter: `basicauth-dummy-passwd=WebSEAL_userid_passwd`. Where `WebSEAL_userid_passwd` is the SSO password for the trusted user account set in created in previous step.
- Restart WebSEAL service
Configure Security Access Manager Runtime for Java component on the application server

- If Web Portal Manager is not installed or deployed on WAS, this step must be done by running the pdjrtecfg command.
  - In our lab environment, the Runtime for Java is already configured as part of pre-requisite for Web Portal Manager (slide X)
- To verify, execute the pdjrtecfg command to confirm that the IBM Security Access Manager Runtime for Java is already configured.

```
C:\Program Files (x86)\Tivoli\Policy Director\bin>pdjrtecfg -action status -java_home "C:\Program Files (x86)\IBM\WebSphere\AppServer\Java\jre"
HP10F0031E This Java Runtime Environment has already been configured.
```
Create PDPerm.properties file by running SvrSslCfg utility

- For WebSphere application server to communicate with Policy Server and the Trust Association Interceptor (TAI) to establish trust for a request, it requires that the SvrSslCfg utility is run on each Application Server in cluster with config action and cfg_action create option. It will result in creating the PDPerm.properties file on each application server.


  - Execute SvrSslCfg command to create the configuration file and key file
    C:\Program Files (x86)\ibm\WebSphere\AppServer\java\jre\bin>java -cp "C:\Program Files (x86)\ibm\WebSphere\AppServer\tivoli\tam\PD.jar" -Dpd.cfg.home="C:\Program Files (x86)\ibm\WebSphere\AppServer\tivoli\tam" com.tivoli.pd.jcfg.SvrSslCfg -action config -admin_id sec_master -admin_pwd P8cm1234 -appsvr_id oclcsocpe52vmm2 -policysvr oclcsocpe52vmm4:7135:1 -port 7135 -authzsvr oclcsocpe52vmm4:7136:1 -mode remote -cfg_file "C:\Program Files (x86)\ibm\WebSphere\AppServer\tivoli\tam\PDPerm.properties" -key_file "C:\Program Files (x86)\ibm\WebSphere\AppServer\tivoli\tam\key.p12" -cfg_action create

  - Two files created under C:\Program Files (x86)\ibm\WebSphere\AppServer\tivoli\tam
    - key.p12
    - PDPerm.properties
Configure single sign-on using trust association interceptor ++ (1/2)

- Configure Trust Association Interceptor (TAI++) on WebSphere Application Server
  - Configure TAI++ in WAS Console, in Global Security - > Authentication -> Web and SIP security -> Trust Association
  - In Trust Association screen, put a check mark on “Enable trust association” check box and click on Interceptors
Configuring single sign-on using trust association interceptor ++ (2/2)

- Configure Trust Association Interceptor (TAI++) on WebSphere Application Server (continued)
  - In Interceptors, click on `com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlus`
  - Specify loginId, configURL, and WebSEAL.id parameters, save configuration, and logout from WAS Console
  - Restart WAS
Check WAS SystemOut.log for successful TAI++ initialization

- Check the messages in the systemout.log, which is the standard out log of WebSphere Application Server. An example is provided below.

```


```
Checkpoint - Verify snoop servlet (1/2)

- Enable TAI++ trace and access snoop via WebSEAL junction
  
  http://ISAM_Server_host/snoop

- Verify that the P8 user can login successfully and the Request headers contain the basic authentication and iv-creds

![Snoop Servlet - Request/Client Information](image)

**Request headers:**

- **Accept**: text/html, application/xhtml+xml, */*
- **Accept-Language**: en-US
- **Authorization**: Basic Y3BIYWWRztW46UDhjYTEyMzQ=
- **Content-Length**: 0
- **Host**: oclscope52vmm2.oc1.elsabs.ibm.com:9080
- **iv-creds**: Version=1, BAKsl5DCRB8YMADCCBYrvw5UFMAgI5ADCBhAxAR8c8CRNTOp4CAwEoNA1CEwQCACgChAgEL0pQGAFBWe
- **iv-user**: cpadmin
- **User-Agent**: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
- **Via**: HTTP/1.1 oclscope52vmm4:30
- **iv-user-l**: uid=cpadmin, os=windows, o=sample
- **iv_server_name**: default-webseal-oclscope52vmm4:cos
Example of successful ISAM authentication is shown in the WebSphere Application Server trace.log with the TAI++ trace options enabled.

...
com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlusvalidateEstablishedTrust(HttpServletRequest) SSO password not cached. Attempting to authenticate webseal_user
...
...
Section 2

- Planning and Preparation
- ISAM 7 Installation and Configuration
- Establishing trust between WebSphere Application Server and ISAM WebSEAL
- Configuring ICN for SSO
- Configuring ICM for SSO
- Known Issues
Redeploy ICN (1/3)

- Run ICN Config and Deployment Tool and open the ICN profile
- In the “Configure IBM Content Navigator Web Application Task”, change the ICN authentication type from “IBM Content Navigator desktop authentication” to “Application server authentication”. Save and run the Task.
- Verify the task completed successfully
Redeploy ICN (2/3)

- Run “Build the Web Application” Task
- Verify the task completed successfully
Redeploy ICN (3/3)

- Run “Deploy the Web Application” Task
- Verify the task completed successfully
Verify ICN SSO

- Access the following URLs via WebSEAL junctions and verify function functionalities
  - http://ISAM_Server_host/navigator/?desktop=admin
  - http://ISAM_Server_host/navigator/?desktop=ECM (non ICM desktop)

- If you receive ICMPlugin error message, verify the junctions for ICM, specifically /ICMClient has been configured properly
Section 2

- Planning and Preparation
- ISAM 7 Installation and Configuration
- Establishing trust between WebSphere Application Server and ISAM WebSEAL
- Configuring ICN for SSO
- Configuring ICM for SSO
- Known Issues
Configure Permission for IBM Case Manager users (1/3)

- Login to WAS console and navigate to IBM Security Access Manager > Web Portal Manager > Groups > Create Group.
- Enter a group name for your IBM Case Manager users, for example, icm-users and a valid Registry GUID for the group, for example, cn=icm-users,cn=SecurityGroups,secAuthority=Default,o=sample
- Add your IBM Case Manager users such as administrator, and any others to the newly-created icm-users group.
Configure Permission for IBM Case Manager users (2/3)

- In IBM Security Access Manager > Web Portal Manager, navigate to Object Space > Browse Object Space.
- Expand the object tree to locate and click on the default access list for Webseal, default-webseal.
- Under General tab, click the Create button to add new ACL entry.
Configure Permission for IBM Case Manager users (3/3)

- In the ACL entry creation, select Group entry type and provide the name for the previously created group icm-users,
- Select permissions and click apply
- ACL entry is created
- Verify the permission
Verify ICM SSO

- Access the following URLs via WebSEAL junctions and verify function functionalities
  - http://ISAM_Server_host/navigator/?desktop=icm
  - http://ISAM_Server_host/navigator/?desktop=icmadmin
  - http://ISAM_Server_host/CaseBuilder

- If you are able to login but receive error messages when performing certain tasks, check that the junction options specifically the scripting support is not enabled.

![Access Manager for Web Login]

- Username: cpeadmin
- Password: ********

![Error Message]

The stepPage page that you attempted to open cannot be found.

The page cannot be opened because the page class ICMT08/SS_ICWSS/ICM/ICMSTEP_DEFAULT_PAGE was not found. The following error occurred: xhresult

Ask the system administrator to ensure that the page is properly deployed.
Section 2

- Planning and Preparation
- ISAM 7 Installation and Configuration
- Establishing trust between WebSphere Application Server and ISAM WebSEAL
- Configuring ICN for SSO
- Configuring ICM for SSO

- Known Issues
Known Issues when SSO is enabled

- After logging into a WebSEAL junction you may receive Not Found error with favicon.ico, see notes later in the Troubleshooting Section on how to handle this.

- To prevent applet sessions from failing with WAS 8.0.x and higher, you must disable the relevant HTTP Only settings for your deployment. Refer to details and WAS configuration needed in Technote 7023814

- The logout button is disabled, this is the expected behavior. To change this behavior a custom SSO logout action via ICN plug-in is needed. Refer to the IBM Developer works article in the link below.
  https://www.ibm.com/developerworks/community/blogs/e8206aad-10e2-4c49-b00c-fee572815374/entry/creating_an_sso_logout_action_in_ibm_content_navigator?lang=en
Section 3

- Tracing and Logging
- Troubleshooting
Section 3

- Tracing and Logging
- Troubleshooting
Tracing and Logging

• Collecting Data for ISAM: WebSEAL (TAI++ issues)
  – Collect the following information for each WebSEAL instance and WebSphere Application Server.

  – WebSEAL:

    – 1. Ensure that 'requests = yes' in the [logging] stanza, and 'text/html = -1'
      at the beginning of the [compress-mime-types] stanza, of the WebSEALd.conf file. If the settings are changed, restart the WebSEAL instance.

    – 2. Create a 'traces' directory under the WebSEAL server var directory (ie. /var/pdweb/www-default for the default instance), or in another temporary storage location, and make it writable by the WebSEAL user (ivmgr by default). If the directory exists, ensure that previous trace files have been removed. The full path to this directory is referred to as <traces>.
Collecting Data for ISAM: WebSEAL (TAI++ issues) (1/2)

3. Enable WebSEAL tracing.
   - pdadmin> server task <WebSEALd-instance> trace set pdweb.debug 9 file path=<traces>/pdweb.debug.txt,rollover_size=100000000
   - pdadmin> server task <WebSEALd-instance> trace set pdweb.snoop 9 file path=<traces>/pdweb.snoop.txt,rollover_size=100000000

4. Recreate the problem (after enabling traces for TAM Java API and WebSphere)
   If possible, use a new browser after clearing the browser cache.

5. Wait 1 minute, then disable WebSEAL tracing.
   pdadmin> server task <WebSEALd-instance> trace set pdweb.debug 0
   pdadmin> server task <WebSEALd-instance> trace set pdweb.snoop 0
Collecting Data for ISAM: WebSEAL (TAI++ issues) (2/2)

- **WebSphere Application Server**
  - Enable TAI++ trace. => trace.log will be generated under WAS log directory.
  - Login WAS admin console of ICM server.
  - Troubleshooting→Logs and trace→Server name (server1)
  - Diagnostic trace→Runtime→Change log detail level
  - Set as follows.
    - `com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlus=all`
    - `com.ibm.ws.security.web.TrustAssociationManager=all`

WebSphere HTTP and Case Client Side Tracing

- WebSphere HTTP tracing:
  - Enable and collect Application Server traces with the following trace string:

    **Trace string for all releases of V7.0, V8.0 and V8.5:**

    * info:com.ibm.ws.webcontainer*=all:com.ibm.wsspi.webcontainer*=all:HTTPChannel=all:GenericBNF=all

    Note: There should NOT be any space or '.' between webcontainer and '*' for the above trace strings.


- Case Client Side Tracing:
  - If the issue is related to a client side script error which is reproducible in the client browser, installing a tool to collect and capture header and response content between the browser and the IBM Case Manager server will help to diagnose and isolate the problem. Tools such as FireBug, Microsoft Internet Explorer Developer Tools, Fiddler, HTTPWatch, or other equivalent tools can be used to capture this information.
Case Manager Client, Case Manager Administration Client, Content Navigator Tracing

- The IBM® Case Manager Client, Case Manager Builder records log messages to the IBM Content Navigator log file. To configure debug level logging for IBM® Case Manager web applications, you must enable debugging on the IBM Content Navigator server and restart the IBM Content Navigator server.

  **Procedure:**
  
  - To configure logging settings in IBM Content Navigator:
    
    - Log in to the IBM Content Navigator administration desktop.
    - Click the Settings tab and then click the Logging subtab.
    - Set the logging level for the applications to Debug.
    - Click Save and then click Close.
    - Log out of the IBM Content Navigator administration desktop.
    - Restart the application server instance where IBM Content Navigator is deployed.

- The IBM® Case Manager Client records log messages to the IBM Content Navigator log file.

  For further information about log files in IBM Content Navigator, see the IBM Content Navigator documentation:
  


Case Builder log files

- Case Builder CBE logs
  - To configure debug level messages for Case Builder, enable cbe logging through the WebSphere server.
  - For more information refer to:

- MustGather: Collecting Data for IBM Case Manager Builder v5.2.0.x issues
Section 3

- Tracing and Logging
- Troubleshooting
Troubleshooting – Scenario 1 (A user is unable to logon to SSO)

- **Problem**
  A user is unable to access SSO enabled applications (such as ICN or Case Builder) due to authentication failure through Access Manager for Web login

- **Symptom**
  User sees this following error when try to login to Access Manager for Web login

![Access Manager for Web Login](image)

**Access Manager for Web Login**
HPDIA0200W Authentication failed. You have used an invalid user name, password or client certificate.

- Username
- Password

Login
Troubleshooting – Scenario 1 (A user is unable to logon to SSO)

- Identifying the issue

1. Verify the user credential by logging into non-SSO snoop page on the WebSphere server that hosts the applications, verify the User Principal has the correct user ID and Request headers should contain basic authentication with valid LTPA token on the Snoop Servlet Request/Client Information output,

Sample snoop URL: http://oclcsocpe52vmm2.css:9080/snoop/

If the non-SSO snoop page does not return correct output or the user is not able to logon to the snoop page, contact the directory service system administrator for assistance.
Troubleshooting – Scenario 1 (A user is unable to logon to SSO)

- 2. Verify the user credential by logging into SSO enable snoop page on the WebSEAL server,

Sample SSO snoop URL: http://oclcsocpe52vmm4.css/snoop/

If the following error is observed, verify if the user ID is imported into ISAM registry.

Access Manager for Web Login

HPDIA0200W Authentication failed. You have used an invalid user name, password or client certificate.

- Username
  icm_user1

- Password
  **********

Login

Access Manager for Web Login

- Username

- Password

Login
Troubleshooting – Scenario 1 (A user is unable to logon to SSO)

**Cause**

The user exists on the TDS registry but not imported into ISAM registry.

User exists in TDS registry but not in the ISAM registry
Troubleshooting – Scenario 1 (A user is unable to logon to SSO)

- **Resolving the problem**

Import the existing P8 user into WebSEAL user registry.

For detailed info as how to import users into WebSEAL registry, please see Section 3: Import an existing P8 user into WebSEAL user registry
Troubleshooting – Scenario 2 (All users are unable to logon to SSO)

- **Problem**

  All user are unable to access SSO enabled applications (such as ICN or Case Builder) due to failed to login to Access Manager for Web login

- **Symptom**

  Users see this following error when try to login to Access Manager for Web login,

  ![Error Message]

Troubleshooting – Scenario 2 (All users are unable to logon to SSO)

- **Identifying the issue**
  - 1. Verify the user credential by logging into non-SSO snoop page on the WAS server that hosts the applications, verify the User Principal has the correct user ID and Request headers on the Snoop Servlet Request/Client Information output,

Sample snoop URL: http://oclcsocpe52vmm2.css:9080/snoop
Troubleshooting – Scenario 2 (All users are unable to logon to SSO)

2. Verify the user credential by logging into SSO enabled snoop page on the WebSEAL server,
Sample SSO snoop URL: http://oclcsocpe52vmm4.css/snoop/
If the following error is observed, go to step 3

![Error 403: AuthenticationFailed]

- Username: p8admin
- Password: *****
Troubleshooting – Scenario 2 (All users are unable to logon to SSO)

- 3. Enable and collect Application Server runtime traces with the following trace string

Trace string for all releases of V7.0, V8.0 and V8.5:


Logging and tracing > server > Diagnostic trace service > Change log detail levels

Use log levels to control which events are processed by Java logging. Click Components to specify a log detail level for individual components, or click Groups to specify a log detail level for a predefined group of components. Click a component or group name to select a log detail level. Log detail levels are cumulative; a level near the top of the list includes all the subsequent levels.

General Properties

☐ Save runtime changes to configuration as well

Change log detail levels

☐ Disable logging and tracing of potentially sensitive data (WARNING: This might cause the log detail level setting to be modified when it is applied on the server.)

Select components and specify a log detail level. Log detail levels specified here will apply to the entire server. Expand Components and Groups and click Components to specify a log detail level for individual components, or click Groups to specify a log detail level for a predefined group of components. Click a component or group name to select a log detail level. Log detail levels are cumulative.

HTTPChannel=all; GenericBNF=all; com.ibm.ws.security.web.TrustAssociationManager=all; com.ibm.ws.security.web.TAMTrustAssociationInterceptorPlus=all

☐ Components and Groups
Troubleshooting – Scenario 2 (All users are unable to logon to SSO)

- Examine the WAS trace and identify which user ID failed authentication,


   [3/12/15 14:38:13:354 PDT] 00000151 channel 1 com.ibm.ws.webcontainer.channel.WCCRequestImpl getHeader header --> Basic cDhhZG1pbjpQOGNtMTIzNDU=


   [HPDAC1373E aznAPI -- User registry authenticate failed.

In our system the user ID that failed authentication is webseal_user is the trusted user account for the TAI++

Note: For any TAI++ related issues, you need to contact WebSphere support
Troubleshooting – Scenario 2 (All users unable to logon to SSO)

- **Cause**

  The password in the relevant WebSEALd.conf file (in the Tivoli\PDWeb\etc dir) for the WebSEAL instance or the supply-password configured in Plug-in for Web Servers is incorrect password for the user specified in the login id property.

![Screenshot of a security trust association configuration in IBM Security Access Manager.](image-url)
Troubleshooting – Scenario 2 (All users unable to logon to SSO)

- Resolving the problem

Reset the password for trusted user account (in our case webseal_user) for the TAI++ in the WebSEALd.conf file.
Troubleshooting – Scenario 3 (users are getting errors when working in Case Client)

- **Problem**
  Users are getting errors when working in Case Client

- **Symptom**
  User clicks on a Task and got the “The stepPage page that you attempted to open cannot be found”
Troubleshooting – Scenario 3 (users are getting errors when working in Case Client)

- **Identifying the issue**

Examine the WAS trace,

1 com.ibm.ws.webcontainer.filter.WebAppFilterManager invokeFilters _filtersDefined->false

1 com.ibm.ws.webcontainer.srt.SRTServletRequest getWebAppDispatcherContext

1 com.ibm.ws.webcontainer.srt.SRTServletRequest getRequestURI uri -->
/icm/action/attachment/AddAttachmentFromRepository.js

:com.ibm.ws.webcontainer.servlet.exception.NoTargetForURIException: No target servlet configured for uri:
/icm/action/attachment/AddAttachmentFromRepository.js

1 com.ibm.ws.webcontainer.srt.SRTServletRequest setAttribute this-
>com.ibm.ws.webcontainer.srt.SRTServletRequest@7469268d: name --> [javax.servlet.jsp.jspException], value -->
target servlet configured for uri: /icm/action/attachment/AddAttachmentFromRepository.js]

1 com.ibm.ws.webcontainer.srt.SRTServletRequest attributeAdded this-
>com.ibm.ws.webcontainer.srt.SRTServletRequest@7469268d: key --> javax.servlet.error.status_code value --> 404

Troubleshooting – Scenario 3 (users are getting errors when working in Case Client)

- Use fiddler Web Debugger to check if there is any HTTP errors; in this case, we see the same "AddAttachmentFromRepository.js" caused 404 error (Object not found)
Troubleshooting – Scenario 3 (users are getting errors when working in Case Client)

- **Cause**

  Based on the error in Fiddler Debugger, the JAVA script files in the `/ICMClient/icm/attachment/` directory are not accessible,

  Run the below command to verify the setting of the “Scripting support” option for “ICMClient” junction,

  ```
pdadmin sec_master> server task default-WebSEALd-oclcsope52vmm4.css show /ICMClient

  Junction point: /ICMClient

  Scripting support: yes
  ```

  The output shows that the “Scripting support” is enabled and caused the JAVA script files under `/ICMClient/icm/attachment/` directory not executed.
Troubleshooting – Scenario 3 (users are getting errors when working in Case Client)

- Resolving the problem

1. Delete the faulty “ICMClient” junction.

2. Recreate the “ICMClient” junction,

   Sample command for recreating the junction again,
   
   ```
   pdadmin sec_master server task wd1-WebSEALd-iam.iamdemo.tivoli.com
   create -t tcp -f -b supply -c iv_creds -x -h oclcsocpe52vmm2 -p 9080 /ICMClient
   ```
Troubleshooting – Scenario 4 (handling favicon.ico)

- Place a favicon.ico file in the WebSEAL document root. For example:
  (UNIX):/opt/pdweb/abc.ibm.com-default/docs/
  (Windows): C:\Program Files\Tivoli\PDWeb\www-default\docs

- Add a definition for the ico file format in the [content-mime-types] of the WebSEAL configuration file:
Handling the favicon.ico cont.

- Create an ACL that allows unauthenticated access to /favicon.ico in Web Portal Manager
  - Create favicon ACL
  - Under General tab, assign “Any-other” and “Unauthenticated” ACL entries with “Traverse” and “read” (Tr) permissions (sec_master by default has full permission)
Handling the favicon.ico cont.

- Create an ACL that allows unauthenticated access to /favicon.ico in Web Portal Manager (continued)
  - Under attach tab, attach this ACL explicitly to /favicon.ico or ensure that the unauthenticated permission is inherited to this point
Presentation Summary:

By attending this presentation, you have learned:

- Understand the Authentication flow with and without ISAM SSO.
- Identify the ISAM components involved in configuring with IBM Content Navigator and IBM Case Manager.
- Perform an ISAM installation and configuration.
- Configuration and deployment of ICN and ICM application for ISAM SSO.
- Have a better scope of where to begin your troubleshooting effort.
References

- Security Access Manager for Web Quick Start Guide  

- Installing Base system component for ISAM 7.0  

- Configuring single sign-on for IBM Content Navigator by using IBM Security Access Manager for Web on WebSphere Application Server (FileNet P8):  

- Configuring IBM Case Manager to support SSO through IBM Security Access Manager for Web  

- IBM Case Manager, Version 5.2.1 Verifying your SSO deployment:  

- Single Sign-On Solutions for IBM FileNet P8  

- SSLv3 is enabled in IBM Security Access Manager for Web, potential "Poodle" vulnerability (CVE-2014-3566). Technote  

- Integrate existing LDAP directory into my ISAM registry  
Survey Questions
Questions?