Inventory & Logistics Specialists

CISS Ltd.
2512 Eberhart Road,
Whitehall, PA 18052

CissItd.com Phone (610) 266-7200 info@cissltd.com Fax (610) 266-3927

SSO Integration

Inventory Pro Online (IPOL) supports Single Sign On (SSO) via Active Directory, Smart Cards, Common Access Cards (CAC), and can be extended for other methodologies as well.

SSO allows a user to authenticate via a single service in your organization, then each application a person uses can tie into that service and identify them. This allows for ease of use and limits the need for unique passwords and security measures for your end users. As the name implies, Single Sign On.

IPOL's implementation of SSO allows for various options, You can allow both password and SSO logon, or require only SSO. Additionally at the first login of a user we can link an account to their SSO details to streamline setup. So a user only has to login once and then should be setup perpetually moving forward.

The following guide will walk through the steps to enable this integration in Windows, IIS and IPOL.

Prerequisites -

- Active IPOL Installation
- Windows Server 2012 or greater
- IIS 8.0 or greater

Active Directory Integration -

Our implementation of SSO for Active Directory in IPOL uses the windows authentication module, This module provides IPOL with a user's information if they can be validated by the server. We then cross reference that user information against entries on our user list. If a match is found the user is logged into IPOL automatically. If it cannot be validated we fall back to the standard logon method. The fallback can optionally be disabled for all users except the CISSADM maintenance account.

Windows Setup – Active Directory

1. To begin, Open the Windows Features Dialog
2. Locate and Enable Internet Information Services → World Wide Web Services → Security → Windows Authentication
3. Reboot the machine

IIS Configuration – Active Directory

1. Open the IIS Manager
2. Navigate to your IPOL Site
3. In the IIS Section of the Features View open Authentication
4. Right-Click the "Anonymous Authentication" entry and select "Disable"
5. Right- Click the "Windows Authentication" entry and select "Enable"

IPOL Configuration – Active Directory

1. Open the IPOL Directory and select the Global.asa file for editing.
2. Change the line "Application("ActiveDirectoryLogon") = False" to "Application("ActiveDirectoryLogon") = True"
   - Change "Application("ActiveDirectoryForce") = False" to "Application("ActiveDirectoryForce") = True" if you want to force active directory
3. Save your changes
4. Open IPOL in a web browser window
5. Navigate to the User List, Select any user account
6. Open the Customize link at the bottom right of the page
7. From this screen you can either activate the option ad_user if it is present or add it if it not
   - If it is available simple toggle the visible option on and save
   - If it is not available Add a new line, Then select ad_user as the column and name it appropriately. Then toggle on the Visible, Add, Modify options. The field type should be text.
8. Save your changes when complete.

CISS Ltd.
2512 Eberhart Road,
Whitehall, PA 18052

CissItd.com Phone (610) 266-7200 info@cissltd.com Fax (610) 266-3927

Smart Card / Common Access Card Integration -

A "smart" card is about the size of a credit card, They are used in various business and government systems. Common Access Card, CAC, is the standard identification system for United States military personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer network and systems.

Our implementation of CAC authentication tracks the unique ID assigned to each card and uses that to identify a user. The underlying validation occurs in IIS using the various DOD certificates installed and setup on the server. So firstly the user attempts to access the system, They will then see a prompt to select their certificate (which is available if the CAC card is connected), Then the certificate is presented to the server and validated, Then we check which account the credentials are linked to and process the login.

Smart cards work similarly but instead we capture a portion of the Smart Card certificate as a signature of sorts, This is intended to be compatible across various implementations as the structure is not as clearly defined between implementations as with CAC cards.

IIS Configuration – CAC/Smart Card

1. Open the IIS Manager
2. Navigate to your IPOL Site
3. In the IIS Section of the Features View open the Authentication
4. Select “Active Directory Client Certificate Authentication” and then right click, “Enable”.

IPOL Configuration – CAC/Smart Card

1. Open the IPOL Directory and select the Global.asa file for editing.
2. CAC IPOL Configuration
   - Change the line “Application("CACCardLogon") = False” to “Application("CACCardLogon") = True”
3. Change the line “Application("SmartCardLogon") = False” to “Application("SmartCardLogon") = True” to turn on smart card logon
   - Change the line “Application("SmartCardForce") = False” to “Application("SmartCardForce") = True” if you want to force smart card log on.
4. Save your changes
5. Open IPOL in a web browser window
6. Navigate to the User List, Select any user account

7. Open the Customize link at the bottom right of the page
8. From this screen you can either activate the option ad_user if it is present or add it if it not
   - If it is available simple toggle the visible option on and save
   - If it is not available Add a new line, Then select ad_user as the column and name it appropriately. Then toggle on the Visible, Add, Modify options. The field type should be text.
9. Save your changes when complete.

