

DAU Identity Management (SSO) CAC Troubleshooting Guide

Overview

DAU's [Identity Management](#) single sign-on (SSO) system completes the authentication process for several web-based applications including: the Virtual Campus for online course delivery, DAU Blackboard to support a paperless classroom environment, and out of the classroom knowledge sharing resources such as the Acquisition Community Connection (ACC), and the Defense Acquisition Portal (DAP). If you are unable to login to any of these resources with your DoD Common Access Card (CAC), this guide will step you through identifying and resolving the underlying cause.

Enabling Smart Card Access Requires Password Change

All users that enroll in a DAU course (or request access to any of the SSO applications listed in the above paragraph) are assigned a **username** and **temporary password** automatically via system-generated emails once the account is initially established. **It is required that all users login manually with these credentials and create a permanent password.** Failure to do so may lead to intermittent login issues (such as a continuous login loop in which you're redirected back to the home page, or possibly connection-related error messages) when attempting to login via smart card. If you do not have record of your username and password, please see the options that follow.

- Self-Service options are available to those who have established profile security questions. Simply access the Identity Management website via <https://identity.dau.mil/> and choose either "I forgot my username" or "reset password & unlock account." Note: If you do not have the username & password, you will need to choose both options in sequence.
- If you are unable to recover your credentials online, please send an email to DAUhelp@dau.mil requesting your SSO login credentials. You may also contact our call center at **1-866-568-6924** and choose option #1 from the initial prompt.

Troubleshooting Connection-Related Error Messages

If you are able to choose the smart card login method, but it presents any type of connectivity error immediately thereafter (examples include: 403 Forbidden: Access Denied, 404 Not Found: This Page Does Not Exist, Internet Explorer Cannot Display the Page: Diagnose Connection Problems) the following steps should be completed.

Step 1: Clear Browser and SSL Cache (Temporary Files):

- Within Internet Explorer, click on your "Tools" menu and select "Internet Options." If you do not see "Tools" or a gear-shaped icon, hold down "ALT" + "T" on your keyboard to access this menu.
- Under the heading for Browsing History, please choose the "Settings" button and ensure that "Every time I visit the webpage" is selected; choose "OK."
- Click on the "Delete" button that also appears under the heading for Browsing History.
- Ensure that the option to "Preserve favorites website data" is **not** checked.
- "Temporary Internet Files" **and** "Cookies and website data," should both **be** checked. The other options on this dialog are recommended, but not required.
- Click on the "Delete" button.
- Next, choose the "Content" tab at the top of the Internet Options dialog.

DAU Identity Management (SSO) CAC Troubleshooting Guide

- Select “Clear SSL State” and choose “OK” on the confirmation prompt.
- Click “OK” to close the Internet Options dialog.
- Close all instances of Internet Explorer.
- Open a new Internet Explorer window and attempt to login to your desired DAU resource. If you continue to experience difficulty at this point, please proceed with Step 2 below.

Please note: the remaining instructions are targeted to **home users** and **system administrators** only.

If you are using a work-issued computer, your organization’s IT policy may prohibit its users from making the recommended configuration changes outlined below. As such, it is important that you confer with your local system administrator and ask for their assistance in confirming these settings. This will ensure that any policies/procedures adopted by your organization are carried out and/or documented appropriately.

Step 2: Confirm Browser Security Settings

- Within Internet Explorer, click on your “Tools” menu and select “Internet Options.” If you do not see “Tools” or a gear-shaped icon, hold down “ALT” + “T” on your keyboard to access this menu.
- Click on the “Security” tab and choose the “Trusted Sites” icon.
- With Trusted Sites highlighted, click on the “Sites” button.
- In the field labeled, “Add this website to the zone,” please enter: ***.dau.mil**
- Click on the “Add” button, then “Close” the Trusted Sites dialog box.
- From the top of the Internet Options dialog, choose the “Advanced” tab.
- Scroll down to the “Security” category towards the bottom of the list.
- Ensure that **at least** one of the following options is enabled/checked:
 - Use TLS 1.0
 - Use TLS 1.1
 - Use TLS 1.2

Note: Due to security concerns, it is recommended that SSL 2.0 and SSL 3.0 be unchecked. However, some organizations may still have these protocols enabled temporarily while internal systems are being upgraded.

- Select "Apply," if applicable, and then “OK” to close out of the Internet Options dialog box.
- If any changes were made to the settings outlined in Step 2, it is recommended that you re-clear the cached items as outlined in Step 1 before testing access to the DAU website. If problems continue, please proceed with Step 3 on the following page.

DAU Identity Management (SSO) CAC Troubleshooting Guide

Step 3: Addressing PKI Chaining Issues

- **This step only applies to work-issued computers. Home users may skip to the next bullet point.** System administrators should ensure that "**Turn off Automatic Root Certificates**" is enabled on all DoD systems (through GPO, when possible) to prevent Internet Explorer from creating "preferred path" certificates to the local computer trusted store.
- Run the [FBCA Cross-Certificate Removal Tool](#) on the affected machine. This tool should be run twice on work-issued computers; once from an administrator role and once from the affected user's profile. Home users will only need to run the tool once. While running this tool, you will be prompted to press "ENTER" within a blank command-line window twice.
- Ensure you have the latest DoD root-level certificates by running [InstallRoot 4.1](#).
 - Click the "InstallRoot 4.1" link above
 - You will be prompted to Open/Run/Save the installation file, "InstallRoot_NonAdmin_4.1.msi." The need to save is not required, so it is your preference on which of the available options you choose.
 - Upon opening the InstallRoot_NonAdmin_4.1.msi file, you will be presented with the InstallRoot Setup Wizard. Simply choose "Next" after reading each step of the Wizard.
 - When prompted to select the features you wish to install, ensure that *at least* the "Graphical Interface" is checked. Afterwards, click on "next" and then "install."
 - After the installation of the tool is complete, click "Run InstallRoot."
 - At this point, you may be prompted to add the certificates to Firefox (if installed on your computer). It is recommended that you select "Yes," but if you primarily access DAU resources with Internet Explorer, this is not required.
 - A "Quick Start" screen will appear showing screenshots of the final steps required to complete the installation. Please read the red text within these screenshots and choose "Next" until you're able to select "Finish."
 - After selecting "Finish," you should be presented with a Microsoft Current User tab and, if you chose to install certificates to Firefox as indicated in step #8, a Firefox tab should also appear for each Firefox profile on your computer. Please look under each of these tabs and make sure that "Install DoD Certificates" has a green checkmark. The other certificates (ECA and JITC) are not required.
 - Click on the "Install Certificates" button.

Note: If you experience any difficulty installing these certificates on a work-issued computer, please consult your local IT group