User Guide

AMPS Procedures for Users and Administrators

Application URL: https://amps.dla.mil

Version 7.1.1 ● 14 December 2023

AMPS Release 23.1.3 ● 14 December 2023

Document Information

The following sections furnish the identifying information and revision history of this document, and contributors' contact information.

Document Identification

The following table provides identification information about this document:

Attribute	Details
Document ID:	Working file: AMPS User Guide Ver 7.1.1.docx Published file: AMPS User Guide Ver 7.1.1.pdf
Document Title:	AMPS User Guide: AMPS Procedures for Users and Administrators
Purpose:	This guide provides users and approvers with the procedures they need to submit, approve, and manage role requests and user profile information. Also included are adjunct procedures, such as removing a role, and sub-processes, such as altering organization or supervisor assignments.

Revision History

The following table outlines and describes successive versions of this document:

Version Number	Revision Date	Summary of Changes	Author
6.1.1	16 January 2019	Updated for Section 508 compliance.	Kurt Herbel
6.2.0	16 July 2019	Updated for changes in External-User Registration and recover User ID and Password processes.	Kurt Herbel
6.3.0	10 June 2020	Updated for CAC/PIV modernization and updated Enterprise Help Desk (EHD) to Enterprise Service Desk (ESD).	Kurt Herbel
6.4.0	29 January 2021	Updated IT assistance information to refer to Amelia first, rather than Enterprise Service Desk (ESD). Removed SAAR returns from AAR. Reduced the user response-period for AAR and Expiry SAARs to 20 days each.	Kurt Herbel
6.5.0	3 June 2021	Updated Role Expiry timing and end-date function, added note about sign out dialog box, and updated images for CUI messaging.	Kurt Herbel
6.5.1	17 November 2021	Updated for Release 21.0.3: Removed references to Amelia.	Kurt Herbel
6.6.0	12 January 2022	Updated for Release 21.0.4/22.0.1: Modified code and settings of External Approver Portal to address vulnerability findings.	Kurt Herbel
6.6.1	11 February 2022	Updated for Release 22.0.2: Moved Onboarding ITSM tickets from DLA Remedy to ServiceNow and IT support from DLA's ESD to DISA's Global Service Desk (GSD) and the DLA Service Portal.	Kurt Herbel
7.0.0	27 June 2023	Updated for Oracle Cloud Infrastructure.	Kurt Herbel
7.1.0	16 October 2023	Updated for Releases 23.1.0 (disabled SSN & DOB fields), 23.1.1 (removed browser alert), and new fonts/format for better accessibility.	Kurt Herbel
7.1.1	14 December 2023	Updated Appendix F for Release 23.1.3 changes. Also, made some minor updates and text corrections for clarity.	Kurt Herbel

Contact Information

The following table lists information about content contributors for this procedural document:

Role	Name	Organization	Job Title	Email Address
Stakeholder	Matthew Morley	DLA CIV INFORMATION OPERATIONS	Program Manager	matthew.moreley@dla.mil
Stakeholder	Carolyn Daniel	DLA CIV INFORMATION OPERATIONS	Project Manager	carolyn.daniel@dla.mil
Reviewer	Jennifer Myers	BMA	Project Manager	Jennifer.myers.ctr@dla.mil
Technical	David Huet	Amyx	Technical Lead	david.1.huet.ctr@dla.mil
Operations	Andrea Boughton	Amyx	Operations Lead	andrea.boughton.ctr@dla.mil
Author	Kurt Herbel	Amyx	Documentation Specialist	kurt.herbel.ctr@dla.mil
AMPS DFAS Systems Integrator	Justin Sipe	DLA CIV INFORMATION OPERATIONS	Financial Management Analyst	justin.snipe@dla.mil

Table of Contents

AMPS Overview

AMPS is an account management and provisioning system that collects data about your identity, job, and location, and sets up your access to the computer application resources you need to complete your job tasks. AMPS either sets up this access automatically or provides information to a provisioner for manual setup.

AMPS supports the practice of Role Based Access Control (RBAC), which is a methodology for controlling user access to computer applications, increasing security, and reducing costs. [1] Using this methodology, the AMPS team works with its customers to create collections of data based on users' access requirements and responsibilities. This data is assembled to create sets of permissions that are identified as "roles." Access to computer systems is controlled through the assignment of roles to users based on their job requirements and authorization.

As a user, your access to a computer system is based on the approval of your request for one or more application roles. Each role is a predefined set of permissions for an application. Application users, both internal (civilians, military, and contractors) and external (vendors, members of the public, and others), can have AMPS accounts that enable them to submit requests for these roles. When a user's role is approved and provisioned, the user has access to the application resource. AMPS automates the processes of requesting and approving roles, along with the automation of related processes, such as role removal, role expiration, and yearly account revalidation.

AMPS has been supporting a wide variety of applications in the Defense Logistics Agency (DLA) for the past several years. In early 2014, the AMPS team implemented support of AMPS for the Defense Finance and Accounting Service (DFAS) organization. Sample procedures and screen images may reflect either DLA or DFAS users. However, AMPS is a single product, and procedures are adaptable for any organization.

AMPS Documentation and Training

The **AMPS User Guide** furnishes you with the procedures and instructions for completing AMPS tasks to get your access rights started:

- End users can find instructions for creating and submitting role requests, as well as removing roles and maintaining their user information.
- Approvers—including Segregation of Duties (SOD) Reviewers, Supervisors, Security Officers, Data Owners, and Information Assurance Officers—can find instructions for handling request approvals and other tasks.
- A short section on Total AMPS provisioning is also included.

The user guide also includes procedures for supporting tasks, such as changing one's Organization or Supervisor assignment, modifying the My Information data under My Profile, and checking the status of SAARs.

The AMPS team provides this user guide, along with other user documentation tools, to acquaint users with AMPS procedures. Additional references, called "Snapshots," provide simplified guides to individual procedures. When a user wants to engage in self-training before using AMPS, the AMPS e-Learning modules for users and approvers furnish instruction and interactive Guided Practice to explain and simulate procedural actions, providing onscreen practice for users before they log in and attempt to request roles or approve role requests.

AMPS user documentation and training materials are updated with fresh screen images, new and revised procedures, and new functions periodically as AMPS is enhanced. Check the version number and date on any document's title page or footer to ensure you have the latest copy. The latest versions of the **User Guide** and other user documentation and training materials will be available through the AMPS Documentation screen.

Note:

Sample images of emails and user interface screens are provided throughout this guide. The specific information presented in these samples represents exemplary data and formatting for reference only, and should not be interpreted as definitive of these user emails or screens.

AMPS URL

Getting access to AMPS is easy. Open Edge, Firefox, or Chrome and navigate to this URL: **https://amps.dla.mil**. CAC-enabled, internal and external users can gain immediate access to AMPS after their Cyber Awareness Training requirement is met and recorded. Non-CAC-enabled users are redirected to a registration and login screen, enabling them to register for an account, manage their passwords, and log in with a user ID and current password. **Please note that the system may require CAC-enabled users to select a CAC certificate more than once.**

AMPS Date/Time Stamps

Please note that AMPS specifies all date and time stamps on screens and in reports using **Eastern Time**: Eastern Standard Time or Eastern Daylight Time, depending on the time of year.

UTC: Coordinated Universal Time.

As of mid-January 2018, AMPS underwent software patches that changed the denotation of time throughout the application. User interface screens—including decision screens for approvers—as well as email notifications now express time as UTC times. Times in reports issued since the implementation date are also expressed as UTC times.

You can fine more information on converting UTC time to local time at the following URL:

http://earthsky.org/astronomy-essentials/universal-time

---

[1] http://csrc.nist.gov/groups/SNS/rbac/

IMPORTANT NOTES: About Oracle Identity Manager (OIM)

AMPS is a standalone application built on the framework of a Commercial Off-the-Shelf (COTS) application called *Oracle Identity Manager* (OIM). This application contains a number of features and functions that are not used by AMPS but that nevertheless may be displayed as part of AMPS. Check the **AMPS Inbox Guide** and the **AMPS User Guide** for instructions on how to complete tasks, rather than attempting to learn AMPS strictly from what you see on the screen. Although AMPS has been enhanced to offer many of these features, not all features have meaningful, corresponding actions in AMPS. These features and functions are labelled "Not used by AMPS" within this guide.

About Web Browsers . . .

DLA has tested AMPS in current versions of Edge, Firefox, and Chrome browsers; users have the best viewing experience in one of these browsers. Use of Web browsers other than Edge, Firefox, or Chrome is not supported by DLA.

Service Desk

Users who need IT assistance with AMPS should contact the DISA Global Service Desk (GSD).

Toll free: (844) DISA-HLP (844-347-2457) ** Press 5, then speak or enter D-L-A

DSN: XX* 850-0032 *DSN prefix if needed

DISA GSD Email (non-urgent ticket request)**:**
disa.global.servicedesk.mbx.dla-ticket-request@mail.mil

DLA Service Portal (.mil only)**:**
https://dla.servicenowservices.mil/sp?id=index

AMPS Help: Documentation and Training

After launching AMPS, all **users** have access to a link to an ***AMPS Help*** screen. The documentation on this screen takes the place of all past guides, job aids, and other documents. All documents listed on this screen are distributed in Adobe PDF format and require Acrobat Reader 9 or later to view.

See the section entitled **How to Launch AMPS** for instructions on starting the AMPS application.

For the e-Learning modules, the AMPS development team recommends you use headphones to hear the optional audio commentary. Always download the modules to a local or network drive to run them. Do not attempt to run the modules while in AMPS.

How to Open the AMPS Help Screen

1. Click on your User ID to open the dropdown menu.
2. Click the **AMPS Help** command from the User ID dropdown.

   AMPS displays the Help for AMPS Users screen (see Figure 2).
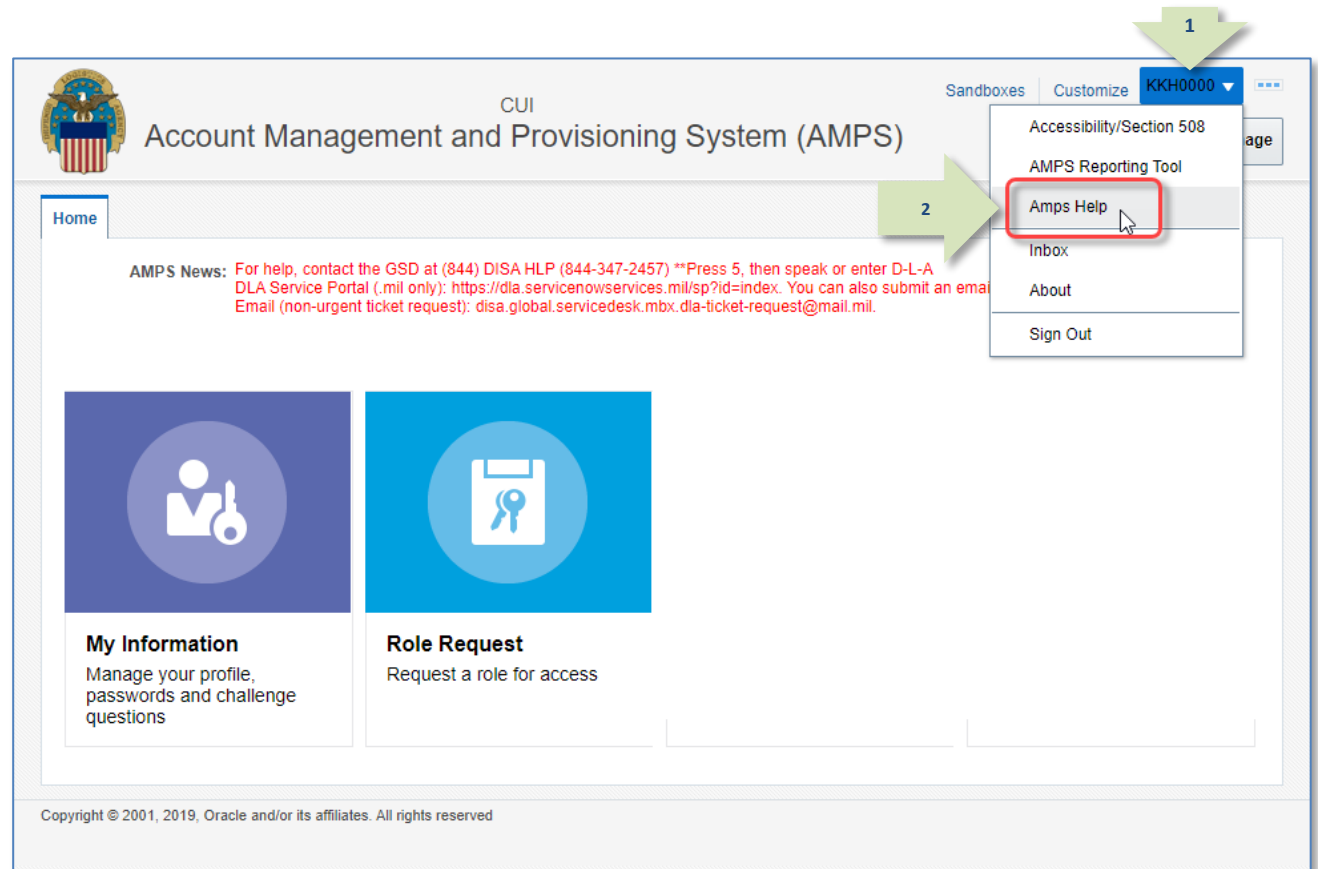
Figure 1: Sample Self Service Home Page - AMPS Documentation Link

3. Review the *Training Library* tab page.

This tab page is displayed first when you open **AMPS Help**.

The page lists all of the available training materials and reference documents sorted into the following categories:

- User Documentation
- Login and Authentication
- Account Maintenance
- Roles
- Primary Roles
- Role Request Approvals and Provisioning
- Role Expiry and Extension

See the category table below Figure 2 for brief descriptions of these categories.

4. To proceed to the next tab page, click the **Tutorials** tab.

AMPS displays the **Tutorials** *tab page (see Figure 3).*
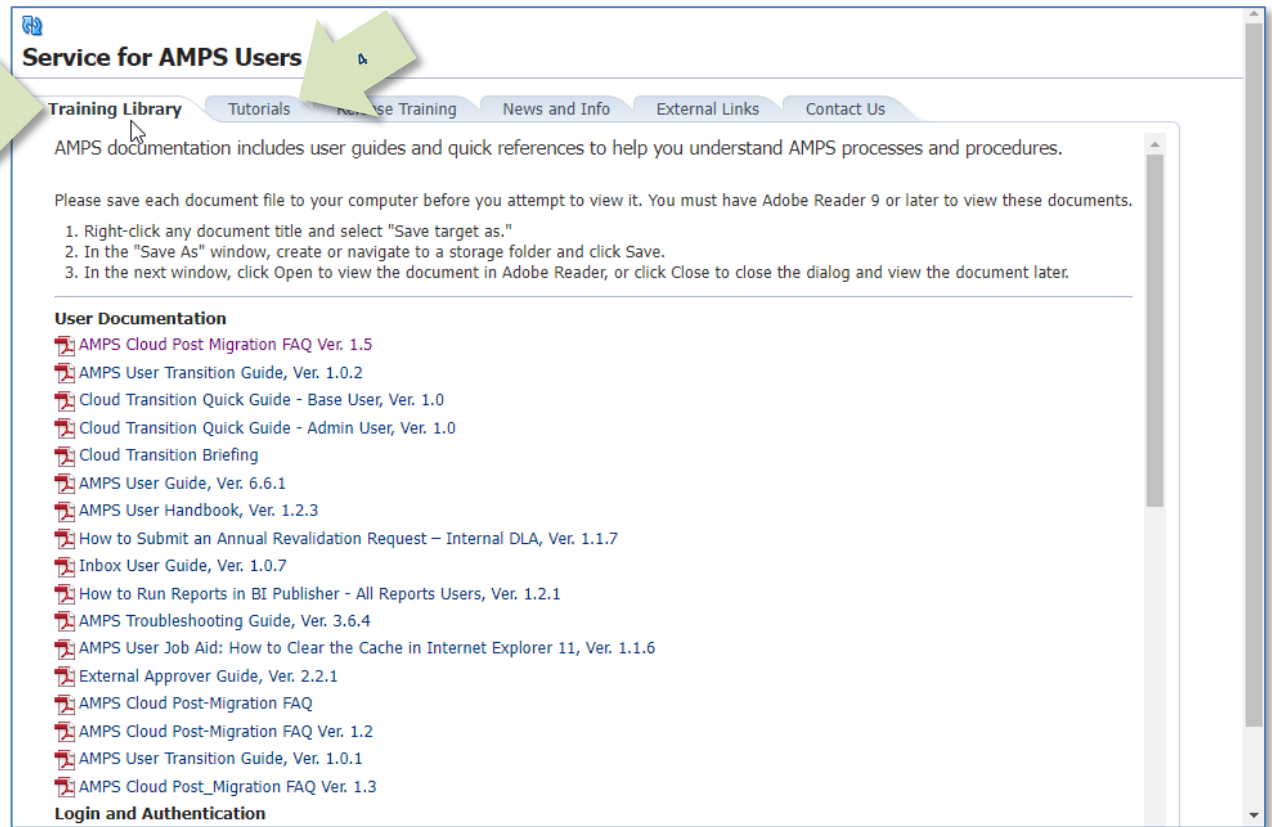
Figure 2: Training Library – Tab Page

This category . . .	Has these document types . . .
User Documentation	Procedures for basic skill training and troubleshooting.
Login and Authentication	Procedures for logging in to AMPS. Information about user authentication, passwords, and security.
Account Maintenance	Procedures for managing information in your AMPS account.
Roles	Procedures on requesting roles.
Primary Roles	Information about choosing and managing role selection and primary roles.
Role Request Approvals and Provisioning	Individual procedures for each approver type and Total AMPS provisioner.
Role Expiry and Extension	Procedures for handling a role expiration or extension notification.

5. Review the *Tutorials* tab page.

    This tab page lists the titles of AMPS e-Learning tutorials. These tutorials are contained in large PDF files that you must download to a local or network drive in order to run them.

Do not run any AMPS tutorial in your browser.

Follow the instructions to download and run each PDF file in Adobe Reader.

Note:

As of the current date, the tutorials are unavailable. They are undergoing an update process and, along with additional new tutorials, will be available at a later date.

6. To proceed to the next tab page, click the **Release Training** tab.

    *AMPS displays the **Release Training** tab page and its contents (see Figure 4).*
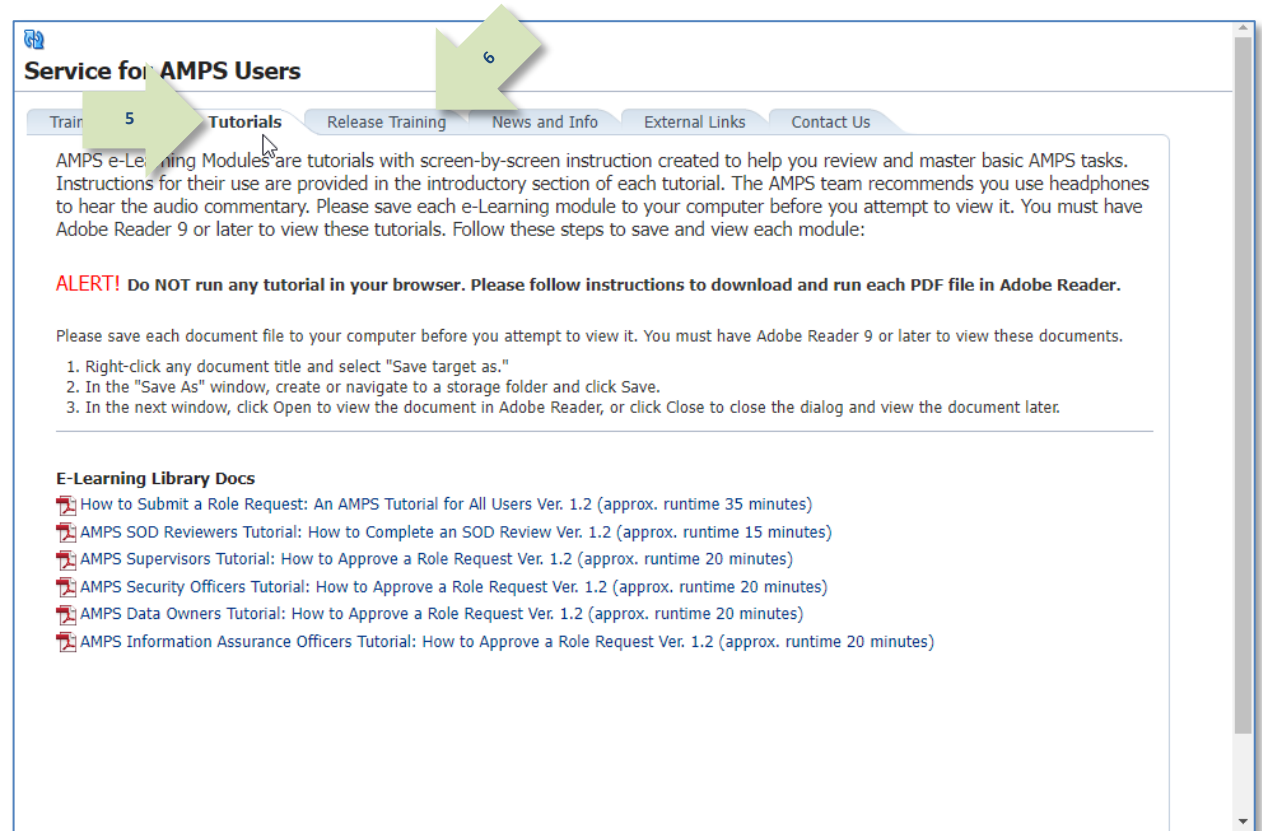
Figure 3: Tutorials – Tab Page

7. Review the *Release Training* tab page.

    This tab page lists the most recent release notes. Each release notes document contains information about the latest changes to the AMPS software implemented in the given release. The latest document represents the current version of the application.

8. To proceed to the next tab page, click the **News and Info** tab.

    AMPS displays the **News and Info** *tab and its contents (see Figure 5).*

Figure 4: Release Training - Tab Page

9. Review the *News and Info* tab page.

   The **News and Info** tab contains various types of documents that do not fit into other categories but that nevertheless contain important, time-sensitive information.

   For example, the AMPS team may post an alert about an AMPS issue to be addressed in the next release.

   Like the other documents listed in **AMPS Help**, these documents are posted in PDF format.

10. To proceed to the next tab page, click the **External Links** tab.

   AMPS displays the **External Links** *tab and its contents (see Figure 6).*
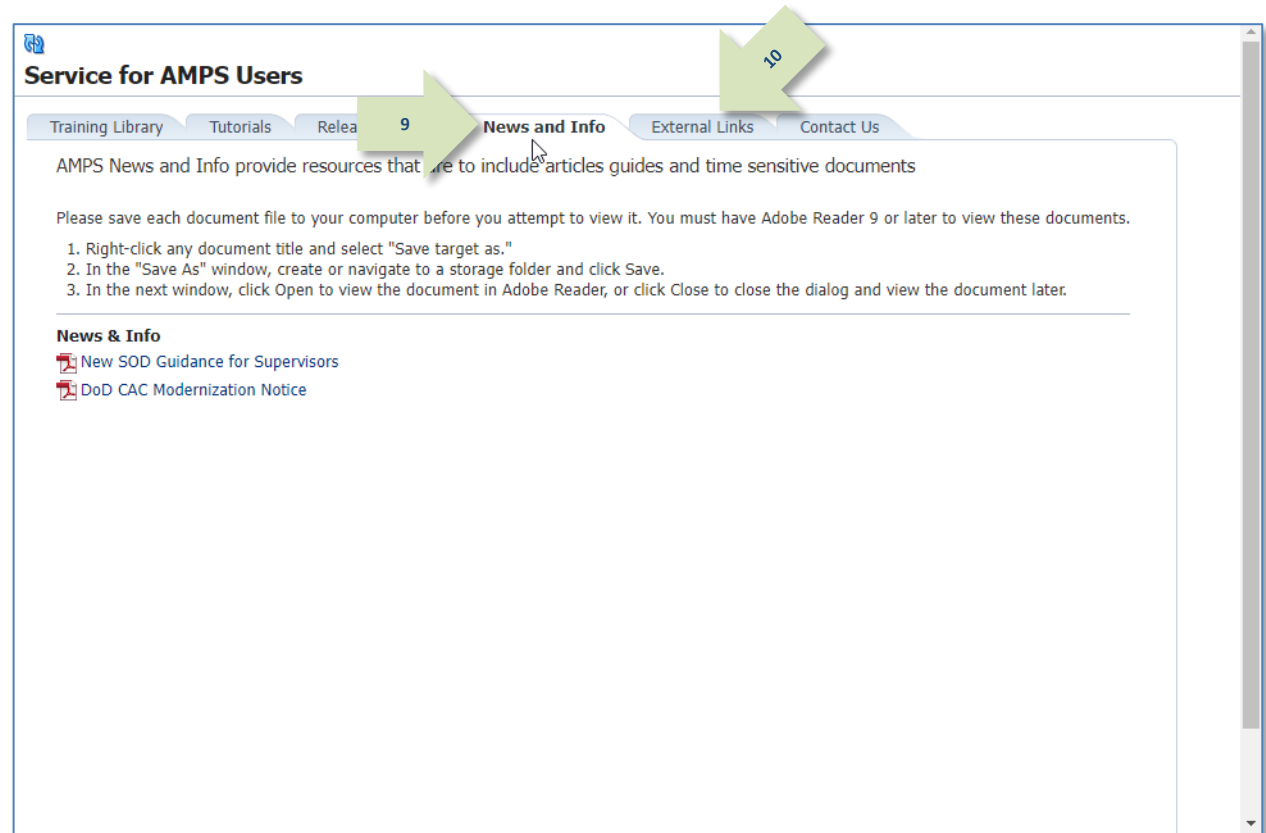
Figure 5: News and Info - Tab Page

11. Review the *External Links* tab page.

The **External Links** tab contains hyperlinks to several sites that may be related to AMPS tasks.

12. To proceed to the next tab page, click the **Contact Us** tab.

AMPS displays the **Contact Us** *tab and its contents (see Figure 7).*

Service for AMPS Users

Training Library | Tutorials | Release Training | Ne... | 11 | **External Links** | Contact Us

The links below are for systems external to AMPS and are provided as a convenience. If there is a link you believe should be added to this page, please create a Request by clicking on the DLA Service Portal link below.

DLA Service Portal
External EBS Business Portal (EEBP) Home Page - The Job Aid link is at the bottom of the home page.
Disposition Services Home Page - The Get Started link is on the right side of the home page.
DLA Energy Home Page - The DLA Energy Portal link is on the left side of the home page.
MEBS - Mapping Customer Operations (MCO) Home Page - The MEBS Application link is on the left side of the home page.

Figure 6: External Links - Tab Page

13. Review the *Contact Us* tab page.

The **Contact Us** tab page contains methods to contact the Enterprise Service Desk.

Three tiers of Service Desk agents are available to assist users with questions and issues regarding AMPS capabilities and tasks:

- Tier 1: Service Desk agents are available to assist you with issues ranging from getting access to the application and resetting passwords to understanding AMPS performance.

- Tier 2: more advanced Service Desk agents can assist you with issues such as understanding and resolving SAAR status questions and account status questions.

- Tier 3: the most advanced Service Desk support staff available. These staff members address issues and coordinate solutions regarding programming or network problems.

You can forward any question or issue to the Service Desk by phone. In addition, you can forward issues to the Service Desk through the DLA Service Portal (see page 9).

14. You can leave the **AMPS Documentation** tab.
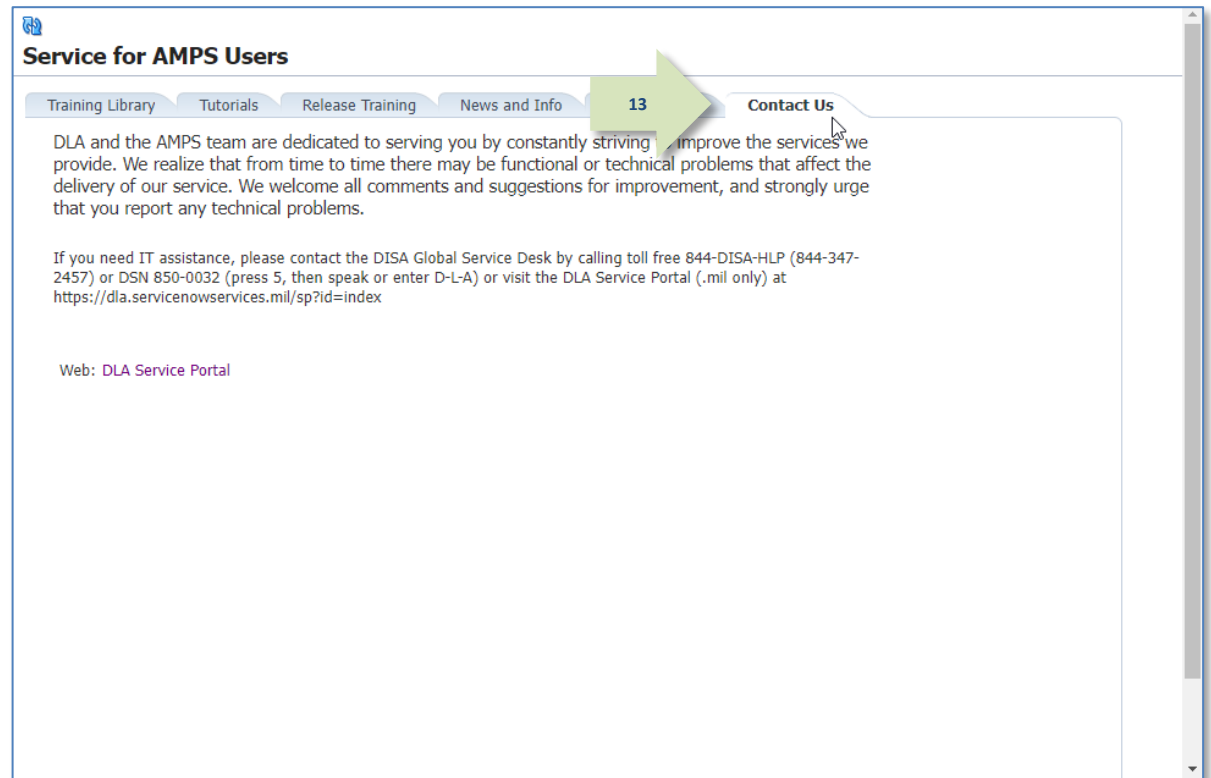
Figure 7: Contact Us - Tab Page

How to View an AMPS Help Document

1. Click the **AMPS Help** command from the User ID dropdown menu.

   AMPS displays the **Help for AMPS Users** *screen (see Figure 2).*
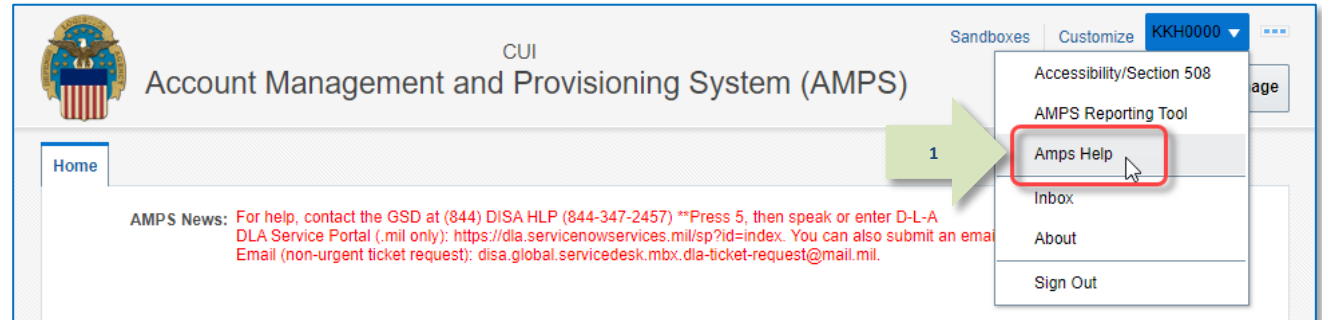
Figure 8: Sample Self Service Home Page - AMPS Documentation Link

2. Select a document title to choose a document for download and view by following these steps:

   a. Right-click a document title to display a context menu.

   b. Click **Save link as**.

   c. Choose a destination folder.

   d. Click **Save**.

   e. Choose an option:

      i. **Open file** to view the PDF now.

      ii. **Close** to close the dialog and view the PDF later.
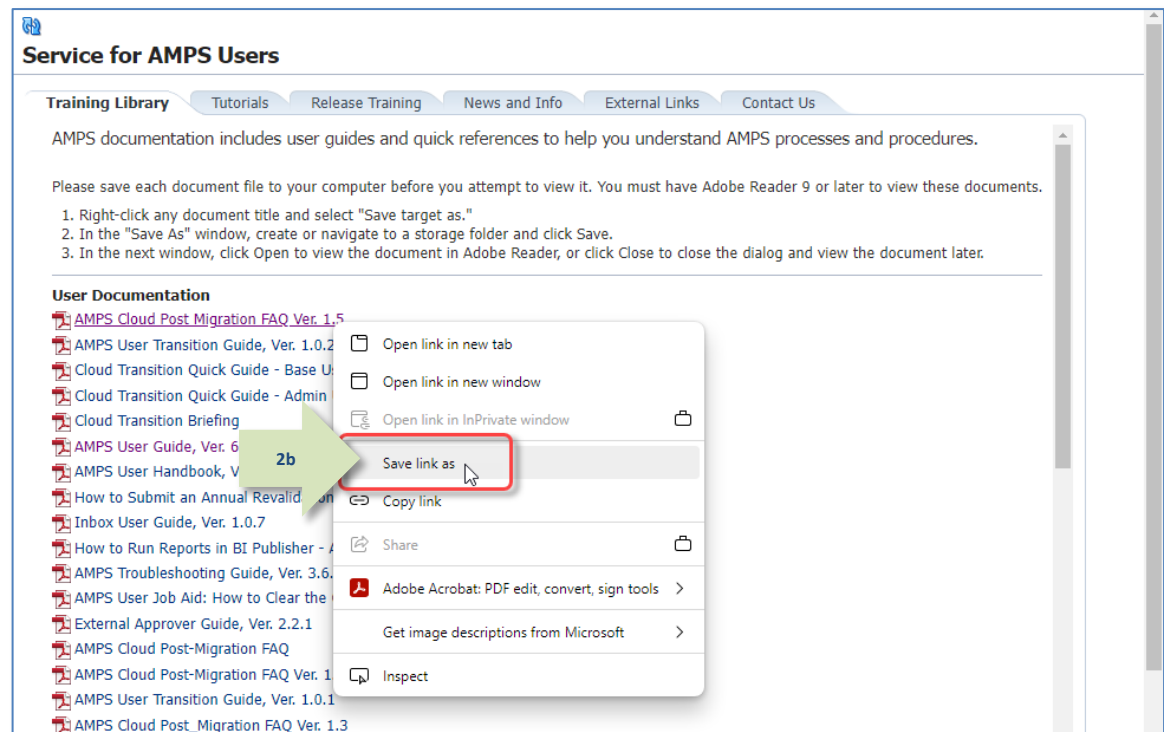
Figure 9: AMPS Training Library

Note:

> **Tutorials listed on Tutorials tab are undergoing revision and updates.**

3. Click the AMPS Tutorials tab to view and download basic tutorials for users and approvers:

    To save a PDF file in the file location of your choice, follow these steps:

    a. Right-click a tutorial title.

    b. Click **Save link as**.

    c. Choose a destination folder.

    d. Click **Save**.

    e. Choose an option:

        i. **Open file** to view the PDF now. Use headphones for maximum sound clarity and availability.

        ii. **Close** to close the dialog and view the PDF later.

Tip!

> **For best results, always save a tutorial to a local drive for easy access and reliable performance.**
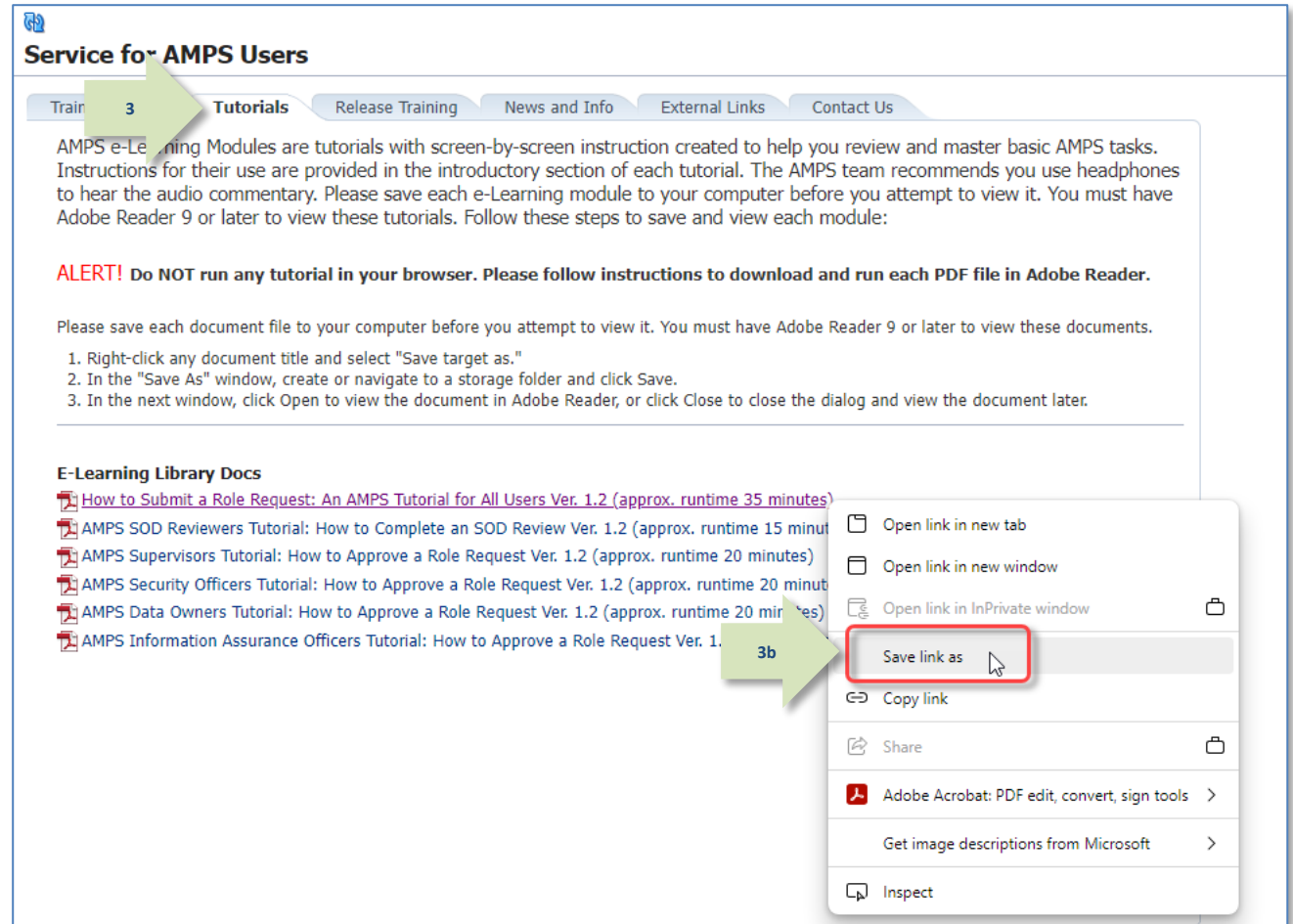
Figure 10: AMPS e-Learning Module

How to Use the *AMPS User Guide*

The AMPS User Guide provides a primary source for information about AMPS processes and procedures. The User Guide covers all of the processes you need to know about with regard to requesting access to the computer systems and resources that help you do your job.

Because you use AMPS only on an as-needed, periodic basis, you will have to refresh your knowledge of AMPS procedures, plus gain an understanding of any features and enhancements added to the system since your previous AMPS sessions. The AMPS User Guide provides the latest information you need to understand how to accomplish a particular task.

The following list outlines the main procedures you need to follow to fulfill your system access needs:

Users' Procedures	User Guide Sections
Request a new role for access to a computer system.	How to Request a Role: Internal User How to Request a Role: External User
Track a role request through the approval and provisioning processes.	How to Check Your Role Status
Cancel a role request.	How to Cancel a Request: End User
Remove a role.	How to Request Removal of a Role
Request an extension of a role assignment.	How to Submit a Role Extension Request
Confirm the expiration of a role.	How to Submit a Role Expiration Request
Update your profile.	How to View and Manage Your AMPS Information
Update your Organization assignment.	How to Update Organization Information
Update your Supervisor assignment.	How to Update Supervisor Information
Review current roles, pending requests, and SAAR history.	How to Check Your Role Status
Update additional attributes for a role.	How to Update Additional Attributes

AMPS Users and Approvers

Everyone who has an AMPS account is an AMPS user. Some users have special responsibilities in AMPS with regard to overseeing how roles are assigned and who is qualified and eligible to receive role assignments. These users receive special roles in AMPS that grant them limited administrative privileges. These privileges, in turn, enable these users to approve end user role requests.

The following table lists some common procedures described in the AMPS User Guide and provides the sections in which the procedures are available.

Approvers' Procedures	User Guide Section
Obtain the AMPS Supervisor role	How to Request the AMPS Supervisor Role
Complete a Segregation of Duties review for a role request.	How to Approve a Role Request: Segregation of Duties Review
Complete an AMPS Supervisor-level approval of a role request.	Supervisor Approval: How to Approve a Role Request Procedure for Internal Supervisor Approvals Procedure for External Supervisor Approvals
Complete an AMPS Security Officer approval of a role request.	How to Approve a Role Request: Procedure for External Security Officer Approval
Complete an AMPS Data Owner approval of a role request.	How to Approve a Role Request: Data Owner Approval
Complete an AMPS Information Assurance Officer (IAO) approval of a role request.	How to Approve a Role Request: Information Assurance Officer Approval
Complete a Total AMPS provisioning ticket.	How to Provision a Role through Total AMPS
Respond to a request for a user's extension of a role assignment.	How to Approve a Role Extension Request

How to Use the Troubleshooting Guide

The **AMPS Troubleshooting Guide**, available on the AMPS Documentation screen, provides topics, with questions and answers that cover common issues. Before you call the Service Desk, consult this guide for information and determine whether a simple solution is already available in the **Topics and Questions/Answers** section.

Figure 11 is intended to represent the general appearance of the Troubleshooting Guide but may vary from the latest version of that document.

Also available are brief descriptions of common processes and definitions of terms. This information helps you understand the purpose of AMPS, as well as your role as an AMPS user. If you need to call the Service Desk after consulting the available documentation, the section titled "**Have this information ready...**" helps you understand what types of information to gather before you make the call.

AMPS: Troubleshooting Guide

Brief Guide to AMPS

What AMPS is . . .

AMPS is an account provisioning system that can set up your access to computer application resources or provide information to a provisioner for manual setup. Access is based on the approval of your request for one or more application roles (see **AMPS Terms**, page 2).

Application users, both internal (civilians, military, and contractors) and external (vendors, public), can have AMPS accounts that enable them to submit requests for these roles. When a role is approved, the user has access to the application resource.

What AMPS is NOT . . .

AMPS is NOT a portal to any application. Having an account in AMPS enables you to request an application role, submit and track the request, and receive a notification when the request is granted.

Access to any requested application is provided through the application itself or through the portal provided by the sponsoring organization.

Getting help with AMPS

For IT assistance, contact the DISA Global Service Desk.

- **Toll-free:**   (844) DISA-HLP (844-347-2457)
- **DSN:**   XX* 850-0032
- **Email:**   DISA GSD Email
- **Service Portal (.mil only):**   DLA Service Portal

* (DSN prefix if needed)

Have this information ready . . .

- What is your telephone number?
- What is your email address?
- When did the problem start?
- Have you had this problem before?
- Is anyone around you having the same problem?
- Is this problem an application access-related issue?
- Is this problem related to a SAAR? If so, do you know the SAAR number?
- Is this issue related to a role request or a role expiration or extension request?

Topics and Questions

Access to AMPS

What is AMPS and how can I get access to it?

Access to AMPS: Network or Browser Problems

Help! I entered the correct URL but AMPS won't open!

Follow these instructions:
If you cannot resolve the issue, report the problem to the DISA Global Service Desk (GSD).

How to Delete Browser History in Internet Explorer

Do you need to clear your browser cache?

Follow these instructions:
If you do not get the results you need, report the problem to the GSD.

How to Refresh Stored Pages in Internet Explorer.

Do you need to refresh all stored pages in Internet Explorer?

Either of the two instruction sets ensure that Internet Explorer refreshes the selected page each time you reopen it.

At the end of the instructions, close the browser and reopen it to continue work.

Answers

AMPS stands for **Account Management and Provisioning System**. AMPS helps you set up accounts on the computer systems you will use in your job. (See **What AMPS is...** at left.)
To launch AMPS, type the following URL into your Internet browser: **https://amps.dla.mil**

Are you seeing "**This page can't be displayed**" or another error in screen display?
Intermittent DLA network issues can cause users to get this message when attempting to launch AMPS. To resolve the issue, try these actions:

- Press the F5 button (on your keyboard) **repeatedly** to get the AMPS screen to load. **Use this method any time AMPS stops responding.** If it does not work, continue with the next steps.
- Close your browser and repeat your effort to open AMPS.
- If this message continues to appear, check the list of known issues on the DLA Service Portal.
- If AMPS is not on the outage list, try the following:
  1. Clear your browser cache and SSL State in the browser Options.
  2. Close all instances of the browser, no matter what website you are on.
  3. Restart the browser and try AMPS again.
  4. If that fails, leave the browser window open and open a new session (option under File menu in Internet Explorer) and navigate to AMPS from the new window.
  5. If you are on VPN, disconnect from the current site and try another one (Ogden/Columbus in the USA or [other available location if in another part of the world]).
  6. If you are in VDI, you can try connecting through the VPN from your main desktop on the thin client (this has not been verified on zero clients):
     a) Exit VDI.
     b) Locate the Telework folder on your desktop.
     c) Double-click the Juniper or Pulse Secure icon.
     d) After connecting to a new location, return to the Telework folder and click the Internal VDI URL.
     e) After you are logged in and back on VDI, try AMPS again.

Follow these steps to delete the browsing history:

1. In Internet Explorer, click the **Tools** command on the main menu.
2. Click the **Delete browsing history** option in the **Tools** menu.
3. In the Delete Browsing History dialog, ensure that the following two options are checked:
   - **Temporary Internet files and website files**
   - **Cookies and website data**
4. Click the **Delete** button.
5. Click the *close* icon in the banner to dismiss the message.
6. Close the browser and reopen it to continue work.

To instruct Internet Explorer to refresh the stored pages each time you open them, follow these steps:

1. In Internet Explorer, click the **Tools** command on the main menu.
2. Click **Internet options** in the **Tools** menu.
3. In the Internet Options dialog, click the **Settings** button.
4. In the Website Data Settings dialog, click the radio button for this option: **Every time I visit the webpage**.
5. Click the **OK** button.
6. In the Internet Options dialog, click **OK** to close the dialog.

As an alternative method, follow these instructions:

1. With Internet Explorer opened, click the gear icon in the upper right corner of the browser window.
2. Click **Internet Options** in the drop-down menu.
3. In the Internet Options dialog, locate the **Browsing History** section and click the **Settings** button.
4. In the Website Data Settings dialog, click the radio button for this option: **Every time I visit the webpage**.
5. Click the **OK** button.
6. In the Internet Options dialog, click **OK** to close the dialog.

AMPS OIM User Troubleshooting Guide Ver 3.6 A.pdf   1 of 3   Property of U.S. Government. 2022

Figure 11: AMPS Troubleshooting Guide

How to Use the AMPS Snapshots

AMPS Snapshot documents are quick references that provide streamlined views of typical AMPS procedures. These quick references provide illustrated, step-by-step instructions for completing common AMPS tasks. The following table lists and briefly describes some of the current AMPS Snapshot documents available through the AMPS Documentation Library. Check the **AMPS Help** page for additional Snapshots.

AMPS Snapshots	Descriptions
Multi-login for AMPS Users with Multiple Accounts	Users who have more than one AMPS account—for example, a user may have a military and a civilian account—AMPS will present an option to choose an account. This snapshot explains the simple procedure for selecting a logon account.
Request the AMPS Supervisor Role	Before a Supervisor can approve a role request submitted by a person who reports to him or her, the Supervisor must request and be approved for the AMPS Supervisor role. This snapshot explains the procedure for submitting a request through AMPS for this role.
Complete and Submit a Role Request - Internal User	Each user takes responsibility for requesting the roles that, when approved and provisioned, furnish the user with the permissions to access and work on computer applications. This snapshot provides stepwise instructions and screen illustrations for submitting a role request through AMPS.
	To submit a role request, check with your Supervisor and obtain the full and correct name of the role you need to perform tasks related to your job.
Complete and Submit a Role Request – External User	Various organizations, including DLA and DFAS, provide limited access to certain applications to users external to the organization. Like civilian, military, and contract employees, these users must apply for AMPS accounts and request the roles that permit them the access they need. This snapshot summarizes the procedure for an external user who wants to submit a role request.
	External users are responsible for knowing the full and correct name of the roles they need, as well as their CAGE Code and DoDAAC account numbers for roles that require them.
Completing an SOD Review - Segregation of Duties Reviewer	Some organizations require an evaluation by a Segregation of Duties (SOD) Reviewer. If a selected role is set up for an SOD Review, the SOD Reviewer will be notified first of the request and will have first responsibility for assessing the user's request to ensure no conflicts exist.
	This snapshot explains how an SOD Reviewer can log in to AMPS, after completing the review, and enter comments that describe the assessment. The SOD Reviewer can then forward the request to the user's Supervisor for action.
Approving an AMPS Role Request – Supervisor	Each user's Supervisor must approve role requests submitted by their direct reports. If a Supervisor cannot approve a role request for some reason—the user has requested the wrong role, for example—the Supervisor can also reject the role request. This snapshot provides the instructions for approving a role request.

AMPS Snapshots	Descriptions
Approving an AMPS Role Request - Security Officer (Internal)	Each organization has Security Officers who review each user's security credentials to obtain computer access to various resources. This snapshot provides the simple procedure followed by a Security Officer to approve a user's initial role request. Security Officers see only the user's first role request unless the user is flagged for continual review.
Approving an AMPS Role Request - Data Owner	Each application has one or more Data Owners assigned to resources. An application's Data Owner has responsibility for approving or rejecting each request for a role that gives access to the application. This snapshot provides the simple procedure followed by a Data Owner to approve a user's application role request.
Approving an AMPS Role Request – IAO	Some organizations, such as DFAS orgs, have Information Assurance Officers (IAOS) who review role requests to ensure a requesting user has recent Cyber Awareness Training as a qualification for obtaining any application role. This snapshot provides the simple procedure followed by an IAO to check the user's training date and approve a request. Note that no IAO review is required for DLA systems.
Change Supervisor Information - End User	If an AMPS user's Supervisor assignment changes, he or she can update the Supervisor's name in AMPS before submitting any action that requires a Supervisor's review and approval. Supervisors handle user role requests and role removals.
Change Organization Information - End User	If a user changes to a different Organization, he or she can update the Organization name in AMPS. Because role requests are submitted to Organizational Security Officers and, in some cases, to IAOs, each user who wants to submit a role request for approval must ensure that the Organization information on his or her account is accurate to ensure the request goes to the correct Security Officers and IAOs. This snapshot provides the procedure for updating Organization information in AMPS.
Change Organization Information - AMPS DFAS End User	This snapshot provides the Organization update procedure DFAS users are required to follow the first time they submit role requests.
How to Request a Role Extension	This snapshot provides steps all users will take to request the extension of a role. This type of SAAR is triggered by the system.
AMPS Transition Quick Guide – Base User	This snapshot provides information about using and navigating the Self Service Home page.
AMPS Transition Quick Guide – Admin User	This snapshot provides information about using and navigating the Self Service Home page and the Manage Home page.

How to Use the AMPS Tutorials

Note:

> The AMPS e-Learning modules are currently undergoing revision and updates.

The **AMPS Tutorials** are self-instructional tutorials for learning and practicing the most widely used procedures in AMPS. Each module is interactive, enabling a user or approver to observe actual AMPS screens and practice the steps in a procedure before engaging in a live session of AMPS. The practice that these tutorials deliver helps each user walk through and understand the basic steps for requesting a role, and help each approver understand the procedure for approving a role request.

The following table lists the tutorials and their approximate runtimes. Each tutorial is available for download in Adobe PDF format:

e-Learning Tutorials	Approximate Runtime
How to Submit a Role Request: An AMPS Tutorial for All Users, Ver. 1.2	35 minutes
AMPS SOD Reviewers Tutorial: How to Complete an SOD Review, Ver. 1.2	15 minutes
AMPS Supervisors Tutorial: How to Approve a Role Request, Ver. 1.2	20 minutes
AMPS Security Officers Tutorial: How to Approve a Role Request, Ver. 1.2	20 minutes
AMPS Data Owners Tutorial: How to Approve a Role Request, Ver. 1.2	20 minutes
AMPS Information Assurance Officers Tutorial: How to Approve a Role Request, Ver. 1.2	20 minutes

Figure 12: Sample Tutorial Screen

How to Launch AMPS

What you can do:	As a Web-based application, AMPS is available through a browser approved for use by DLA, such as the latest versions of Edge, Firefox, or Chrome. Getting access to AMPS is as simple as opening a browser instance and entering the AMPS URL. • **Internal users and external users with CAC authentication, or authentication through External Certificate Authority (ECA) or Federal Bridge Certificate Authority (FBCA):** These users can gain access to their accounts using a CAC or other authentication card, such as a PIV or PIV-1 card. Internal users cannot employ user IDs and passwords to gain access to AMPS. • **External users (non-certificate users):** User registration, user ID, and password are required for non-certificate-enabled external users. • **Internet Explorer 11 users:** Users equipped with Internet Explorer 11 may be required to use IE11 in emulation mode. See Appendix B.
Where to start:	For instructions on downloading certificates other than CAC, see Appendix G. Start the latest version of Edge, Firefox, or Chrome.

AMPS Gateway: Quick Tour

The **AMPS Gateway** screen provides access to AMPS for all users who have recognized authentication credentials. This screen is displayed after you enter the URL to launch AMPS. The following items describe the features available on this screen:

A. **AMPS News:** Area containing announcements about AMPS changes, releases, or other information.

B. **Link for Access to AMPS:** Link to AMPS for all users.
   - Users with government-issued certificates are authenticated and taken directly into AMPS.
   - Users bearing user ID and password credentials are taken to a login screen.

C. **Downloadable User Guides and Job Aids:** List of AMPS documentation, especially relevant to external users.

D. **Accessibility Help and Information:** Link that opens a separate screen providing information about Section 508 compliance and Accessibility information.

Figure 13: Tour of the AMPS Gateway Screen

After you click the **Accessibility/Section 508** link on the AMPS Gateway screen, AMPS opens a new browser instance and displays the Web site at the following URL: http://dodcio.defense.gov/DoDSection508/Std_Stmt.aspx

Figure 14: DoD Section 508 – Accessibility Help and Information

Recommended Web Browsers

The AMPS team recommends you use the latest version of Microsoft Edge, Mozilla Firefox, or Google Chrome.

Note that if you use a Web browser other than the latest version of Edge, Firefox, or Chrome, your experience may be less than optimal. If you continue to use AMPS in an alternate browser, some functions may not work or be displayed as expected.

Figure 15: Logos for Recommended Web Browsers

How to Launch AMPS: Users with CAC or PIV Cards

1. Ensure the CAC or PIV is inserted in the card reader (not shown).

2. In the URL address field, enter the following URL:

    https://amps.dla.mil/

    Click the appropriate icon in the Web browser to launch the URL search, or press your keyboard's **Enter** key.

    AMPS displays a Windows Security certificate request dialog (see Figure 17).
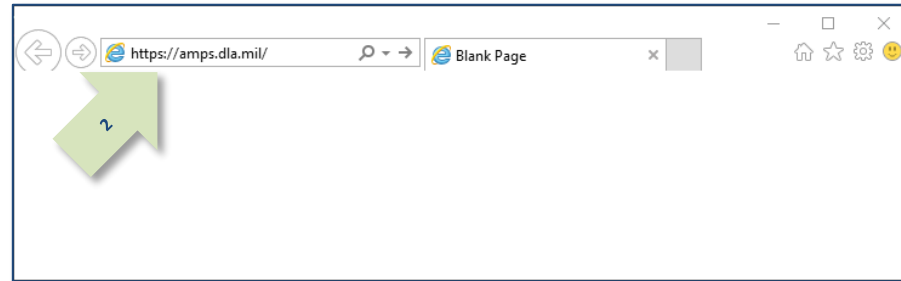
Figure 16: Sample Web Browser Screen – AMPS URL

3. Select your Authentication certificate and click **OK**.

    AMPS displays the **AMPS Gateway** *page (see Figure 18).*

Tip!

AMPS supports authentication with DOD, ECA, and FBCA Certificate Authorities.

The following procedure uses a CAC login procedure as an example.

Follow your certificate authority instructions for installing your authentication certificates.

Note:

CAC users must select the Authentication certificate during login.

If a CAC user selects the wrong certificate, AMPS displays an error message. To log in correctly, restart the launch process and choose the Authentication certificate.

Figure 17: Security Dialog – Certificate Selection

4. Locate and click the command line that reads
Click HERE for access to AMPS.

AMPS takes the following actions, depending on the user's authentication credentials:

- *To CAC-enabled users and users of ECA or Federal Bridge certificates, AMPS displays the* **Single Sign-on Authentication** *page from which users can proceed to the AMPS Home page (see Figure 19).*

- *To External users who are not using a CAC or PIV card, to vendors, and to members of the Public, AMPS displays a login screen (see Figure 23).*
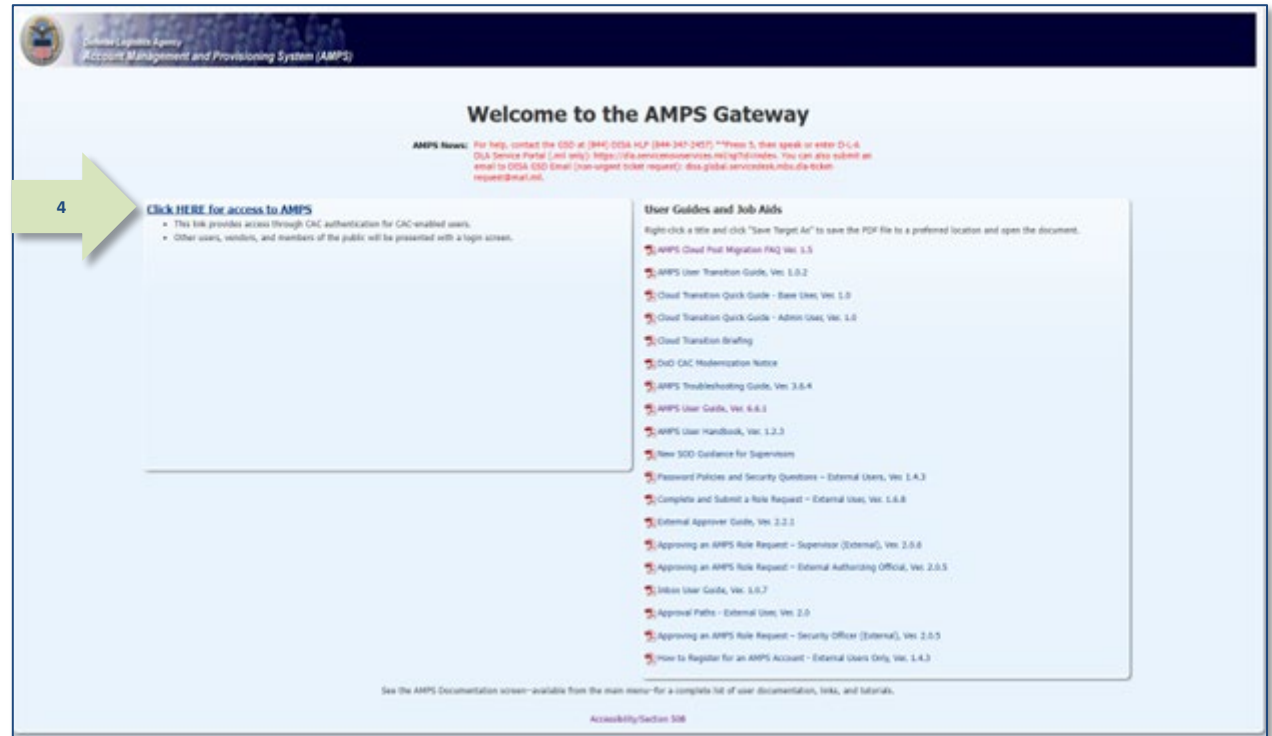
Figure 18: Welcome to the AMPS Gateway

5. Read the Consent to Monitoring (CTM) screen for information system access and click **OK** to acknowledge your understanding and agreement.

    AMPS opens the **Self Service Home** *page (see Figure 20).*

Tip!

For more information about the AMPS Home pages, check these resources from the AMPS Splash screen or Help page:

- AMPS User Transition Guide
- Cloud Transition Quick Guide – Base User
- Cloud Transition Quick Guide – Admin User
- Cloud Transition Briefing
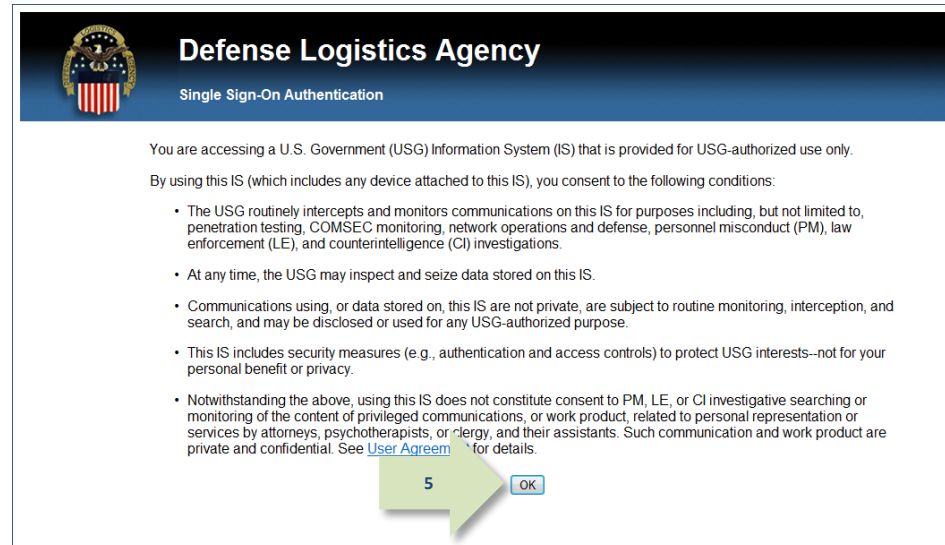
Figure 19: Single Sign-on Authentication - Acknowledgement Confirmation

Note:

The sample shown here displays the commands and tiles available to any user from the Self Service Home page.

Certain AMPS administrative roles have additional commands and tiles, not shown here, that enable administrators to complete their tasks within AMPS.
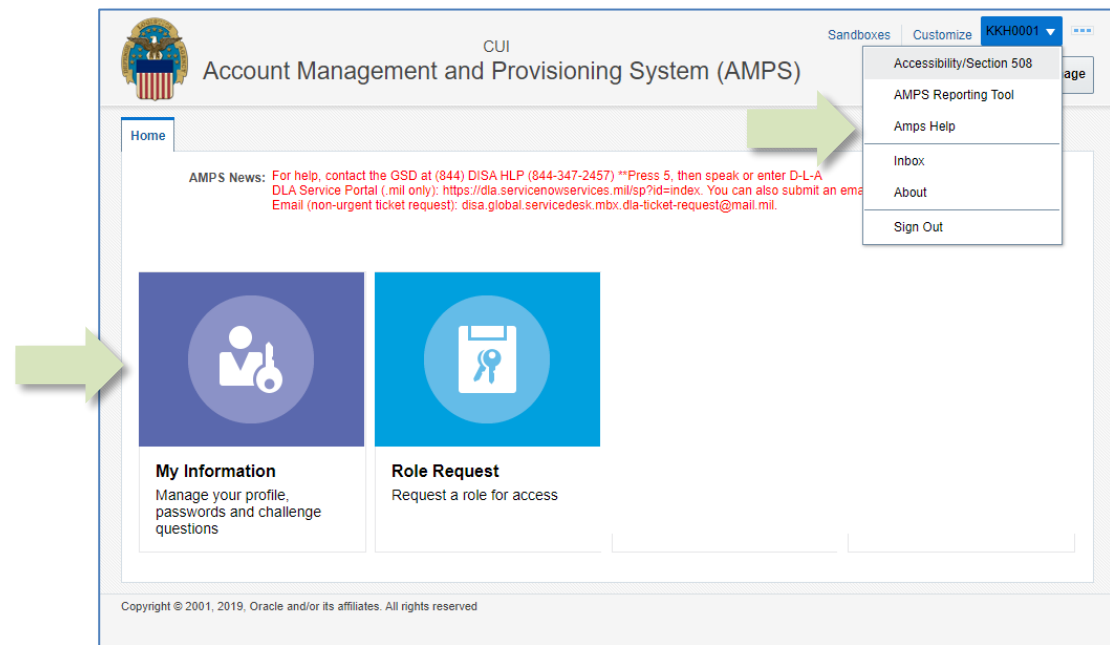
Figure 20: AMPS Self Service Home Page - Sample User

How to Launch AMPS: External Users

External Users who do not have a CAC or other smart card credential must log in with a user name and password.

- The user name is issued to the user during the registration procedure.

- The user creates a password during the registration procedure.

1. In the URL address field, enter the following URL:

   https://amps.dla.mil/

2. Click the appropriate icon in the browser to launch the URL search, or press your keyboard's Enter key.

   *AMPS displays the splash screen: **Welcome to the AMPS Gateway** (see Figure 22).*
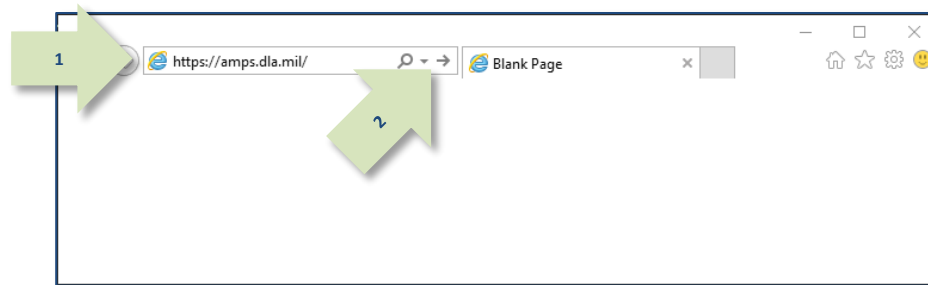
Figure 21: Sample Browser Screen – AMPS URL

3. Locate and click the link that reads **Click HERE for access to AMPS**.

   AMPS takes the following actions, depending on the user's authentication credentials:

   - *To CAC-enabled users and users of ECA or Federal Bridge certificates, AMPS displays a Single **Sign-on Authentication** page from which users can proceed to the AMPS Home page (see Figure 20).*

   - *To External users, Vendors, and members of the Public, AMPS displays a login screen (see Figure 23).*
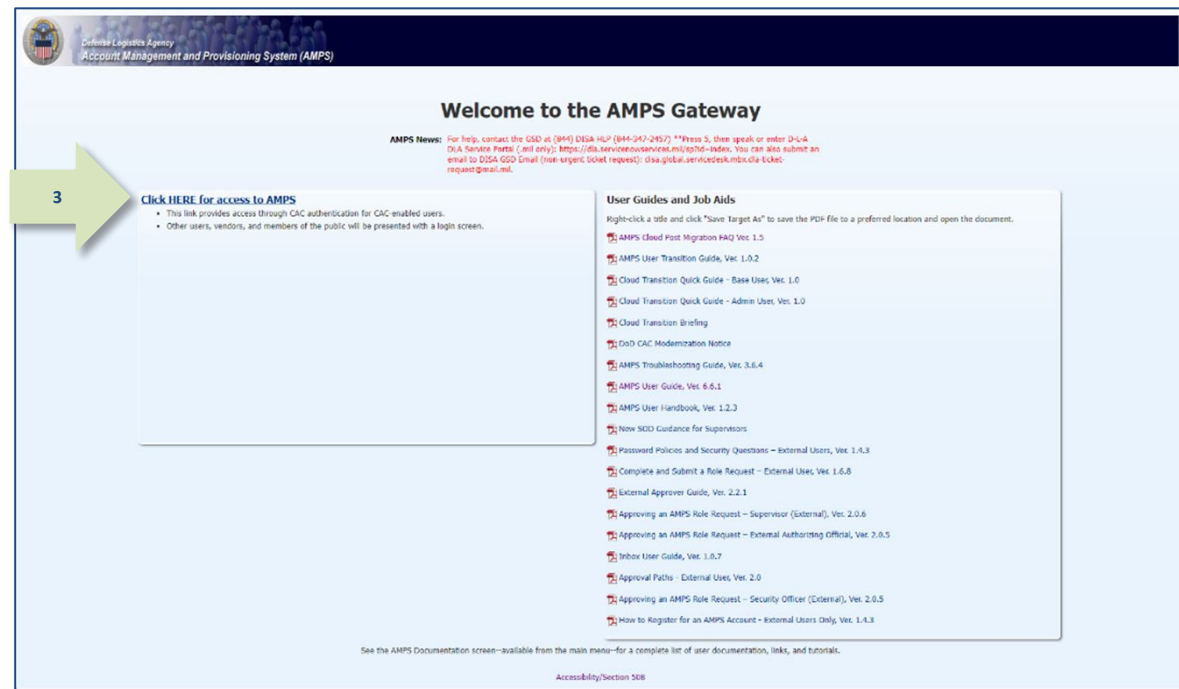
Figure 22: Welcome to the AMPS Gateway

4. Choose the option you need to set up or log in to your external account:

To register for an account, choose this option...

First Time User?:
*Click this link to register for a new account as an external user. Choose this option if you are not a DLA or DFAS employee, and you do not already have an AMPS account. See **How to Register for an AMPS Account** on page 31 for more information.*

To recover forgotten login credentials, choose one of these two options...

Forgot your User ID?:

Click this link to retrieve a forgotten user ID for an existing external AMPS account.

AMPS sends an email message with the correct user ID to the address on file.

Forgot your Password?

Click this link to reset your password if you have a valid external AMPS account and you have set up answers to your authentication questions.

You must submit answers to the authentication questions during this procedure. Otherwise, you must ask the Service Desk for a password reset.

Users who have registered for an account and do not use a CAC or PIV, choose this option...

User ID and Password:
*Enter your AMPS credentials in these fields and click the **Login** button.*

Figure 23: External User's Login Screen

How to Register for an AMPS Account

Non-Smart-Card Users' Login Options

External users are application users who are not employed by DLA or DFAS. External users vary among the following user types:

- Military
- Civilian
- Contractor
- Vendor
- Public

External users may be able to use a CAC or PIV for authentication purposes, while users who do not have smart card authentication credentials accepted by AMPS must create a user ID and password for authentication purposes. During the registration process, an external user fills in information about himself or herself as a user, sets up a password, and sets security questions and answers that enable the user to re-authenticate the account in the case of a forgotten password.

The following procedure helps you understand how to register for an account. Some differences in the information requested are noted in the procedure. For example, if you are a Vendor, AMPS requires you to enter a CAGE code, which is used during business transactions carried out with DLA or DFAS.

Also, persons who are members of the military, civilian employees of the USG, or USG contractors must supply the name and contact information for an External Security Officer (ESO), External Supervisor (ESU), and External Authorizing Official (EAO). The roles you request as one of these user types require a more stringent approval process of which these personnel are a part. The ESO, ESU, and EAO must be three different individuals with different email addresses.

The following section helps you prepare for registration before you begin.

How to Prepare for Registration

1. Set up a password according to the AMPS password rules.

1
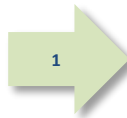
Password Character Rules

The following list shows the characters acceptable in an AMPS password:

- Minimum length of characters:　　15 Characters.
- Maximum length of characters:　　32 Characters.
- Minimum alphabetic characters:　4
- Minimum numeric characters:　　2
- Minimum lowercase characters:　2
- Minimum uppercase characters:　2
- Minimum special characters:　　2
- Must begin with:　　　　　　　Alphabetic character.
- Can use the following characters: a-z A-Z 0-9 + ! # ^ : . ~ - _
- Cannot use these characters:　　 & " / ' ` \ [ ] ( ) % { } @ $? < >

Password Exclusion Rules:

- ✓ Must not use any of your previous 10 passwords.
- ✓ Must not contain your login name (User ID), first name, last name, or email address.

2. Choose three of the four available security questions and set answers to them, according to the limitation rules.

   AMPS requires you to choose three different questions and answers.

   Note that questions having answers not recorded on an official document, such as a birth certificate, can make a more secure choice.

Security Question Limitation Rules:

✓ Choose answers between 3 and 40 characters in length, including spaces and punctuation.
✓ Do not use a word that is contained in the question itself.

Security Question Available Questions:

2

- What is the city of your birth?
- What is the name of your pet?
- What is your favorite color?
- What is your mother's maiden name?
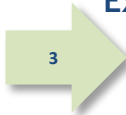
3. If you intend to choose a **Military**, **Civilian**, or **Contractor** user type, provide contact information for an **External Security Officer**.

   Entering the correct email address is especially important.

   AMPS sends notifications for approval of role requests to the Security Officer whom you identify by email address during registration.

   This data is not requested of or required from Vendors or members of the Public.

External Security Officer Data:

3

- Email Address

4. If you intend to choose a **Military**, **Civilian**, or **Contractor** user type, provide contact information for an **External Supervisor**.

   Entering the correct email address is especially important.

   AMPS sends notifications for approval of role requests to the Supervisor whom you identify by email address during registration.

   This data is not requested of or required from Vendors or members of the Public.

External Supervisor Data:

4

- Email Address

5. If you intend to choose a **Military**, **Civilian**, or **Contractor** user type, you also have the option to provide contact information for an **External Authorizing Official**.

   Entering the correct email address is especially important.

   AMPS sends notifications for approval of role requests to the EAO whom you identify by email address during registration.

   The EAO must be different and distinct from the ESO and the ESU.

   This data is not requested of or required from Vendors or members of the Public.

Note:

The EAO email address is an optional field when you register for an AMPS account.

If you later request a role that requires an External Authorizing Official, the field becomes a required field.

External Authorizing Official Data:

5 ➤

- Email Address

---

6. Enter the required user information as shown in this list:

   The fields listed are fields that require entries. AMPS includes several fields for optional contact information.

Note:

Your Cyber Awareness Training date must be within one year of the current date. AMPS displays an error message if the date is out of range, and the system will not allow you to proceed.

Required User Information:

6 ➤

- First Name
- Last Name
- Email
- Title
- Cyber Awareness Training (for Military, Civilian Contractor user types only)
- User Type (automatically entered for *Vendor* or *Public* user types)
- Country of Citizenship
- Official Telephone
- Address

---

7. If you are a Vendor, have your **CAGE** code ready to enter.

7 ➤ CAGE Code (Commercial and Government Entity): Unique five-character identifier assigned to government suppliers.

How to Register for an AMPS Account

AMPS displays the screen illustrated in Figure 24 to an external user when you start the application . . .

- If you are new to AMPS and do not have login credentials, and
- If you are new to AMPS and do not use a CAC or PIV smart card.

Follow the instructions in this section to set up an account, create a user ID, and create a password.

CAC, PIV, and Other Smart Card Users…

If you intend to authenticate with a smart card—CAC, PIV, or other authorized smart card—close all browser instances, insert the smart card in the card reader, and restart the registration process by launching AMPS.

If you do not have a CAC or PIV smart card inserted in a card reader, you will see a message that states the following alert:

"No certificate was detected. If you have a valid DoD, Federal Bridge, or ECA certificate and were not prompted to provide it, please contact the DISA Global Service Desk for further assistance. Otherwise, you may log in with your user ID and password below."

Only users with CAC or PIV smart cards should heed this message and contact the Service Desk, if AMPS did not detect certificates from a card already inserted in a card reader.

---

1. To register for an AMPS account, click this link:
   First-Time User? Click Here to Register

   Click this link if . . .

   - *You have never had a DLA or DFAS account, or*
   - *You have access to an existing DLA or DFAS application but have not registered for an account in AMPS.*

   Before you can proceed with registration, you must verify your email address.

   After you click the link in step 1, AMPS displays the first email-address verification screen (shown below).

   a. Enter a properly formatted email address in the text box.
   b. Click the **Submit** button.

   AMPS displays the second email-address verification screen.

Figure 24: Single Sign-on Authentication - First Time User? Click Here to Register

c. Read the verification message and close your browser window.

d. Open your email inbox and locate the AMPS notification.

e. Open this email and click the tokenized link in the message.

Note:

You must click on the tokenized link in the email within one hour or it will expire and you will have to request a new link.

*AMPS displays the **User Registration** screen (see Figure 25).*

AMPS User Registration: External Users

This screen contains some key information that directs you to the correct registration path.
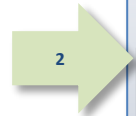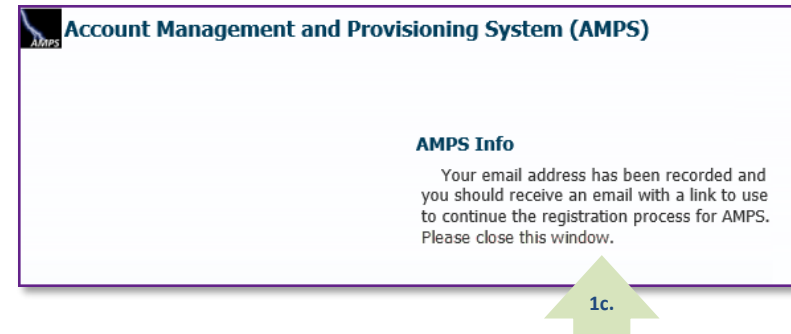
The two important guidelines on this page are . . .

- DLA employees **SHOULD NOT USE** this screen to register for an account. If you are a DLA employee and you see this screen, close the browser and contact the Service Desk for assistance (see page 9).
- CAC, PIV, and other external users with smart cards should already have a card inserted in the card reader. If not, close all browser instances, insert the smart card in the card reader, and relaunch AMPS.

2. Select your **User Type** by clicking the button that corresponds to your type:

- You work for a non-DLA Federal Agency:
  - o Member of the Military
  - o Government Civilian
  - o Government Contractor
- You are a supplier or vendor to DLA.
- You are a member of the public.

*AMPS displays the **Privacy Act Statement** (see Figure 26).*

Figure 25: AMPS User Registration - Select a User Type

Privacy Act Statement

3. Review the Privacy Act Statement.

    Click the links provided to display additional information about how your information may be used.

4. Click **Accept** to proceed.

    AMPS displays a **User Information** *screen appropriate for the selected user type (see Figure 28).*
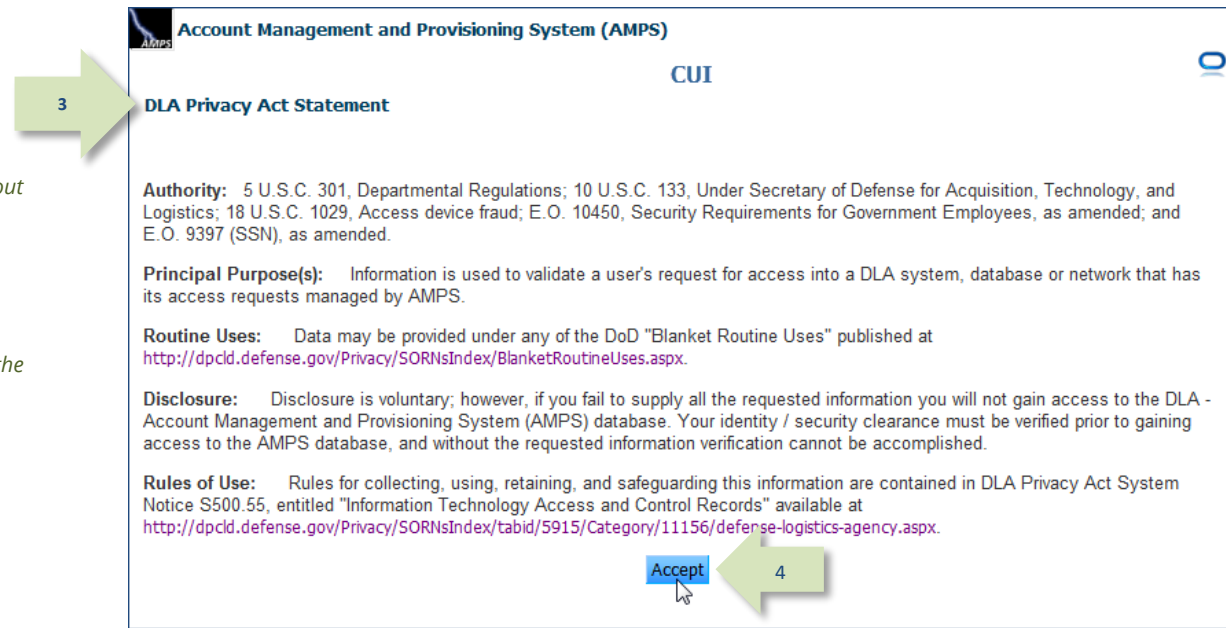
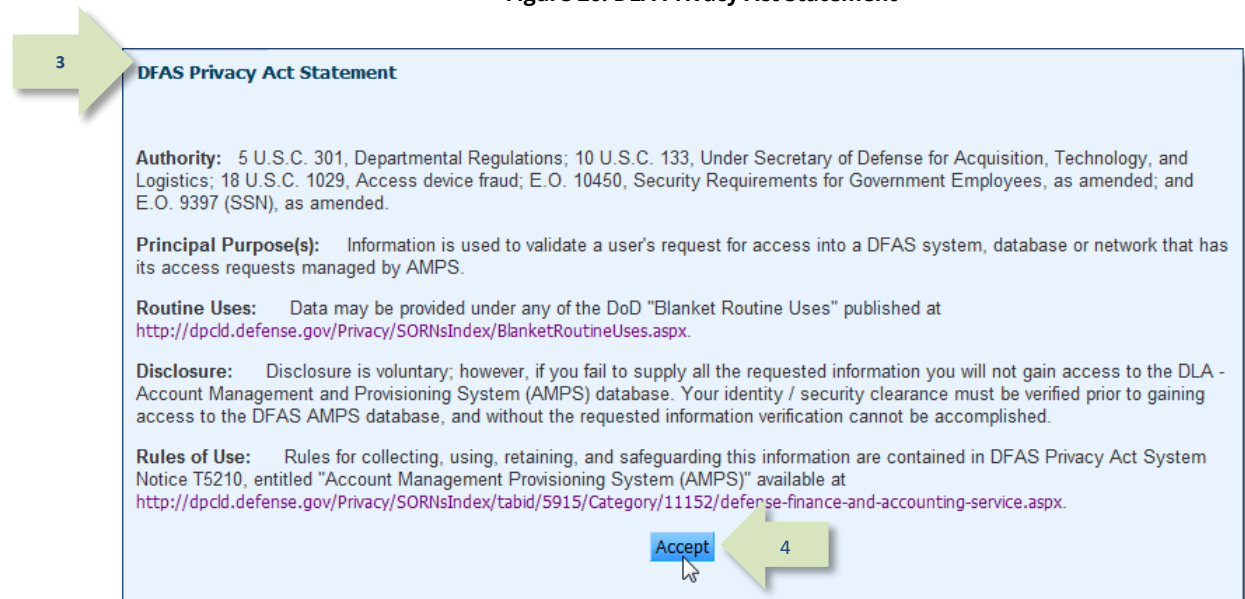**Figure 26: DLA Privacy Act Statement**

Figure 27: DFAS Privacy Act Statement

User Information: Federal Agency User or Contractor

5. Enter required **User Information** in the fields marked with an asterisk.

    Enter a middle name, as needed, to help ensure your name entry is unique.

6. In the **User Information** section, choose a specific User Type from the dropdown list and enter corresponding information (see sample screens in Figure 28):

    a. Civilian

    i. Select your employment **Grade** from the dropdown list.

    b. Military

    i. Select your **Branch** of the military from the dropdown list.

    ii. Select your **Rank** from the dropdown list.

    c. Contractor

    i. Enter your Contract Number.

    ii. Enter the name of the **Contract Company** that employs you.

    iii. Enter or select the Contract Expiration Date.

    iv. Fill in optional information, as needed or instructed.

7. Enter required **Contact** Information.

    Enter optional information, as needed, to ensure completeness.

8. Enter the email address of your **External Supervisor**.

    Must not duplicate the External Security Officer or External Authorizing Official.

9. Enter the email address of your external **Security Officer**.

    Must not duplicate the External Supervisor or External Authorizing Official.

10. Enter the email address of your E**xternal Authorizing Official**.

    Must not duplicate the External Supervisor or External Security Officer.

Figure 28: AMPS User Registration – Federal Agency/Contractor User Information
Required fields are marked with an asterisk.

Military User Type

Contractor User Type

User Information: Vendor or Member of the Public

If you are a Supplier or Vendor . . .

11. AMPS displays a CAGE Code field if you chose the **Supplier/Vendor** user type:

    Enter your five-digit CAGE code.

If you are a Supplier, Vendor, or Member of the Public . . .

12. Enter User Account Information and User Contact Information.

    *Only fields marked with an asterisk (star *) require entries. Information for the other fields is optional.*

Figure 29: AMPS User Information - Vendor Information

All registrants, after completing the appropriate fields . . .

13. Click **Next**.

    AMPS displays a **Security Information** *screen (see Figure 31).*

Figure 30: AMPS User Registration - Public User Information

AMPS User Registration: Security Information for Authentication – All User Types

Note:

The purpose of the security questions is to protect your account from unauthorized changes. If you have to reset a forgotten password, AMPS presents these questions to you for authentication. Ensure that only you have the correct answers.

14. After reviewing the security question rules, choose one security question from each dropdown list.

15. Enter an answer for each question.

    Do not share these answers with anyone.

16. Set and confirm an AMPS password.

17. Click **Next**.

    AMPS displays the **Summary** *screen (see Figure 33).*
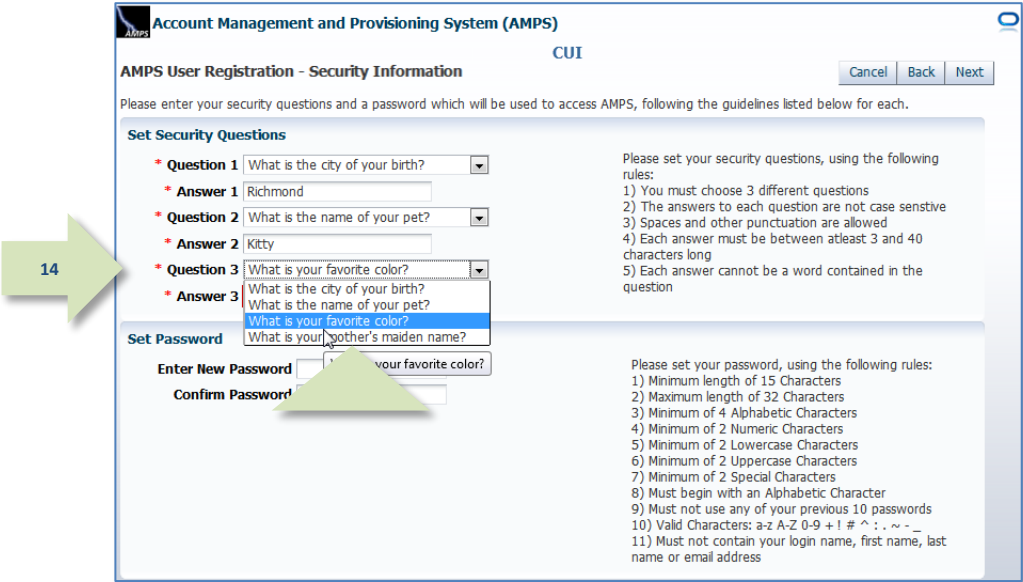
Figure 31: Security Information - Set Security Questions
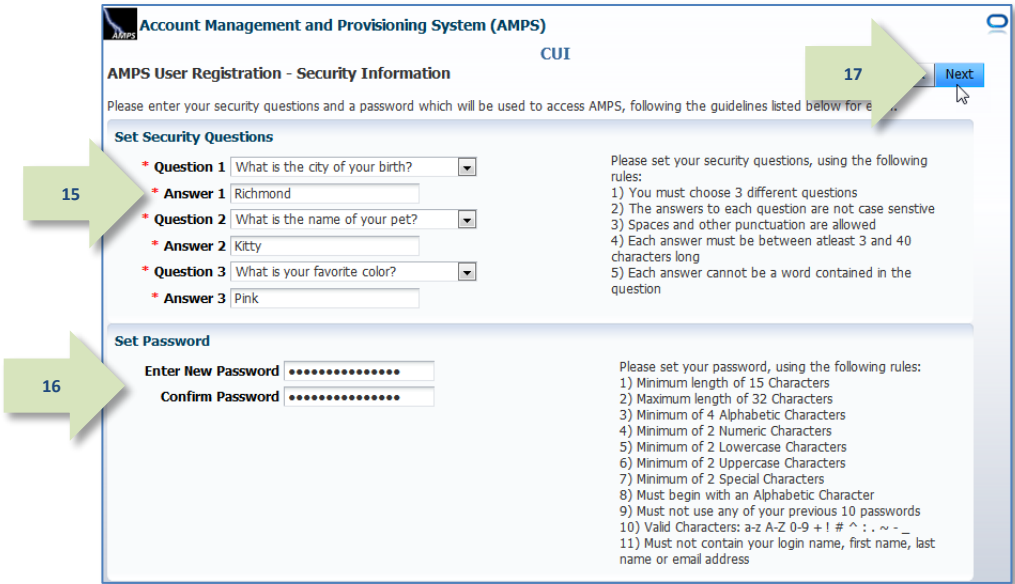
Figure 32: Security Information - Set Password

18. Review entries.

*Click the **Back** button, if necessary, to return to previous screens and make changes or corrections.*

19. Click Create Account.

AMPS performs the following tasks:

- *Starts creating your account and*
- *Displays a **Confirmation** screen containing your new AMPS ID, also called a "login name" (see Figure 34).*

Figure 33: AMPS User Registration - Summary

20. Make a note of your login name, which is also called a "user ID."

    If you lose or forget your user ID, open the external user's login screen (see Figure 35) and click the following link:

    Forgot your User ID? Click Here
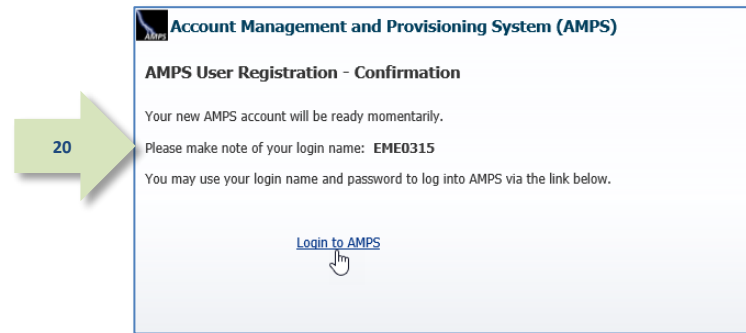
Figure 34: AMPS User Registration Confirmation - User ID

21. To log in to AMPS, enter your AMPS user ID and password.

22. Click **Login**.

    *The system displays the **AMPS Home** page (see Figure 20).*

Figure 35: Single Sign-on Authentication - External User Login Screen

23. After you log in to AMPS, the system displays the main screen open to the **Home** tab. This tab page area is the work area of the screen.

Clicking on the Home tab displays the Home tab screen when you have two or more tabs open. Unlike other tabs, the Home tab cannot be closed.

The User ID is always displayed in the top right area of the AMPS baner, found at the top of the screen.

Click on the User ID to open the User ID dropdown menu or click elsewhere on the screen to collapse the menu (see Figure 36). To reopen the menu, click the User ID again.

The following list outlines the menu options:

Accessibility/Section 508: opens a DoD accessibility Web site.

AMPS Reporting Tool: opens BI Publisher in a separate window. You must have one or more BI Publisher roles to use this application.

AMPS Help: displays the AMPS Help screen, which lists training materials and references that explain AMPS processes and procedures.

Inbox: displays the AMPS Inbox and lists any tasks assigned to your account.

Sign Out: clicking the Sign Out link will close your current session and log you out of AMPS.

The following list outlines the clickable tiles available to all users:

My Information: displays the My Information tab, which enables you to update some items in your profile, such as contact information and Cyber Awareness Training Date.

Role Request: starts the Role Request process, enabling you to submit requests for roles you need to gain access to software applications.
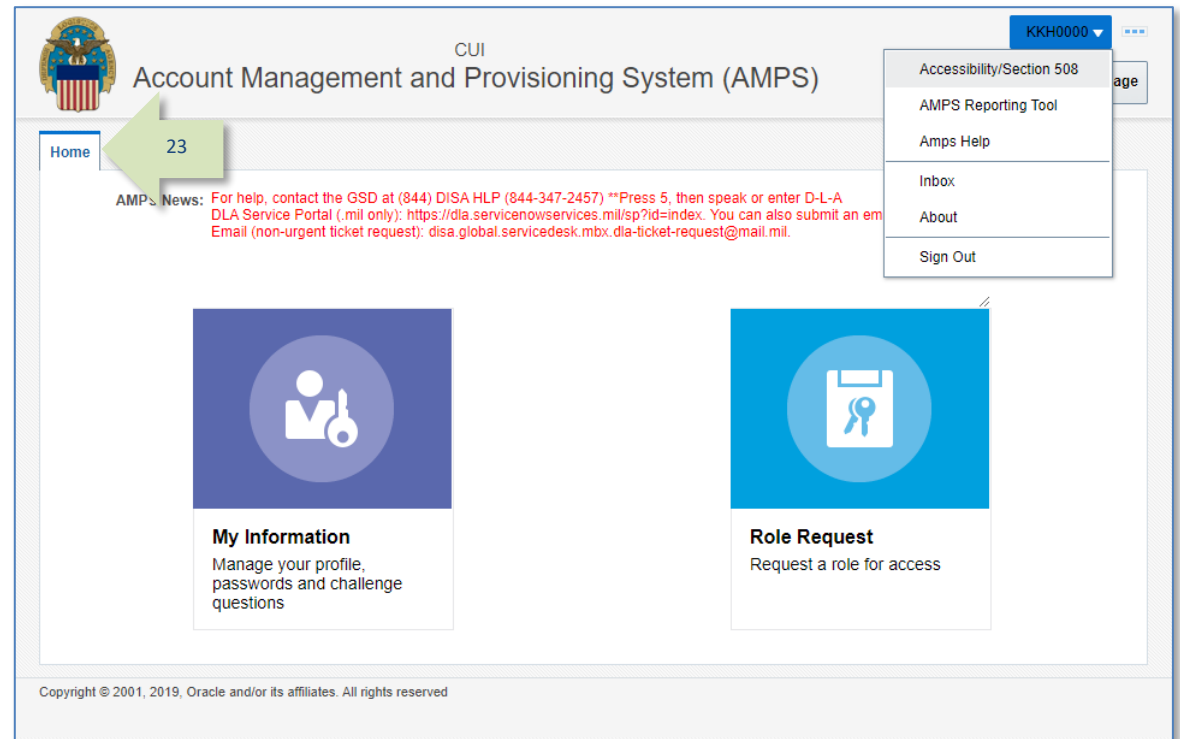
Figure 36: AMPS Self Service Home Page – User ID dropdown menu

How to Retrieve Your User ID: External User Login Option

AMPS generates a user ID for each non-CAC-enabled external user at the end of the registration process.

If you forget your user ID, click the link on the login page to retrieve the ID securely:
Forgot Your User ID? Click Here

AMPS sends an email message with the correct user ID to the address on file.

1. In the Single Sign-on Authentication screen, click this link:
   Forgot your User ID? Click Here

   *AMPS opens the **Retrieve User ID** screen.*
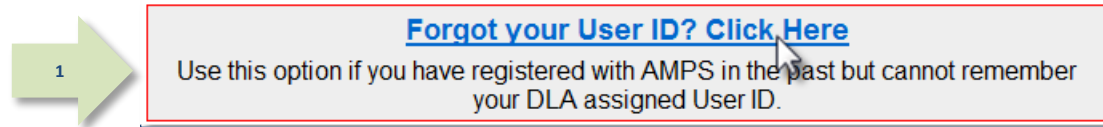
Figure 37: Forgot Your User ID? Click Here

2. Enter the email address stored in AMPS for your account.

   The AMPS email address forms a part of your credentials. AMPS displays an error message if you enter an improperly formatted email address.

3. Click the **Continue** button.

   *AMPS opens the **Send User ID** screen (see Figure 39).*

Figure 38: Retrieve User ID

4. Review the **Send User ID** message and close the browser.

If you have entered the correct email address, AMPS locates your account, finds the correct user ID, and sends the ID to the email address you entered (see Figure 40).
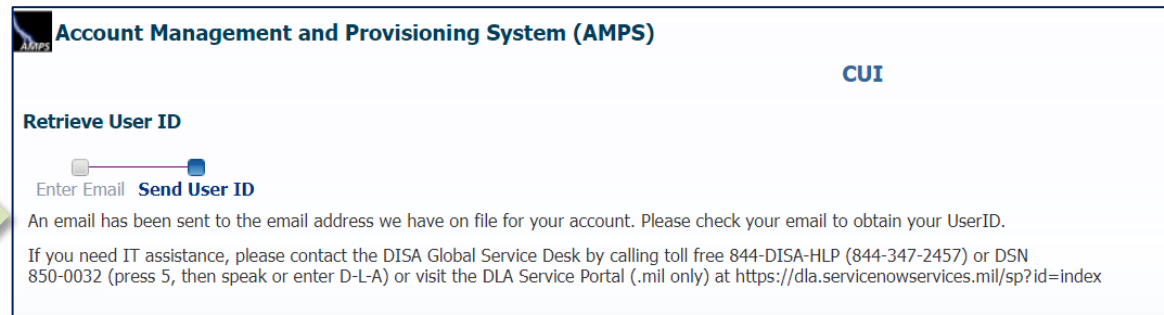
Figure 39: Send User ID

5. Check your email inbox for an AMPS email message. The user ID is included in the message.

You can now reopen the login screen, enter the correct credentials, and log in to AMPS.
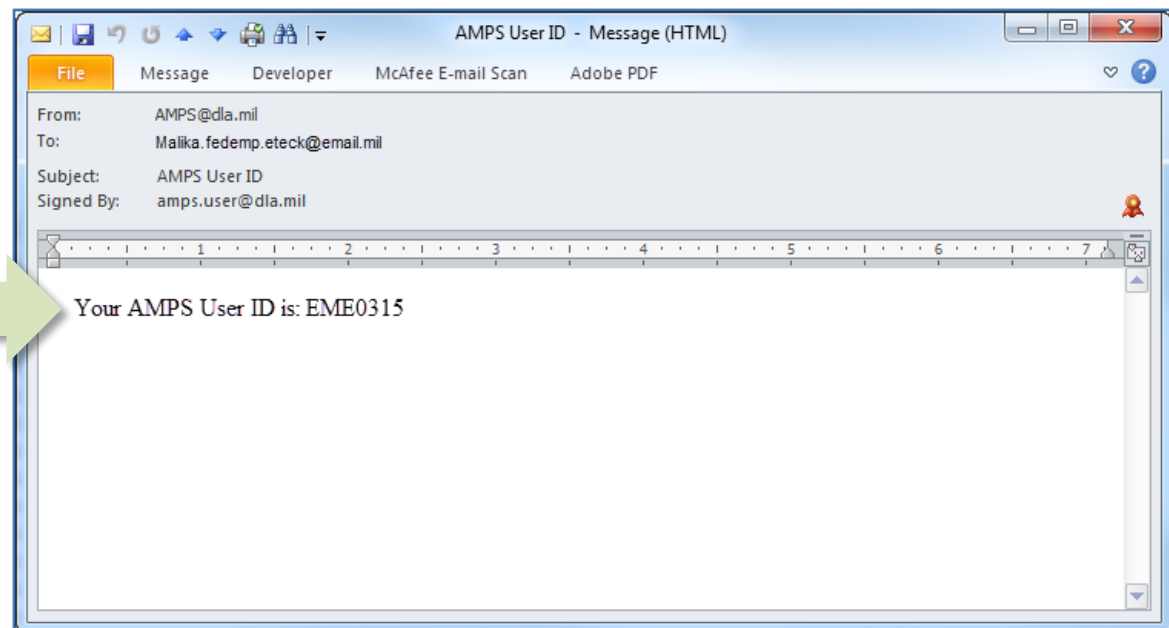
Figure 40: Sample ID Recovery Email Message

How to Reset a Forgotten Password: External User Login Option

During the registration process, each external user sets up an AMPS password. AMPS adheres to a number of password policies and rules to ensure that each user defines a safe, secure password. The user is responsible for memorizing the password, but those who do not use the password feature often may forget this important credential.

If you forget your password, click this link to reset the password securely: **Forgot Your Password? Click Here**. AMPS sends an email message with a link that starts the **Reset Password** process.

You will need the answers to your AMPS Security Questions to proceed. You defined these question-and-answer selections during the registration process.

1. In the login screen, click this link:
   Forgot Your Password? Click Here

   *AMPS opens the **Forgot Password** screen (see Figure 42).*
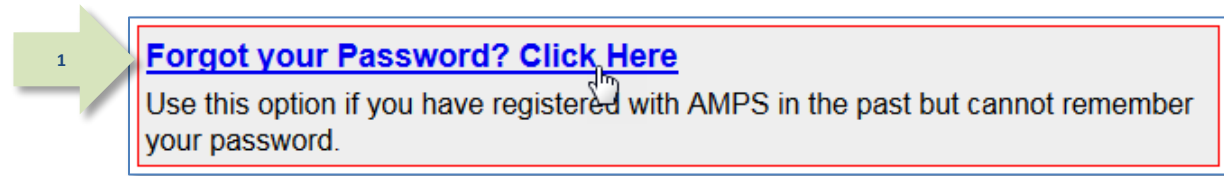
Figure 41: Forgot Your Password? Click Here

2. Enter your AMPS user ID.

   The AMPS User ID forms a part of your credentials. Be sure to enter the correct user ID. AMPS will not generate an error message should you enter an improper user ID.

3. Click the **Go** button.

   *AMPS opens the **Send Email** screen (see Figure 43).*
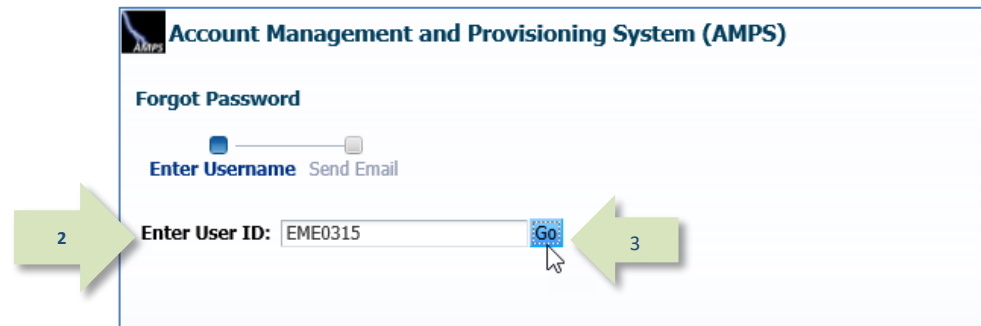
Figure 42: Forgot Password – Enter User ID

4.   Review the **Send Email** message and close the browser.

If you have entered the correct User ID for your AMPS account, AMPS locates the account and sends an email message to the associated address (see Figure 44).

Account Management and Provisioning System (AMPS)

CUI

Forgot Password

Enter Username **Send Email**

An email has been sent to the email address we have on file for your account. Please use the link in the email to reset your password.

If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 43: Forgot Password – Send Email

5.   Check your email Inbox for an AMPS email message. A link that starts the **Reset Password** process is included.

The email Inbox you choose should be that associated with the email address defined for your AMPS account.

You can now follow these steps:

- *Reopen the browser,*
- *Copy and paste the link into your browser's URL address field, and*
- *Start resetting your password.*

Wed 9/6/2017 2:36 PM

AMPS_TEST_OIM@dla.mil

Reset Your Password

To

Signed By   amps.user@dla.mil

You have requested to reset your password. Please click the link, or copy the the URL below into your browser to reset your password.

https://ampst.use2.ad.dla.mil//SelfService/faces/adf.task-flow?adf.tfId=reset-password-token&adf.tfDoc=/WEB-INF/reset-password-

This link will expire on 09/07/2017 02:36 PM EDT

Figure 44: Sample ID Recovery Email Message

6. Enter the correct answer for each security question you set up during the registration process.

   Note that answers to all three questions are required.

7. Click the **Next** button.

   *AMPS displays a **Reset Password** screen (see Figure 46).*

Figure 45: Answer Security Questions

8. Using the current AMPS password policies and rules listed, define a new password and type it into the **Enter New Password** field.

   *Refer to **Appendix C: Password Rules** in this User Guide for a complete list of AMPS password policies and rules.*

   *Refer to the **AMPS Snapshot** called **Password Policies and Security Questions** for a thorough reference to defining security questions and answers, and resetting AMPS passwords that are compliant with AMPS policy. AMPS Snapshots are available on the AMPS Documentation screen.*

9. Retype the same password in the **Confirm Password** field.

10. Click the **Reset Password** button.

    AMPS displays a message confirming the password has been reset.

    If your new password is compliant with the rules, AMPS resets your password and stores it with your account.

Figure 46: Define a New Password

11. If you enter a password with one or more incorrect characters, AMPS displays an error message and identifies the invalid characters.

Type in a correctly configured password and click the **Reset Password** button again.

AMPS displays a confirmation message indicating the password has been reset (see Figure 48).

Figure 47: Password Reset - Error Message

12. Review the instructions in the confirmation message, then close the screen and log in to AMPS with the new password.

Figure 48: Password Reset Confirmation

13. For security purposes, AMPS sends you an email notification indicating that your password has been reset.

If you did not reset your password but receive a password-reset notification, notify the Service Desk immediately (see page 9).
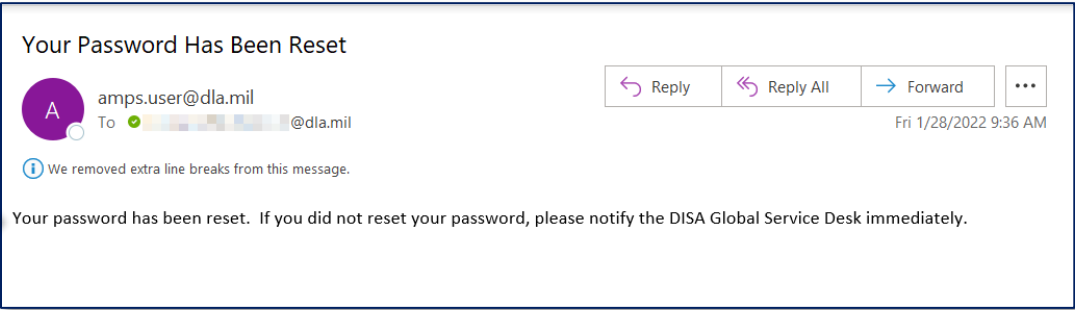

Figure 49: Password Reset Email Notification

AMPS Screen: Quick Tour

A. **User ID:** clicking your User ID opens a drop-down menu with links to many common AMPS tasks (see Figure 51).

B. **Tabbed screens** provide parallel access to multiple task types.

*For example, you can open your **My Information** screen, update attributes in your profile, and then start the role request process without having to close the **My Information** tab first.*

C. **Navigation buttons** provide the method for proceeding forward and backward through a series of task screens on a tab.

D. **Close button** closes any tab without completing the task on that screen. You can also close multiple tabs.

E. **Required fields** are fields that require you to enter information before you proceed and are marked with an asterisk (*).

F. **"Train" screen navigation tool:** some tasks, such as **Role Request**, furnish a connected series of screen names; this series is informally called a "train." If you are familiar with the Web page "breadcrumb trail" as a navigation tool in Web sites, you will find that the AMPS "train" works in a similar way. As you proceed through the series of screens in a task process, AMPS turns each screen name in the train into a link you can click to reopen the corresponding screen. If you need to display a previously viewed screen, click any active screen name in the train to jump backward or forward.

Using the train links as a screen navigation tool, you can skip multiple screens in the sequence.

*For example, when you reach the **Summary** screen in **Role Request**, you can jump back to **User Information** without having to navigate backward through every screen in sequence.*

The "train" is a timesaving way to help you view and change any screen before you complete a process such as requesting a role.

G. **Sign Out** command: **Sign Out** provides a method for exiting AMPS. The User ID displayed shows the identity of the currently logged in user.

> **Note:** AMPS displays a confirmation screen when you log out, you can close the browser or click the link to log back in.

Figure 50: Sample Screen with Tabs

Figure 51: User ID Dropdown Menu

AMPS Inbox

The change from **Pending Approvals** to the **Inbox** as a repository for storing pending tasks was introduced in AMPS version 16.2.0.

Who Uses the Inbox Feature?

All users have access to an **Inbox** that contains any SAARs assigned to them for action.

If you use AMPS to view and open SAARs assigned to your account for action, you should read this guide and become familiar with these procedures. This guide is prepared mainly for the following user groups:

- All users who have been assigned a SAAR for a new user confirmation, a role expiration request, or a role extension request.

- All approvers who need to locate and open online SAAR approval forms that have been assigned to them for action.

- Provisioners who have the task of provisioning or deprovisioning roles and closing each Total AMPS ticket after role provisioning is completed.

Items not covered in this guide are actions that a system administrator can perform. For more information on these actions, please call the Service Desk (see page 9).

Why Was Inbox Added to AMPS?

AMPS is built on the framework provided in a Commercial Off-the-Shelf (COTS) application called **Oracle Identity Manager** (OIM). Oracle provides a range of features, most of which AMPS employs in its own implementation. OIM does not contain many DLA-specific features, such as a built-in workflow for the approval process with decision screens that accommodate the business processes adopted by the Defense Logistics Agency (DLA) and the Defense Finance and Accounting Service (DFAS). To customize the OIM COTS application for AMPS, the DLA sponsors a sustainment team whose members add programming changes to OIM to meet the requirements provided by customers for reviewing and approving requests, among many other requirements. Other custom software supports key features, such as the role request processes. The sustainment team must integrate custom features and functions with the OIM framework, even though many OIM features are not used.

When OIM updates its framework, AMPS must adapt to changes in the software. The update, implemented on 31 October 2016, called Patch Set 2 (PS2), formed part of the 16.2.0 release. The PS2 update provided a set of changes in the AMPS user interface. These changes streamlined and expanded the features supporting the **My Tasks** list and the AMPS approval screens. One of the most comprehensive changes was the new **Inbox** feature.

How Do I Learn to Use the Inbox?

The **AMPS User Guide** provides you with basic instructions in how to use the **Inbox** and **My Tasks** view features. This section of the **User Guide** gives you a quick start so that learning new features does not interfere with your AMPS work. You can also consult the **AMPS Inbox Guide**, which is available for download on the AMPS Help>Documentation Library screen.

You should be able to read through this section or the **AMPS Inbox Guide** to prepare yourself for navigating the AMPS user interface. The assistance provided in this section gives you an overview of basic knowledge and instructions. Detailed instructions for opening specific SAAR types are provided in the applicable procedural sections, such as "Role Request Approval Process," "Provisioning Process: Total AMPS," and "Role Expiration and Extension."

What is the My Tasks View?

The **My Tasks** view is the table of SAAR tasks that are assigned to you. The **My Tasks** view is available to all users through the AMPS **Inbox**. This is the default view.

On this screen, AMPS lists the SAAR or SAARs that require action from you as a user or an approver. You also have the option to view completed SAARs by changing the **My Tasks State** search criterion from "Assigned" to "Completed." Refer to subsections in this area of the guide to understand where to find search criteria and how to change them.

While displaying the **My Tasks** view is the primary function of the Inbox, it can also display certain predefined views that you can use. You also have the capability to modify the default list of tasks to display the data you want to see in a view.

The next section explains the concept and use of **Views**.

What is a View?

A "view" in the **Inbox** is the display of a list of SAARs in AMPS. The view is set up according to a predefined set of criteria that governs which data are displayed related to a SAAR.

For example, if you want to find a specific SAAR by number, look in the **Title** column of the **My Tasks** list. The display of the **Title** column is part of the current view's defined display criteria. A view is a named set of these criteria. In AMPS 16.2.0 or later, you can find a specific view name in the **Views** menu to filter SAARs, or modify your **My Tasks** view to get better control over the display of SAARs.

Previous versions of AMPS included only one preset collection of data represented by the column headings in the **My Tasks** list. See the following sections for more information.

AMPS Inbox: Quick Tour

The following list provides you with a quick map of features available through the **Inbox** feature. The subsections that follow explain these features in more detail.

1. **Inbox command:** this command is always available from the User ID dropdown menu. Click the User ID, then click this command to display the **Inbox** and view your tasks (see Figure 51).

2. **Views panel:** this panel identifies the list of views available to the user.

3. **Task column headers:** these headers identify the type of data specified for each SAAR. Different views can have different column headers.

4. **Refresh button:** click this button to refresh the task list in the current view.

   When you complete a task—such as an extension request or SAAR approval—and close the task screen, AMPS does not automatically refresh the inbox screen. Click the refresh button to see the latest task list.

5. **Current View:** the currently selected view is indicated by a vertical bar to the left of the view name. The My Tasks view is selected in the example.

6. **Search field:** search criteria are entered here. To search for a specific SAAR or range of SAARs, enter a SAAR number or partial number in this field and click the search button (🔍).

7. **User category:** by default, this item is set as **Me & My Group**. System administrators, such as Service Desk agents, can make selections to view SAARs assigned to other users.

8. **Status:** identifies the status of each SAAR in the current list. In the example, all SAARs listed are Assigned (Status) to the currently logged in user (Me & My Group).
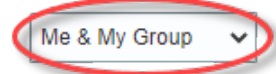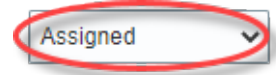

Figure 52: Map of Inbox Functions on the AMPS Screen

How to Work with Inbox Functions

Inbox functions are available through unlabeled icons and fields on the **Inbox** menu bar. These functions enable you to perform tasks to list specific SAARs and change the current **Inbox** task list. For example, if you want to search for a specific SAAR, you can enter the SAAR number in the **Search** field and click the **Search** icon. AMPS clears the full list of SAARs and displays a record for the matching SAARs in the **My Tasks** list.

The **Inbox** functions provide various ways to filter the **Inbox** list temporarily in order to locate a specific SAAR or set of SAARs that require your action. You can also edit the default **My Tasks** list to display more data or different data in the list of SAARs.

To perform this task . . .	Follow these steps . . .	For this result . . .	See these sample icons and fields . . .
Identify the current view. *Example:* *I want to know which view is currently defining what I see in the* **Inbox***.*	➢ **Locate the Views panel. Look for the vertical bar next to a view name.**	Read the name of the view you have activated.	This sample field contains the view named "My Tasks." The numeral in parentheses indicates how many tasks are displayed in the current view.
Edit the Inbox display settings. *Example:* *I want to add a column to the My Tasks view.*	➢ **Select the My Tasks view. AMPS automatically opens this view when you click the Inbox command to display tasks.** ➢ **Click the *Edit* icon.**	Open the Edit Inbox Settings dialog.	
Search for a specific SAAR by number or other search criterion, using a free-text search. *Example:* *I want to find a SAAR assigned to me that is labeled with the number 102162.*	➢ **Enter a search criterion in the *Search* field.** ➢ **Click the *Search* icon.**	Filter the *My Tasks* list to show only the SAAR or SAARs that match the search criterion. You can enter a partial SAAR number to display a range of SAARs, but the partial number must be the first one to five numbers of the SAARs you want to list, and the numbers must be in order.	
Change the *Assignee* designation. *Example:* *I need to see all the SAARs assigned only to "Me."*	➢ **Click the drop-down box.** ➢ **Choose a different assignee.**	Filter the SAARs to list only those assigned to the designated user and/or group. Lists of SAARs assigned to multiple assignees are limited to administrators.	
Change the State search criterion. *Example:* *I want to see all SAARs of a specific* **State***, such as Assigned or Completed.*	➢ **Click the *State* drop-down box.** ➢ **Select a *State* assigned to the SAARs you want to review.**	Display all matching SAARs assigned to the currently logged in user, if the Assignee is either Me or Me & My Group. Lists of SAARs assigned to multiple assignees are limited to administrators.	
Display a bar graph showing SAAR counts. *Example:* *I want a visual comparison of assigned SAARs in all available Status types.*	➢ **Click the bar graph icon.**	Display a bar graph for a pictorial comparison of SAAR counts in different statuses. You can edit the displayed data by status.	
Refresh the list of tasks after completing a task. *Example:* *I have just completed a SAAR action and want to refresh the current list of SAARs so that it reflects the result.*	➢ **Click the *Refresh* icon.**	Fetch and display an updated list of SAARs, assigned to the current user from the database.	

Views Panel

1. **Inbox:** this heading identifies the out-of-the box default view.

2. **Views:** this heading identifies the list of alternate views available in this panel.

3. **Pin icon:** clicking this icon closes the Views panel to allow more space in the main task area. After you close the panel, a small window appears on the far left of the column header row, which displays the name of the current view; clicking the window opens a dropdown menu of the views. Another pin icon appears in the dropdown menu; clicking that pin reopens the Views panel.

4. **Refresh button** (not shown)**:** click this button to refresh the list of views after creating a new view. Creating new views is limited to system administrators.

   If you want to request a different view after trying the available views, please contact the Service Desk (see page 9).

5. **Collapse Pane:** clicking this icon collapses the Views Panel to the left. The Restore Pane icon appears next to the left of the header column row when you collapse the Views Panel.

In the **Views** list, AMPS includes a set of predefined, nonmodifiable views. These views enable you to display a subset of SAARs according to either priority, date, or role:

a. **My Tasks:** The default list contains all tasks that match the current **Status** criterion. The numeral in parentheses indicates the current number of tasks in the list.

b. **Due Soon:** SAARs assigned and due for approval within the next two days.

c. **High Priority:** Tasks assigned a priority of 1 or 2 by the user.

d. **MANUAL_PROVISIONING_VIEW:** Total AMPS provisioning tasks assigned to the current user.

e. **Past Day:** SAARs updated within the past day.

f. **Past Week:** SAARs updated within the previous seven days.

g. **Past Month:** SAARs updated within the previous 30 days.

h. **Past Quarter:** SAARS updated within the previous 90 days.

i. **New Tasks:** SAARs assigned that were created within one day of the current date.

j. **PENDING_APPROVALS_VIEW:** SAARs assigned to the current user. This view shows more extensive data than the **My Tasks** view. After you select and open a view, AMPS displays the number of tasks included in that view. In the example shown, both the My Tasks view and the Pending Approvals view have been opened; the My Tasks view and the Pending Approvals view indicate zero tasks for both.

Note:

The views listed in the Views panel are subject to change without notice.

If you have questions about a view or need help with a custom view, contact the Service Desk (see page 9).

Contrasting Views

Views differ in the types of data they display, as well as in the various time period filters they apply to the SAARs displayed. The My Tasks view is the default, but you can switch to the Pending Approvals view whenever you need to see more data about SAARs in your task list.

My Tasks View

The **My Tasks** view displays the following data:

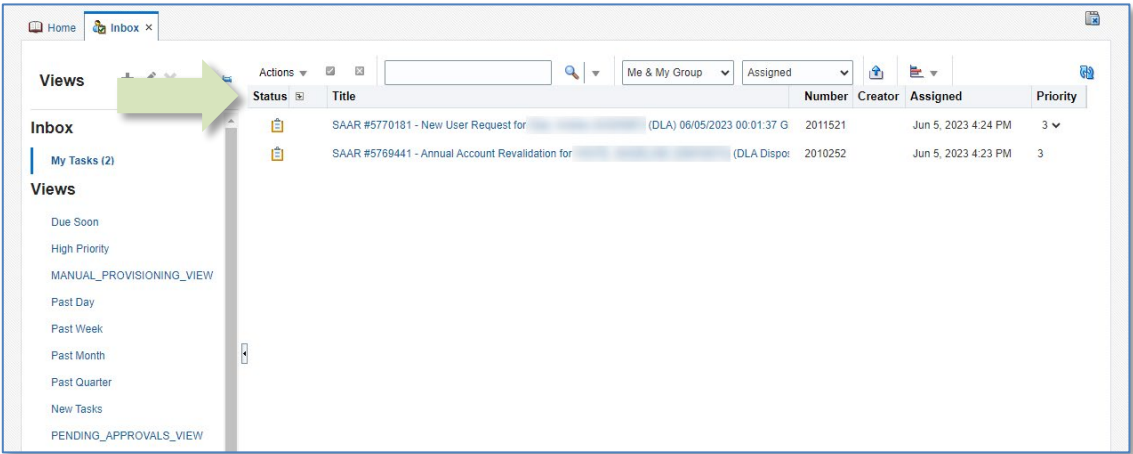**Title:** SAAR number, the request type, the user's name, ID, and organization, and the date and time the SAAR was created.

Number: Transaction number generated by OIM. (Not used by AMPS.)

Creator: Name of the user who created the transaction. (Not used by AMPS.)

Assigned: Date and time the SAAR was assigned to the logged-in user.

Priority: Default priority setting of **3**.

This list displays the most recent SAAR first in the list.

Pending Approvals View

The **Pending Approvals** view displays the following data for each SAAR:

Title: SAAR number, the request type, the user's name, ID, and organization, and the date and time the SAAR was created.

Assignees: The name of the approver to whom the SAAR is assigned.

Assigned: Date the SAAR was assigned to the approver.

Created: Date the SAAR was created.

Expires: Date the SAAR expires due to inaction by an approver.

Priority: Default priority setting of **3**.

State: Current state of the SAAR.

Outcome: Most recent state of the SAAR.

This list displays the most recent SAAR last in the list.
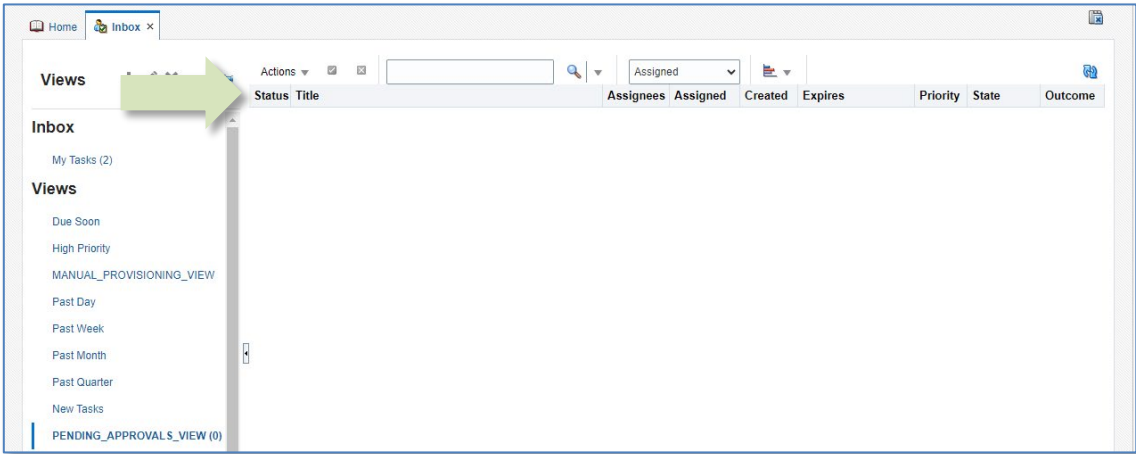
How to Work with Standard Views

The list of views presented in the **Views** section of the Inbox is a list of standard views installed with OIM and are not modifiable by a user.

However, if you want a quick view of a task lists organized and filtered through preset criteria, you can choose these standard views. Refer to the table under *Standard Views: Summary of Users and Criteria* for directions on which view to select.

Each of these views displays data in the following columns:

Column	Description
Title	SAAR number, request type, name of request user, ID of user, user's Organization, SAAR creation date and time. **Serves as a link to opening the SAAR**.
Assignees	Name of the approver responsible for a current action on the SAAR.
Assigned	Date the SAAR was given to the Assignee.
Created	Date the SAAR was created originally.
Expires	Date the SAAR expires due to inaction from the current Assignee.
Priority	Level of urgency. The default Priority assignment is **3**.
State	Condition of the task. The State is assigned by the system based on approver actions.
Outcome	The final **State** assigned to the task.

Standard Views: Summary of Uses and Criteria

Click this view name…	If you want to see…	Assignee	Criteria	Sort Criteria
Due soon	A list of SAARs due for approval within the next two days.	Me & My Group	SAAR expires in next two days. State: Assigned	Sort: **Expires** date in ascending order.
High Priority	A list of SAARs that you have assigned a priority of 1 or 2.	Me & My Group	Priority "Highest" (1) Priority "High" (2)	Sort: **Expires** date in ascending order.
Past Day	SAARs assigned to you and updated in the past day.	Me & My Group	Updated Date in the last **1** day.	Sort: Created date in ascending order.
Past Week	SAARs assigned to you and updated in the past 7 days.	Me & My Group	Updated Date in the last **7** days.	Sort: Created date in ascending order.
Past Month	SAARs assigned to you and updated in the past 30 days.	Me & My Group	Updated Date in the last **30** days.	Sort: Created date in ascending order.
Past Quarter	SAARs assigned to you and updated in the past three months.	Me & My Group	Updated in the last **90** days.	Sort: Created date in ascending order.
Manual Provisioning	Provisioning tasks assigned to the currently logged-in user, if the user is a provisioner.	Me & My Group	Task Type: AMPS Ticket State: Assigned	Sort: Created date in ascending order.
My Staff Tasks	SAARs assigned to approvers who are the Direct Reports of one or more users who report to the logged-in user.	(direct reports)	Open SAARs State: Assigned	
New Tasks	All SAARs assigned to you and created during the previous one-day period.	Me & My Group	Last **n** days – 1 State: Assigned	Sort: Created date in ascending order.
Pending Approvals	All SAARs assigned to you.	Me & My Group	State: Assigned	Sort: Created date in ascending order.

Sample View: High Priority

AMPS has a Priority criterion that is automatically assigned to every SAAR created. The default value is **3**, which is a medium priority. You can assign a 2 or 1 as high priority settings to the SAARs assigned to you and then view the resulting list using the **High Priority** view. Follow the steps in this procedure to change the priority of a SAAR and then view the High Priority SAARs in a separately chosen view.

Note:

If your active view is a group view that displays tasks assigned to a group of approvers, changing an approval task's priority will assign that task to you and keep other approvers from taking action on the task. Use with caution.

Set a Goal, Set the Criteria, and Display the Results

1. Set a goal: I need to assign Priority numbers to the SAARs in the My Tasks list and view the high priority items only.

   The default view shows all SAARs assigned to the current user have the default setting of 3. This user wants to change the priority numbers to the following settings:

   - *Highest priority for SAARs assigned for user DCS9808.*

   - *High priority for SAARs assigned for user DDT0020.*

   - *Low priority to a SAAR assigned for user DBD0014.*

   - *Lowest priority to a SAAR assigned for user DBD0014.*
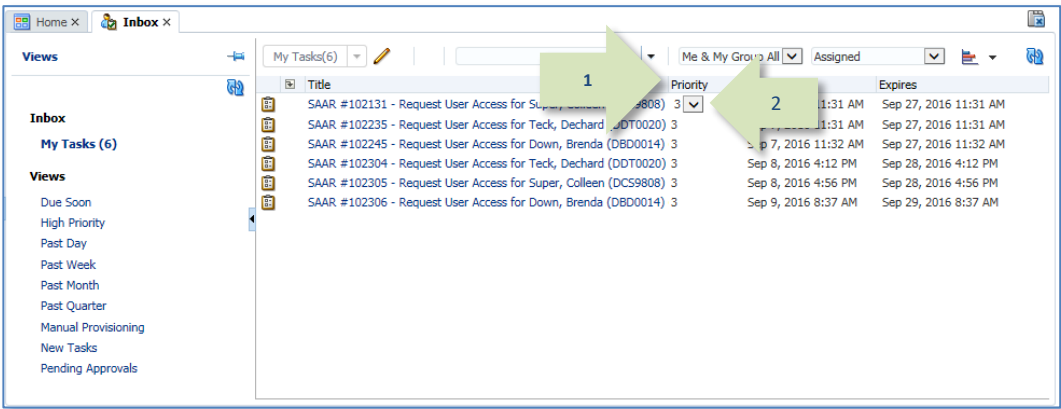
Figure 53: My Tasks – Custom View with Priority

2. Click the **Priority** drop-down arrow (see Figure 53).

   *AMPS displays the menu of **Priority** numbers 1 through 5 in the drop-down box.*

3. Use the mouse cursor to click a **Priority** number on the list.

   AMPS displays a drop-down list of numerals from 1 to 5, each representing a priority level.

   The numerals 1 and 2 represent the "highest" and "high" priorities respectively, and the numeral 5 represents the lowest priority.

   In this example, the user has identified her top priorities as the SAARs that await approval for a supervisor who reports to her.
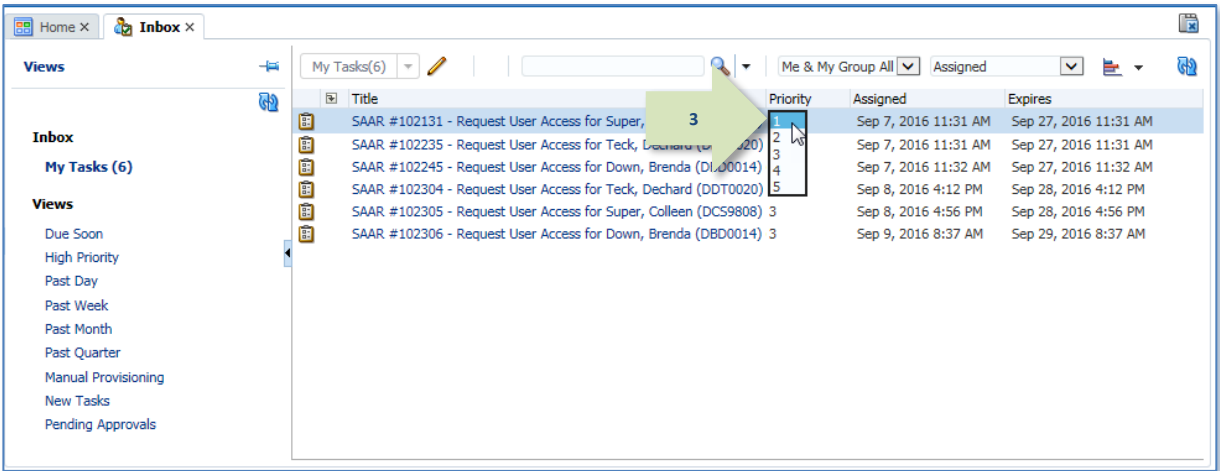
Figure 54: My Tasks - Priority Drop-down List

4. Repeat Step 3 as needed to change the **Priority** number for other SAARs.
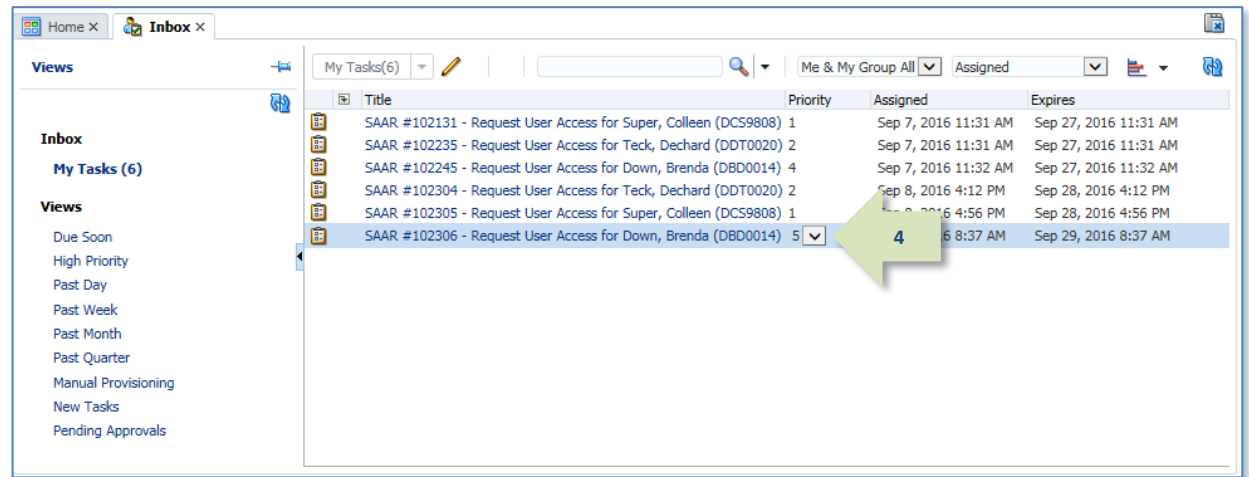
Figure 55: My Tasks - Priority List Changes Completed.

5. Click the **High Priority** View link.

*The **High Priority** view is listed in the standard **Views** menu.*

*AMPS filters the current **My Tasks** list and applies the priority criteria established in the **High Priority** view.*

AMPS also expands the number of columns to match those columns defined for this view.

See the resulting list in Figure 57.
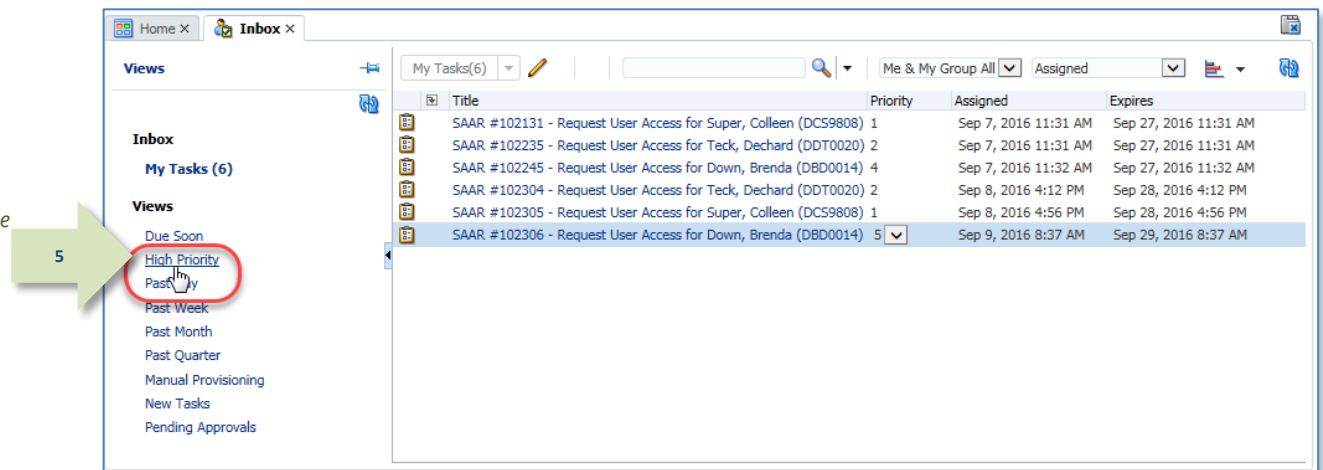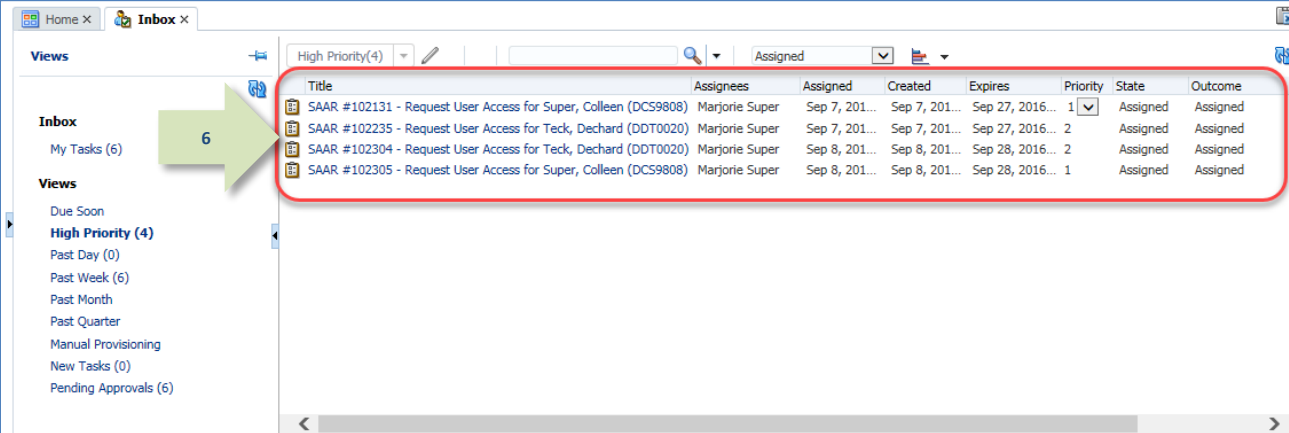
Figure 56: Select the High Priority View

6. Review the list of **High Priority** SAARs.

The resulting list displayed from selecting a different view also displays the columnar data defined for the selected view.

Note:

To return to the default view, click My Tasks under the Inbox heading on the left.

Figure 57: High Priority View
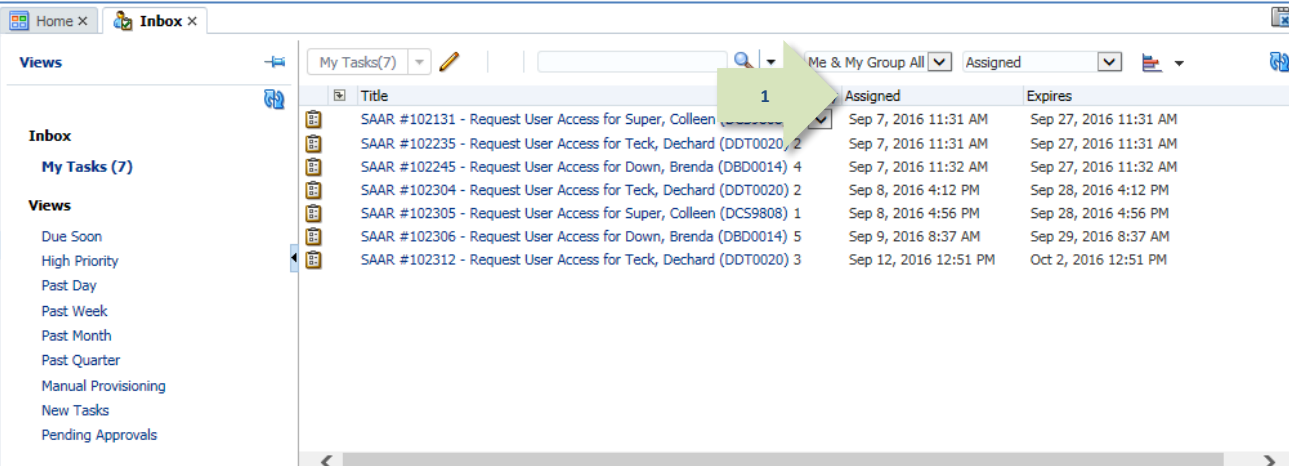
Sample *New Tasks* View: Set a Goal and Display the Results

The New Tasks view displays all SAARs assigned to the current user and created within the previous day.

1. **Set a goal:** I want to view all the tasks assigned to me that were created in the previous one-day period.

    My Tasks, *the default view, shows all the SAARs assigned to the current user.*

    In contrast, the **New Tasks** view shows the user only the most recently created SAARs assigned to the current user.

Figure 58: Inbox - My Tasks List - All SAARs Assigned to the Current User

2. Click **New Tasks** in the **Views** menu.

This action applies a filter to the **New Tasks** *list, in which SAARs created before the previous one-day period will not be displayed (see Figure 60).*
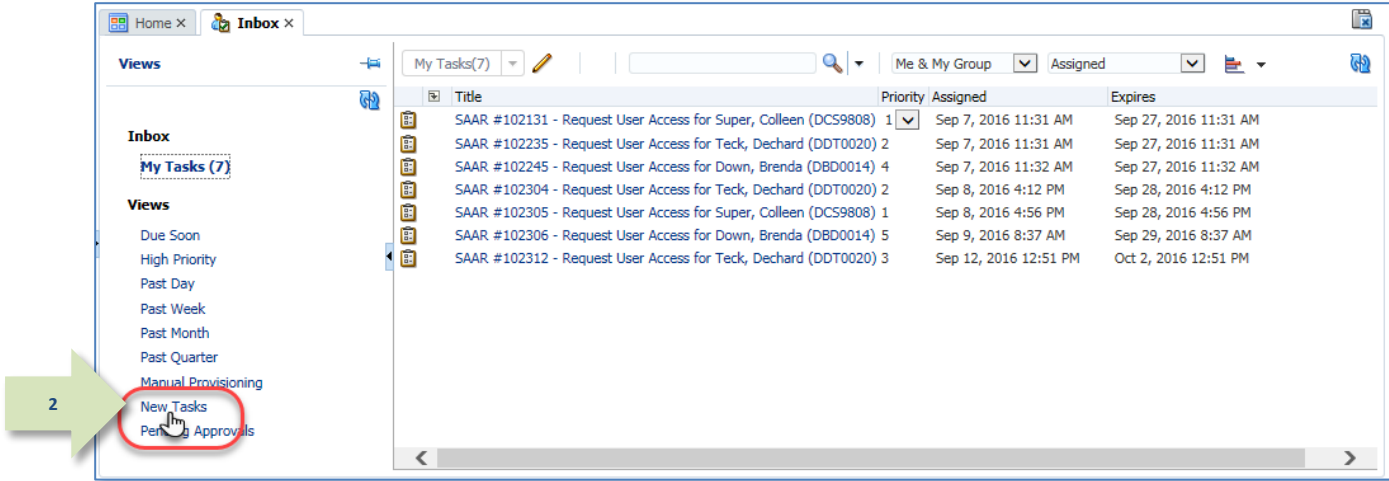
Figure 59: Inbox - Views Menu - New Tasks

3. Review the list of SAARs created during the previous one-day period.

The **New Tasks** *list displays tasks created during the previous one-day period.*

In this example, the **New Tasks** *view was applied on September 12, 2016, and captured one task created that day. All other tasks exceed the defined time period of one day.*
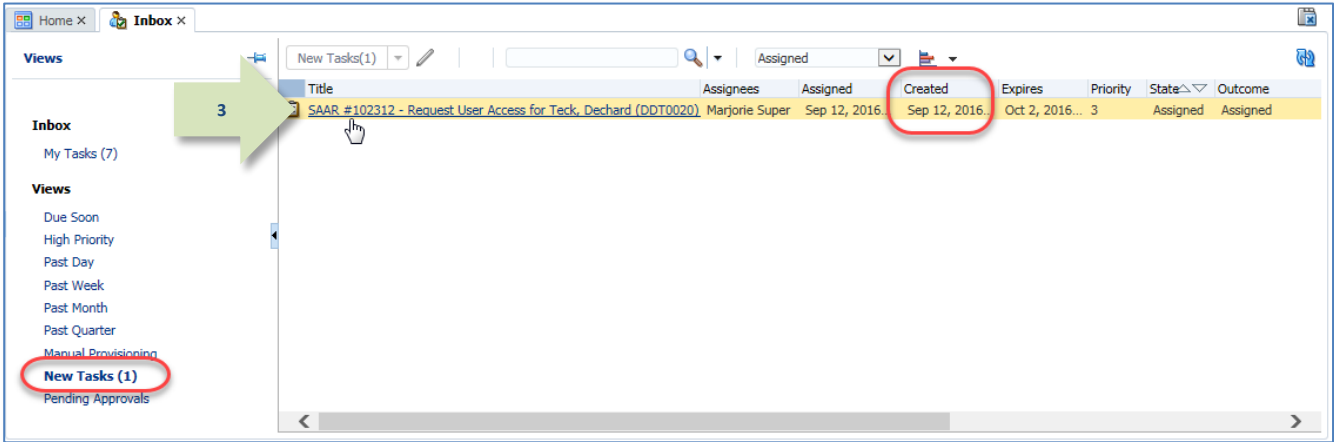
Figure 60: Inbox - New Tasks List

How to Edit the Inbox *My Tasks* View

The **My Tasks** view is the default view for the **Inbox**. The **Inbox** settings for this view display columns for **Title, Number, Creator, Assigned**, and **Priority** fields. However, you can edit this view with modifications to suit your preferences for a general view that fits your needs.

Process for Customizing the Inbox *My Tasks* View

Start customizing the **Inbox**'s default **My Tasks** view by following these steps:

1. **Determine what your goal is:** in this example, the Supervisor knows that the default Assignee is herself. She wants to know ONLY the information in the SAAR Title, the SAAR Assignment date, and the SAAR expiration date.

2. Next, launch AMPS.

3. Display the **Inbox**. The default view is the **My Tasks** view.

Set a Goal and Customize the Inbox

1. Set a goal for the view you want to create:

   For example: I want the default *My Tasks* view to show me the following information:

   - All SAARs currently assigned to me.
   - The **Title** data for each SAAR.
   - The date each SAAR was assigned to me.
   - The date each SAAR expires.
   - Sort the tasks so that the tasks that expire first are displayed at the top of the list.

   The default view shows all SAARs assigned to the current user and her group. "Group" means anyone holding the same role as the user.

2. In the **Inbox** menu bar, click the **Edit** icon (✏).

   AMPS displays the **Edit Inbox Settings** *dialog (see Figure 63).*
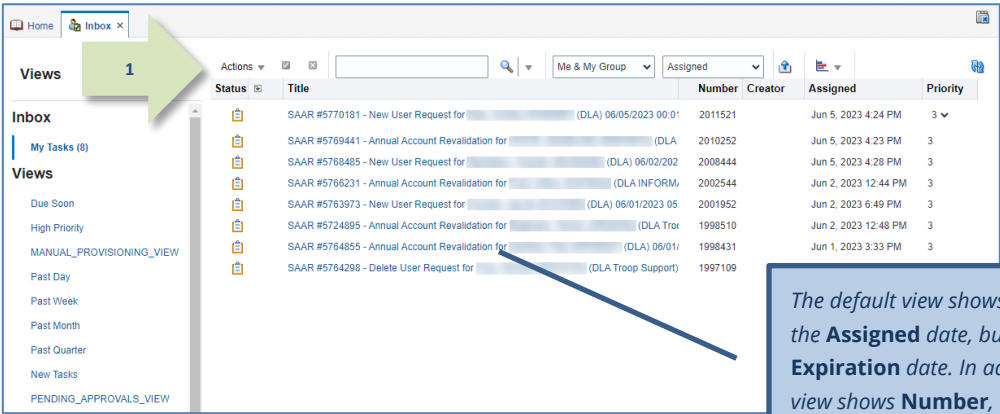
Figure 61: Inbox and My Tasks View

The default view shows the **Title** *and the* **Assigned** *date, but not the* **Expiration** *date. In addition, this view shows* **Number**, **Creator**, *and* **Priority.**

Number and Creator *are not used by AMPS. The* **Priority** *setting is* **3** *by default but can be changed in the task list if the user wants to sort by priority. See the subsection in this Guide entitled "Sample View: High Priority" for instructions.*
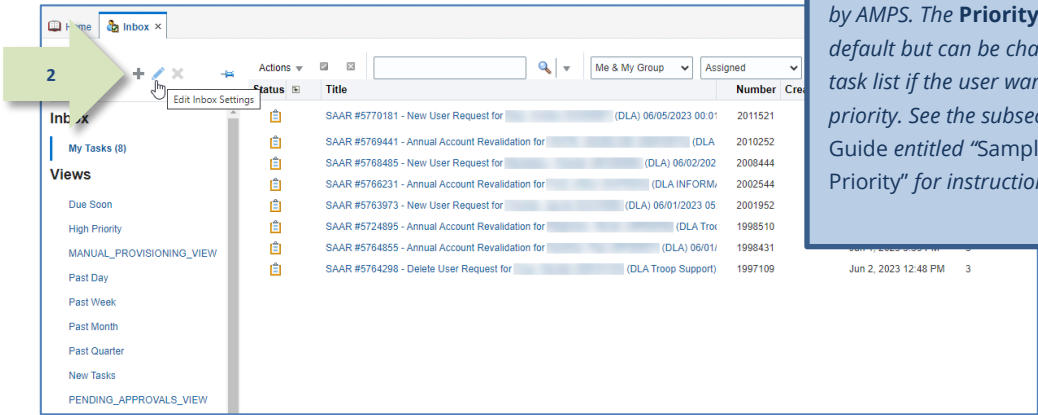
Figure 62: Inbox Menu Bar – Edit Inbox Settings Icon

3. The **Edit Inbox Settings** dialog contains several options for changing the display of the currently selected view.

    For this example, you will use the following options:

    a. **Show Columns**

    b. **Sort** *options*

    c. **Sort Order**

4. You can change the number of SAARs displayed at one time by increasing or decreasing the **Number of tasks per fetch**.

    *A "fetch" represents the act of pulling a set number of SAARs from the database. In this case. The higher the number of SAARs, the longer AMPS must take to display the records. You can reduce the number of records by reducing the **Number of tasks per fetch**.*

    *Otherwise, with the default setting of **20**, AMPS displays 20 tasks. As you scroll down the list, AMPS fetches another 20 until all tasks that match the view criteria are displayed.*
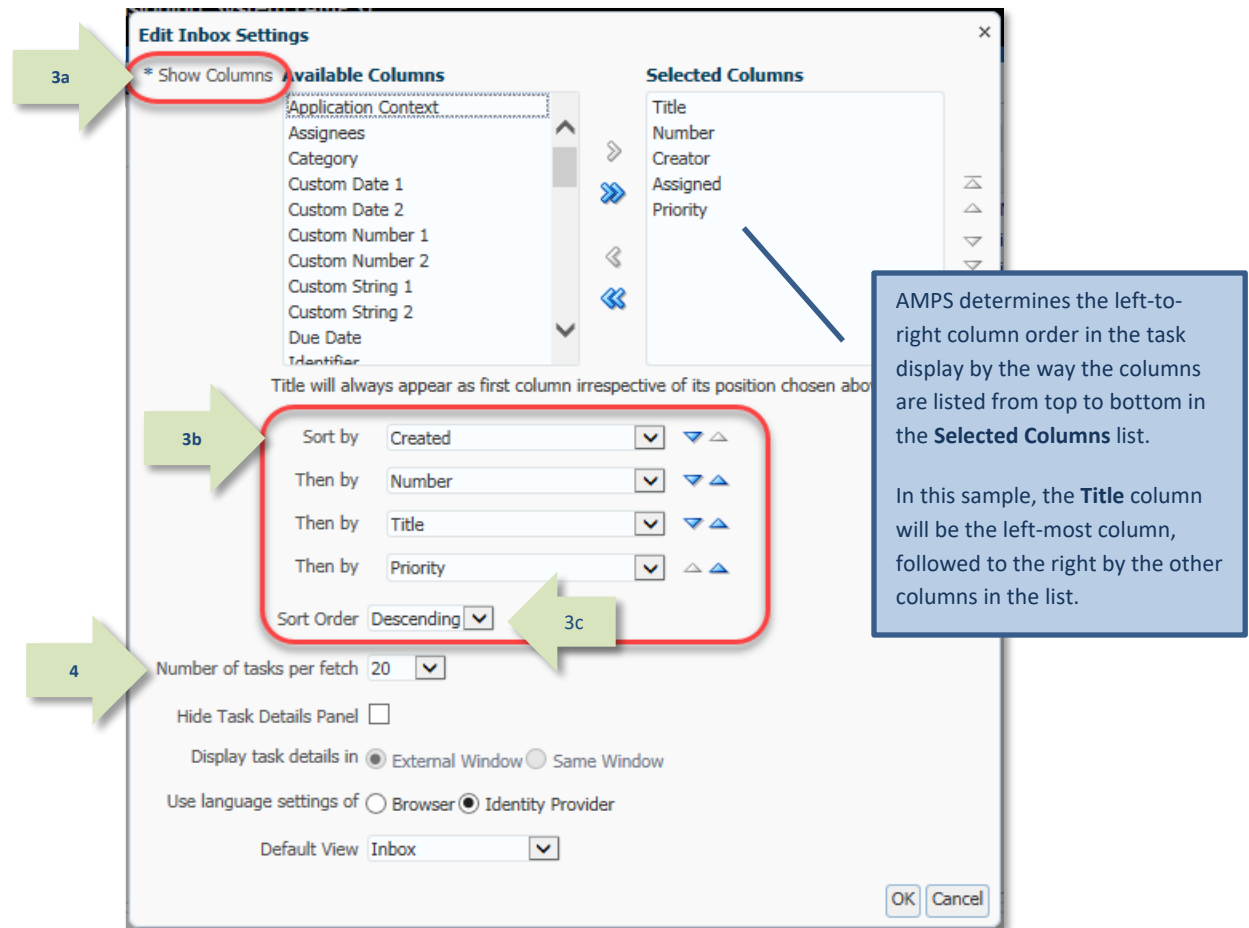
Figure 63: Edit Inbox Settings

5. Starting at the **Selected Columns** text list, select the column you want to remove by clicking the column name.

6. Click the remove icon (◀) to move the column name to the **Available Columns** list.

    Repeat Steps 5 and 6 to remove one column at a time.

    These actions remove the selected column from the view.
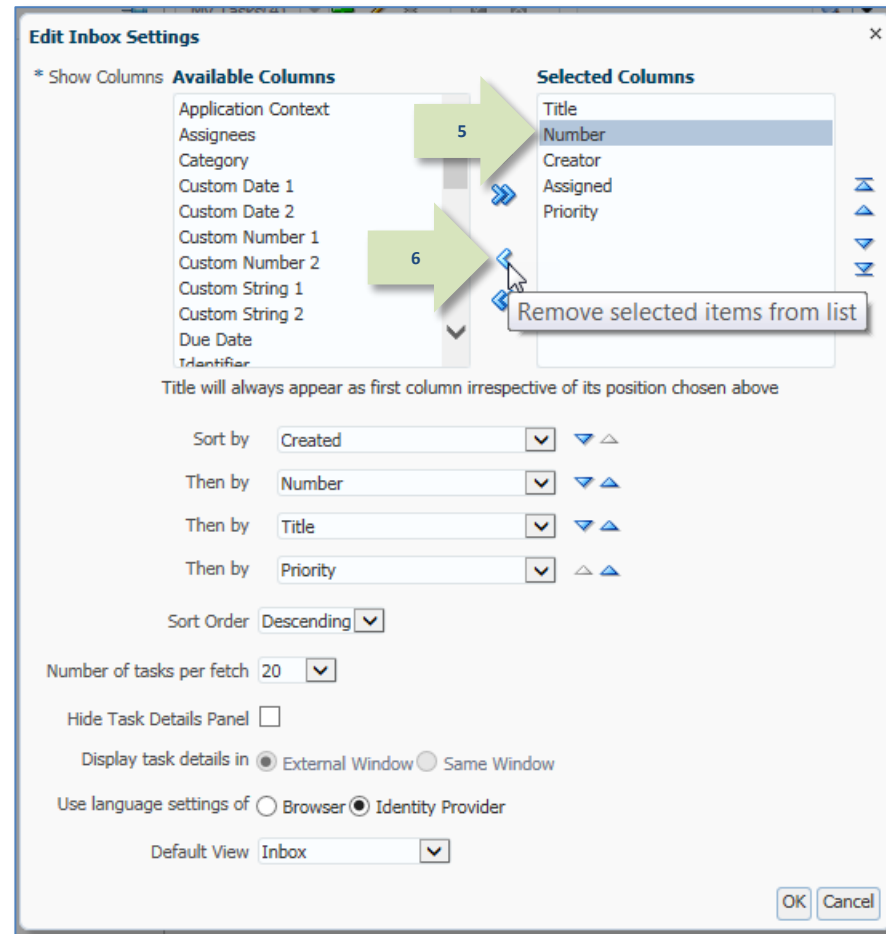
Figure 64: Select and Remove Columns

7. To add a column, select a column name from the **Available Columns** text list by clicking the column name.

8. Click the add icon (≫) to move the column name to the **Selected Columns** list.

    This action adds the selected column to the view.

    In this example, the user has selected the third of the three columns to be displayed.

Figure 65: Edit Inbox Settings - Select and Add New Columns

9. Change the **Sort** selections.

    In this example, you want to sort by the expiration date only.

    *You can create a hierarchical sort order by selecting additional sort criteria in the **Sort** section.*

10. Change the **Sort Order**: click the **Sort Order** drop-down box and click **Ascending**.

    *In this example, you want to see the tasks that expire first at the top of the task list. Sorting the **Expires** date column in **Ascending** order provides the result you want.*

Figure 66: Edit Inbox Settings - Change Sort Criteria and Sort Order

11. After you have selected all the display criteria needed to help you develop the default view you want, click the **OK** button.

AMPS closes the **Edit Inbox Settings** *dialog and returns to the* **My Tasks** *list on the* **Inbox** *screen.*

To create a view, you must select one or more columns.

If the *Selected Columns* list does not have at least one column name, AMPS displays an error after you click the *OK* button.

Figure 67: Edit Inbox Settings - Complete the View Changes

12. On the **Inbox** screen, click the **Assignee** drop-down list and click **Me** from the selections.

   *To ensure that the tasks listed in this view are assigned only to you, select **Me**.*
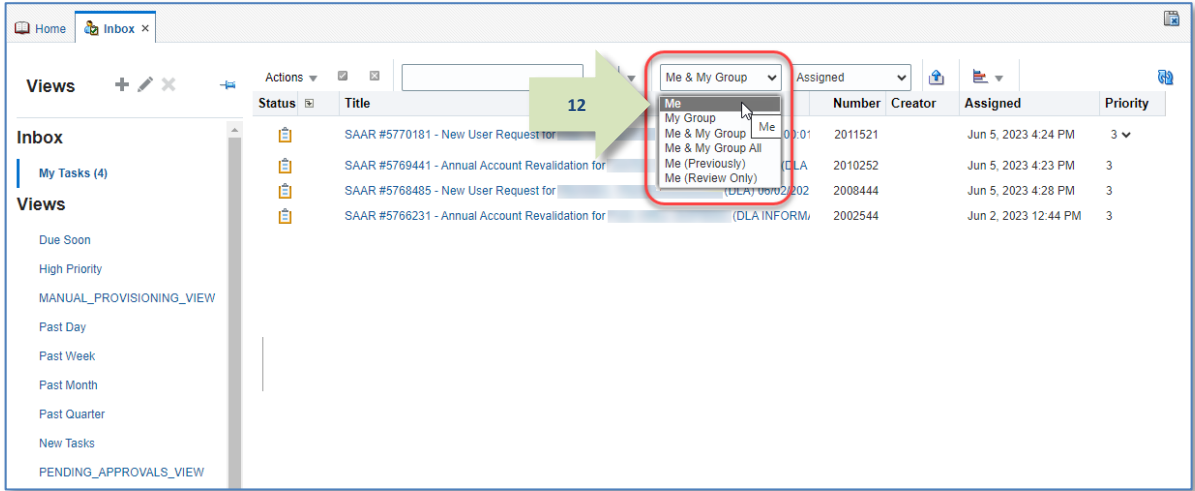
Figure 68: My Tasks List - Change the Assignee

13. AMPS has changed the columnar data and the sort order to match the criteria you have set.
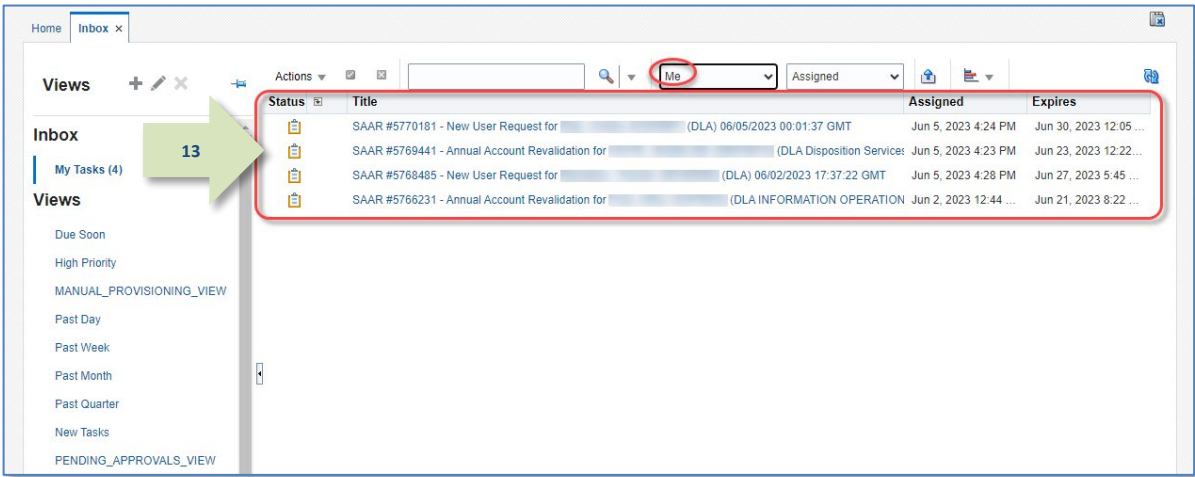
Figure 69: New View for the My Tasks List

My Profile: AMPS Information

The clickable tile labeled **My Information** enables you to view and manage information about yourself, your roles, and your accounts.

What you can do:	If you need to . . .	Navigate this path to this specific screen . . .
	Identify the roles assigned to you through AMPS, or, as a Supervisor, check the current roles assigned to a direct report. (See below for Direct Reports.)	Self Service (Home page) > My Information > Application & Roles tab > **Current Roles**
	Check the status of a pending role request.	Self Service (Home page) > My Information > Application & Roles tab > **Pending Requests**
	Review or modify basic information or contact data.	Self Service (Home page) > My Information > User Information > **User Information**
		Self Service (Home page) > My Information > User Information > **Contact Information**
	Manage your password or challenge questions (external users only).	Self Service (Home page) > My Information > User Information > **Change Password**
		Self Service (Home page) > My Information > User Information > **Set Security Questions**
	Update your Organization (internal users only).	Self Service (Home page) > My Information > User Information > **Organization**
	Change your Supervisor.	Self Service (Home page) > My Information > User Information > **Supervisor**
	View your Direct Reports (Supervisors only).	Self Service (Home page) > My Information > **Direct Reports**
Where to start:	Launch AMPS to start these procedures on the AMPS Home page.	

How to View and Manage Your AMPS Information

What you can do:	The section labeled **User Information** on the **My Information** screen contains identifying personal, location, and job-related data.
	Some of the data is displayed during the role request process and may affect the types of roles you can request. For example, if the **User Type** is **Civilian**, **Military**, or **Contractor**, AMPS displays only roles that provide access to systems those three user types require during the role request process. Similarly, if the **User Type** is **Vendor** or **Public**, AMPS displays roles available to these two types of users only during a role request (vendors have access to vendor and public roles).
	Much of this information is maintained in an Active Directory account for internal users who have such accounts, and it is updated in AMPS periodically. However, you can update data that appears in modifiable fields on the **My Information** screen, as needed.
What about Social Security Number (SSN) and Date of Birth?	The user's Date of Birth (DOB) and Social Security Number (SSN) are no longer required entries for a role request. **AMPS no longer collects this information.**
	Neither of these values are stored with a user's profile in the system. AMPS does not provide the means to enter and store these values anywhere. Where these fields are present, they will be "grayed out" and display non-editable faux data.
Where to start:	Start by clicking the **My Information** tile on the **Self Service Home** page. The screen displays the **User Information** screen by default.

View the *User Information* Screen through *My Information*

1. Log in to AMPS.

   *AMPS displays the **Self Service Home** page. Your ID is displayed in the banner to indicate you are the logged-in user.*

2. On the **Self Service Home** page, click the **My Information** tile.

   *AMPS displays the **My Information** screen.*
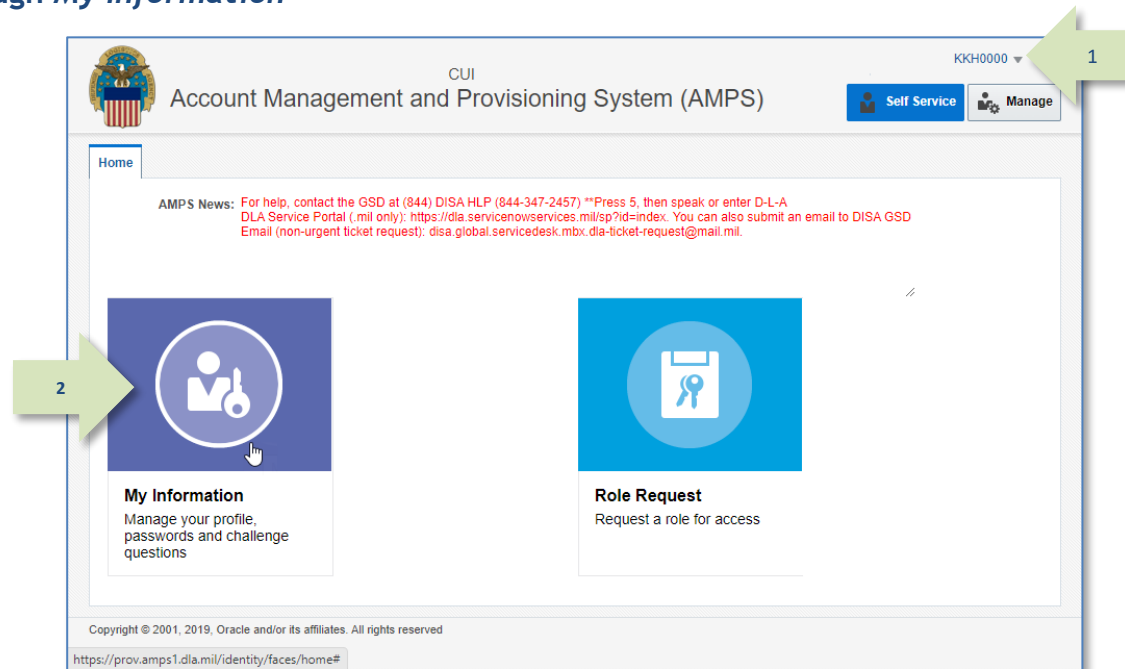
Figure 70: AMPS Self Service Home Page - My Information Tile

Internal User: User Information

3. Enter changes or new entries in the modifiable data fields.

   3a. Fields marked with an asterisk ( )
   are required entries.*

   *3b. Any of the bordered fields in **User
   Information** and **Contact
   Information** are modifiable. These vary
   depending on your account type. To
   modify data in non-modifiable fields,
   contact the Service Desk (see page 9).*

   *3c. Optional: Click the **Update
   Organization** command above the
   Organization Name field to update
   your Organization (internal users only).
   The IA Officers and Security Officers
   listed correspond to the selected
   Organization. These persons are
   approvers in the AMPS role request
   process.*

   *3d. Optional: Click the **Update
   Supervisor** command above the
   Name field to update your AMPS
   Supervisor name and information.*

   *The **Direct Reports** tab (not pictured)
   is for AMPS Supervisors who have staff
   members reporting directly to them. An
   AMPS Supervisor handles all approval
   requests and other changes to AMPS
   records for staff members listed under
   Direct Reports.*

4. Click **Save** to save your changes.

   *AMPS displays a confirmation message
   indicating your changes are saved (not
   shown). Click the **OK** button in the
   message box to close the message
   .*

Figure 71 : Internal User's *User Information* Screen

How to Update User Information: Internal Users

Enter changes or new entries in the modifiable data fields.

Fields marked with an asterisk (*****) are required entries.

1. Modify the following fields in the **User Account Information** section, as needed:

   *1a. Title: Enter your job title. This data item appears as part of the identifying information to your Supervisor in the **Direct Reports** screen, as well as to all approvers in the role request approval workflow. An approver handling your role request may require this data.*

   1b. Cyber Awareness Training Date: your last certification date.

   ***DFAS users (& External users):** If this field does not display the correct date, update it. AMPS saves the date in its database.*

   ***DLA users:** This date field is read-only.*

   *1c. User Type: The values available for external users are **Civilian**, **Military**, and **Contractor**.*

   ***DLA users:** This field is read-only.*

   *(**External users**: If this field does not display the correct user type, update it.)*

   1d. Citizenship: Select your citizenship type from the drop-down list.

2. Click **Save** to save your changes.

Figure 72 : User Information Section—Internal Users

User Type: Available values for internal users are Civilian, Military, and Contractor. User Type information appears as part of your identifying information in the role request approval workflow. The following list describes the additional User Type fields available under each of these user types:

- **Civilian** User Type fields: **Grade** (required) – select your grade from the drop-down list AMPS displays for this user type.
- **Military**: **Branch** (required) and **Rank** (required) – select a branch and rank from the drop-down lists AMPS displays for this user type.
- **Contractor: Contract Number** (required), **Contract Company** (required), **Contract Expiration Date** (required) – enter this data in the text fields AMPS displays for this user type.

> *Note:*
> If you need to change a field that is not modifiable, please contact the DISA Global Service Desk.

How to Update Contact Information: Internal Users

1. Enter changes or new entries in the modifiable data fields.

2. Modify the fields, as needed:
   - Most fields are modifiable text fields.
   - The **State** and **Country** fields are modifiable drop-down lists of predefined entries.

Note:

All fields marked with an asterisk (*****) require entries. AMPS displays an error if you attempt to leave the User Information screen without ensuring that all required fields have valid entries.

Figure 73 : Contact Information Section

Field Descriptions:

- **Official Telephone:** (*Required*) Displayed on role request approval screen and stored for information purposes.
- **Official Fax:** Stored for information purposes.
- **DSN Phone:** Stored for information purposes.
- **DSN Fax:** Stored for information purposes.
- **Mobile:** Stored for information purposes.
- **Office/Cube:** Stored for information purposes.

- **Street:** (*Required*) Stored for information purposes.
- **PO Box:** Stored for information purposes.
- **City:** (*Required*) Stored for information purposes.
- **State:** (*Required*) Stored for information purposes.
- **Zip:** (*Required*) Stored for information purposes.
- **Country:** (*Required*) Stored for information purposes.

3. Click **Save** to save your changes.

   *(See step 2 of Figure 72 to see the location of the **Save** button. It is located at the top right area of the screen beside the **Cancel** button.)*

How to Update the Organization: Internal Users Only

An Organization name is a required field on the *My Information* screen and on the *User Information* screen in the *Role Request* sequence.

An **Organization** is assigned to an internal user during account setup. If the Organization information requires a change, the following procedure enables you to make the change on

the **My Information** screen, and the new Organization assignment then appears on the *User Information* screen in the *Role Request* sequence.

Please note that if you are an external user, you cannot change your organization.

1. Click the **Update Organization** command above the *Organization Name* field.
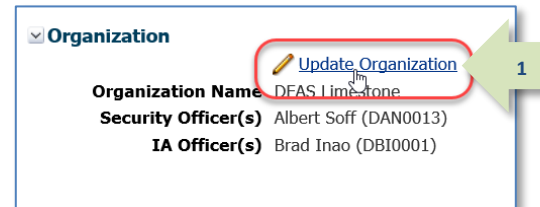
Figure 74: Organization Information

2. Enter part or all of an organization name in the *Organization Name* field.

3. Click **Search**.

   AMPS displays search results in the **Organization** *table.*

4. In the *Organization* results list, click a new organization name to select it.

5. Click **OK**.

   AMPS closes the **Find an Organization** *dialog and enters the new selection in the* **Organization Name** *field (see Figure 76).*
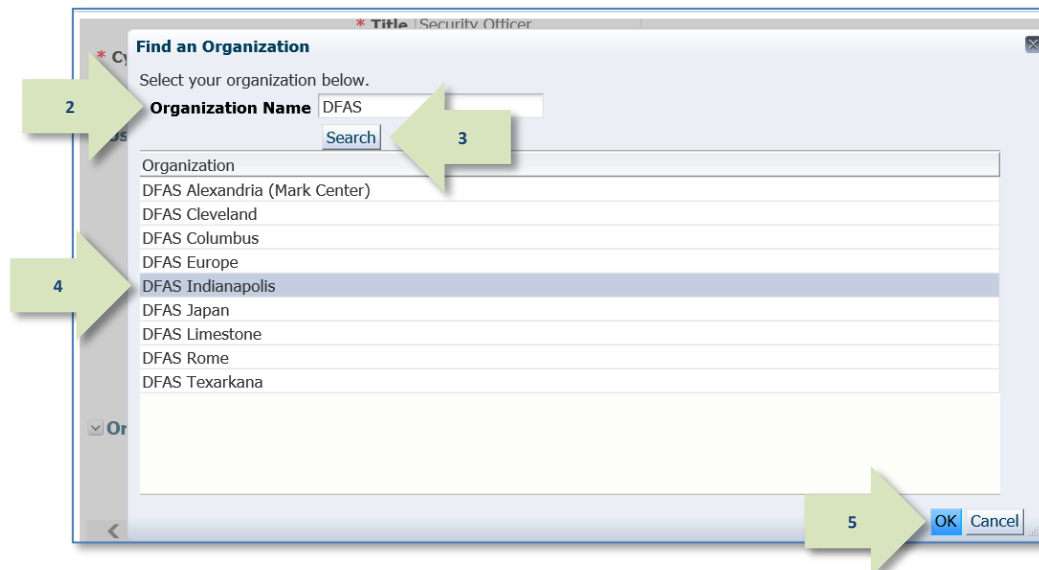
Figure 75: Search and Select Organization Name Dialog

6. Click **Save** (not shown).

   See step 2 of Figure 72 to see the location of the **Save** *button on the* **My Information** *tab.*
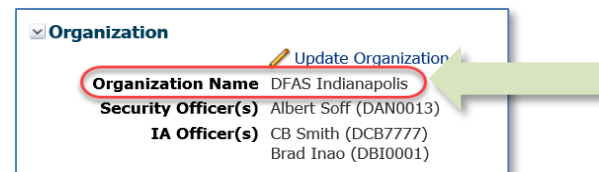
Figure 76: Organization Name Change Result

How to Update the Supervisor: Internal Users Only

Supervisor Name is a required field on the **My Information** screen and on the **User Information** screen in the **Role Request** sequence. An AMPS Supervisor is assigned to an internal user during account setup. In addition, the information for each user assigned to an AMPS Supervisor is displayed in that AMPS Supervisor's **Direct Reports** tab.

If your AMPS Supervisor or Supervisor's status changes, the following procedure enables you to enter a corrected Supervisor name on the **My Information** screen, and the new Supervisor assignment then appears on the **User Information** screen in the **Role Request** sequence.

Note that the Supervisor selected must maintain an active account. The screens in the following list prompt the user to select a new supervisor if the current one is disabled or deleted:

- Role Request
- My Information
- User Approval

Note, also, that if you must change your Supervisor's name after submitting role requests, and the role requests are still not approved by the former Supervisor, AMPS performs the following tasks:

- Notifies the new Supervisor of the SAAR or SAARs that require action. This notification occurs automatically.
- Replaces the former Supervisor's information with the new Supervisor's name on the SAAR itself.

---

1. Click the **Update Supervisor** command above the *Supervisor Name* field.

Figure 77: Supervisor Information

---

2. Enter supervisor search criteria in the *Name* and/or *User ID* fields.

3. Click *Search.*

4. In the search results list, click the Supervisor you want to select.

5. Click **OK**.

   The update to the assigned Supervisor is displayed in the **Supervisor Name** *field (see Figure 79).*

Figure 78: Search and Select Supervisor Name Dialog

6. Click the **Save** button in the **My Information** screen (not shown).

    *(See step 2 of Figure 72 for the location of the **Save** button. It is located at the top right area of the screen, next to the **Cancel** button.)*

    After you click the Save button, AMPS saves the new Supervisor's information to your profile and notifies the new Supervisor of all your "in-flight" SAARs that require his or her approval.

Figure 79: Supervisor Name Change Result

Internal Supervisor: Direct Reports

1. Log in to AMPS.

*If you have the **AMPS Supervisor** role, the system displays a Direct Reports subtab on your **My Information** tab.*

This tab automatically lists all the users who have selected you as their AMPS Supervisor.

*The following information is available for each entry in the **Direct Reports** table.*

- **User ID**
- **Last Name**
- **First Name**
- **Middle Name**
- **Email**
- **Title**
- **Street**
- **City**
- **State**
- **Zip Code**
- **Phone**
- **Fax**
- **DSN Phone**
- **DSN Fax**
- **Status (status of the user account)**

2. Click the user's ID to open the direct report's details screen.
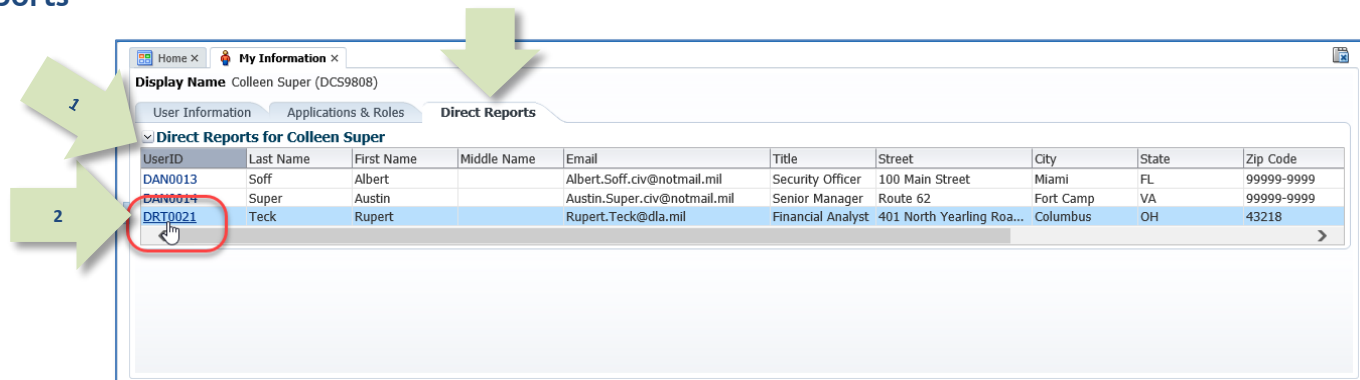
Figure 80: Internal Supervisor – Direct Reports Tab

3. In the **User Information** tab, AMPS displays a view of the user's account information, contact information, organization, and supervisor in read-only format.

Figure 81: Direct Report Details - User Information

4. Click the Applications & Roles tab.

   AMPS displays a read-only view of the direct report's role status.
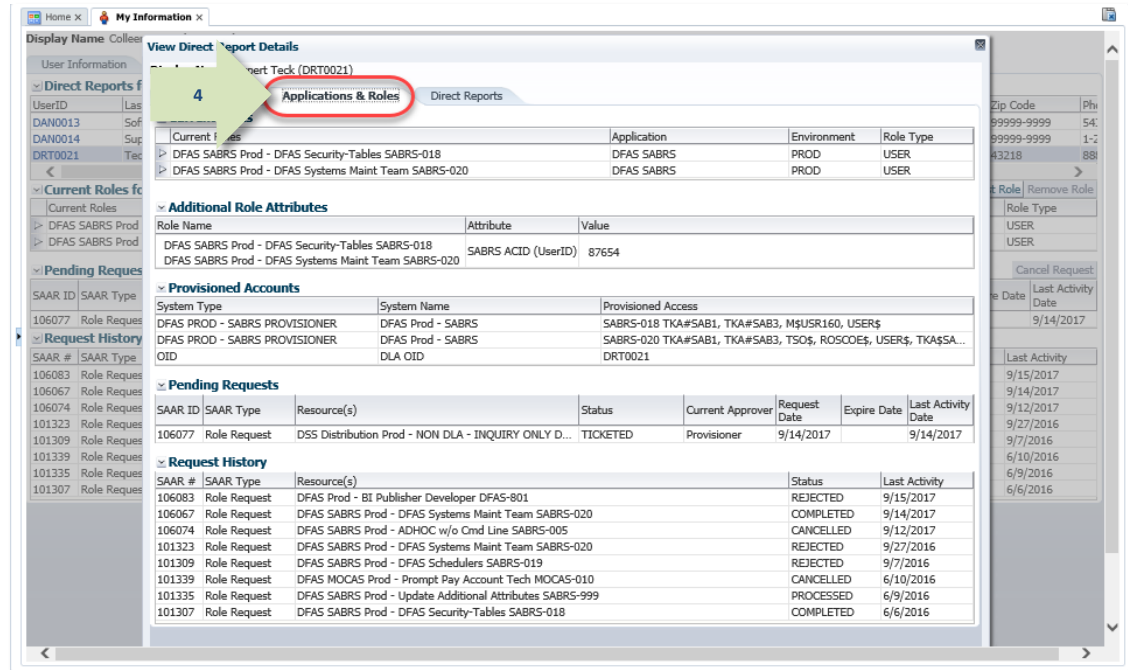
Figure 82: Direct Report Details - Applications & Roles

5. Click the **Direct Reports** tab.

   If the user has the AMPS Supervisor role, the system displays a list of any direct reports assigned to the user.

   If the user has no direct reports, the system displays the following message: "User has no direct reports at this time."

   Click the close icon in the upper right corner to close the Details screen.
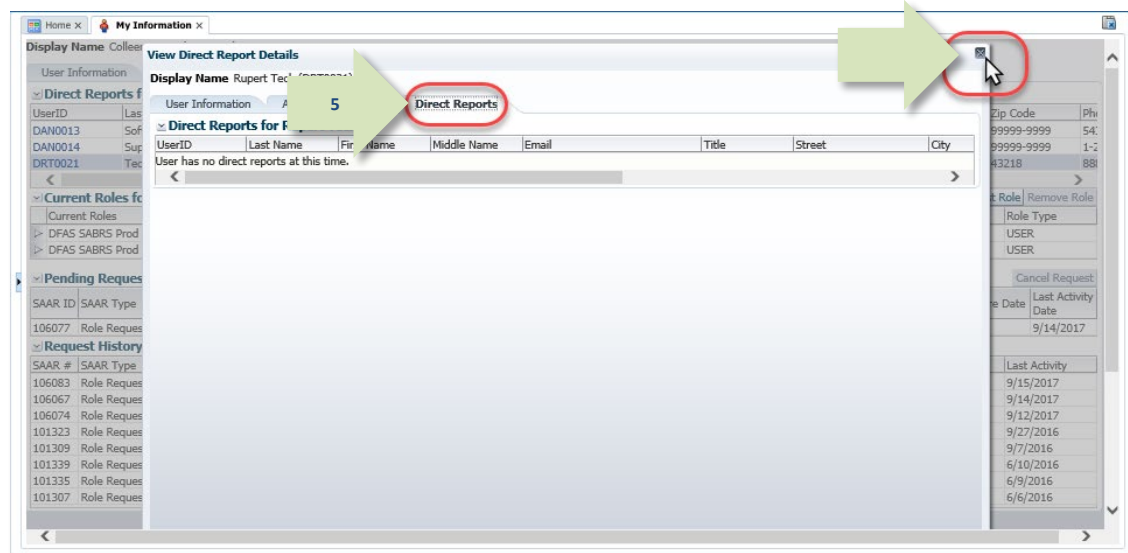
Figure 83: Direct Report Details - Direct Reports

External User: User Information

1. Enter changes or new entries in the modifiable data fields.

    1a. Fields marked with an asterisk (*) are required entries.

    *1b. Any of the <u>bordered</u> fields in **User Information** and **Contact Information** are modifiable. To modify data in non-modifiable fields, contact the Service Desk (see page 9).*

    1c. Required: Enter email addresses for each of the following external approvers:

    - **External Supervisor**
    - **External Security Officer**
    - **External Authorizing Official**

Note:

These external approvers must be three distinct and separate individuals with different email addresses.

2. Click **Save** to save your changes.

    AMPS displays a confirmation message indicating your changes are saved (not shown).

    *Click the **OK** button in the confirmation message box to close the message.*

Figure 84: External User's *User Information* Screen

How to Update the User Information Section: External Users

Enter changes or new entries in the modifiable data fields.

Fields marked with an asterisk (*****) are required entries.

1. Modify the following fields as needed:

   *1a. Title: Enter your job title. This data item appears as part of the identifying information to your Supervisor in the **Direct Reports** screen, as well as to all approvers in the role request approval workflow. An approver handling your role request may require this data.*

   1b. Cyber Awareness Training Date: If this field does not display the correct date, update it. AMPS saves the date in its database and displays this date to the IAO who may review your role requests if you are part of an organization that requires IAO review. The IAO can update this field, as needed, when you submit a role request.

   Note that no IAO review is required for DLA systems.

   1c. User Type: Available choices for external users are Civilian, Military, and Contractor.

   1d. Citizenship: Select your citizenship type from the drop-down list.

2. Click **Save** to save your changes.

Figure 85 : User Information Section—Internal Users

User Type: Available choices are Civilian, Military, and Contractor. User Type information appears as part of your identifying information in the role request approval workflow. The following list describes the additional User Type fields available under each of these user types:

- **Civilian** User Type fields: **Grade** (required) – select your grade from the drop-down list AMPS displays for this user type.
- **Military**: **Branch** (required) and **Rank** (required) – select a branch and rank from the drop-down lists AMPS displays for this user type.
- **Contractor: Contract Number** (required), **Contract Company** (required), **Contract Expiration Date** (required) – enter this data in the text fields AMPS displays for this user type.

Note:
If you need to change a field that is not modifiable, please contact the DISA Global Service Desk.

How to Update Contact Information: External Users

1. Enter changes or new entries in the modifiable data fields.

Figure 86 : Contact Information Section

2. Modify the fields, as needed:
   - Most fields are modifiable text fields.
   - The **State** and **Country** fields are modifiable drop-down lists of predefined entries.

Note:

All fields marked with an asterisk (*****) require entries. AMPS displays an error if you attempt to leave the User Information screen without ensuring that all required fields have valid entries.

Field Descriptions:

- **Official Telephone:** (*Required*) Displayed on role request approval screen and stored for information purposes.
- **Official Fax:** Stored for information purposes.
- **DSN Phone:** Stored for information purposes.
- **DSN Fax:** Stored for information purposes.
- **Mobile:** Stored for information purposes.

- **Office/Cube:** Stored for information purposes.
- **Street:** (*Required*) Stored for information purposes.
- **PO Box:** Stored for information purposes.
- **City:** (*Required*) Stored for information purposes.
- **State:** (*Required*) Stored for information purposes.
- **Zip:** (*Required*) Stored for information purposes.
- **Country:** (*Required*) Stored for information purposes.

3. Click Save to save your changes.

   (See step 2 of Figure 85 for the location of the Save button. It is located at the top right area of the screen beside the Cancel button.)

How to Update the Supervisor: External Users Only

External Supervisor is a required field on the **My Information** screen and on the **User Information** screen in the role request and role attribute update procedures. You, as an external user, can identify an AMPS External Supervisor first during the user registration by entering an email address in the External Supervisor field.

Supervisor Email Address Changes

You can change your Supervisor's email address, or identify a different External Supervisor with a new email address, after submitting role requests or attribute change requests. If requests are not yet approved by the previous Supervisor, AMPS performs the following tasks:

- Redirects the SAAR or SAARs from the prior Supervisor's approval work queue to the new Supervisor's work queue.
- Notifies the new Supervisor of the SAAR or SAARs that require action. AMPS delivers this notification by email automatically.

- Replaces the former Supervisor email address with the new Supervisor's address on the SAAR.

Supervisor Contact Information: Name and Telephone Number

The Supervisor's contact information makes up a part of the External Approvers' Portal (EAP). The first time a Supervisor receives an approval request for a SAAR, the EAP presents fields that require the Supervisor to verify the email address and fill in the Supervisor's first name, last name, and phone number. The Supervisor can correct this information when he or she receives an approval request.

If your Supervisor changes or if your current Supervisor's email address changes, the following procedure enables you to enter the correct Supervisor email address on the **My Information** screen, and AMPS then displays the new email address in the **User Information** screen of the role request and attribute change procedures.

---

1. After you log in to AMPS, click the **My Information** tile on the Self Service Home page.

   AMPS opens the My Information screen (see Figure 88).
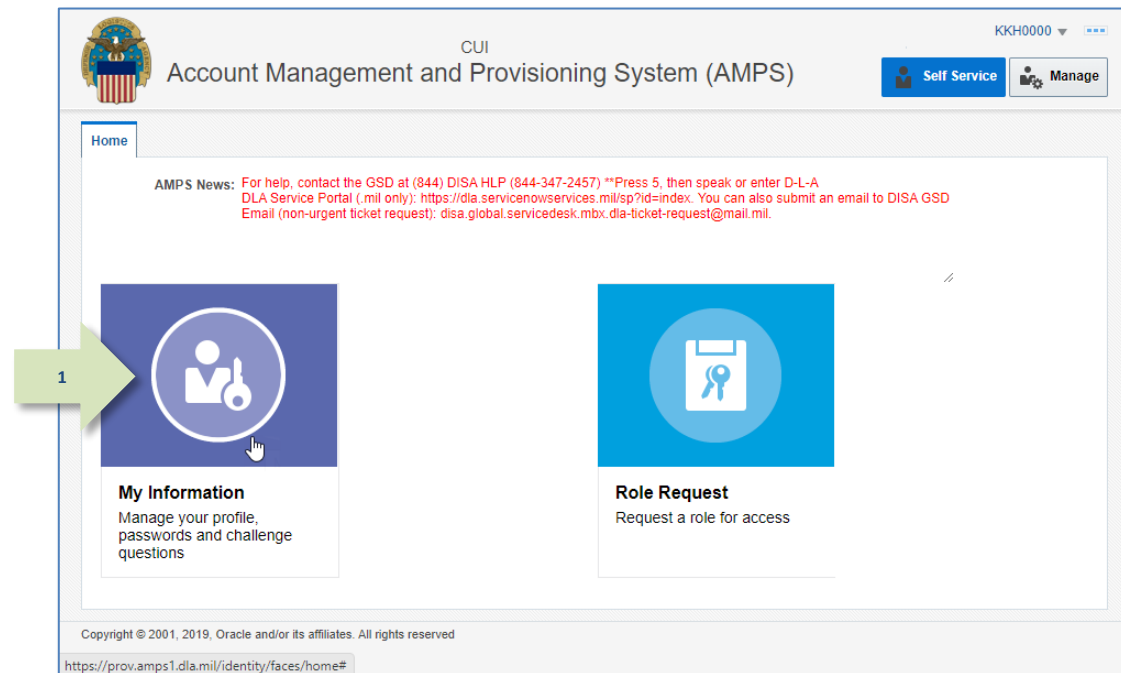
Figure 87: Self Service Home Page – My Information Tile

2. Locate the **External Supervisor** section in the **User Information** subtab.

Figure 88: My Information – Supervisor Section

3. In the **Supervisor** section, enter the Supervisor's correct email address.

   The email address must be accurate. AMPS sends all notifications resulting from your requests to this email address.

4. Click the **Save** button.

   *If all required fields on the **User Information** tab page have appropriate entries, AMPS displays a confirmation message (see Figure 90).*

Figure 89: External Supervisor Name Change Result

5. Click the **OK** button to close the **Information** message.

   AMPS saves the new Supervisor's email to your profile, reassigns your SAARs awaiting Supervisor approval to the new Supervisor's Work Queue, and notifies the new Supervisor of all your "in-flight" SAARs that require his or her approval.

Figure 90: Change Confirmation Message

How to Update the Security Officer: External Users Only

External Security Officer is a required field on the **My Information** screen and on the **User Information** screen in role request and role attribute update procedures. You, as an external user, can identify an AMPS External Security Officer first during user registration by entering an email address in the External Security Officer field.

Security Officer Email Address Changes

You can change your Security Officer's email address, or identify a different External Security Officer with a new email address, after submitting role requests or attribute change requests. If requests are not yet approved by the previous Security Officer, AMPS performs the following tasks:

- Redirects the SAAR or SAARs from the prior Security Officer's approval work queue to the new Security Officer's work queue.

- Notifies the new Security Officer of the SAAR or SAARs that require action. AMPS delivers this notification by email automatically.

- Replaces the former Security Officer email address with the new address on the SAAR.

Security Officer Contact Information: Name and Telephone Number

The Security Officer's contact information makes up a part of the External Approvers' Portal (EAP). The first time a Security Officer receives an approval request for a SAAR, the EAP presents fields that require the Security Officer to verify the email address and fill in the Security Officer's first name, last name, and phone number. The Security Officer can correct this information when he or she receives an approval request.

If your Security Officer changes or if your current Security Officer's email address changes, the following procedure enables you to enter the correct Security Officer email address on the **My Information** screen, and AMPS then displays the new email address in the **User Information** screen of the role request and role attribute change procedures.

1. After you log in to AMPS, click the **My Information** tile on the Self Service Home page.

   AMPS opens the **My Information** *screen (see Figure 92).*
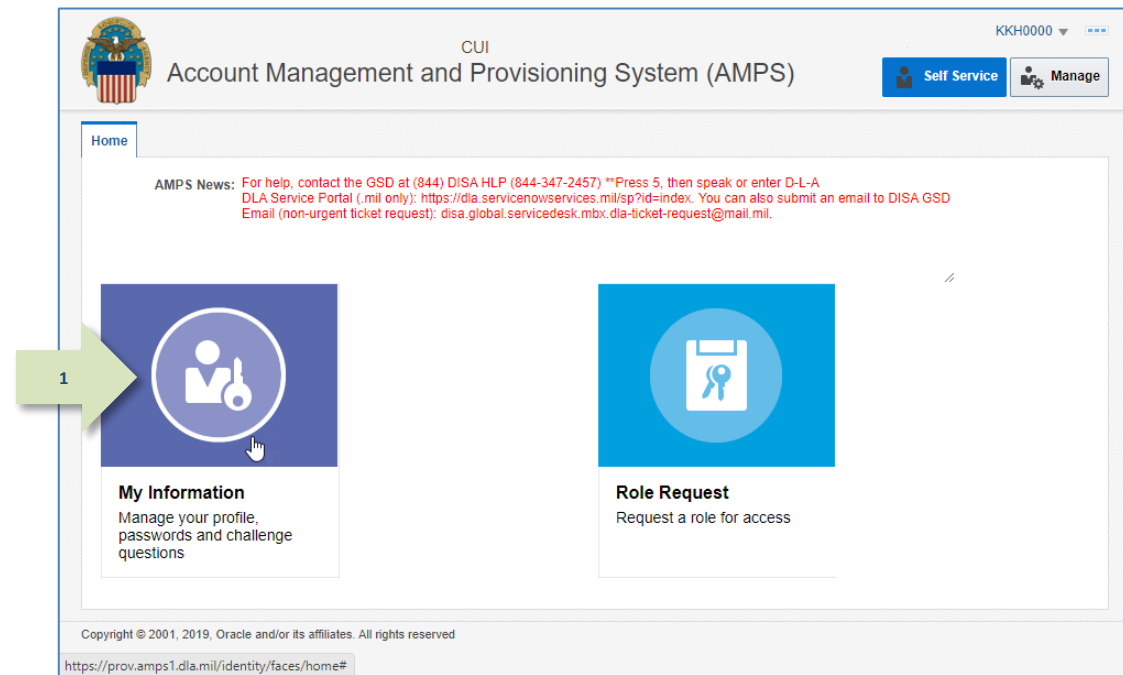
Figure 91: Self Service Home Page – My Information Tile

2. Locate the External Security Officer section in the My Information screen.

Figure 92: My Information – External Security Officer Section

3. In the **External Security Officer** field, enter an updated email address.

4. Click the **Save** button.

   *If all required fields on the **User Information** tab page have appropriate entries, AMPS displays a confirmation message (see Figure 94).*

Figure 93: External Security Officer Name Change Result

5. Click the **OK** button to close the **Information** message.

Figure 94: Change Confirmation Message

How to Update the External Authorizing Official: External Users Only

External Authorizing Official is a required field on the **My Information** screen and on the User Information screen in role request and role attribute update procedures. You, as an external user, can identify an AMPS **External Authorizing Official** first during user registration by entering an email address in the **External Authorizing Official** field.

The **External Authorizing Official** field is required for roles that require an EAO approval. If you do not have an EAO email address entered through the **User Information** interface, AMPS requires you to enter this information in the role request's **User Information** screen while you are creating certain role requests or attribute change requests.

External Authorizing Official: Change in Orientation

With the release of AMPS 17.2.0, the External Authorizing Official (EAO) is no longer an additional role attribute. EAOs are now a required part of an external user's profile, and external users manage their EAOs through the **User Information** screen.

EAO Email Address Changes

You can change your EAO's email address, or identify a different EAO with a new email address, after submitting role requests or attribute change requests. If requests are not yet approved by the previous EAO, AMPS performs the following tasks:

- Redirects the SAAR or SAARs from the prior EAO's approval work queue to the new EAO's work queue.

- Notifies the new EAO of the SAAR or SAARs that require action. AMPS delivers this notification by email automatically.

- Replaces the former EAO email address with the new address on the SAAR.

EAO Contact Information: Name and Telephone Number

The EAO's contact information makes up a part of the External Approvers' Portal (EAP). The first time an EAO receives an approval request for a SAAR, the EAP presents fields that require the EAO to verify the email address and fill in the EAO's first name, last name, and phone number. The EAO can correct this information when he or she receives an approval request.

If your **External Authorizing Official** changes or if your current EAO's email address changes, the following procedure enables you to enter the correct EAO email address on the **My Information** screen, and AMPS then displays the new email address in the **User Information** screen of the role request and role attribute change procedures.

Note:

The External Supervisor, External Security Officer, and External Authorizing Official must be three separate and distinct individuals with different email addresses.

1. After you log in to AMPS, click the **My Information** tile on the Self Service Home page.

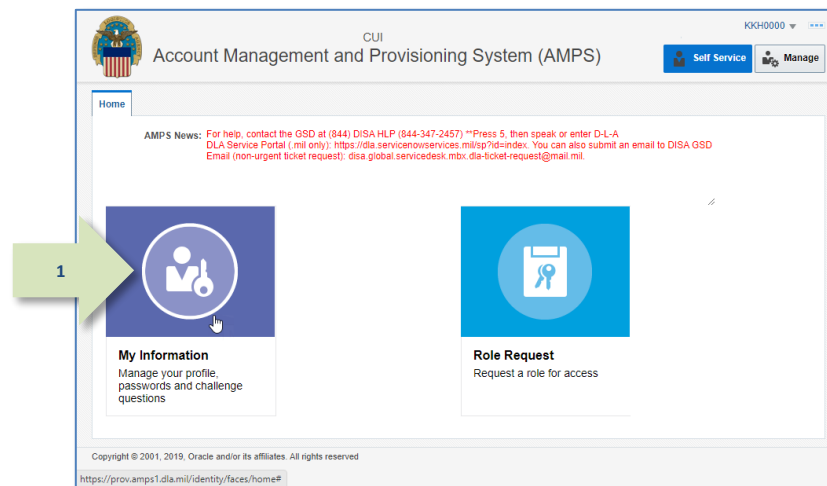   *AMPS opens the **My Information** screen (see Figure 96).*

Figure 95: Self Service Home Page – My Information Tile

2. Locate the External Authorizing Official section in the My Information screen.

Figure 96: My Information – External Authorizing Official Section

3. In the **External Authorizing Official** field, enter an updated email address.

Note:

> The external approvers must be three separate and distinct individuals with different email addresses.

4. Click the **Save** button.

*If all required fields on the **User Information** tab page have appropriate entries, AMPS displays a confirmation message (see Figure 98).*

Figure 97: External Authorizing Official Name Change Result

5. Click the **OK** button to close the **Information** message.

Figure 98: Change Confirmation Message

How to Change Your Password

An alternate means of authenticating an external user's identity in AMPS requires the use of a user ID and password. While the identity of an internal user, and certain external users, can be authenticated with a CAC or other certificate authority, most external users register for an account in AMPS, which includes authentication setup.

> ### Note:
>
> For users with accounts in applications that AMPS automatically provisions, the password change set for AMPS is also set for any applications that are automatically provisioned.
>
> If you have auto-provisioned application accounts and do not want all applications to have the same password, first change your AMPS password. Then, call the Service Desk for assistance in changing application passwords.

An external user creates a password, sets up answers to three security questions for backup authentication, and acquires an AMPS-generated user ID during the AMPS registration process. Internal users have the option of setting up passwords and security question responses after they have an account set up for them. However, because internal users have CACs to use for authentication, the user ID and password are not necessary for this purpose.

Internal and external users can follow the same procedure to maintain their passwords and their security questions. The following sections explain how to maintain passwords and security question responses.
To create a valid, strong password, refer to **Appendix C: Password Rules**.

1. After launching AMPS, click the **My Information** tile on the Self Service Home page.

   AMPS opens the **My Information** *screen and the* **User Information** *tab screen (see Figure 100).*
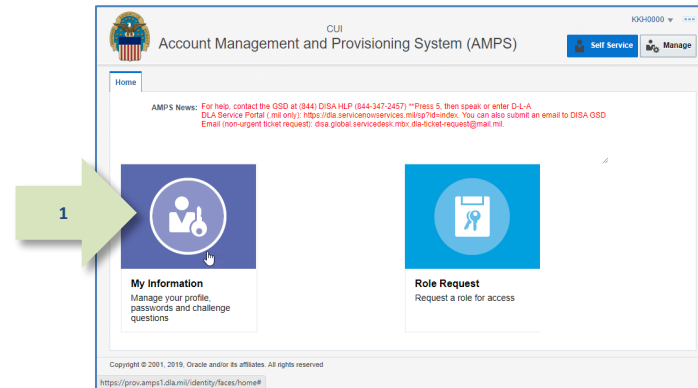
Figure 99: AMPS Self Service Home Page - My Information Tile

2. Click the **Change Password** button.
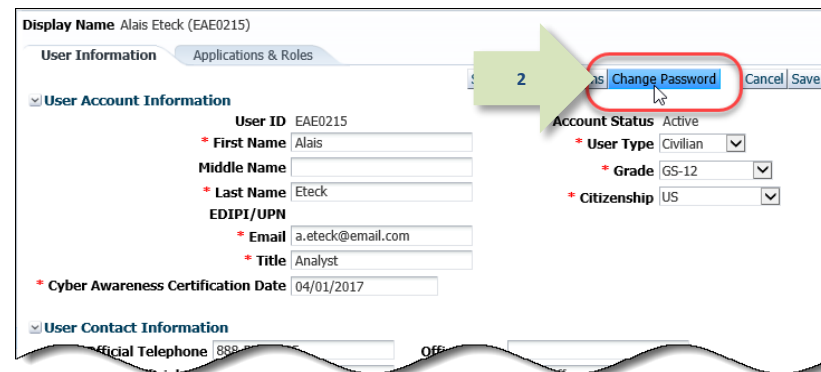
Figure 100 : My Information Screen – User Information Tab

3.　Fill in the **Change Password** dialog as follows:
　　-- Enter your current password.
　　-- Enter a new password.
　　-- Reenter the new password to confirm it.

Note:

Remember that this password affects all application passwords, if the applications are auto-provisioned by AMPS.
Contact your Supervisor if you have questions about your application passwords.

4.　Click **OK**.
　　AMPS displays an Information message box to confirm the change.

Note:

If you include one or more invalid characters in the new password entry, AMPS displays an error message and identifies the invalid characters. You can change the character to a valid entry based on the password rules provided in the dialog and retry saving the new password.

5.　In the **Information** message box, click **OK**.

　　AMPS closes the message box, updates your password to the new one just created, and expires your current session. Use the new password the next time you log in to AMPS.

6.　Close your current browser.

Note:

Even though your browser may remain open, AMPS has expired your session. If you try to continue in the open browser, AMPS displays the Single Sign-On Authentication screen (see Figure 23). You must log back in with your User ID and new password to re-authenticate.

Figure 101: Change Password Dialog
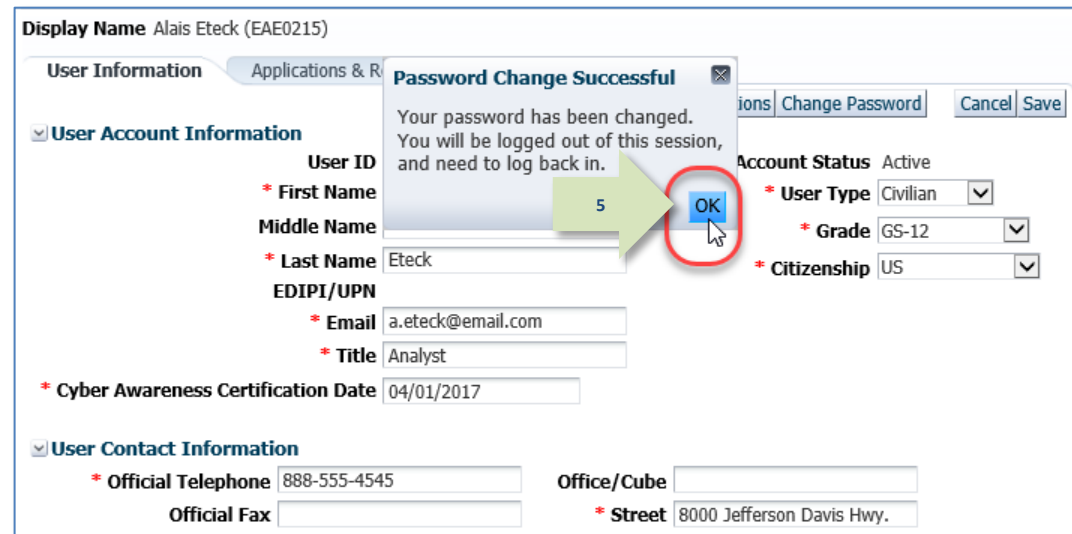
Figure 102: Password Change Confirmation Message

How to Set Security Questions

Any time you forget your password or user ID, AMPS provides you with the option to recover your ID or reset your password. To authenticate your request, AMPS presents three question-and-answer pairs called "Security Questions." You must answer these questions in order to proceed. During the AMPS account registration process, you set up answers to three different security questions. This procedure shows you how to choose different questions and reset the answers. This capability adds a layer of security to your login process.

1. After launching AMPS, click the **My Information** tile on the Self Service Home page.

   *If AMPS displays a Privacy Act Statement, read the text and click **Accept** to proceed. AMPS then displays a **My Information** tab (see Figure 104).*
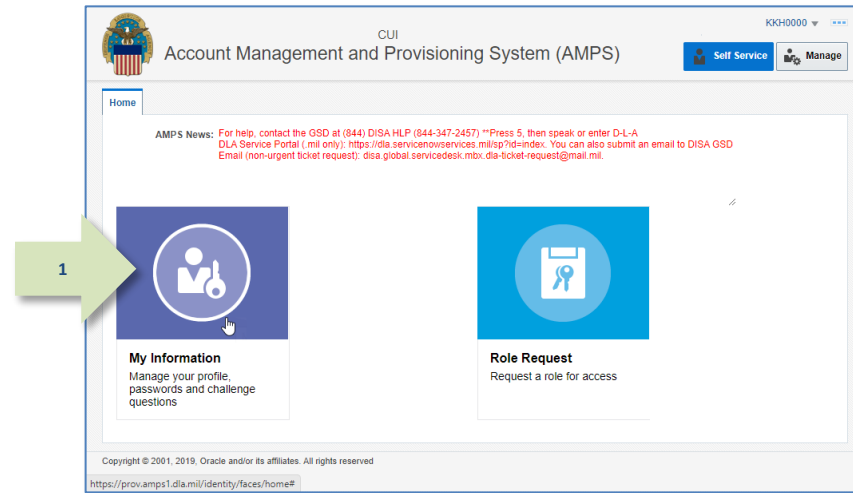
Figure 103: AMPS Self Service Home Page - My Information Tile

2. Click the Set Security Questions button.

   *AMPS displays the **Manage Security Questions** dialog (see Figure 105).*
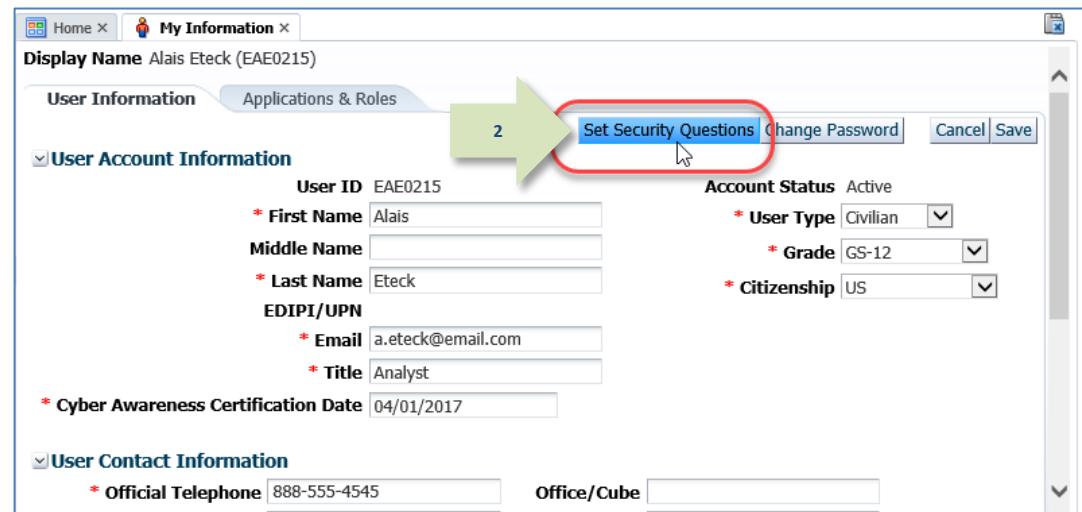
Figure 104 : My Information Screen – User Information Tab

3. Click the drop-down box for each of the three questions to select a different option.

   Options include the following questions:
   - What is the city of your birth?
   - What is the name of your pet?
   - What is your favorite color?
   - What is your mother's maiden name?

Note:

The asterisk (*) beside each question and answer field indicates that a selection and entry are required. You must select three questions and enter three answers that you can remember.

Figure 105: Manage Security Questions

4. Enter an answer for the newly selected question.

Note:

Each answer must contain three or more alphanumeric characters.

5. Click **OK**.

   If the answers are valid, AMPS closes this dialog.

   If the answers lack the minimum number of three characters, AMPS displays an error message and provides the opportunity to correct the answers. Repeat Steps 4 and 5, as needed.

   Ensure you have memorized these answers in case you need them. The Service Desk cannot help you recover these answers.

Figure 106: Manage Security Questions - Answers

6.   In the **Information** message box, click **OK**.

AMPS updates the answers to your security question.

Figure 107: Security Question Reset - Confirmation

All Users: Applications and Roles

How to Check Your Role Status

1. Launch AMPS.

   The user ID in the banner indicates the identity of the currently logged-in user.

2. On the **Self Service Home** page, click the **My Information** tile.

   AMPS displays the **Privacy Act Statement** (Not shown. *See* **Appendix A***).*

3. Click **Accept** in the **Privacy Act Statement** screen to proceed (not shown).

   AMPS displays the My **Information** *screen (see Figure 109).*

4. Click the **Applications & Roles** tab.

   AMPS displays the **Applications & Roles** *screen (see Figure 110).*
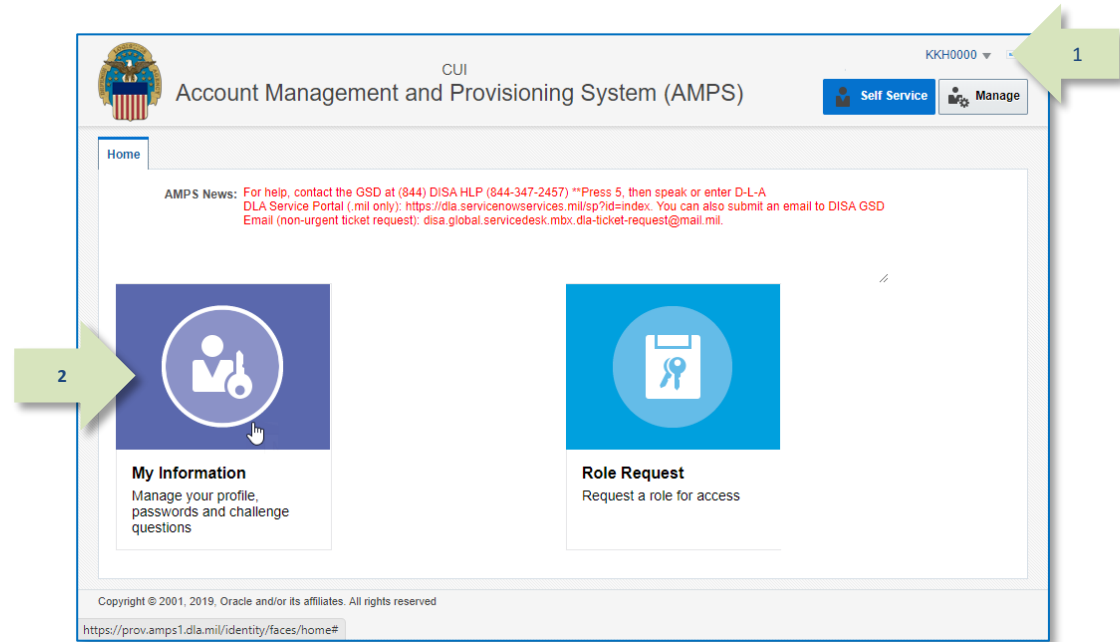
Figure 108: AMPS Self Service Home Page – My Information Tile
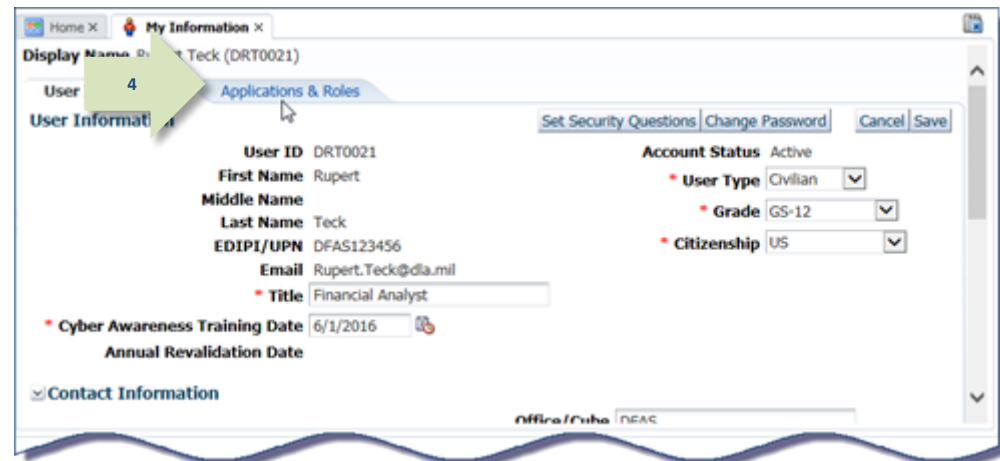
Figure 109: My Information – User Information

5. Review the **Current Roles** section to view the roles you are currently assigned.

AMPS displays the following information:
- Role name
- Application
- Environment (Production)
- Role Type (User or Admin)

6. Review the **Pending Requests** section to check the status of a role request according to SAAR number.

AMPS displays the following data (reposition cell borders, as needed, to see complete entries):
- SAAR ID
- SAAR Type
- Role Name
- Status
- Current Approver
- Request Date
- Expiry Date
- Last Activity Date (not shown)

By checking this data, you can determine the current approval status, the expiration date of the current SAAR, and the date of the last approver's action. Using this information, you can track the progress of a SAAR (see **Approval Process Summary** *for more information about the role request approval process).*

7. Review the **SAAR History** section to review SAARs that have been completed, cancelled, rejected, or otherwise terminated.

Home ✕　　**My Information** ✕

Display Name Rupert Teck (DRT0021)

| User Information | **Applications & Roles** |

Current Roles　　　　　　　　　　　　　　　　[Request Role][Remove Role]

Role Name	Application	Environment	Role Type
AMPS BASE USER ROLE	AMPS	PROD	User Role
DFAS SABRS Prod - DFAS Security-Tables SABRS-018	DFAS SABRS	PROD	User Role

Additional Role Attributes　　　　　　　　　　　[Update Additional Attributes]

Role Name	Attribute	Value
DFAS SABRS Prod - DFAS Security-Tables SABRS-018	SABRS ACID (UserID)	98765

Provisioned Accounts

System Type	System Name	Provisioned Access
DFAS PROD - SABRS PROVISIONER	DFAS Prod - SABRS	SABRS-018 TKA#SAB1,...
OID	DLA OID	DRT0021

Pending Requests　　　　　　　　　　　　　　　[Cancel Request]

SAAR ID	SAAR Type	Role Name	Status	Current Approver	Request Date	Expiry Date
101309	Role Request	DFAS SABRS Prod - DFAS Schedulers SABRS-019	PENDING APPROVAL	Security Officer	2016-...	2016-

SAAR History

SAAR ID	SAAR Type	Role Name	Status	Last Activity Date
101307	Role Request	DFAS SABRS Prod - DFAS Security-Tables SABRS-018	COMPLETED	6/6/2016
101287	New IT User R...	AMPS BASE USER ROLE	COMPLETED	6/2/2016

Figure 110: Applications & Roles Tab Page

Role Request Process

The **Role Request** process enables you to select and enter information required to submit a role request. At the end of the process, AMPS creates an automated SAAR, gives it a number, and submits the SAAR to the approval process. The request process displays four information entry screens in sequence. At the top of each role request screen is a series of screen names that help you trace your location in the sequence. Click the name of any screen already visited to return to it, and add or correct information before submitting the request. The current screen's name is displayed in bold text:
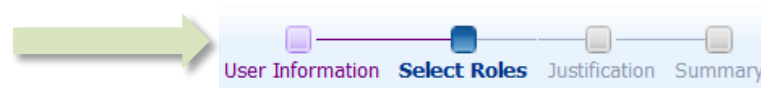
Figure 111: Role Request Navigation

Roles are sorted into the following categories:

- **Role Types:** Additional Approver, Data Owner, Information Assurance Officer, Security Officer, Segregation of Duties Reviewer, Supervisor, Total AMPS Provisioner, various User types
- **Role Levels:** User, Administrator (Admin)
- **Role Environments:** Dev (Development), Prod (Production)
- **Role Hierarchies:** Primary, Primary and Additional, Additional Only, Not Applicable

Your Supervisor can clarify which categories are applicable to your role choice. These categories are also visible on the role description panel (see Figure 116 for an example). Approvers can check the option to **Display Admin Roles** to add administrator roles to the **Select a Role** list panel (see Figure 116).

A Note on Additional Attributes

Some roles provide a table for entering one or more **Additional Attributes**. For example, attributes can include a training certification date, an identifier, or a DoDAAC. AMPS labels each attribute to indicate what a valid entry is, and whether or not the attribute entry is required:

- **Y** means an entry is required.
- **N** means an entry is optional.

Follow your Supervisor's or Application Owner's instructions explicitly when you enter an attribute. AMPS does not validate the characteristics of any attribute, such as character count or character type. See Figure 118: Request Role - Justification - Additional Attribute Sample for an illustration.

How to Request a Role: Internal User

1. Log in to AMPS.

   *AMPS displays the **Self Service Home** page. Your ID is displayed to indicate you are the currently logged-in user.*
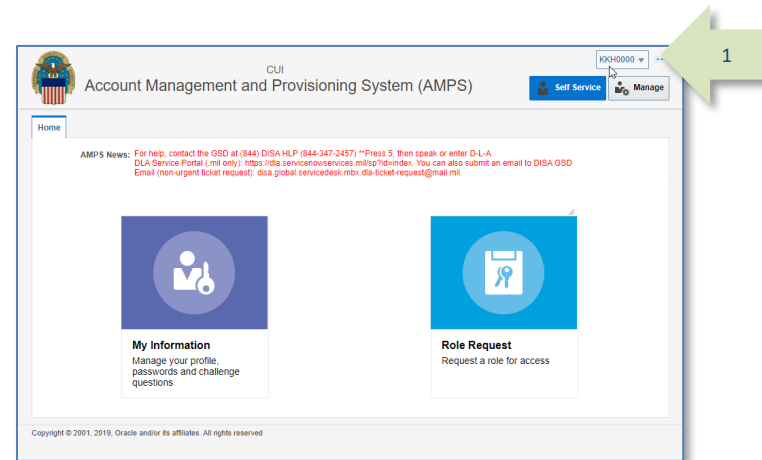
Figure 112: AMPS Self Service Home Page

2. On the **Self Service Home** page, click the **Role Request** tile.

    If this action is the first time during the current session when you request a role, AMPS displays a **Privacy Act Statement**. *Read the statement and click the* **Accept** *button to proceed. For more information, see* **When is the Privacy Act Statement Displayed in AMPS?** *in Appendix A.*
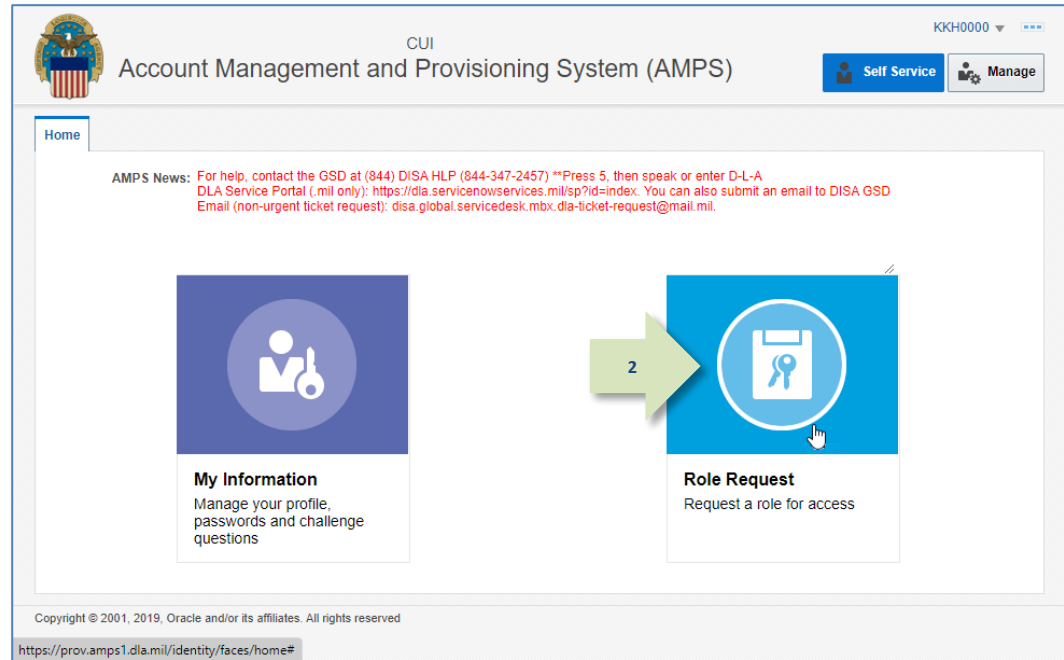
Figure 113: AMPS Self Service Home Page – Role Request Tile

3. On the **Request Role > User Information** screen, enter or correct the **Title** entry (required).

4. DFAS users, enter your most recent Cyber Awareness Certification Date (required).

   This date must fall within the previous 12 months.

   DLA users: *this date field is read only.*

5. Your **Date of Birth** is no longer required.

   *AMPS does not save or store the **Date of Birth** for any user. Where this field is present, it will contain non-editable faux data.*

6. Your **User Type** is a non-modifiable field. Follow the instructions below concerning the additional user type fields for each user type (required):

   a. **Civilian**: select your **Grade** in the field displayed when you select this user type.

   b. **Military**: select your **Branch** and **Rank** from the fields displayed when you select this user type (see Figure 115).

   c. **Contractor**: enter your **Contract Number**, **Contract Company**, **Contract Expiration Date,** and **Contract Officer** (optional) in the fields displayed when you select this user type (see Figure 115).

7. Update Contact Information, as needed.
   See **How to Update Contact Information: Internal Users** *for instructions.*

8. Update your Organization, as needed (internal users only).
   See **How to Update Organization Information** *for instructions.*

9. Update your Supervisor, as needed (internal users only).
   See **How to Update Supervisor Information** *for instructions.*

10. Click the **Next** button.

Figure 114: Request Role - User Information

Figure 115: User Type Samples - Military and Contractor

AMPS Displays the Select Roles Screen

The **Select Roles** screen features two methods for locating a particular role name: **Search** and **Browse**.

The following procedure tells you how to use the **Search** method to find a role name. To browse for a role, see the section entitled **How to Browse for a Role**.

11. In the **Select Roles** screen's **Search Roles** section, enter all or part of any search criteria you have available.

    For example, if you have the role name, you can enter part of the name in the **Role Name** *field.*

12. Click the **Search** button.

    AMPS displays the names of all roles having a name or other criteria that match the **Search** *string.*

13. Locate the role you want to request in the **Select a Role / Role Name** panel:

    a. To verify your choice, click the **Expand** button to display the role description panel. This panel lists details about the role that help you verify your role selection.

    b. EBS users: If you select an **Additional** role without first requesting and receiving a related **Primary** role, AMPS displays an error message.

14. Click the role selection and then click the right arrow (→) button.

    AMPS copies the role name to the **Selected Roles** *list panel on the right.*

    To request multiple roles, repeat steps 8 through 11 if you do not require, or already have, a primary role.

15. Click the **Next** button.

Figure 116: Request Role - Select Roles

AMPS Displays the Justification Screen

16. In the **Justification** screen, fill in the following information:

   a. Enter comments in the **Justification** field to clarify the request (required). Note that the request may be rejected if the justification is inadequate. Contact your Supervisor if you have questions.

   b. You can enter further comments in the **Optional Information** text area to supply additional information that supports your request.

Note:

Comments and file name shown in the sample screen are for illustration purposes only. Please enter information relevant to each specific request.

17. As an option, you can click the **Browse** button to locate and attach a supporting document. Repeat this procedure to attach an additional two documents, as needed. *Note that any PDF file you upload may NOT have PII included.*

18. Click the **Next** button.

Roles with Additional Attributes

*Some roles require or request additional attributes to be supplied by the requestor during the role request process. One example is a **Department of Defense Activity Address Code** (**DoDAAC**) number. Another example is an **Accessor Identification** (**ACID**) code.*

*AMPS displays an additional section, called **Role Attributes**, on the **Justification** screen for each role that calls for additional attributes. (See Figure 118 for a sample view.)*

*A letter **Y** in the **Required** column indicates the attribute value is a required entry; **N** means the entry is optional. Enter the appropriate value, as needed.*

Figure 117: Request Role – Justification

Figure 118: Request Role - Justification - Additional Attribute Sample

AMPS Displays the Summary Screen

19. Review the information in the **Summary** screen.

    - Click the **Back** button to return to previous screens and make corrections, as needed.

    - After making corrections, click the **Next** button or the **Summary** node in the train to return to the **Summary** screen.

20. Click **Submit** to complete the role request.

Note:

Click Cancel to discard this request and start again, as needed.

Figure 119: Request Role – Summary

AMPS Confirms the Role Request

21. Note that the SAAR number is listed here, along with role name and status information on the **Role Request Confirmation** screen.

    Your status notifications and **Pending Requests** record will refer to this SAAR number.

22. Click the **OK** button in the **Role Request Confirmation** screen.

    AMPS adds a listing for the new SAAR in the user's Pending Requests table (see *Figure 110*).

23. (Optional) Follow the instructions in the section **How to Check Your Role Status** (page 97) to determine the status of your SAAR in the approval process.

Figure 120: Confirmation

Note:

Initially, the SAAR goes to the Supervisor for approval, unless the customer's organization requires a prior Segregation of Duties (SOD) review of this role request type.

How to Request a Role: External User

DLA and DFAS offer application access to various types of external users. These user types are provided to identify users who are not employed by DLA or DFAS but who require some kind of limited access to computer applications offered and maintained by these organizations. External users include the following user types, which are subject to the specified requirements and characteristics:

- **Military:** An external user who is required to supply contact information for an External Security Officer and an External Supervisor. Persons with this user type are assigned to an external organization.

- **Civilian:** An external user who is required to supply contact information for an External Security Officer and an External Supervisor. Persons with this user type are assigned to an external organization.

- **Contractor:** An external user who is required to supply contact information for an External Security Officer and an External Supervisor. Persons with this user type are assigned to an external organization.

- **Vendor:** An external user who is a DLA or DFAS vendor. Persons with this user type are assigned to an external organization. This user type is not modifiable in the user's profile. Vendors do not have to supply name and contact information for an External Security Officer or External Supervisor.

- **Public:** An external user who is a member of the public interested in information about goods available to the public. This user type is not modifiable in the user's profile. Members of the public do not have to supply name and contact information for an External Security Officer or External Supervisor.

Note:

Your external approvers must be three separate and distinct individuals with different email addresses.

1. Log in to AMPS.

   *AMPS displays the **Self Service Home** page. Your ID is displayed to indicate you are the currently logged-in user.*

2. On the **Self Service Home** page, click the **Request Role** tile.

   *The first time you request a role in the current session, AMPS displays the **Privacy Act Statement** appropriate for your organization (see Appendix A). Click the **Accept** button to proceed.*

   *AMPS opens the **Request Role** tab, beginning with the **User Information** screen (see Figure 122).*
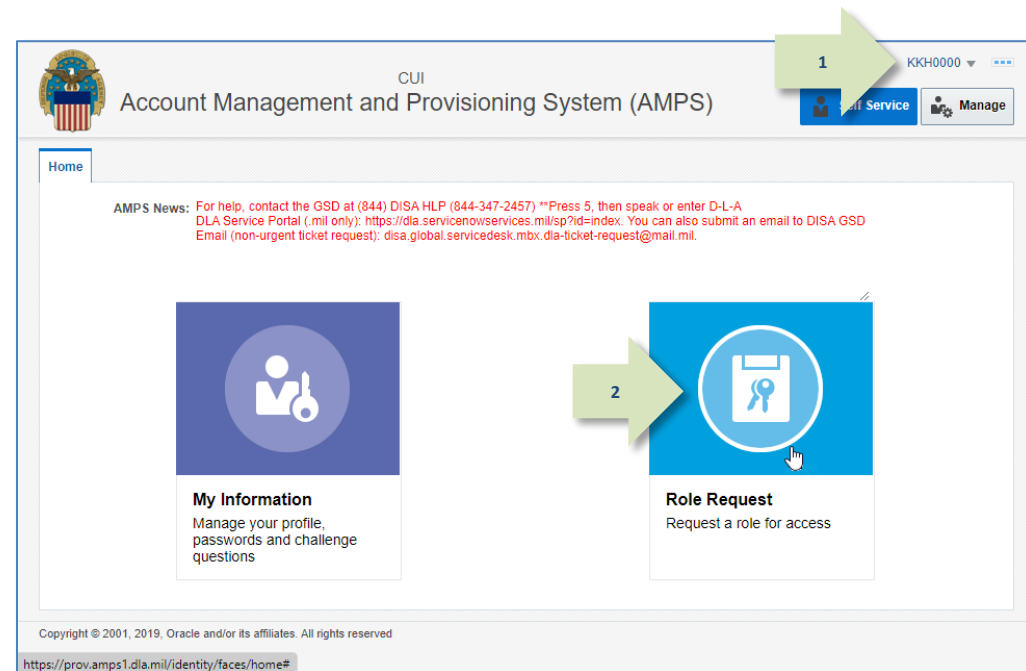
Figure 121: AMPS Self Service Home Page – Role Request Tile

3. Complete all required fields, including your latest **Cyber Awareness Certification Date.**

   The Cyber Awareness Certification Date must fall within the previous 12 months. If it does not, AMPS displays an error message.

4. You no longer need to enter your Date of Birth.

   AMPS does not save or store the date of birth for any user.

   NOTE: External users who authenticate their access identity with a user ID and password no longer need to enter the Social Security Number (SSN) when an SSN field is displayed.

   These data are no longer collected by AMPS.

   Where these data fields are present, they will display non-editable faux data.

5. Select your **User Type** and values for the additional user type fields from the following choices (required):

   a. **Civilian**: select your **Grade** in the field displayed when you select this user type (required).

   b. **Military**: select **Branch** and **Rank** from the fields displayed when you select this user type (see Figure 123).

   c. **Contractor**: enter **Contract Number**, **Contract Company**, and **Contract Expiration** date in the fields displayed when you select this user type (see Figure 123).

6. Update **Contact Information** as needed to ensure required fields are completed.

7. Update your **External Supervisor** email address, as needed.

8. Update your **External Security Officer** email, as needed.

9. Update your **External Authorizing Official** email, as needed.

10. Click the **Next** button to proceed. It is located beside the **Cancel** button.

Figure 122: Request Role - User Information

Figure 123: User Type Samples - Military and Contractor

AMPS Displays the Select Roles Screen

The **Select Roles** screen features two methods for locating a particular role name: **Search** and **Browse**.

The following procedure tells you how to use the **Search** method to find a role name. To browse for a role, see the section entitled **How to Browse for a Role**.

11. In the **Search Roles** section, enter all or part of any search criteria you have available.

    For example, if you have the role name, you can enter part of the name in the **Role Name** *field.*

12. Click the **Search** button.

    AMPS displays the names of all roles having a name or other criteria that match the **Search** *string.*

13. Locate the role you want to request in the **Select a Role / Role Name** panel:

    To verify your choice, click the Expand button (▷) to display details about the role.

14. Select the role and click the right arrow (→) button, also known as the Add button.

    AMPS copies the role name to the **Select Roles** *list panel on the right.*

    To request multiple roles, repeat steps 12 through 15 if you do not require, or already have, a primary role.

15. Click the **Next** button to proceed. It is located beside the **Back** button.

Figure 124: Request Role - Select Roles

AMPS Displays the Justification Screen

The Justification screen requires you to enter complete reasoning for requesting the current role. Ensure your comments are complete, or an approver may reject your request for lack of justification. You can also enter more information in the Optional Information text area, and attach as many as three PDF files to support your request.

16. In the **Justification** screen, fill in the following information:

    a. Enter comments in the Justification text area to clarify the request (required). Note that the request may be rejected if the justification entered is inadequate. Contact your Supervisor if you have questions.

    b. As an option, you can enter further comments in the **Optional Information** text area to supply additional information that supports your request.

Note:

Comments and file name shown in the sample screen are for illustration purposes only. Please enter information relevant to each specific request.

*Attachments are NOT required. Each attachment must be formatted as an Adobe Portable Document Format (PDF) file of two megabytes or less in size. **You must not attach any file containing Personally Identifiable Information (PII).***

Roles with Additional Attributes
Some roles require or request additional attributes, such as a **DoDAAC** *number or* **ACID** *code, from the requestor during a role request.* AMPS displays an additional section, called **Role Attributes**, on the **Justification** screen for each role that calls for additional attributes. (*See Figure 126 for an example*).

Figure 125: Request Role – Justification

Figure 126: Request Role - Justification - Role Attributes Sample

17. As an option, you can click the **Browse** button next to any of the three **Attachment** fields to locate and attach a supporting document. Repeat this procedure to attach an additional two documents, as needed.

18. Click the **Next** button to proceed. It is located beside the **Back** button (see Figure 126).

    *AMPS saves the **Justification** information and any additional **Role Attributes** data, and displays the **Summary** screen (see Figure 127).*

AMPS Displays the Summary Screen.

19. Review the information in the **Summary** screen.
    - Click the **Back** button, beside the **Cancel** button, to return to previous screens and make corrections, as needed.
    - After making corrections, click the **Next** button or the **Summary** node in the train to return to the **Summary** screen.

20. Click the **Submit button** to complete the role request. It is located beside the **Back** button.

Note:

Click the **Cancel** button to discard this request and start again, as needed.

Figure 127: Request Role – Summary

AMPS Submits the Role Request for Approval.

21. Note that the SAAR number is listed here on the **Role Request Confirmation**, along with role name and status information on the **Role Request Confirmation** screen.

    Your status notifications and **Pending Requests** *records on the* **Applications & Roles** *screen refer to the SAAR number.*

21

Role Request Confirmation
Your request has been submitted for approval. The following SAARs have been created:

SAAR   Role
106086 DFAS DJMS Navy Prod - Navy Input User Field DJMSNAV-007

AMPS will notify you by email message regarding the status of each SAAR.

If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

22. Click the **OK** button on the **Confirmation** screen.

22   [OK]
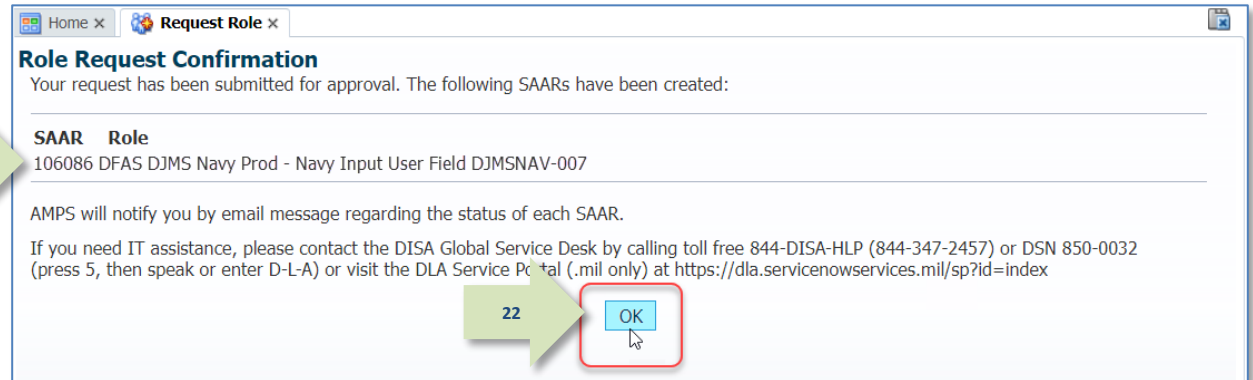
Figure 128: Confirmation

23. (Optional) Follow the instructions in the section **How to Check Your Role Status** (page 97) to determine the status of your SAAR in the approval process.

Note:

Initially, the SAAR goes to the External Supervisor for approval.

Role Request Subprocesses

How to Update Your Organization: Internal Users Only

What you can do:	Your Organization assignment affects the list of roles that appear in the **Select Roles** screen during a role request. DLA users, for example, see only DLA roles, while DFAS users see only DFAS roles. Lists of roles are further delimited by the sub-organization you select. If your Organization is incorrect, use this procedure to find and select the name of the correct Organization. When you submit the completed role request, AMPS saves the updated information to your profile and directs your role request to the correct Security Officers and Information Assurance Officers.
Where to start:	Begin the process of creating a role request and start on the **User Information** screen.

Role Request: Find the *Update Organization* Command.

1. Click the **Update Organization** command on the **User Information** screen.

    *AMPS displays the **Find an Organization** dialog (see Figure 130).*

Figure 129: User Information - Update Organization

2. Enter all or part of an **Organization** name in the **Organization Name** field.

3. Click **Search**.

    AMPS displays matching Organization names in the search results list (see Figure 130).

4. Select the name you want to use from the **Organization** section.

5. Click **OK**.

    *AMPS enters the selected name and corresponding information in the **Organization Information** section of the Role Request's **User Information** screen (see Figure 131).*

Figure 130: Select Organization – Search

6. Review the **Organization** update and proceed with the role request.

*When you update the **Organization**, AMPS automatically identifies the updated organization name and populates the **Security Officer** and **IA Officer** fields with the names of the current organization's Security Officers and IAOs.*

Figure 131: Select Organization - Search Results

How to Update Your AMPS Supervisor – Internal Users

What you can do:	Follow this procedure if you are a user submitting a new role request and you need to correct your AMPS Supervisor. AMPS updates this information in your profile. The following business rules apply to the process of selecting an AMPS Supervisor:

- **Every Organization must have one or more AMPS Supervisors** to handle role request approvals for their users.
- **Each user who requests a role must have an AMPS Supervisor.** Use the **Update Supervisor** function to select an AMPS Supervisor if the **Supervisor** area is blank.
- **Internal users can select only another internal user as an AMPS Supervisor.**
- **A user cannot select a contractor as an AMPS Supervisor**. Only government employees can be Supervisors in AMPS. AMPS controls the selection process by restricting the display of Supervisor names to government employees, either Civilian or Military.
- **A user can select an internal user from another Organization as a Supervisor**.
- **All AMPS Supervisors must request and be granted the AMPS Supervisor role**. However, a user can select a user who does not have the Supervisor role. An AMPS Supervisor who does not have the appropriate role sees a message in the **Pending Approvals** list under the **My Tasks** tab for the SAAR that awaits an approval. The message advises the Supervisor to request the AMPS Supervisor role in order to address and complete any role request approval action.

Where to start:	Begin the process of creating a role and start on the **User Information** screen.

Locate the *Update Supervisor* Command on the *User Information* Screen.

1. Click **Update Supervisor**.

   *AMPS displays the **Find a Supervisor** dialog (see Figure 133).*

Figure 132: User Information - Update Supervisor Command

2. Enter all or part of any one or more of the following search criteria:

   a. First Name,

   b. Last Name, or

   c. User ID

3. Click **Search.**

   AMPS displays matching names in the search results area (see Figure 134).

Figure 133: Find a Supervisor – Search Criteria

4. Click the name you want from the search results.

5. Click **OK**.

   *AMPS enters the selected name and corresponding information in the **Supervisor** section of the role request's **User Information** screen (see Figure 135).*

Figure 134: Supervisor Search Results

6. Review the Supervisor Information section to ensure you selected the correct supervisor.

    See the section on **How to Update the Supervisor: Internal Users Only** *for instructions on updating your Supervisor information through* **My Information***.*

    When you complete the role request procedure, AMPS will update your profile with the new Supervisor's information and notify the new Supervisor of all your "in-flight" SAARs that require his or her approval.

    Proceed with the role request for the selected user.

Figure 135: User Information - Supervisor Updated

How to Browse for a Role

What you can do:	Follow this procedure if you are browsing for a role name, rather than using the **Search** function.
	Follow this procedure if you are a **Supervisor** submitting a new role request for a subordinate and you want to browse for a role, rather than use the **Search** function.
Where to start:	Begin the process of creating a role, starting on the **User Information** screen, and navigate to the **Select Roles** screen.

1. In the **Select Roles** screen's **Browse Roles by Application** section, expand the application category that contains your application name.

   AMPS displays the names of all roles associated with the category in the Select a Role area.

2. Select your application.

   AMPS displays all roles associated with the application in the Select a Role area.

3. Locate the role you want to request.

   a. To verify your choice, click the **Expand** button (▷) to display details about the role.

   b. If you select an **Additional** role without first selecting a related **Primary** role, AMPS displays an error message.

4. Select the role and click the right arrow (→) button. AMPS copies the role name to the **Select Roles** list panel on the right.

5. To request multiple roles, repeat steps 1 through 4 (not shown). (EBS users must have an application-specific primary role assigned before proceeding.)

6. Click **Next** to proceed with your role request.
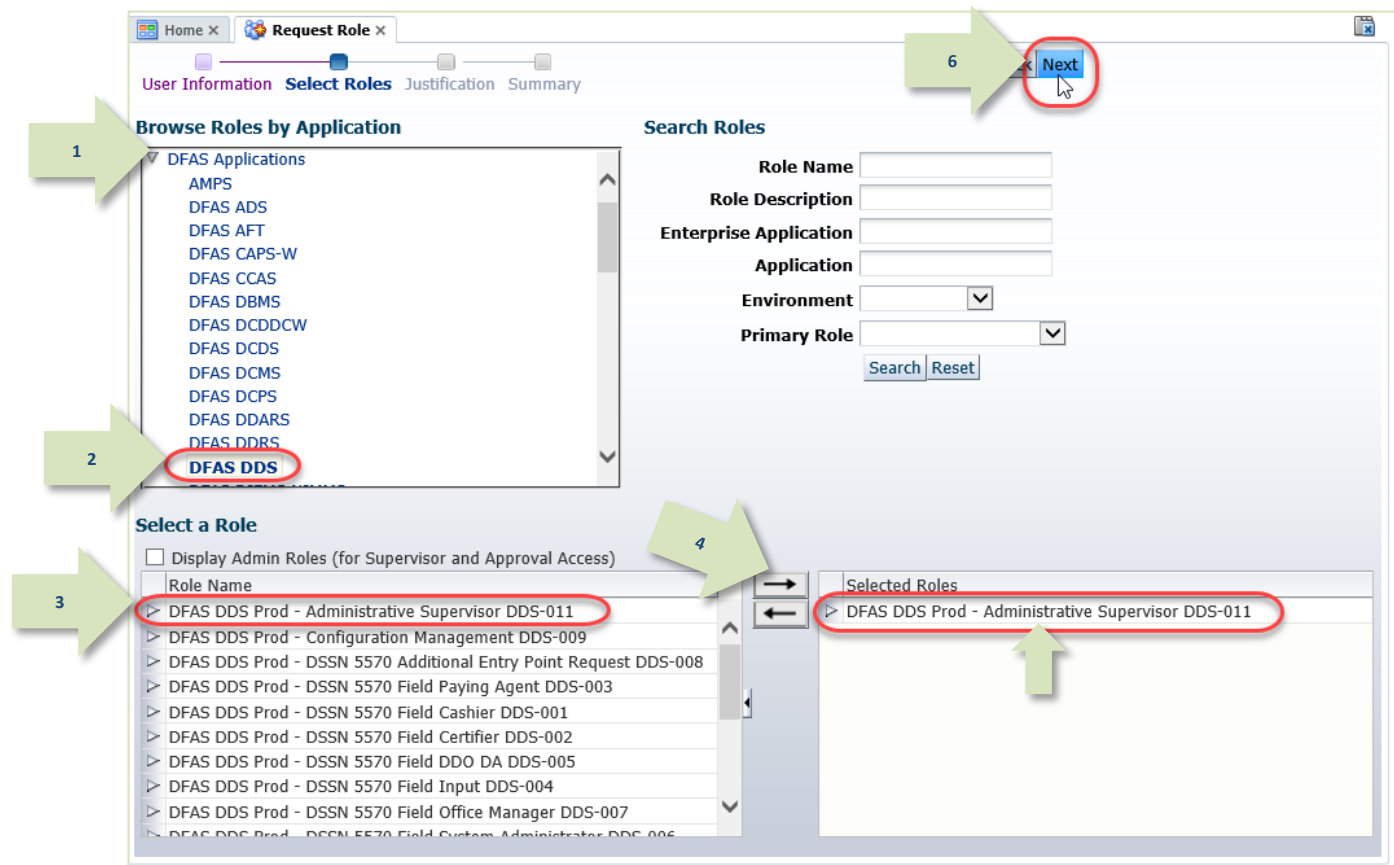
Figure 136: Request Role Select Roles

How to Cancel a Request: End User

What you can do:	Follow this procedure if you have submitted a role request, and you need to cancel the request. Reasons for cancelling a request vary, but often the problem is requesting the wrong role. You can cancel an existing request during the approval phase only. During the provisioning phase, the status field indicates the request is "TICKETED" and you cannot cancel the request through the AMPS interface. After a provisioner has provisioned your account, you must request a role removal (see page 286 for information on role removal).
Where to start:	Obtain the SAAR number for the request you want to cancel. Check your email notifications to obtain the SAAR number or find the SAAR on your **Pending Requests** table. This table is located on the **Applications & Roles** tab of the **My Information** screen. You may start the **Cancel Request** procedure on this screen.

1. Check your AMPS email notification to obtain the SAAR number for the request you want to cancel.

   The text of the sample email at right is provided to illustrate email formatting only.

   1
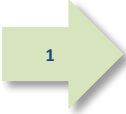
Sample User Notification: Confirmation

Subject: Notification: SAAR #106074 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DFAS SABRS) 09/12/2017 16:19:11 EDT

Body: Your request for role DFAS SABRS Prod - ADHOC w/o Cmd Line SABRS-005, with access to DFAS SABRS, SAAR 106074 has been submitted for approval.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2. Launch AMPS and open the **Applications & Roles** tab of the **My Information** screen.

   Each role request is submitted as a SAAR with an assigned SAAR number.

   *SAARs moving through the approval workflow are listed in the **Pending Requests** table with their current status.*

Figure 137: Applications & Roles - Pending Requests

3. In **Pending Requests**, select the SAAR you want to cancel.

Figure 138: Pending Requests - Select a SAAR

4. Click the **Cancel Request** button.

   AMPS displays a confirmation message (see Figure 140).

Figure 139: Pending Requests - Cancel Request Button

5. Click the **Yes** button to confirm the cancellation request.

AMPS displays an information message confirming the SAAR has been cancelled (see Figure 141).
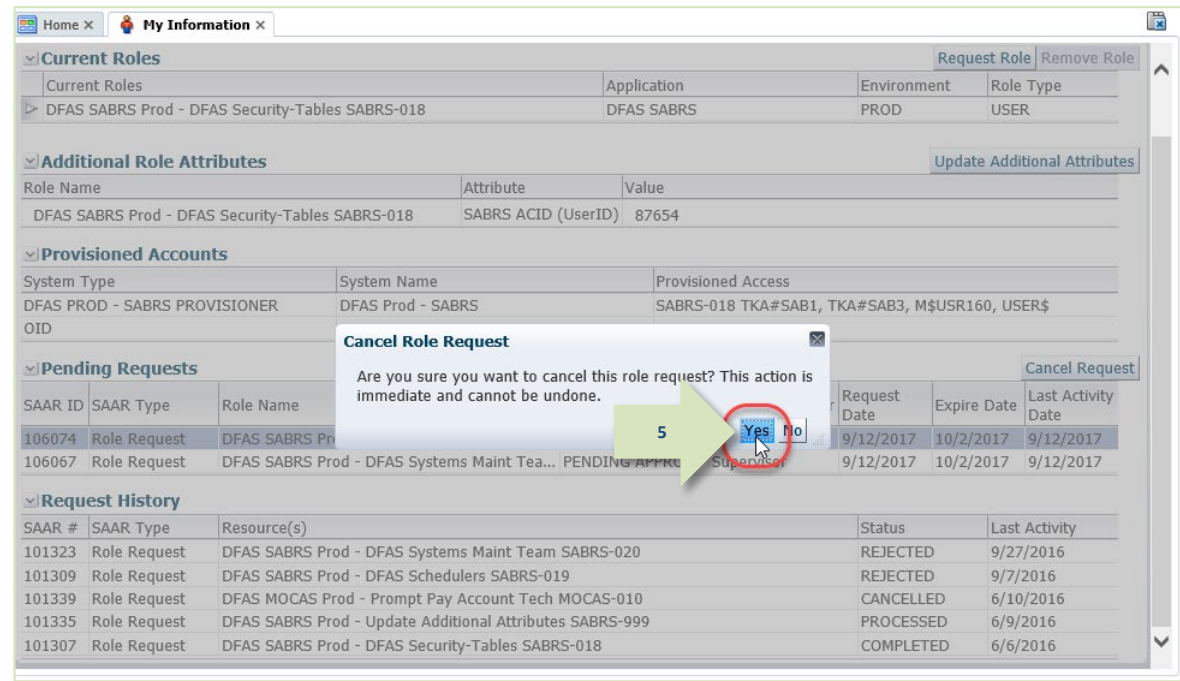
Figure 140: Message - Confirm Cancel Role Request

6. Click the **OK** button to close the **Information** message box.

*AMPS removes the cancelled SAAR from the **Pending Requests** table and adds a record for the SAAR to the **SAAR History** table. The status of the SAAR is changed to **CANCELLED**.*
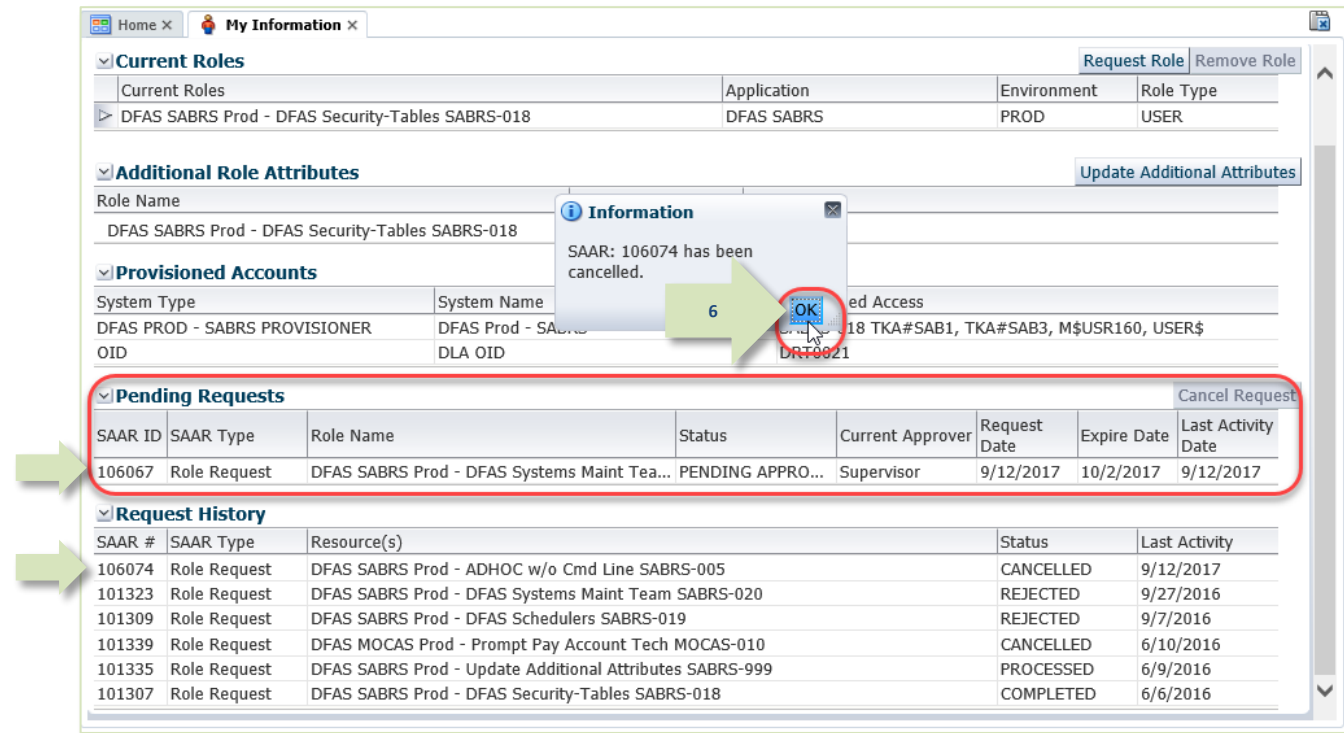
Figure 141: Role Request Cancelled

Role Request Approval Process

AMPS handles notifications and the role request approval process by supporting approval business processes that are followed by the DLA and DFAS user communities. These business processes include the submission of requests for roles that provide access to computer applications maintained by various organizations. To initiate the role request process, the user logs in to AMPS, completes several online screens, and submits the data in those screens to the AMPS SAAR approval process.

At that stage, AMPS automatically creates and numbers a SAAR, and forwards the SAAR to a sequence of approvers who have been assigned the appropriate AMPS administrative roles authorizing them to approve or deny requests. If the data warrants approving the request, the approvers approve the request in sequence, from the Supervisor to the Security Officer to the Data Owner, and—in the case of DFAS applications—concluding with the Information Assurance Officer. Additional approvers—such as a Segregation of Duties Reviewer or External Authorizing Official—may also be required for some roles.

The only exceptions in the DLA application standard sequence occurs when AMPS determines that conditions warrant a Security Officer bypass or an automatic approval. A Security Officer bypass may be set by Security Officers on an as-needed basis for individual users. An automated approval, however, must meet certain conditions, each of which is outlined in the Security Officer sections located throughout SO approval sections in this User Guide. Starting with AMPS Release 17.1.2, DLA requests for IT3 roles do not require a Security Officer approval.

In the default setup of user security clearance information, the Security Officer sees only the first role request from a user until the user's account is submitted for revalidation or is otherwise flagged for the Security Officer's attention. Additional requests or any request for an IT3 roles by DLA users bypass the Security Officer unless the flag for review is reset (see Figure 183 for an example). The Security Officer bypass ensures that Security Officers are not inundated with multiple role requests that require the same data entries already set in a previous approval process. The Security flag, on the other hand, ensures that a Security Officer can cancel the bypass function in the case of a user whose record must be reviewed continually or out of the normal sequence.

To receive an automatic approval, a role request must generally meet certain criteria:

- The IT level of the requested role cannot exceed the current IT level of the user.
- The user must have a value recorded for the four clearance-related fields that AMPS tracks, including the following fields:
  - Security Clearance
  - IT Level, or Position Sensitivity
  - Background Investigation Type
  - Last Investigation Date
- The user's record must not be flagged for review by a Security Officer (for an example, see Figure 183).
- The user's recorded IT level satisfies one of the following conditions:

- If the user's IT level is IT1 or IT2, the date of the user's investigation must be less than 5 years old, or . . .
- If the user's IT level is IT3, the date of the user's investigation must be less than 10 years old.
- The user is a member of the DLA organization or any organization under DLA.

All approvers receive email notifications, which AMPS automatically sends to their official email addresses. Each approver has 20 days to act before a role request expires. AMPS sends reminder email messages to each approver every day until the approver completes an action on the request. AMPS handles the sequential submission for approval to each approver automatically, and then submits the approved request for provisioning.

Approver Roles

The following AMPS administrative personnel are part of most approval workflows. Each of the approvers who have AMPS accounts must have specific administrative roles assigned to their accounts to ensure that AMPS can send role requests to the appropriate approvers. External approvers for external users do not require these roles, as noted in the following list. This list identifies administrative roles that each optional or standard approver must be assigned in AMPS:

Approver	AMPS Role
SOD Reviewer (optional)	SOD Reviewer role defined for the reviewer's organization (additional approver).
Supervisor	AMPS Supervisor, required only for internal users. External Supervisors do not require the AMPS Supervisor role.
Security Officer	Security Officer role defined for the organization (standard approver except for IT3 role requests in DLA applications, which do not require SO review). External Security Officers do not require an organizational Security Officer role.
Data Owner	Data Owner role defined for the resource (standard approver).
Information Assurance Officer	IAO Approver role defined for an organization (standard approver for DFAS or customers other than DLA applications).
External Authorizing Official (external users)	The EAO does not have an AMPS account, and therefore does not require an AMPS role to perform approvals for external role requests.

External Approvals: Authentication Rules and Practices

The approval process for external user requests has one significant variance from the process implemented for internal users: the requests of external users are submitted for approval to their external Supervisors and external Security Officers whom the users themselves identify and for whom the users provide an email address. The external users themselves must identify their assigned Supervisor and Security Officer during their account setup. Unlike internal approvers who must log in to AMPS and present authentication credentials, external approvers get access to online approval forms through a separate module that is external to AMPS itself.

As a consequence, neither the external Supervisor nor the external Security Officer must have an account set up in AMPS, and no standard authentication credentials to AMPS at login are required. Instead, the external approval process for these two approvers occurs outside the AMPS application in a separate module. The module sends the approval information it collects to AMPS where the system forwards the approval request to the role application Data Owner, the next approver in the role request approval process.

Rather than presenting AMPS credentials, the external approvers authenticate to the external approval module instead. This authentication process ensures a secure process by preventing external users from approving their own requests and by preventing the same user from applying approvals in multiple stages. In other words, a user cannot be his or her own Supervisor or Security Officer. The requesting user and the two approvers must be three distinct individuals. Please see Appendix G or the External Approver Guide for detailed information about approver authentication.

Authentication Rules

Rule	Description
Approver setup in AMPS	When an external user registers for an account in AMPS, he or she also identifies an external security officer and an external supervisor. The user is responsible for updating the contact information through the **My Profile>My Information** screen.
CAC-enabled external approver	An external security officer or supervisor who logs in to the External Approval Portal with a CAC or other smart card supported by AMPS requires the approver to use the CAC or smart card for all subsequent approvals.
Non-CAC-enabled external approvers	For external approvers who do not use a CAC or other smart card, AMPS captures the approver's email address. The user and approver are responsible for maintaining the accuracy of their contact information (see Procedure for External Supervisor Approvals for an example).

Supervisors: Internal Users

AMPS requires each user to have an AMPS Supervisor identified and assigned to the user's account. The Supervisor reviews the user's role request and determines whether or not the requestor has chosen the correct role for the completion of related application tasks. If not, the Supervisor can reject the user's request and advise the user on how to proceed with a correct request, if necessary.

Unlike the case with other approver roles, a user has only one AMPS Supervisor. This Supervisor must request and obtain the **AMPS Supervisor** role before he or she can administer role request approvals (see **How to Request the AMPS Supervisor Role**).

Note:

For quick instructions on obtaining the AMPS Supervisor Role, see *AMPS Snapshot: Request the AMPS Supervisor Role*. This document is available from the AMPS Help screen.

Supervisor Setup in AMPS

During the setup of administrative roles, each organization and sub-organization must determine who has the highest Supervisory level. This determination is required because of the hierarchical nature of the supervisory structure in AMPS. That is, each user must have a Supervisor, these Supervisors must also have Supervisors, and so on up the hierarchy. However, the final responsibility must rest with the appropriate person in the Supervisor hierarchy. In each case, this person is assigned a Supervisor role by a system administrator, without a requirement for a Supervisor to be assigned to his or her account.

Supervisors: External Users

All external users, except members of the public, must identify an External Supervisor in AMPS. This Supervisor does not require an AMPS account or the AMPS Supervisor role to perform the duties of an External Supervisor. However, an External Supervisor must supply contact information, through the external user, to ensure he or she receives email notifications of role request approvals.

Note that an external user cannot identify himself or herself as the user's External Supervisor; AMPS business rules prevent users from approving their own role requests.

An external user in one of the following categories must identify email address for an External Supervisor:

- Military
- Civilian
- Contractor

The External Supervisor must supply the following information through the External Approval Portal (EAP) when AMPS assigns an approval task:

- First Name
- Last Name
- Telephone Number

When an external user in one of the specified categories requests a role, AMPS sends an email notification to the External Supervisor advising the supervisor of an action required in AMPS. The notification includes a URL that, when entered in a browser instance, takes the supervisor directly to an AMPS work queue containing links to requests that require action.

The section on how to approve an external role request explains the procedure an External Supervisor uses for approving or rejecting a role request from an external user.

Security Officers: Internal and External SO Review Requirements

The DLA has altered requirements for Security Officer reviews in an effort to streamline DLA role request processes while maintaining the appropriate security safeguards. Some requests do not require a Security Officer review, while others can be automatically approved. Still other requests do require a Security Officer review. Moreover, conditions differ according to whether the user is a DLA user or a DFAS user.

As a quick reference, the following table summarizes the conditions that apply for each of these review scenarios:

Scenario	Security Officer Review Requirement
A DLA user requests a DLA IT3 role.	SO review is not required.
A DLA user requests a DFAS IT3 role.	SO review is not required.
A DFAS user requests a DFAS IT2 role.	SO review from a DFAS Security Officer is required.
A DFAS user requests a DLA IT3 role.	SO review from a DFAS Security Officer is required.
An external user requests a DLA or DFAS IT3 role	External SO review is required.

The following sections provide more detailed descriptions of various scenarios to explain how and when Security Officer reviews are either bypassed, automatically approved, or required.

Security Officer: Internal Users

The Security Officer is responsible for ensuring that the role requestor's clearance level meets or exceeds the requirement as defined in the requested role. The Security Officer can reject a role request if security standards are not met. The Security Officer is advised in email messages of each initial request for a role submitted by a user. After conducting a security review and entering the required data, the Security Officer can approve the request.

The Security Officer who reviews each user's requests is part of a group that is assigned within the user's organization. A user's organization has multiple Security Officers, all of whom receive role request email notifications forwarded by AMPS to their official email addresses. However, a role request needs the review and approval of only one SO.

Not all DLA role requests require a Security Officer review. See the following sections to understand when AMPS does not require a Security Officer review is not required and when AMPS can apply an automatic approval.

Security Officer Approval: Not Required for IT3 Roles

In specific circumstances, a Security Officer review is not required in certain role requests or role extension requests. If the role or extension request meets the following criteria, a Security Officer review is not required:

- The IT level of the role is IT3.
- The user who requests the role or role extension is a DLA user.

Note: for DLA User Requests · · ·

For a case in which a DLA user's security information is incomplete in AMPS and the role specified in an original request or an extension request is also IT3, AMPS does not require completion of security clearance information fields.

Email Notifications

AMPS does not send approval stage email notifications to a user when a Security Officer review is not required.

Audit Log Entries

When a Security Officer is not required, AMPS captures and stores the following information in audit logs:

- The Security Officer's approver ID is not recorded in the audit logs. That is, the entry is blank.
- The Status recorded in the audit logs is "NOT REQUIRED."
- The comment in the audit logs states, "Security Officer approval for DLA user requesting an IT3 role is not required."

Automatic Security Officer Approvals

AMPS can apply an automatic Security Officer approval to a role request, role expiry request, or role extension request that meets specific criteria. The automatic approval speeds the approval process for role requests that present no specific content requiring an immediate security review.

For role requests, role expiries or extensions, and attribute change requests, AMPS can automatically apply an approval for a Security Officer, if all of the following conditions are met:

- The requesting user is a DLA user.
- The IT level of the requested role is IT1 or IT2. This condition applies to DLA and DFAS roles available to DLA users.
- The user has an IT level of IT1 or IT2 and the most recent Investigation Date is less than five years old.
- The IT level of the requested role does not exceed the current IT level of the user.

- The user has a value recorded for the four clearance-related fields that AMPS stores, including the following fields:
  - Security Clearance
  - IT Level or Position Sensitivity
  - Background Investigation Type
  - Last Investigation Date
- The user is not flagged for review by a Security Officer.

Email Notifications

After a user submits a role request that receives an automatic Security Officer approval, the next email notification a user receives is either the next step in the process or the final email notification if the automated approval is the last step in the process.

Audit Log Entries

When an automatic approval occurs, AMPS logs the automatic approval with the following data:

- The approver's user ID, normally reported in the audit logs, will be blank.
- The Status recorded in the audit logs will be "AUTOAPPROVE."
- The audit log comment contains the following statement: "This request has been automatically approved by AMPS, per the conditions specified by the DLA CIO (the Designated Approving Authority [DAA]) per the DLA Account Management Policy - Signed 6 Nov 2014."

Note:

AMPS reports all date and time stamps in the audit log in Coordinated Universal Time (UTC).

Security Officer: External Users

All external users, except members of the public, must identify an External Security Officer in AMPS. This Security Officer does not require an AMPS account or the AMPS Security Officer role to perform the duties of an External Security Officer. However, the external user must provide an email address for the External Security Officer during new user registration to ensure he or she receives email notifications of role request approvals.

Note that an external user cannot identify himself as his own External Security Officer; AMPS business rules prevent users from approving their own role requests.

An external user in one of the following categories must identify the email address for an External Security Officer:

- Military
- Civilian
- Contractor

The External Security Officer must supply the following information through the External Approval Portal (EAP) when AMPS assigns an approval task:

- First Name
- Last Name
- Telephone Number

When an external user in one of the specified categories requests a role, AMPS sends an email notification to the External Supervisor advising the supervisor of an action required in AMPS. After the External Supervisor approves the role request, AMPS moves the role request to an EAP work queue specifically set up for the External Security Officer. Then, AMPS sends an email notification to the External Security Officer advising the Security Officer of an action required in AMPS. The notification includes a URL that, when entered in a browser instance, takes the Security Officer directly to the EAP work queue containing links to requests that require action.

The section on how to approve an external role request explains the procedure an External Security Officer uses for approving or rejecting a role request from an external user.

Data Owner (DO)

The Data Owner is responsible for reviewing the request of a role associated with an application. Because each role is associated with a specific application and role-owning organization, requests for these roles are submitted to the Data Owners associated with the same application and role-owning organization. One of the Data Owners reviews and either approves or rejects requests for these roles.

An organization may have multiple Data Owners, all of whom receive role request email notifications forwarded by AMPS to their official email addresses. However, a role request needs the review and approval of only one Data Owner. In addition, Data Owners handle all requests from users, internal or external.

Information Assurance Officer (IAO)

No IAO review is required for DLA systems, but some AMPS customers, such as DFAS, employ an IAO for approvals. The primary responsibility of the Information Assurance Officer is to verify the requestor's compliance with Department of Defense information assurance training initiatives, now called *Cyber Awareness Training*. When a group of IAOs receive notification of a DFAS or external role request SAAR, an IAO opens the SAAR, verifies the entry of the user's Cyber Awareness Certification Date and ensures the date is the most recent date and that it is accurate. The IAO may check other details in the SAAR, but the Cyber Awareness Training Certification Date is the data AMPS requires for approval of a SAAR by the IAO.

An organization that employs IAO approval has multiple IAOs, all of whom receive role request email notifications forwarded by AMPS to their official email addresses. However, a role request needs the review and approval of only one IAO. In addition, IAOs handle all requests from users, internal or external.

Additional Organization- or Application-Specific Roles

Some organizations or application owners have specific additions to the approval process. In the current version of the system, the additional approver added most often is a Segregation of Duties (SOD) Reviewer.

SOD Reviewer

Some roles are set up in AMPS with a requirement for an additional reviewer who checks for conflicts of interest between a newly requested role and existing role assignments. This additional reviewer is the first in the approval sequence to see a role request. If a conflict between a requested role and a current role exists, the SOD Reviewer enters an explanation of the conflict and completes the review. After SOD Review completion, AMPS forwards the role request to the requestor's Supervisor and subsequent approvers, each of whom can reject the role request based on the conflict of interest noted by SOD Reviewer.

External Authorizing Official (EAO)

A number of roles available to external users require an extra approver called an "External Authorizing Official" or "EAO." External users identify an EAO with an email address entry in the user's **My Information** screen or during a role request.

Top-level Manager Roles

AMPS also provides a top-level role, called a "Manager" role. A Manager role serves a particular purpose in the overall approval process. In the majority of cases, a role request proceeds through the steps described in the Approval Process Summary section, and each request is reviewed by a predefined approver in prescribed approval stages. These approvers are identified in AMPS as users who have been assigned specific roles, such as Security Officer or Role Data Owner.

However, if a staff member is not assigned to the appropriate approver role to receive role requests for action, AMPS must have a way to redirect role requests to a contingent approver with an appropriate role. This contingent approver role is called a Manager role. **For example:** A DFAS user requests the Prompt Pay 101 role, AMPS forwards the request to the SOD Reviewer. After the SOD Reviewer completes the assessment and submits a recommendation as a part of the completion of the review, AMPS sends the role request to the requestor's AMPS Supervisor.

After the Supervisor approves the request, AMPS sends the request to the organizational Security Officer. After the SO approves the request, AMPS sends the request to the Prompt Pay 101 Data Owner for approval. This Data Owner should be predefined and assigned the appropriate Data Owner role in order to receive AMPS notifications and exercise the authority to administer approvals.

If no staff member has been assigned to Prompt Pay 101 Data Owner role, for whatever reason, AMPS sends the request to the Prompt Pay 101 Data Owner Manager for approval. That person has two responsibilities:

- Approve or deny the request.
- Find out why the request came to the Data Owner Manager, rather than a Data Owner associated specifically with that role.

To correct the situation and ensure that AMPS can forward role requests for Prompt Pay 101 to the appropriate Prompt Pay 101 Data Owner, the Data Owner Manager makes sure that one or more staff members, with the appropriate responsibilities and credentials, requests and receives the Prompt Pay 101 Data Owner role.

When staff members receive the Prompt Pay 101 Data Owner role, AMPS can direct the approvals for associated Prompt Pay 101 role requests to the correct Data Owner, rather than the Data Owner Manager.

AMPS contingency coverage also includes an SOD Reviewer Manager, a Security Officer Manager, an Information Assurance Manager, and a Provisioner Manager. Staff members who hold these roles have the same type of responsibilities for handling contingent role requests that have no corresponding approvers.

Cross-organizational Role Request Approvals

In the AMPS user community, some users may need access to systems outside their own agency. For example, a DFAS user may need access to a DLA system, or a DLA user may need access to a DFAS system. Typically, users do not have access to roles beyond their own agencies, but the unique relationship between DLA and DFAS requires AMPS to accommodate inter-agency users. Therefore, roles for applications associated with one agency have been published in a way that enables a user from one agency to request one or more roles for applications associated with the other agency.

A cross-organizational request is a role request, including an attribute update request, that meets one of the following criteria:

- A DLA user requests a DFAS role or an attribute update for a DFAS role.
- A DFAS user requests a DLA role or an attribute update for a DLA role.
- An external user requesting any role.

Approval Constraints for Cross-organizational Role Requests

DLA and DFAS have different standard approval paths for role requests. For example, AMPS does not require an approval by an Information Assurance Officer (IAO) from any DLA user who submits a DLA role request. However, DFAS requires IAO approvals for roles providing access to its systems.

Because the two agencies have different rules for handling requests, AMPS first identifies the requesting user's organization—DLA or DFAS—and follows the rules set up for that organization when determining how to direct an approval for a cross-organization request. This organizational distinction excludes external users. These users belong to a single organization called "DLA External," whether they are DFAS or DLA users, and DLA External does not have assigned IAOs to receive approval requests. AMPS determines which organization the role belongs to, and follows the IAO approval rules for that organization.

For a cross-organizational role request, AMPS uses the following criteria to determine which organization has priority in determining the rule set to follow:

- For external users who submit cross-organizational requests . . .
    - o AMPS always routes Security Officer approvals to the user's External Security Officer.

- o AMPS routes approvals to IAOs based on the organization of the role:
    - ▪ For a DFAS role request, AMPS forwards the request to an IAO group for approval.
    - ▪ For a DLA role request, AMPS bypasses the IAO approval stage.
- For internal users who submit cross-organizational requests AMPS determines the role's organization and follows the rules set up for that organization.

Annual Revalidation Requests and Cross-organizational Roles

Starting with AMPS release 17.2.0, DLA internal users are required to submit annual revalidation requests on their specified anniversary dates. DFAS users will be required to submit annual revalidation requests at a later date. Some DLA and DFAS users may hold cross- organizational roles. However, AMPS determines which approval path rules to follow based on the user's organization. Hence, DLA annual revalidation requests follow DLA approval requirements; and DFAS annual revalidation requests will follow DFAS approval requirements.

The following subsections describe how AMPS resolves the differences in approval paths for cross-organizational role requests.

Security Officer (SO) in Cross-organizational Requests

DLA has a more complex set of rules for directing approvals to Security Officers. The aim of these rules is to simplify and streamline the approval procedure by skipping the Security Officer approval step in many circumstances. The AMPS User Guide explains these rules in detail in the section entitled *Security Officers: Internal and External SO Review Requirements*.

These rules are also applicable in cross-organizational requests:

- If a DLA user requests a DFAS IT3 role, SO approval is not required.
- If a DFAS user requests a DLA IT3, IT2, or IT1 role, DFAS requires an SO approval; the approval is performed by a DFAS Security Officer.
- All external user role requests for any DLA or DFAS roles are required to have External Security Officer approval.

Information Assurance Officer (IAO) in Cross-organizational Requests

Per DLA policy, AMPS no longer forwards any type of request to Information Assurance Officers when DLA users submit role requests involving DLA roles. Although DLA no longer requires direct approval of any role request by an Information Security Officer, DFAS approval paths continue to require an approval by an IAO. To resolve the difference in approval requirements, the two agencies have agreed to manage IAO role request approvals for in-organization and cross- organization requests in the following manner:

- If any user requests a DLA Role, AMPS skips the IAO approval step and marks the request approval as not required by an IAO.
- If a DFAS internal user requests a DFAS Role, AMPS assigns the IAO approval to the user's DFAS IAO.
- If a DLA or External user requests a DFAS Role, AMPS assigns the IAO approval to the role's DFAS IAO.

Approval Process Summary

The procedures in this section describe how each approver handles the approval of a role request in AMPS. The procedures include the text of sample email notifications that AMPS sends to users and approvers at each stage of the approval process. Only users who have been assigned one of the AMPS roles identified in Table 1 can follow these procedures. Although the AMPS screens look different, the process is very similar to Legacy AMPS.

In AMPS, the approver . . .

- Receives a notification that an action is required on a role request.
- Logs in to AMPS and navigates to a list of pending tasks.
- Selects the pending task to open the approval decision screen.
- Selects or enters data in required and optional fields.
- Approves, rejects, or cancels the role request.

Table 1 summarizes approvers and their tasks.

Table 1: Role Request Approvers and Provisioners

This Administrator…	Is assigned…	Notes	For more information…
Segregation of Duties (SOD) Reviewer	To your organization.	If a role requires a review to ensure segregation of duties policies are enforced, the SOD Review is defined as part of the role itself. The SOD review provides a point of entry to the approval process for roles that require an SOD check for each role request.	**Users:** • **Segregation of Duties Review** **Segregation of Duties Reviewers:** • **Segregation of Duties Reviewers** • **Segregation of Duties Review**
Supervisor	To your account when the account is created initially.	If a change occurs that is not reflected in AMPS, you can change your Supervisor in AMPS during the role request process. If a SAAR is assigned to Supervisor whose account is Deleted or Disabled, the SAAR is automatically approved and sent to the next approver in the workflow. External users identify a specific External Supervisor in their User Information and can update Supervisor information during a role request.	**Users:** • **How to Update Your AMPS Supervisor** **Supervisors:** • **Supervisor Approval** • **How to Reject a Role** • **How to Suspend a Role Request**
Security Officer	To the Organization to which you belong.	You cannot change this assignment. However, Organizations may have two or more Security Officers assigned. You can identify them during the role request process. External users identify a specific External Security Officer in their User Information and can update the External Security Officer information during a role request.	**Users:** • **How to Request a Role** • **How to Update Organization Information** **Security Officers:** • **Security Officer Approval** • **How to Reject a Role Request** • **How to Suspend a Role Request**
External Authorizing Official (EAO)	To a role request by an external user.	This approver affects only an external user who requests a certain type of role.	**Users:** • **How to Request a Role** **External Authorizing Officials:** • **External Authorizing Official Approval**
Data Owner	To the application associated with the role you are requesting.	Data Owners see all role requests for access to their application data.	**Users:** Ask your Supervisor if you have questions about the Data Owner. **Data Owners:** • **Data Owner Approval** • **How to Reject a Role** • **How to Suspend a Role**
Information Assurance Officer (IAO)	To the Organization to which you belong.	You cannot change this assignment. However, Organizations may have two or more IAOs assigned. You can identify them during the role request process. Some customer applications do not require IAO approval, in which this administrator task is not applicable. DLA systems do not require an IAO review.	**Users:** • **How to Request a Role** **IAOs (not applicable to DLA systems):** • **Information Assurance Officer Approval (applicable only to customers that require IAO administration)** • **How to Reject a Role** • **How to Suspend a Role Request**
Total AMPS Provisioner	To the application associated with the role you are requesting.	In the manual provisioning method, a provisioner creates a user account based on information provided in a Total AMPS ticket or Remedy ticket. In the automated provisioning method, AMPS works directly with the application's system to set up the account.	**Total AMPS Customers, Users, and Provisioners:** • **Provisioning Process: Total AMPS**

External Approvers Authentication Error Messages: CAC Users Only

External users must enter the email addresses of the following three external approvers in his or her My Information profile:

- External Supervisor
- External Security Officer
- External Authorizing Official

Note:

> The external approvers whose email address you enter or update must be three separate and distinct individuals with different email addresses.

Error Message: Non-matching Email Addresses

These addresses are associated with the external user's account and provide a component in the authentication process for external approvers. Some external approvers use a CAC or other smart card to authenticate their identities. CACs and other smart cards store the card owner's authentication data. When an external approver attempts to gain access to a user's request approval screen, AMPS reads and compares this with the information it has stored for the approver. The role of the "Action Required" email message to the approver is key to the authentication process.

This process starts when an external approver receives an email notification indicating that a request has been submitted for approval (see step 1 in the following procedure).

The email instructs the approver to copy and paste the URL from the email message to a browser instance. This URL contains an encrypted copy of the approver's email address, which was provided by the requesting user. AMPS captured and stored this address after the user entered it during registration. The user can also update this information later (see How to Update the Supervisor: External Users Only).

If the email address detected on the approver's smart card does not match the approver email address stored in the requesting user's profile, AMPS displays an error message and prevents the approver from opening the SAAR's approval decision screen.

The first procedure in this section describes the error message that AMPS displays if the system detects a discrepancy between the two email addresses. The instructions in this procedure also explain how to resolve this error.

Error Message: Incorrect CAC Certificate

During the process of opening the External Approval Portal, a smart card-enabled approver may attempt to authenticate with a CAC or other smart card. As part of the process, the system asks the approver to choose a certificate. With the implementation of the DoD's CAC modernization directive in AMPS, CAC-enabled approvers should choose their "Authentication" certificate, also referred to as the "PIV" certificate. If the approver chooses another certificate, the system may display an error message.

If you see this error message, follow the instructions in the procedure to start over and choose the correct certificate. Refer to the second procedure in this section for details on how to resolve this error.

Error Message: Missing Authentication Certificate

During the process of opening the External Approval Portal, a previously authenticated, smart card-enabled approver must authenticate with a certificate selected from their smart card. For CAC users, this should be the "Authentication" certificate. If the approver closes or cancels out or the security dialog without providing their certificate, the system will display an error message.

If you see the error message, follow the instructions in the procedure and restart the process. Select the correct certificate when prompted. See the Missing Authentication Certificate procedure below for more details.

Non-matching Email Addresses

1. Review the email notification requesting an approval action.

   The email provides a URL that leads to the external approver's work list.

2. From the email message, copy and paste the URL into a browser.

Sample External Approver Notification

Subject: Action Required: SAAR #106420 - Request User Access for zoltan zvendor (EZZ0024) (DLA External) (DFAS SABRS) 10/18/2017 07:44:00 EDT

Body: SAAR #106420 - Request User Access for zvendor, zoltan (EZZ0024) (DLA External) has been submitted for approval. This request for DFAS SABRS Prod - MC General User SABRS-001 was submitted in AMPS on 10/18/2017 07:44:00 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=7425%3AN7f3dfitXAVJU%2BYqDo8Sj9j9mBaNeEx%2BDETmlcWxmCQ%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 11/07/2017 06:44:10 EST.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

3. After pasting the URL into the browser's address bar, press **Enter**.

   *The email address stored on your smart card certificate must match the email address in the user's profile (see the user's **My Information** screen).*

   If these email addresses do not match, AMPS displays this error message.
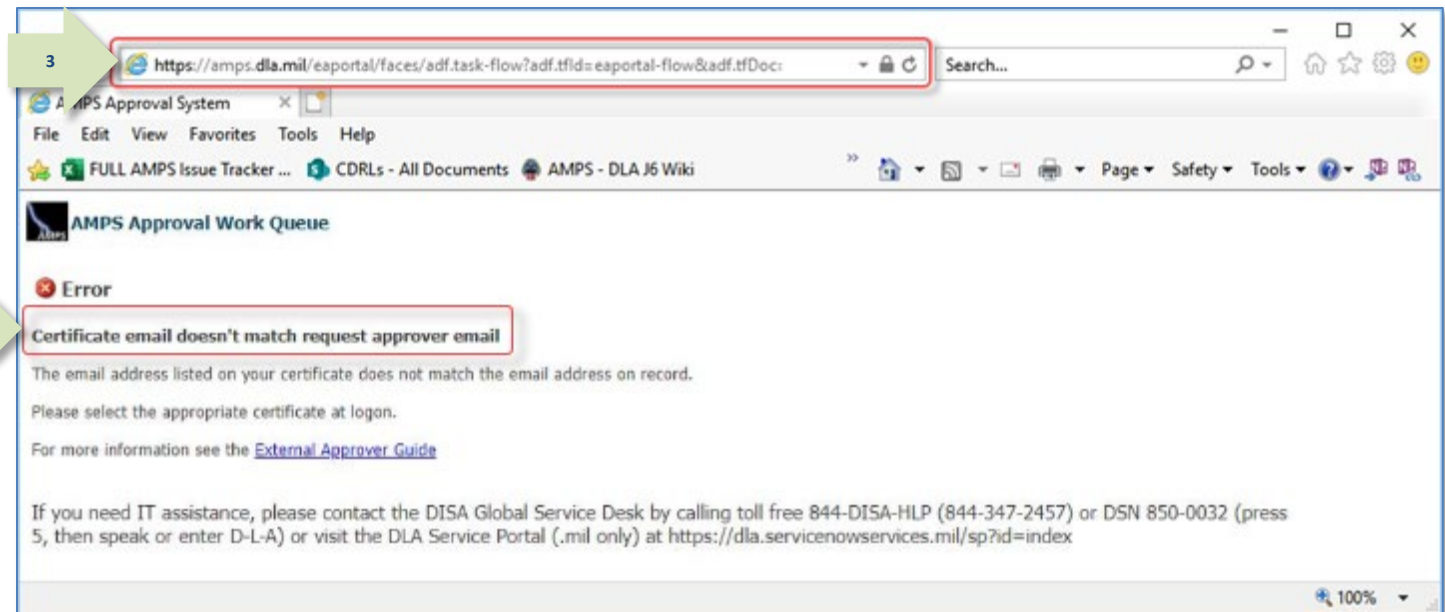
Figure 142: URL Entry and External Approval Work Queue

4. Review the error message and follow the instructions below.

   An email address mismatch may occur if the user changes the approver's address in their profile after the approval task in question was created. It may also be caused by a certificate error. In either case, AMPS blocks access to the approval task.

5. Close your browser.

6. Open a new browser and log in using the URL provided in the email. Be sure you select the appropriate certificate.

7. **Next Steps** (not shown): If, after following the above procedure, you are still unable to access the approval task, call the Service Desk, and report the problem to the Service Desk agent.
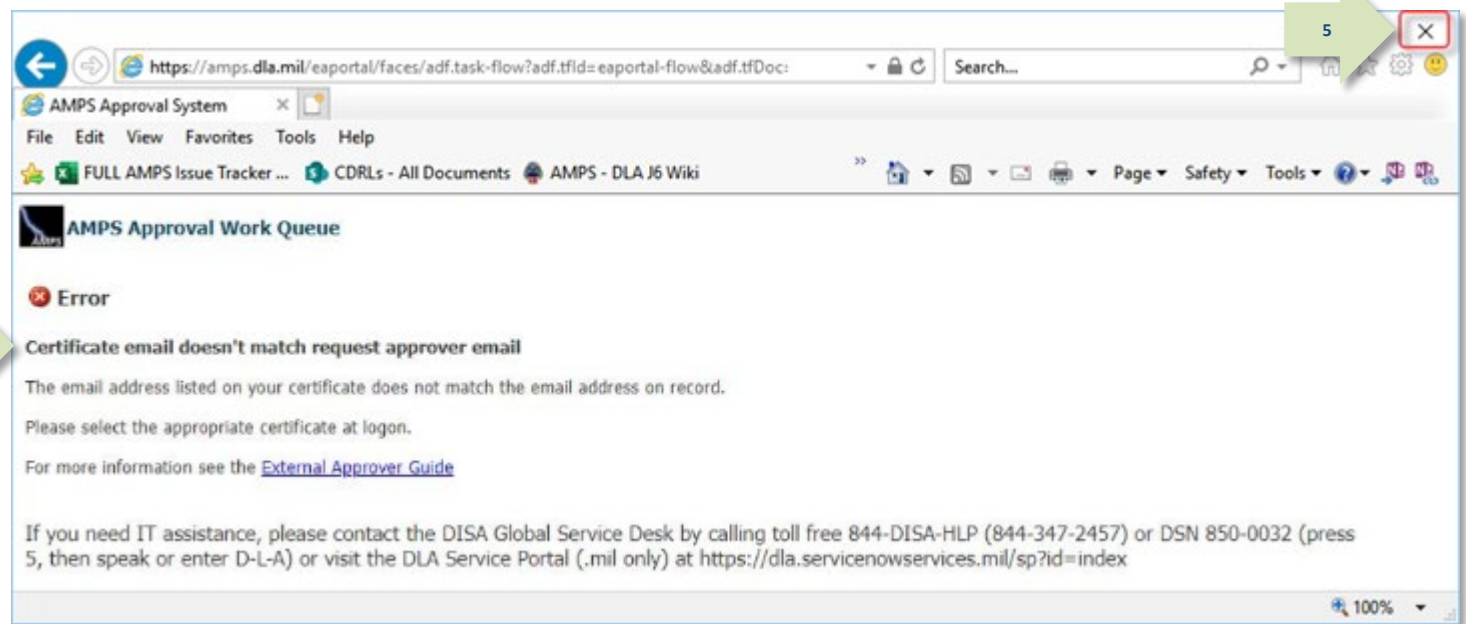
Figure 143: Certificate Email Error Message

Authentication with the Wrong CAC Certificate

During your log in to AMPS, you must choose the correct certificate when the system displays a security dialog requesting a certificate choice. AMPS is configured to support only a few certificate types. If you have authenticated in AMPS with a CAC (or other smart card), you must provide that certificate whenever you log in.

When you choose the wrong certificate while opening the External Approval Portal, the system responds with an error message. Step through the following procedure to exit the message and clear the certificate issue.

1. Review the email notification requesting an approval action.

   The email provides a URL that leads to the external approver's work list.
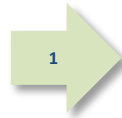
Sample External Approver Notification

Subject: Action Required: SAAR #106421 - Request User Access for zoltan zvendor (EZZ0024) (DLA External) (DFAS SABRS) 10/18/2017 07:44:01 EDT

Body:
SAAR #106421 - Request User Access for zvendor, zoltan (EZZ0024) (DLA External) has been submitted for approval.
This request for DFAS SABRS Prod - HQMC CTAB SABRS SABRS-002 was submitted in AMPS on 10/18/2017 07:44:01 EDT.

2. From the email message, copy and paste the URL into the address bar of a browser.

   Press the **Enter** key.

   AMPS displays a Windows Security dialog (see Figure 145).

Please visit AMPS at this URL:
https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=0457%3AVH%2FCyYdFHWdxFNpHCMpmLaClgCSctFbU3toHYOrsZ48%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 11/07/2017 06:44:09 EST.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

Figure 144: Sample Browser Address Bar

3. In the Windows Security dialog, select the appropriate certificate.

   In the sample dialog, the approver has selected an unsupported certificate.

   For CAC users, the correct certificate for AMPS authentication is the Authentication certificate issued by the DoD.

4. Click the **OK** button.

   If you select an unsupported certificate, AMPS displays an error message (see Figure 146).
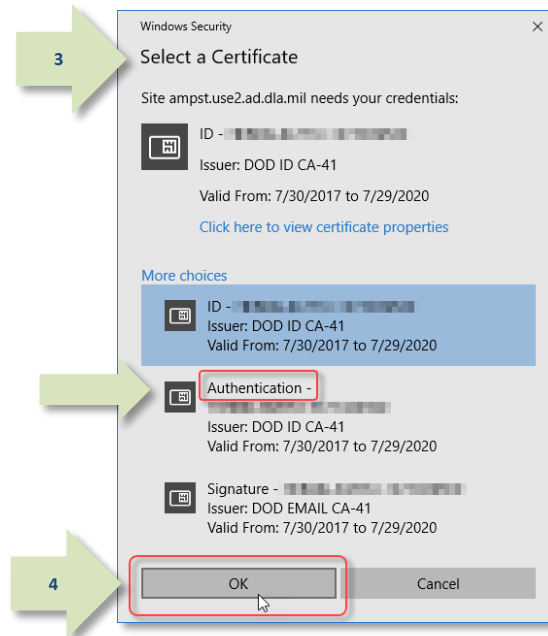
Figure 145: Sample Certificate Selection

5. Review the error message and follow the instructions below.

   In this message, the system confirms that AMPS does not support the certificate selected.
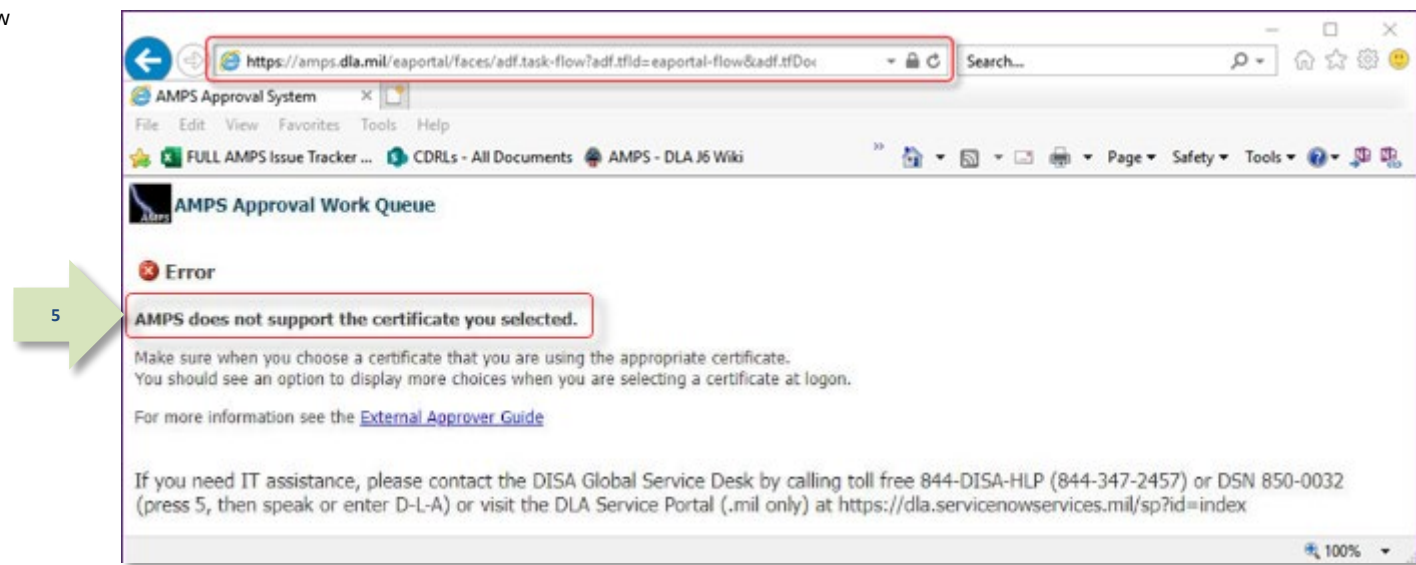
Figure 146: Unsupported Certificate Error Message

6. Close your browser.

7. Repeat the access process, beginning with step 1 in this procedure.

   Ensure that you select a certificate in the Windows Security dialog that is supported in AMPS.

8. **Next Steps** (not shown): If, after following the above procedure, you are still unable to access the approval task, call the Service Desk, and report the problem to the Service Desk agent.
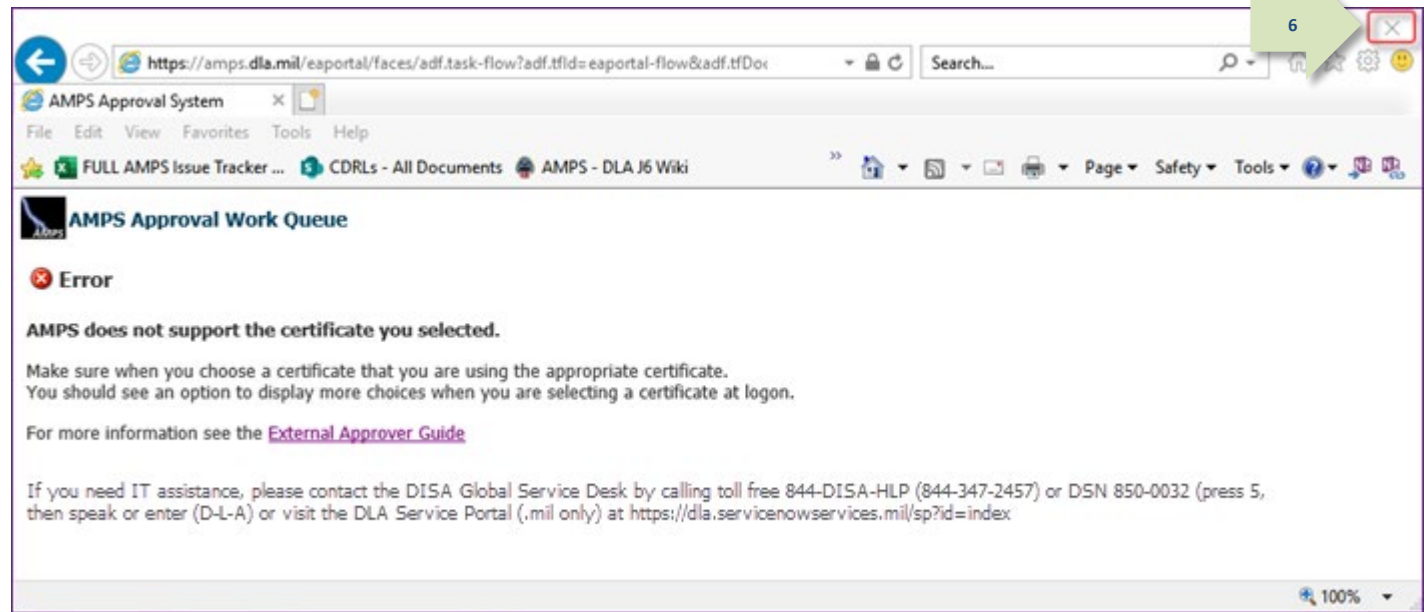
Figure 147: Unsupported Certificate Error Message – Browser Exit

Missing Authentication Certificate

During your log in to AMPS, you must choose a certificate when the system displays a security dialog requesting a certificate choice (see steps 3 and 4 above). AMPS is configured to support a few certificate types. If you have previously authenticated in AMPS with a CAC (or other smart card), you must provide that certificate whenever you log in. CAC users should use their "Authentication" certificate.

1. If you see the error at right, close your browser.

2. Repeat the access process, beginning with step 1 in the previous procedure.

   Ensure that you select the correct certificate in the Windows Security dialog.

3. **Next Steps** (not shown): If, after following the above procedure, you are still unable to access the approval task, call the Service Desk, and report the problem to the Service Desk agent.

If you choose to cancel or close the security dialog requesting a certificate while opening the External Approval Portal, the system responds with an error message. If you see the below error message, close your browser, and restart the process with a fresh browser (Note: you may need to clear your browser's cache). Select the correct certificate when prompted by the security dialog.
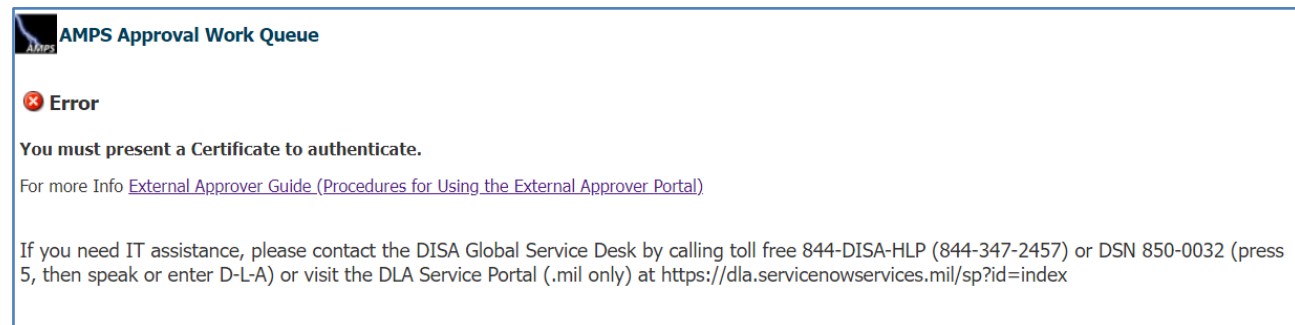
Figure 148: Missing Certificate Error Message

Required Approvals and Time Limits

The AMPS process for submitting and approving a user's role request is called a "workflow." A workflow automates the process of sending notifications of required actions and of forwarding action items to approvers in sequence. The AMPS approval workflow automatically tracks and reports on the status of each approval request.

After a user submits a role request, AMPS forwards the request to the approval workflow. During the workflow process, several approvers review the request before the role is provisioned to the user's account.

The number of approvers who review a request is defined in AMPS, and the number may vary according to which application and role make up the request. As AMPS forwards the request to each approver, AMPS also sends each user email notifications indicating the request's current status and pending approval requirements. Each approver receives email notifications from AMPS for role requests that require his or her action.

Approval Period and Automatic Cancellation

From the time an approver receives the initial email notification for a role request approval, AMPS provides 20 days for the approver to complete an action on the request: either approve or deny. After the initial notification, AMPS delivers additional email notifications every day to the current approver until the request is approved or denied, or the 20-day approval period expires.

If an approver does not act on a request before the end of the approver's time limit, the SAAR expires. AMPS then notifies the requestor that the request has expired. If the requestor still needs the role, he or she should consult a Supervisor and, if necessary, submit a new request. The following chart summarizes approvers in the workflow, approval requirements, and approval time limits.

> **Note:** If a request is submitted to an approver type, but there is no one assigned to the associated approver role, AMPS immediately escalates the approval to the next approver type in the hierarchy before the 20-day timeout period begins. A timeout results in a rejected SAAR.

Table 2 : Required Approvals and Time Limits

Required Approvals	Role/Application	Reminder Notifications	Time Limit for Approval
Segregation of Duties (SOD) Reviewer	All internal role requests for applications that require an SOD Review to ensure Segregation of Duties policies are enforced before the role request is approved.	Every day after initial notification.	20 days.
Supervisor	All role requests for all applications.	Every day after initial notification.	20 days.
Security Officer (applicable only when AMPS does not apply an automatic approval)	All internal that require an SO review. External role requests for all applications. All role requests from users flagged for an additional Security Officer Review. Role requests that qualify for automatic approval are approved immediately.	Every day after initial notification.	20 days.
External Authorizing Official	Requests by external users for certain roles preset to include the EAO as an approver.	Every day after initial notification.	20 days.
Data Owner	All internal user role requests.	Every day after initial notification.	20 days.
Information Assurance Officer (applicable only to customers who require IAO approval)	All internal user role requests for customers that require IAO approval. Not applicable to DLA systems. Roles requests that qualify for automatic approval are approved immediately.	Every day after initial notification.	20 days.
Information Assurance Manager (applicable only to customers who require IAO approval)	Requests for an IAO role. Not applicable to DLA systems.	Every day after initial notification.	20 days.
Provisioners (System Administrators, Database Administrators)	All Total AMPS Solution requests approved during the approval workflow.	Once a week after initial notification.	No expiration of the ticketed provisioning request.

How to Request the AMPS Supervisor Role – Internal Users Only

What you can do: Follow this procedure if you are an AMPS Supervisor but you do not have the **AMPS Supervisor** role assigned to your account.

If you do not have the AMPS Supervisor role, AMPS displays a screen like the sample in Figure 149 when you click a user's SAAR in your **My Tasks** list.

Note:

The Supervisor role is reserved for internal AMPS Supervisors only.

External approvers do not need to request this role.
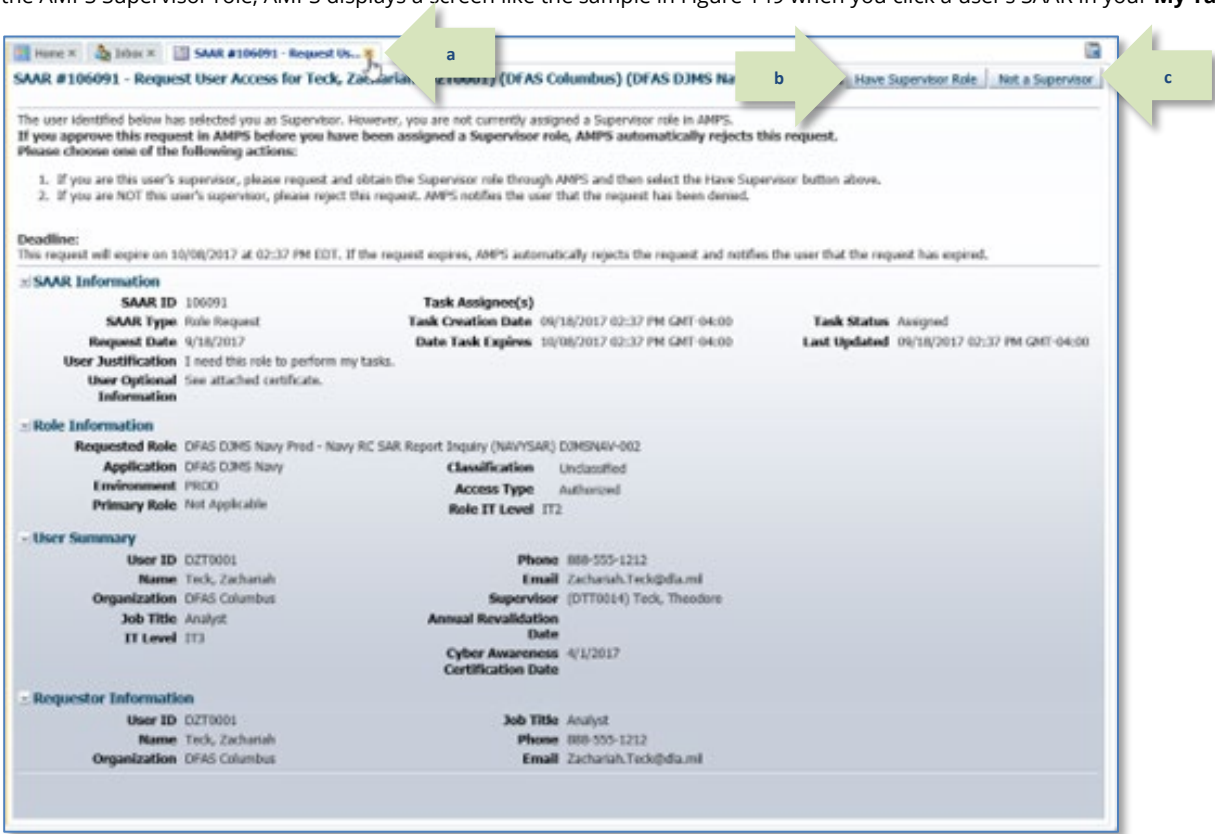
Figure 149: Supervisor Role Notification

AMPS displays this notification if you do not have the AMPS Supervisor role.

Where to start: AMPS provides the following three options on the **Supervisor** screen:

a. **Click the close icon if you do not already have the AMPS Supervisor role assigned to your account:** follow the instructions in this section to request this role. This role request must be approved during the role approval process described in the next section: **How to Approve a Role Request.**

b. **Click *Have Supervisor Role* only after you have acquired the AMPS Supervisor role:** after the AMPS Supervisor role has been assigned to you, AMPS displays this role in the **Current Roles** table (see Figure 158). You can reopen the approval task that triggered the screen shown by example in Figure 149. After you click **Have Supervisor Role**, you can proceed with the role request approval.

c. **Click *Not a Supervisor* only if you are not the requesting user's AMPS Supervisor:** if you click this option, AMPS marks the user's request as rejected and notifies the user of the reason for the rejection. The user must select a different AMPS Supervisor.

Request the AMPS Supervisor Role

In the following AMPS Supervisor role request procedure, all data entry fields marked with an asterisk (*****) are required fields.

1. Log in to AMPS.

    AMPS displays the **Self Service Home** *page. Your ID is displayed to indicate you are the currently logged-in user.*

2. On the Self Service Home page, click Request Role tile.

    If this role request is your first during the current session, AMPS displays a Privacy Act Statement appropriate for your organization. Click the **Accept** *button to proceed.*

    AMPS displays the **Request Role: User Information** *screen (see Figure 151).*
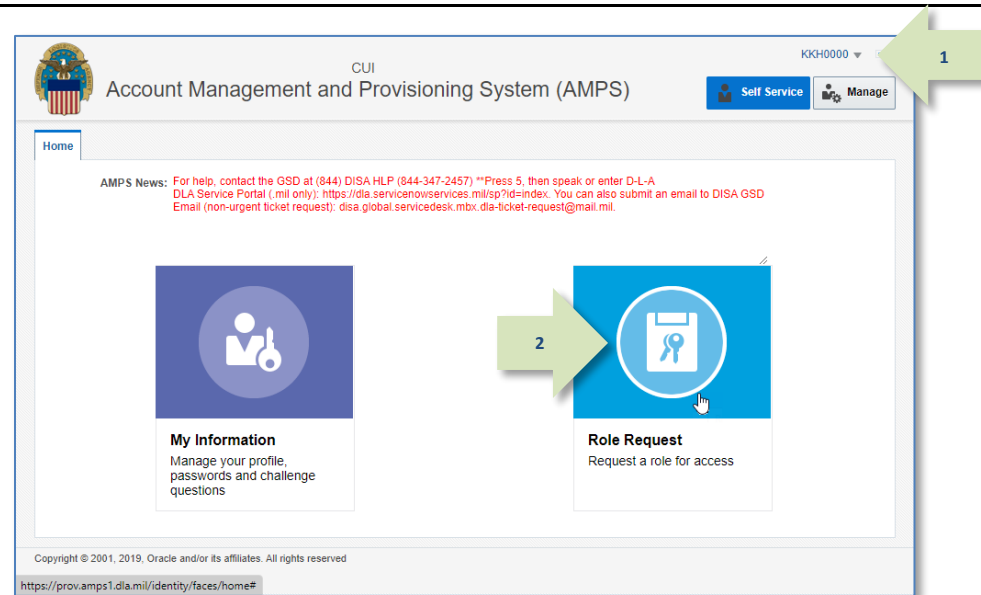
Figure 150: AMPS Self Service Home Page – Role Request Tile

3. Enter your **Cyber Awareness Certification Date** (required). This date must fall within the previous 12 months.

   - *DFAS users: update this field to display the latest date.*

   - *DLA users: this date is read-only.*

4. You no longer need to enter your Date of Birth.

   AMPS does not save or store the DOB of any user. This data is no longer collected by AMPS. When present, this field displays non-editable faux data.

5. **User Type** is a nonmodifiable field. However, there are fields associated with your user type that require an entry:

   a. **Civilian**: select your **Grade** in the field displayed (required).

   b. **Military**: select **Branch** and **Rank** from the fields displayed (see Figure 152).

6. Update your Contact Information, as needed.
   See **How to Update Contact Information: Internal Users**.

7. Update your **Organization**, as needed.
   See **How to Update Additional Attributes** *for more instructions.)*

8. Update your Supervisor, as needed.
   *(See **How to Update Your AMPS Supervisor – Internal Users** for more instructions.)*

9. Click the **Next** button to proceed. It is located next to the **Cancel** button.

Figure 151: AMPS Supervisor Role Request - User Information

Figure 152: User Type Sample – Military

AMPS Displays the Select Roles Screen

In the **Select Roles** screen, you have two choices for locating the role name you want to select: **Search** and **Browse**. The following procedure tells you how to search for the AMPS Supervisor role.

10. In the **Search Roles** section, enter **AMPS** in the *Role Name* field.

11. Click the **Search** button.

    *AMPS displays the names of all roles having **AMPS** in the **Role Name**.*

12. Click the checkbox next to **Display Admin Roles (for Supervisor and Approval Access)**.

    Checking this option displays AMPS approver role names, including the **AMPS Supervisor** *role.*

13. Locate and click the **AMPS Supervisor** role in the **Select a Role / Role Name** list.

14. Click the right arrow (→) button, also known as the Add button.

    AMPS copies the role name to the **Selected Roles** *list panel on the right.*

15. Click **Next**.

Figure 153: AMPS Supervisor Role Request – Search for the AMPS Supervisor Role

AMPS Displays the Justification Screen

In the **Justification** screen, enter comments relevant to the **AMPS Supervisor** role request. These comments explain to approvers why you need the **AMPS Supervisor** role.

---

16. Enter comments justifying this role request in the **Justification** text area.

> *Note:*
>
> The comment provided is for illustration purposes only. Please enter specific content related to the AMPS Supervisor role request.

17. Click **Next**.

Figure 154: AMPS Supervisor Role Request – Justification

AMPS Displays the Summary Screen

18. Review the information in the Role Request **Summary** screen.

    a. Click any node in the **Request Role** train to return to previous screens and make corrections, as needed.

    b. After making corrections, click the **Summary** node in the train to return to the **Summary** screen.

19. Click **Submit** to complete the role request.

Figure 155: AMPS Supervisor Role Request – Summary

AMPS Displays the Role Request Confirmation Screen

In the **Confirmation** screen, review the confirmation data to ensure AMPS created a SAAR for the AMPS Supervisor role, and that the SAAR has been submitted.

20. Review the Role Request Confirmation data.

Note:

The SAAR number associated with your request appears in the confirmation data.

21. Click **OK** to close the Confirmation message and proceed.

Figure 156: AMPS Supervisor Role Request – Confirmation

Check the Status of the Supervisor Role Request in Pending Requests

1. On the Self Service Home page, click the My Information tile (not shown) to display User Information and Applications & Roles tabs.

2. Click the Applications & Roles tab.

3. View the **Pending Requests** section to check the status of your request as it proceeds through the approval process.

   *Check **Pending Requests** to determine the location of any SAAR in the approval process.*

   Figure 157 illustrates the status of the sample SAAR created in this procedure.

Figure 157: User's Applications & Roles Tab - Pending Requests

Check *Current Roles* to Confirm the AMPS Supervisor Role is Assigned

4. After you have been notified through an AMPS email message that the request approval is complete, check the **Current Roles** section on the **Applications & Roles** tab.

    This section shows that the AMPS Supervisor role has been assigned to your account.

5. Check the Request History section on the **Applications & Roles** tab to verify the SAAR has been completed.

Figure 158: Applications & Roles

The *Current Roles* table on the Applications & Roles tab lists all the roles currently assigned to your account, including the newly assigned AMPS Supervisor role.

Reopen the SAAR and Proceed with Approval

1. Return to the My Tasks view in your Inbox and reopen the SAAR task (see How to Approve a Role Request for more information).

   *AMPS opens the **Supervisor** notification screen for the selected SAAR.*
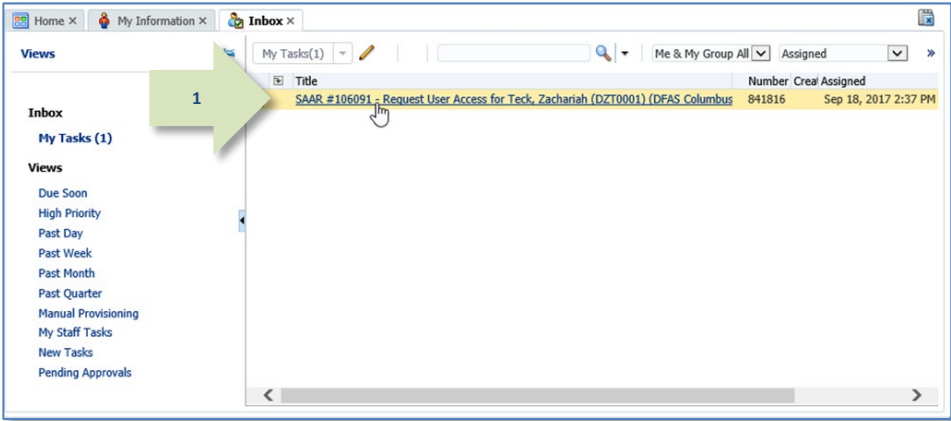
Figure 159: Approval Details - My Tasks

2. Click **Have Supervisor Role** to continue with the approval.

    *AMPS opens the **Supervisor's Decision** screen, enabling you to continue the approval procedure.*

    *See **How to Approve a Role Request** for more information.*

Figure 160: Supervisor Role Notification

How to Approve a Role Request

What you can do:	Follow this procedure if you are a designated SOD reviewer or approver, and have received an email notification indicating a SAAR awaits your action in AMPS. You must have the appropriate SOD reviewer role to receive the email notifications and have access to the SAARs.
Where to start:	To begin the process of reviewing or approving a role, review relevant email notifications, log in to AMPS, and click the **Inbox** command.

Segregation of Duties Review

A Segregation of Duties (SOD) Review is an *optional* stage in the approval workflow, required only by certain customers and organizations for certain roles. **If the request does not require an SOD review as part of the approval workflow, you can skip this section and go to the Supervisor Approval section.** The following procedure explains how to complete an SOD review of a role request in AMPS for compliance with SOD business practices.

1. After a user requests a role, AMPS sends an email notification confirming the request submission and indicating the role request is awaiting approval.

   1

   ### Sample User Notification: Confirmation

   Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

   Body: Your request for role DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319, with access to DSS Distribution, SAAR 106077 has been submitted for approval.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. AMPS also sends an email notification to the user indicating the role request is waiting for the SOD Reviewer's comments and action.

   2

   ### Sample User Notification: Status

   Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

   Body: SAAR #106077 is awaiting Segregation of Duties Review approval.

   This request was submitted in AMPS on 09/14/2017 09:27:35 EDT.
   No action is required from you at this time.
   This task expires on 10/04/2017 09:27:50 EDT.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

3. After a user requests a role, AMPS sends an email notification to the Segregation of Duties (SOD) Reviewer indicating that a SAAR has been submitted for an SOD review.

   3

   ### Sample Review Notification: Action Required

   Subject: Action Required: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

   Body: SAAR #106077 - Request User Access for Teck, Rupert (DRT0021) (DFAS Columbus) has been submitted for approval.
   This request for DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319 was submitted in AMPS on 09/14/2017 09:27:35 EDT.

   Please visit AMPS at this URL: https://amps.dla.mil/
   Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/04/2017 09:27:50 EDT.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

4. The SOD Reviewer clicks the **Inbox** command from their **User ID** dropdown menu.

    *AMPS displays the **Inbox** tab. By default, this screen opens with the **My Tasks** view displayed (Figure 162): "My Tasks" refers to the tasks assigned to the logged-in user.*
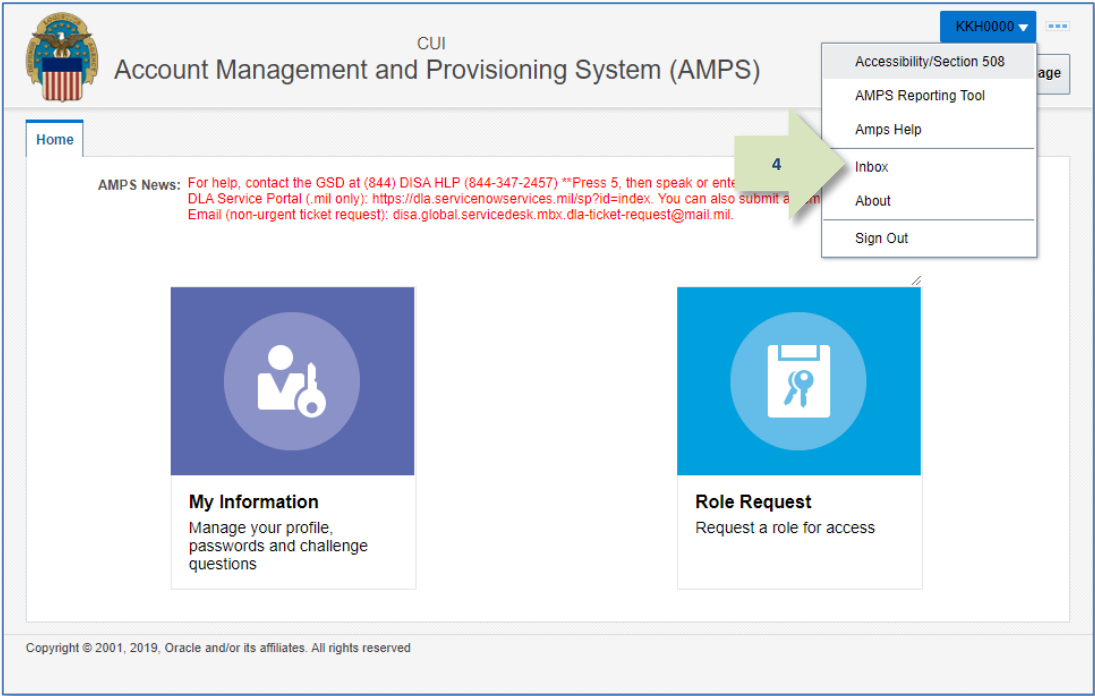
Figure 161: Inbox Command

5. On **My Tasks**, click the SAAR entry indicated in the email notification.

    *AMPS displays the **Segregation of Duties Reviewer** screen for the specified SAAR (see Figure 163).*
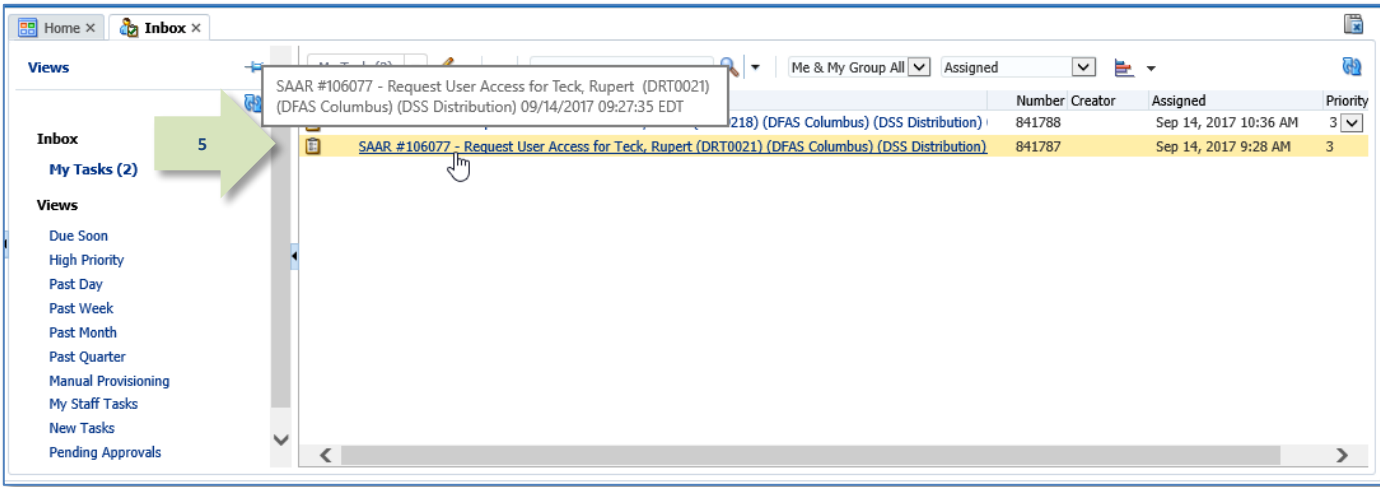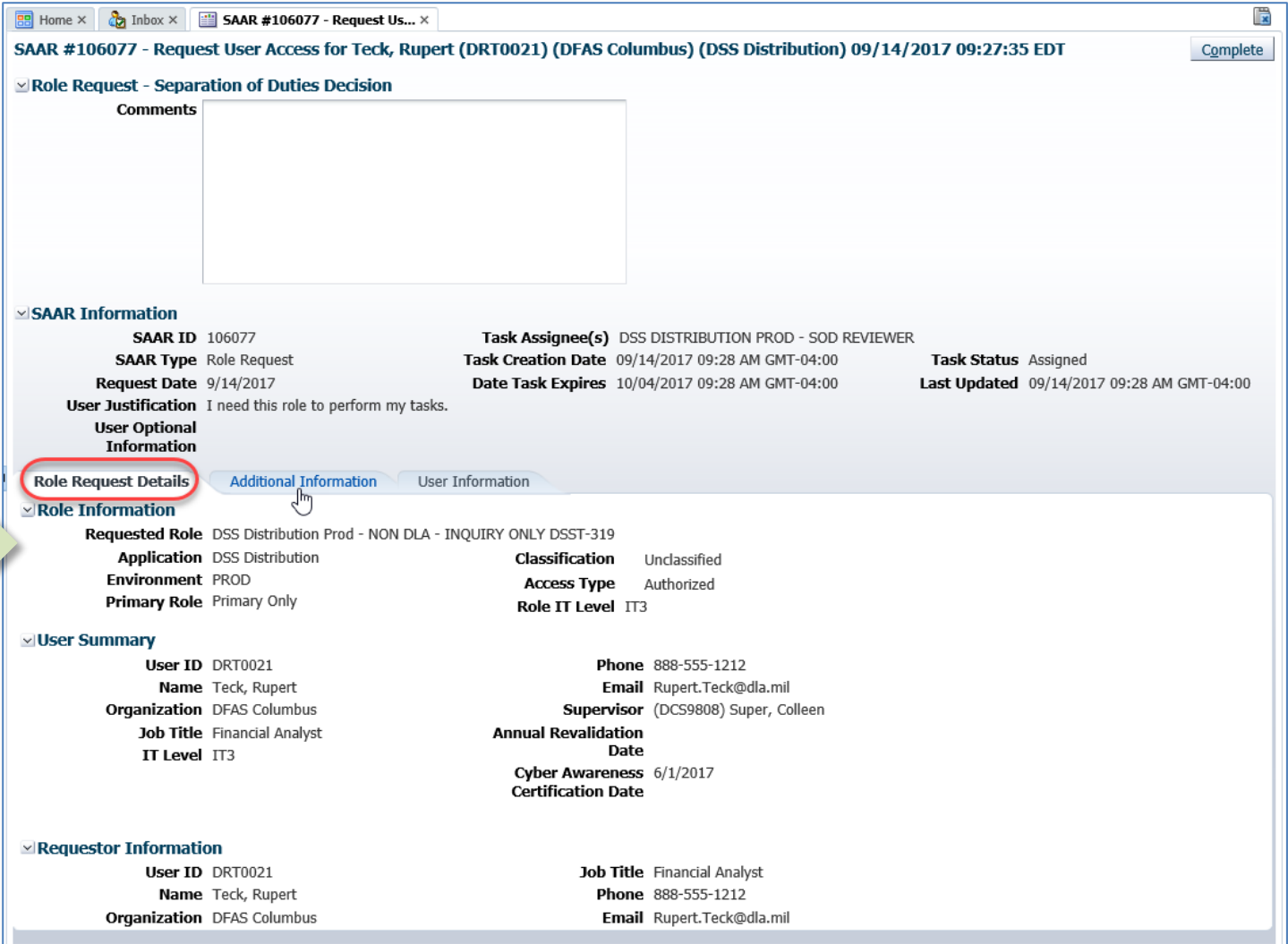
Figure 162: Approval Details - My Tasks Tab

6. Review the **Role Request Details** tab information to help determine whether an SOD conflict may exist.

*More information about the request is available in the **Additional Information** and **User Information** tabs (See Figure 164 and Figure 165).*

Figure 163: Segregation of Duties Reviewer Comments Screen

7. Select the **Additional Information** tab.

AMPS displays the following information:

- *Links to any supporting documentation the requesting user may have submitted.*

- **SAAR Approval History:** *the SOD reviewer's contact data, and decision information will be included in the SOD row of this table after the SOD decision has been completed.*

   SAAR approval history is available in a SAAR report through BI Publisher.

Note:

AMPS reports all date and time stamps in reports and on screens using Eastern Time: Eastern Standard Time or Eastern Daylight Time, depending on the time of year.

Figure 164: Segregation of Duties Decision - Additional Information

8. Select the **User Information** tab.

    AMPS displays key data about the requesting user:
    *   *Account information*
    *   *User Contact information*
    *   *Supervisor contact information*
    *   *Requesting user's organization*
    *   *Requesting user's current roles*
    *   *Requesting user's pending requests, including the current request.*

9. After making a determination, you have the option to fill in the **Comments** field explaining the review decision.

    You can enter comments to support the completion of the review. AMPS passes these comments to the next approver after the reviewer submits the completed review.

    Note:

    The Comments text shown in sample screens is for demonstration purposes only. Please enter Comments applicable to the current request.

10. Click **Complete**.

    AMPS automatically . . .
    *   *Sends the SAAR to the Supervisor for approval and*
    *   *Removes the SAAR as assigned to the SOD Reviewer from the* **My Tasks** *tab.*

Figure 165: Segregation of Duties Decision - User Information

11. After the SOD review decision is submitted, AMPS sends an email notification to the user regarding the approval's status.

AMPS also notifies the Supervisor of a pending approval action on the SAAR.

11

Sample User Notification: Status

Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: The Segregation of Duties Reviewer has completed an approval task for SAAR #101765 regarding your request for the following role: DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319 with access to DSS Distribution.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

12. In addition, AMPS displays SAAR information and status in the user's **Pending Requests** table.

Supervisor Approval

The following procedures explain how a Supervisor approves a role request.

Procedure for Internal Supervisor Approvals

This procedure explains how an internal user's Supervisor handles a role request approval.

1. After a User requests a Role, AMPS sends an email notification confirming the request submission and indicating the role request is waiting for approval.

   This type of notification appears ONLY if there has been no prior SOD approval administered.

   1

Sample User Notification: Confirmation

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: Your request for role DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319, with access to DLA DSS Distribution, SAAR 106077 has been submitted for approval.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2. AMPS sends an email notification to the user indicating the role request is waiting for the Supervisor's approval.

   2

Sample User Notification: Status

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: SAAR #106077 is awaiting Supervisor approval.

This request was submitted in AMPS on 09/14/2017 09:27:35 EDT.
No action is required from you at this time.

This task expires on 10/04/2017 12:25:03 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

3. After a User requests a Role, AMPS sends an email notification to the User's Supervisor indicating that a SAAR has been submitted for the Supervisor's approval.

   3

Sample Approver Notification

Subject: Action Required: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: SAAR #106077 - Request User Access for Teck, Rupert (DRT0021) (DFAS Columbus) has been submitted for approval.
This request for DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319 was submitted in AMPS on 09/14/2017 09:27:35 EDT.

Please visit AMPS at this URL
https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/04/2017 12:25:03 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

4. In the AMPS banner, click your User ID to
    open the User ID dropdown menu, then
    click **Inbox** from the menu.

    AMPS displays the **Inbox** *screen. By default,*
    this screen opens with **My Tasks** *displayed*
    (see Figure 167).

    "My Tasks" refers to the tasks assigned
    to the logged-in user.
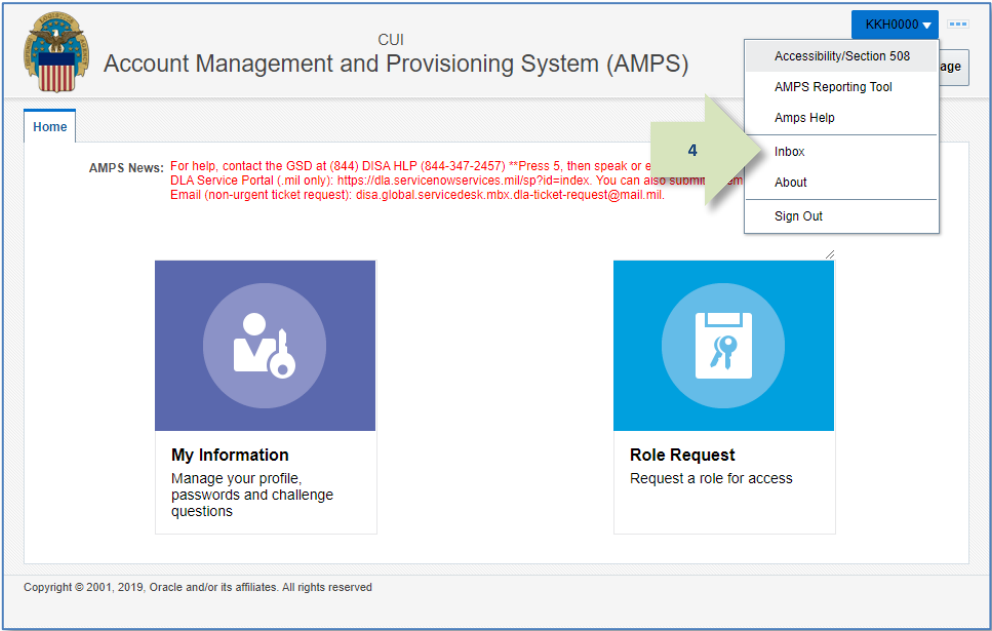
Figure 166: Inbox Command

5. In the **My Tasks** list, click the SAAR entry
    indicated in the email notification.

    AMPS displays the **Supervisor**
    Application Access Decision
    screen for the specified SAAR
    (see Figure 168).
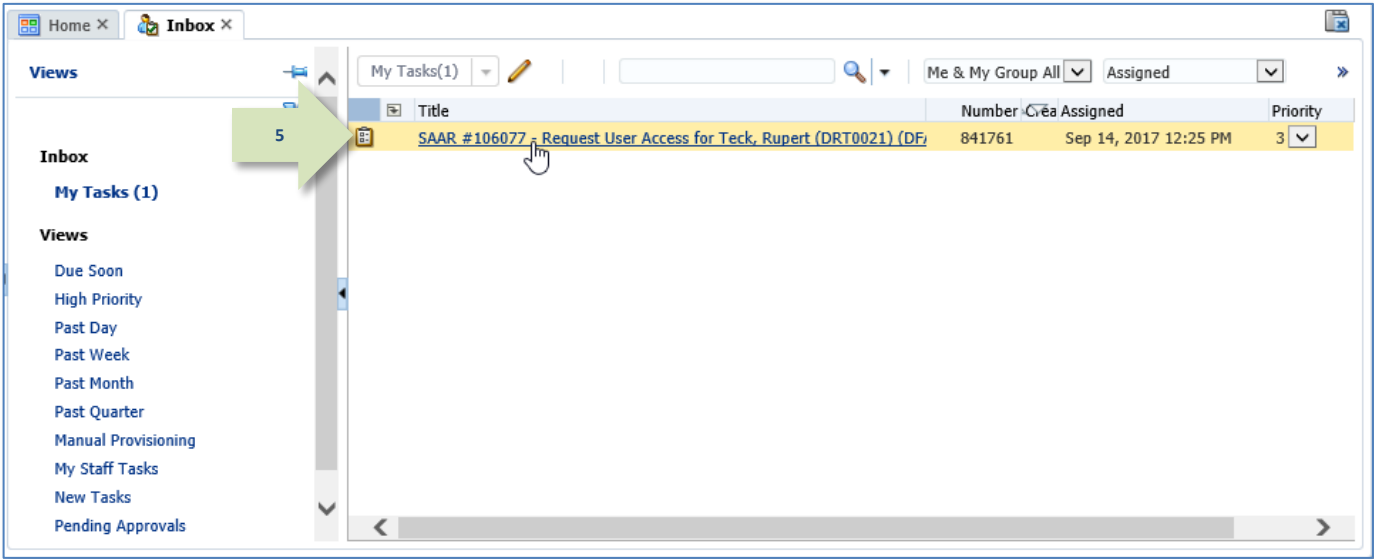
Figure 167: Approval Details - My Tasks Tab

Standard Approval Screens: Supervisor

Most approval screens for Supervisors have standard content as shown in the sample screens. EBS Supervisors see a screen with an additional Segregation of Duties/Governance, Risk and Compliance (SOD/GRC) section that reports possible SOD conflicts. See **Appendix F: SOD/GRC Reports in the Role Request Approval Process** for more information.

6. Fill in the required fields, as needed.

   a. **Start Date** (required and auto-filled): this entry must be no earlier than the current date.

   b. **End Date** (required and auto-filled): adjust as needed.

Note:

EBS Supervisors, see **Appendix F** for information about the SOD/GRC report section
(not shown).

7. Review the **Role Information** to verify the user has requested the correct role.

8. Click **Additional Information**.

   *AMPS displays the **Additional Information** tab (see Figure 169).*

Figure 168: Supervisor Decision Screen – Role Request Details

9. As an option in the **Additional Information** tab, you can download and review any of the documents the user has included as supporting information.

    To view a document, click **Download and Review Document**.

    AMPS downloads the PDF file and automatically opens the document in Adobe Reader (not shown).

10. Click **User Information.**

    AMPS displays the User Information tab (see Figure 170).

Figure 169: Supervisor Decision Screen - Additional Information

11. In the **User Information** tab, review the user account, contact, organization, and supervisor information to help verify the correct user is requesting the role specified in the **Pending Requests** table (see bottom of screen). You can also enter Comments as follows:

12. As an option, enter supporting comments in the **Comments** text area.

    *Comments are not required for an approval but will be passed to the next approver in the **Additional Information** screen.*

Note:

Comments text shown in sample screens is for demonstration purposes only. Please enter Comments applicable to the current request.

13. Click **Approve**.

    AMPS automatically sends the SAAR to the next approver.

Figure 170: Supervisor Decision Screen - User Information Tab

14. After the approval is submitted, AMPS sends an email notification to the user regarding the approval's status.

14

Sample User Notification: Status

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT
Body: The Supervisor has completed an approval for SAAR #106077.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

---

15. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

*If the requestor is a DLA user and the current request is the requestor's initial role request for the application, the status shows the SAAR has been forwarded to the **Security Officer** for approval.*

For DLA users, the Security Officer may be bypassed, or AMPS may administer an automatic Security Officer approval under some circumstances.

All role requests for DFAS users go to the Security Officer automatically.

Note:

In DLA applications, if the Security Officer is bypassed or an automatic approval is granted, AMPS automatically sends the role request to the application Data Owner for approval.

Procedure for External Supervisor Approvals

An External Supervisor does not have an AMPS account. Instead, AMPS maintains a separate work queue for each External Supervisor; the work queue is accessible from a URL incorporated in the "Action Required" email notification sent to an external approver for each approval request. The procedure in this section provides the steps for getting access to an External Supervisor work queue and addressing the action required to approve a role request.

1. After an External User requests a Role, AMPS sends an email notification to the external user confirming the request submission and indicating the role request is waiting for the External Supervisor's approval.

Sample User Notification: Confirmation

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: Your request for role DFAS DJMS Navy Prod - Navy Input User Field DJMSNAV-007, with access to DFAS DJMS Navy, SAAR 106086 has been submitted for approval.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. AMPS also sends an email notification to the external user indicating the role request is waiting for the External Supervisor's approval.

Sample User Notification: Status

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: SAAR #106086 is awaiting External Supervisor approval.
This request was submitted in AMPS on 09/18/2017 09:36:54 EDT.
No action is required from you at this time.
This task expires on 10/08/2017 09:37:10 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

3. After an External User requests a Role, AMPS sends an **Action Required** email notification to the user's External Supervisor indicating that a SAAR has been submitted for the External Supervisor's approval.

   Each approval notification contains a unique URL that leads to a corresponding External Supervisor's AMPS Work Queue.

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: SAAR #106086 - Request User Access for Teck, Denny (EDT0379) (DLA External) has been submitted for approval.
This request for DFAS DJMS Navy Prod - Navy Input User Field DJMSNAV-007 was submitted in AMPS on 09/18/2017 09:36:54 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=1597%3Avn90ZwVpp8Q3GinRj9Fn6%2FasHd8Cz56VuIQMi6UeadM%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/08/2017 09:37:10 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

4. Copy the URL provided in the Supervisor's **Action Required** notification, paste this URL into a browser instance, and navigate to the **AMPS Approval Work Queue**.

    AMPS displays the **Approval Work Queue,** *which lists all the pending* **Approval Actions** *assigned to the External Approver (see Figure 172).*
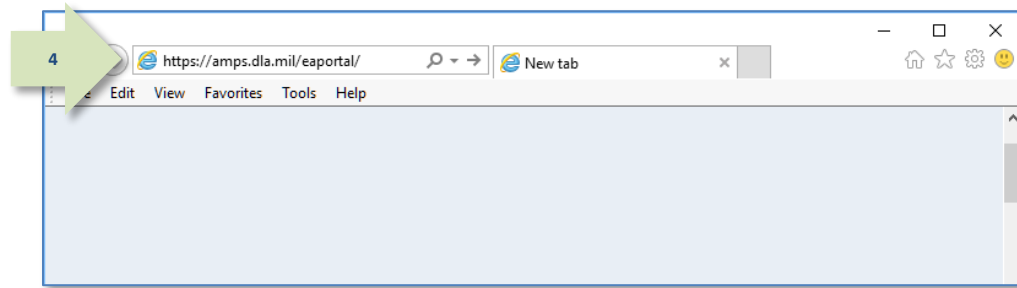
Figure 171: Browser Instance

5. Locate the SAAR you want to approve and click the link in the **Approval Action** column.

    AMPS displays one of two possible screens:
    - **Verify Approver** *(see Step 6), or*
    - *The* **Supervisor Application Access Decision** *screen for the specified SAAR (see Step 7).*
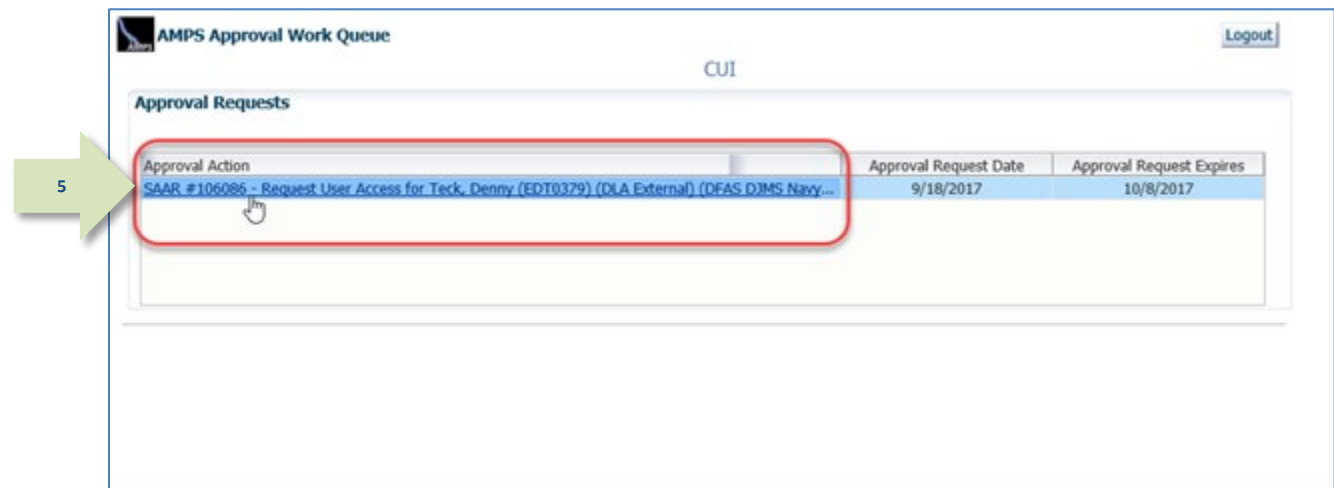
Figure 172: AMPS Approval Work Queue

6. If this approval is the first request to the Supervisor from the identified Requestor, AMPS asks the Supervisor to verify his or her identity as the external user's Supervisor.

    If the approver's name in the **Verify Approver** screen is the name of the logged in Supervisor, the approver should click the **Verify** button.

    To proceed, click the **Verify** button.

    This step eliminates the possibility that any other approver can act on the named requestor's role requests in the future.
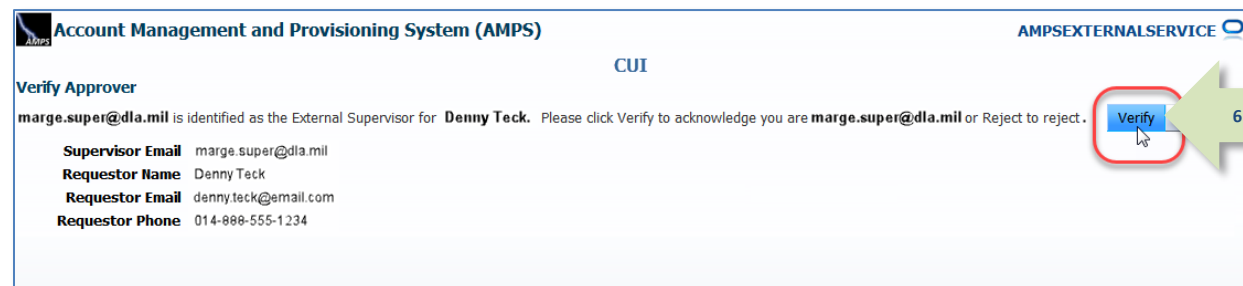
Figure 173: Verify Approver – Supervisor

7. Edit the required fields, as needed:
    a. **Start Date** (auto-filled): this entry
        must be no earlier than the current date.
        Adust as needed.
    b. **End Date** (auto-filled): adjust as needed.
        External User role assignments are limited
        to 365 days.

8. Click the **Additional Information** tab.

    AMPS displays the **Additional Information** *screen
    (see Figure 175).*

Figure 174: External Supervisor Approval Screen – Application Access Decision

9. In the **Additional Information** screen, note the option to download and review attached documents.

10. Click the **User Information** tab.

    AMPS displays the **User Information** *screen (see Figure 176).*

Figure 175: External Supervisor Decision - Additional Information

11. In the **User Information** screen, review the **User Account Information** and other data to verify the user's request.

    Note that this screen contains identity and contact information for all external approvers.

12. As an option, enter any comments relevant to the approval.

    Comments are optional for an approval. Entering text in the Comments field activates the Reject button.

13. Click **Approve**.

    AMPS automatically . . .
    - *Closes the External Supervisor Decision screen,*
    - *Sends the SAAR to the next approver,*
    - *Removes the SAAR as assigned to the External Supervisor from the Supervisor's AMPS Approval Work Queue, and*
    - *Displays a Task Completed message (see Figure 177).*

Figure 176: External Supervisor Decision - User Information

14. Click the link labeled **Return to the External Approval Worklist**.

    *AMPS displays the refreshed **Approval Work Queue** (see Figure 178).*

Task Completed

Approval task for SAAR 106086 has completed.

Return to the External Approval Worklist

https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow...
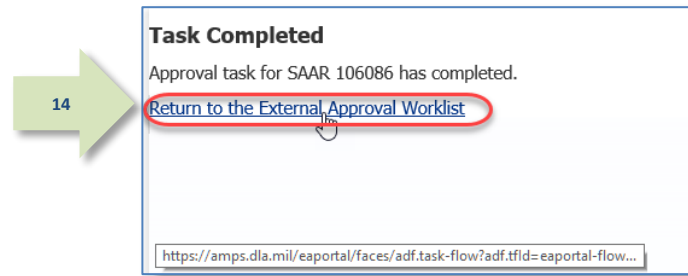
Figure 177: AMPS Message - External Approval Completed

15. When finished with the Approval Work Queue for the current session, click the **Logout** button.

    AMPS displays a logout confirmation message (see Figure 179).

AMPS Approval Work Queue

Logout

CUI

Approval Requests

Approval Action		Approval Request Date	Approval Request Expires
There are no pending approvals awaiting your attention. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index			

Figure 178: Modify Approver Information

16. Review the logout message and close the browser.

https://ampst.use2.ad.dla.mil/eap   AMPS Approval System

File   Edit   View   Favorites   Tools   Help

AMPS Approval System

You have been logged out of the AMPS Approval System. Please use the URL provided in your email notification to return to this system and perform any additional approvals.
If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 179: AMPS Approval System - Logout Message

17. After the approval is submitted, AMPS sends an email notification to the user regarding the approval's status.

17

Sample User Notification: Status

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT
Body: The External Supervisor has completed an approval for SAAR #106086.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

---

18. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

A user can check SAAR listings in **Pending Requests** *to track the progress of any open SAAR.*

Note:

After a SAAR has been fully approved or rejected, AMPS moves this listing to the SAAR History table.

Security Officer Approval

The procedure for Security Officers in this section explains how to approve a role request for roles that require a Security Officer review.

Security Officer Bypass: Approval Not Required

Note that a DLA Security Officer may not necessarily see every role request submitted by a DLA user. The Security Officer may be bypassed under the following conditions:

- The user has already submitted a role request with a valid investigation date.
- All clearance-related required fields in the user's profile have valid values entered.
- The user's account has not been flagged for additional Security Reviews in future requests.

When these conditions are met, the role request bypasses the Security Officer and goes directly to the Data Owner. See also the section entitled **Security Officers: Internal and External SO Review Requirements** for more information about Security Officer review requirements.

Security Officer Automatic Approval

For DLA users, a role request is granted an automatic Security Officer approval if the user's account fulfills certain conditions. See the section entitled **Security Officer: Internal Users** in this user guide for more details.

Procedure for Internal Security Officer Approvals

This procedure explains how an Internal Security Officer handles a role request approval.

---

1. After a User's Supervisor approves a role request, AMPS sends an email notification to the user indicating the outcome of the Supervisor's decision.

   1
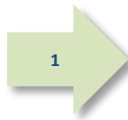
   ### Sample User Notification: Status of Supervisor Approval

   Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

   Body: The Supervisor has completed an approval for SAAR #106077.

   The outcome for this task is APPROVE.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

2. After a User's Supervisor approves a role request, AMPS sends an email notification to the user with the request's status, indicating the role request is waiting for the Security Officer's approval.

   2
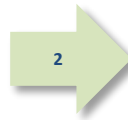
   ### Sample User Notification: Status of Security Officer Approval

   Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

   Body: SAAR #106077 is awaiting Security Officer approval.

   This request was submitted in AMPS on 09/14/2017 09:27:35 EDT.
   No action is required from you at this time.
   This task expires on 10/04/2017 12:45:53 EDT.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

3. After a Supervisor approves a role request, AMPS sends an email notification to the user's organizational Security Officer indicating that a SAAR has been submitted for the Security Officer's approval.

3

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: SAAR #106077 - Request User Access for Teck, Rupert (DRT0021) (DFAS Columbus) has been submitted for approval.

This request for DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319 was submitted in AMPS on 09/14/2017 09:27:35 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/04/2017 12:45:53 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

4. In the AMPS banner, click your User ID to open the User ID dropdown menu, then click **Inbox** from the menu.

    AMPS displays the **My Tasks** *tab in the* **Approval Details** *screen (see Figure 181).*

    "**My Tasks**" *refers to the tasks assigned to the logged-in user.*
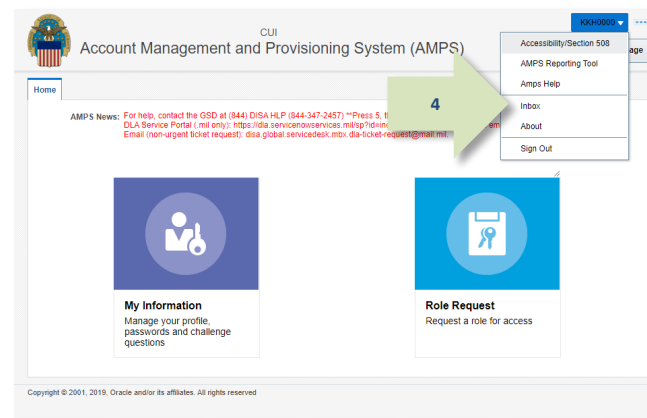
Figure 180: Inbox Command

5. In the **My Tasks** tab, click the SAAR number indicated in the email notification.

    AMPS displays the **Security Officer Application Access Decision** *screen (see Figure 182).*
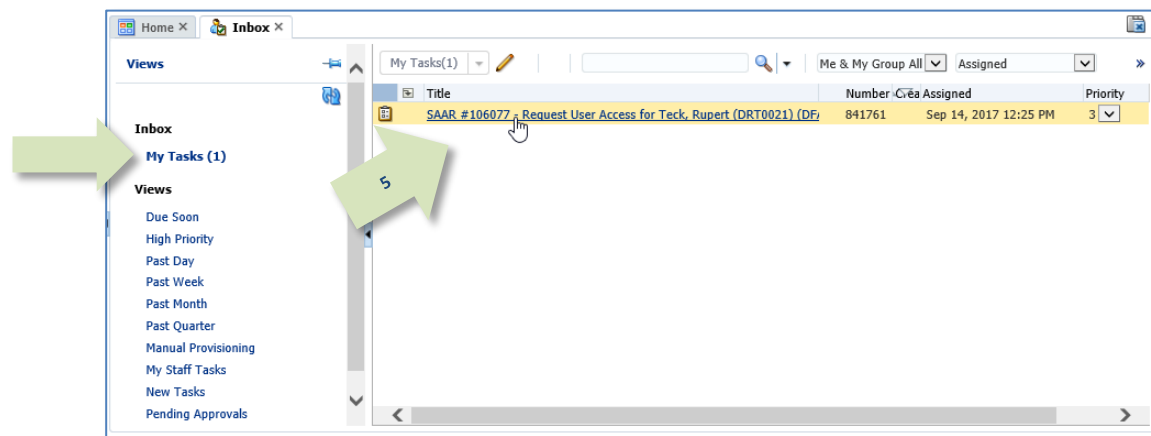
Figure 181: Approval Details – My Tasks Tab

6. Fill in the required and optional fields, as needed:

   a. **Start Date** (required and filled in by the Supervisor): this entry must be no earlier than the current date.

   b. **End Date** (required and filled in by the Supervisor): adjust as needed.

   c. **IT Level (**required)**:** select the requestor's **IT Level** from the drop-down list.

   d. **Clearance Level** (required)**:** select the requestor's **Clearance Level** from the drop-down list.

   e. **Type of Investigation** (required)**:** select the investigation type conducted for the requestor from the dropdown list.

   f. **Date of Investigation** (required)**:** enter the requestor's most recent investigation date.

   g. **Security Review Flag** (required): DLA Security Officers can accept the default if they do not need to review a request from the user on every request. This flag does not affect DFAS Security Officers.

Note:

The user's Date of Birth is no longer collected by AMPS. This field only displays faux data.

7. Click **Additional Information**.

   *AMPS displays the **Additional Information** tab (see Figure 183).*

Figure 182: Security Officer Decision Screen – Role Request Details

8. As an option in the **Additional Information** tab, you can download and review any of the documents the user has included as supporting information.

    To view a document, click **Download and Review Document**.

    AMPS downloads the PDF file and automatically opens the document in Adobe Reader.

9. Click **User Information.**

    AMPS displays the **User Information** *tab (see Figure 184).*

Figure 183: Security Officer Decision - Additional Information Tab

10. In the **User Information** tab, review the user account, contact, organization, and supervisor information to help verify the correct user is requesting the role specified in the **Pending Requests** table (see bottom of screen, Figure 184).

11. As an option, you can enter comments at any time during this procedure to support the decision.

Comments are required on a request decision only when you want to use the Reject *button to reject the SAAR.*

*Comments are not required for an approval but will be passed to the next approver in the **Additional Information** screen.*

12. Click **Approve**.

AMPS automatically . . .
- *Sends the SAAR to the next approver, and*
- *Removes the SAAR as assigned to the Supervisor from the **My Tasks** tab.*

Figure 184: Security Officer Decision Screen - User Information

13. AMPS sends an email notification to the user regarding the approval's status.

Sample User Notification: Status

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: The Security Officer has completed an approval for SAAR #106077.

13 →

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

14. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

After the Security Officer approves the request, the status shows the SAAR has been forwarded to the **Data Owner** *for approval.*

A user can check SAAR listings in **Pending Requests** *to track the progress of any open SAAR.*

Note:

After a SAAR has been fully approved or rejected, AMPS moves this listing to the SAAR History table.

Procedure for External Security Officer Approval

An External Security Officer does not have or need an AMPS account to administer a security review of a role request. Instead, AMPS maintains a separate work queue for each External Security Officer that is accessible from a URL through a browser instance.

The procedure in this section provides the steps to follow for getting access to an External Security Officer work queue and addressing the action required to approve a role request.

1. After a user's External Supervisor approves a role request, AMPS sends an email notification to the user indicating the request has been approved by the Supervisor.

1

Sample User Notification: Confirmation

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: The External Supervisor has completed an approval for SAAR #106086.
The outcome for this task is APPROVE.
AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2. After a User's Supervisor approves a role request, AMPS sends an email notification to the user with the request's status, indicating the role request is waiting for the **External Security Officer's** approval.

2

Sample User Notification: Status

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: SAAR #106086 is awaiting External Security Officer approval.
This request was submitted in AMPS on 09/18/2017 09:36:54 EDT.

No action is required from you at this time.
This task expires on 10/09/2017 09:58:00 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

3. After a Supervisor approves a role request, AMPS sends an **Action Required** email notification to the user-specified **External Security Officer** indicating that a SAAR has been submitted for the Security Officer's approval.

3

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: SAAR #106086 - Request User Access for Teck, Denny (EDT0379) (DLA External) has been submitted for approval.
This request for DFAS DJMS Navy Prod - Navy Input User Field DJMSNAV-007 was submitted in AMPS on 09/18/2017 09:36:54 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=4141%3AatbBWr4PLzynMDEbn2x5YAqE%2FZOzw0H5fL6qMr9SILc%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/09/2017 09:58:00 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

4. Copy the URL provided in the Security Officer's **Action Required** notification, paste this URL into a browser instance, and navigate to the ***AMPS Approval Work Queue***.

If the AMPS displays a Consent to Monitoring *screen, review the content and click OK to proceed.*

AMPS displays the Approval Work Queue listing SAARs that require action from the logged in External Security Officer (see Figure 186).
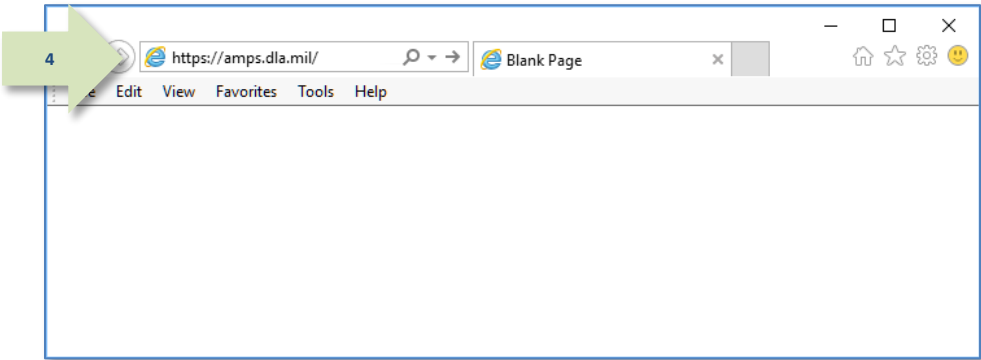
Figure 185: Requests Menu

5. In the **Approval Actions** list, click the SAAR number that was included in the email notification.

AMPS displays one of two possible screens:

- **Verify Approver** *(see Step 6), or*
- *The **Supervisor Application Access Decision** screen for the specified SAAR (see Steps 8).*
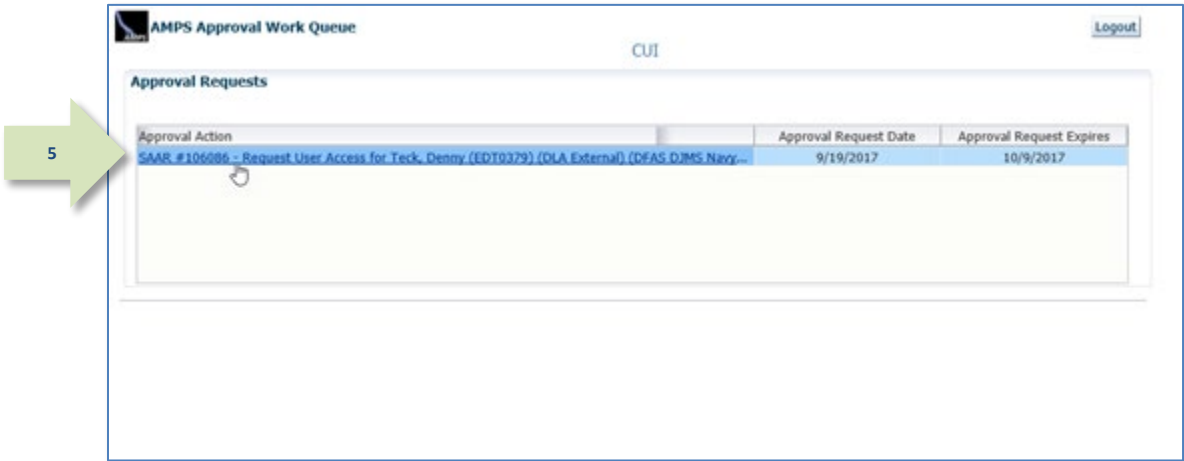
Figure 186: Approval Work Queue - Select an Approval Action

6. **OPTIONAL STEP:** If this approval is the first request to the External Security Officer from the identified Requestor, AMPS asks the Security Officer to verify his or her identity as the external user's Security Officer.

If the approver's name in the **Verify Approver** screen matches the name of the logged in External Security Officer for this requestor, the approver should click the **Verify** button.

This step eliminates the possibility that any other approver can act on the named requestor's role requests in the future.

Choose one of the following options:

- Click *Verify* if you ARE the requestor's Security Officer

- Click *Reject:* if you ARE NOT the requestor's Security Officer.

7. To proceed with the approval, click **Verify**.

AMPS displays the **Application External Security Officer Approval** *screen (see Figure 188).*
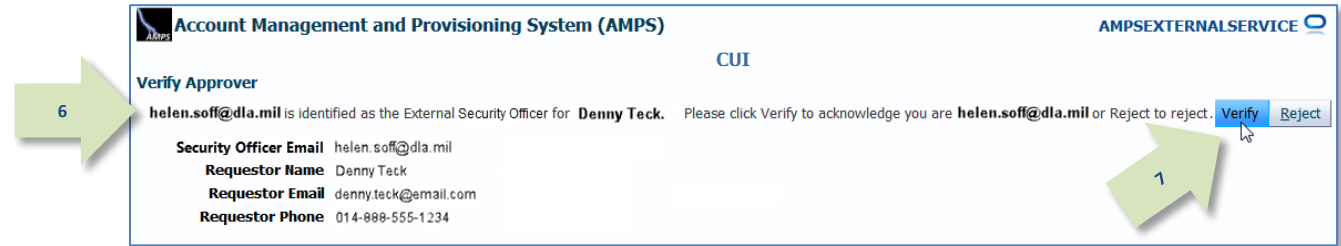
Figure 187: Security Officer Verification

8. Fill or correct entries in the required fields:

   ▪ **IT Level Designation:** select the requestor's IT level from the drop-down list.

   ▪ **Clearance Level:** select the requestor's Clearance Level from the drop-down list.

   ▪ **Type of Investigation:** select the investigation type conducted for the requestor from the drop-down list.

   ▪ **Date of Investigation:** select or enter the requestor's investigation date.

   ▪ **Security Review Flag:** DLA Security Officers can accept the default if they do not need to review a request from the user more than once a year. This flag does not affect DFAS Security Officers.

9. Click the **Additional Information** tab.

   *AMPS displays the **Additional Information** screen (see Figure 189).*

Figure 188: External Security Officer Decision – Role Request Details

10. In the **Additional Information** screen, note the **SAAR Approval History**.

    After the External Security Officer's decision is complete, AMPS displays identifying contact information, the decision outcome, and any Comments added to the SAAR history table.

    Also note the option to download and review any attached documents.

11. Click the **User Information** tab.

    AMPS displays the User Information screen (see Figure 190).

Figure 189: External Security Officer Decision - Additional Information

12. As an option, enter **Comments** to support the decision.

    Comments are not required for an approval, but AMPS passes them to the next approver when they are entered.

    Comments are required ONLY for a **Reject** *action. If you must reject the role request, AMPS requires you to enter text in the* **Comments** *area.*

13. Click **Approve**.

    AMPS automatically . . .
    - *Sends the SAAR to the next approver,*
    - *Removes the SAAR as assigned to the Supervisor from the AMPS Approval Work Queue, and*
    - *Displays a* **Task Completed** *message (see Figure 191).*

Figure 190: External Security Officer Decision - User Information

14. Click the link that reads **Return to the External Approval Worklist**.

    *AMPS displays the refreshed **Approval Work Queue** (see Figure 192).*
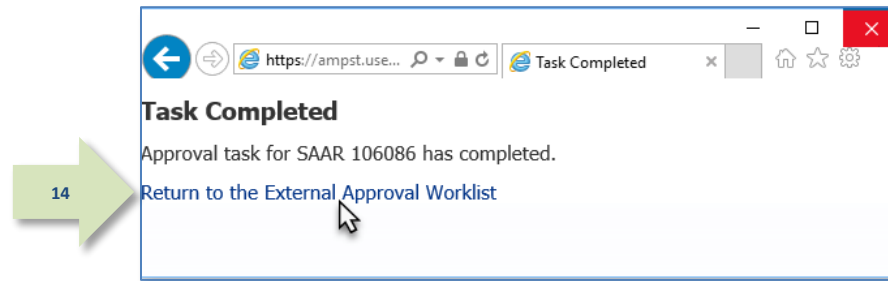
Figure 191: Approval Completed

15. If you have completed work for the current session, click the **Logout** button in the AMPS **Approval Work Queue** window.

    AMPS displays a logout message (see Figure 193).
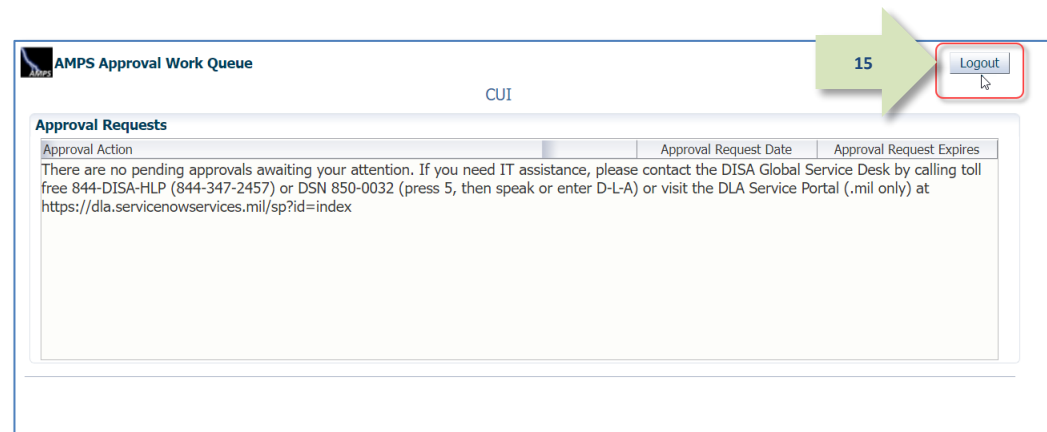
Figure 192: Modify Approver Information

16. Review the logout message and close the browser.
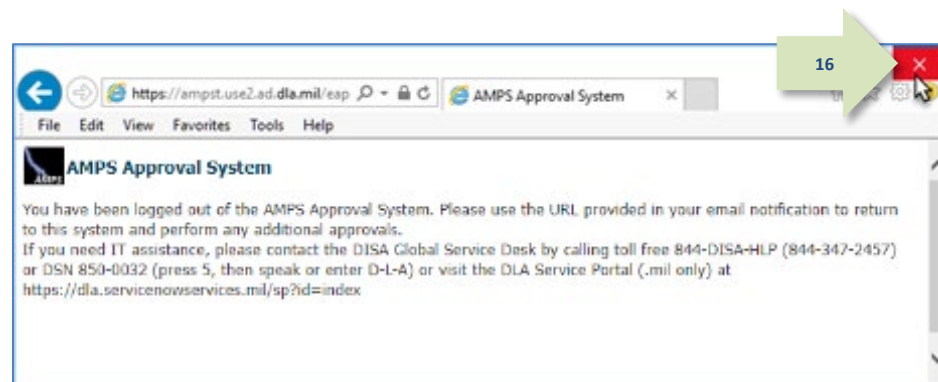
Figure 193: AMPS Approval System - Logout Message

17. After the approval is submitted, AMPS sends an email notification to the user regarding the approval's status.

17

Sample User Notification: Status

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: The External Security Officer has completed an approval for SAAR #106086.
The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

18. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

After the External Security Officer approves the request, the status shows the SAAR has been forwarded to the External Authorizing Official for approval. If there is no External Authorizing Official for the role being requested, the next approver in the queue is the Data Owner.

*A user can check SAAR listings in **Pending Requests** to track the progress of any open SAAR.*

Note:

After a SAAR has been fully approved or rejected, AMPS moves this listing to the SAAR History table.

External Authorizing Official Approval

An External Authorizing Official (EAO) is required as an approver for certain roles available to some external users. AMPS notifies this approver of a pending approval action after the Security Officer submits an approval for the role request.

The procedure in this section provides the steps to follow for getting access to an External Authorizing Official work queue and addressing the action required to approve a role request.

Procedure for EAO Approval

Note:

> Your external approvers must be three separate and distinct individuals with different email addresses.

1. After a User's Security Officer approves a role request, AMPS sends the following email notifications to the user with the request's status, indicating the role request is waiting for the **External Authorizing Official's** approval.
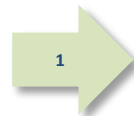
Sample User Notifications: Status

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: The External Security Officer has completed an approval for SAAR #106086.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

1

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: SAAR #106086 is awaiting External Authorizing Official approval.
This request was submitted in AMPS on 09/18/2017 09:36:54 EDT.
No action is required from you at this time.
This task expires on 10/09/2017 12:32:26 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After a Security Officer approves a role request, AMPS sends an email notification to the user-specified **External Authorizing Official** indicating that a SAAR has been submitted for the EAO's approval.

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

2

Body: SAAR #106086 - Request User Access for Teck, Denny (EDT0379) (DLA External) has been submitted for approval.
This request for DFAS DJMS Navy Prod - Navy Input User Field DJMSNAV-007 was submitted in AMPS on 09/18/2017 09:36:54 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=0210%3Ay1Rq24i%2BQEQ3KDaRobgXRHvLMwXFTmqj2iRA8qVufK4%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/09/2017 12:32:26 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

3. The EAO copies the URL provided in the EAO's **Action Required** notification, pastes this URL into a browser instance, and navigates to the *AMPS Approval Work Queue*.

AMPS displays a link to the SAAR that requires an action from an External Authorizing Official (see Figure 195).
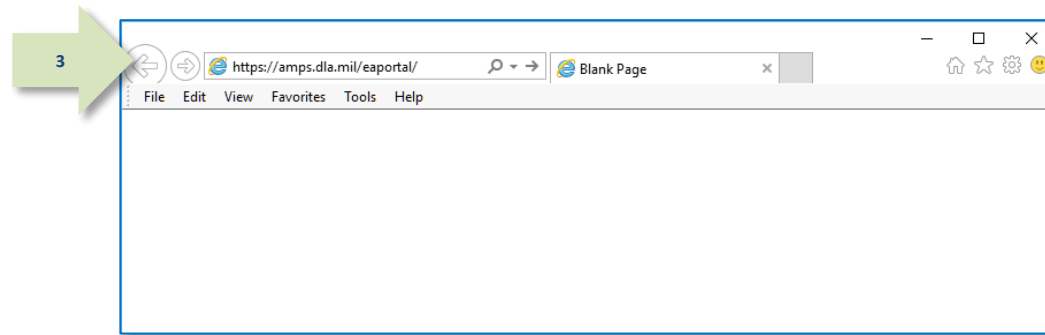
Figure 194: External Approver's URL

4. In the **Approval Actions** list, the EAO clicks the SAAR indicated in the email notification.

AMPS displays one of two possible screens:

▪ **Verify Approver** *(See Step 5),* or

▪ *The* **External Authorizing Official Approval** *screen for the specified SAAR (see Step 6).*
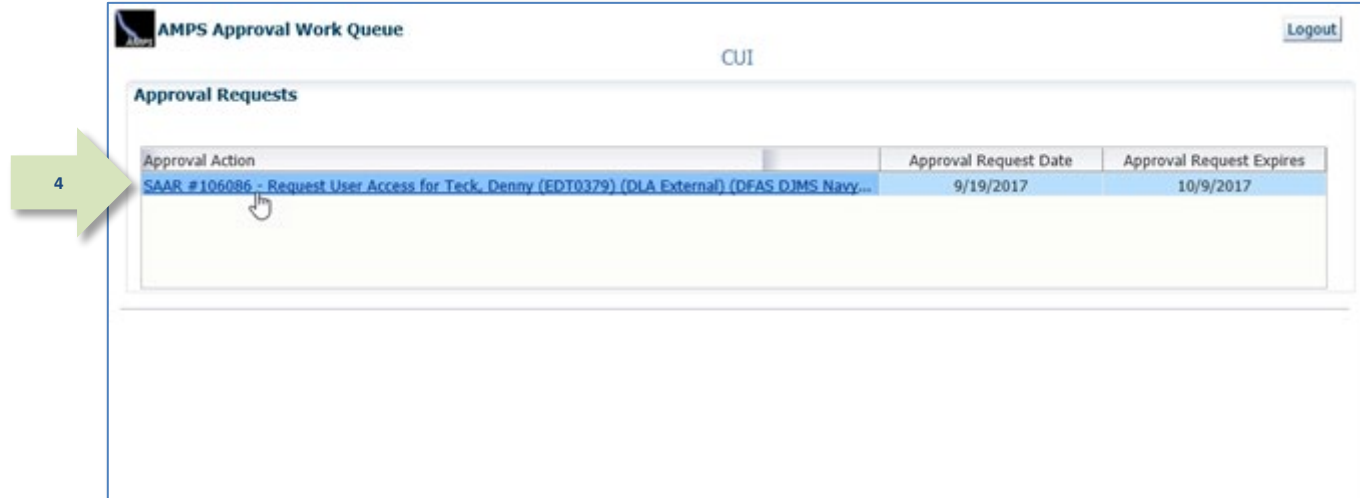
Figure 195: Approval Work Queue - Select an Approval Action

5. **OPTIONAL STEP:** The EAO reviews
    the content of the External
    Authorizing Official **Verify
    Approver** screen, if it is displayed.

    If this approval is the first request
    for the External Authorizing Official
    from the identified Requestor,
    AMPS asks the EAO to verify his or
    her identity as the external user's
    EAO.

    If the approver is the correct
    External Authorizing Official for this
    requestor, the approver should
    click **Verify**.

    *This step eliminates the possibility
    that any other EAO approver can act
    on the named requestor's role
    requests in the future.*

Figure 196: Verify Approver Screen - External Authorizing Official

6. The EAO fills in the required fields, as needed, and reviews the role and user information to ensure the user has requested the correct role.

7. The EAO clicks the **Additional Information** tab.

   AMPS displays the Additional Information screen (see Figure 198).

Figure 197: External Authorizing Official Decision – Role Request Details

8. In the **Additional Information** screen tab, note the **SAAR Approval History**.

   *The **SAAR Approval History** table records the identifying contact information for the current role request. Entries for the current approver are entered after the approver completes and submits a decision.*

   Also note the option to download and review any attached documents.

9. The EAO clicks the **User Information** tab.

   AMPS displays the User Information screen (see Figure 199).

Figure 198: External Authorizing Official Decision - Additional Information

10. As an option, the EAO can enter comments to support the decision.

Comments are not required for an approval, but AMPS passes them to the next approver after the approval is submitted.

*Comment text is a **required** entry if you want to **Reject** the user's request. These comments are forwarded to the user in an email that notifies the user about the request's rejection.*

11. The EAO clicks **Approve**.

AMPS automatically . . .
- *Sends the SAAR to the next approver,*
- *Removes the SAAR as assigned to the EAO from the **AMPS Approval Work Queue**, and*
- *Displays a **Task** Completed message (see Figure 200).*

Figure 199: External Authorizing Official Decision - User Information

12. The EAO clicks **Return to the External Approval Worklist** in the **Task Completed** message.

    *AMPS returns to the **Approval Work Queue** (see Figure 201).*

Task Completed

Approval task for SAAR 106086 has completed.

12 Return to the External Approval Worklist
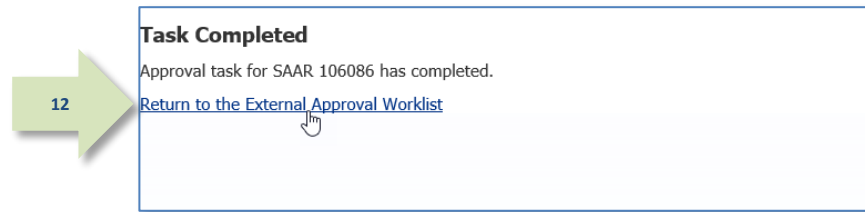
Figure 200: Approval Completed

13. The EAO clicks the **Logout** button in the AMPS **Approval Work Queue** window.

    AMPS displays a logout message (see Figure 202).

AMPS Approval Work Queue

13 Logout

CUI

Approval Requests

Approval Action			Approval Request Date	Approval Request Expires

There are no pending approvals awaiting your attention. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 201: Approval Work Queue – Logout Button

14. The EAO reviews the logout message and closes the browser.

14

https://ampst.use2.ad.**dla**.mil/eap   AMPS Approval System

File   Edit   View   Favorites   Tools   Help

AMPS Approval System

You have been logged out of the AMPS Approval System. Please use the URL provided in your email notification to return to this system and perform any additional approvals.
If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 202: AMPS Approval System - Logout Message

15. After the approval is submitted, AMPS sends email notifications to the user regarding the approval's status.

Sample User Notification: Status

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: The External Authorizing Official has completed an approval for SAAR #106086.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

15

Subject: Notification: SAAR #106086 - Request User Access for Denny Teck (EDT0379) (DLA External) (DFAS DJMS Navy) 09/18/2017 09:36:54 EDT

Body: SAAR #106086 is awaiting Data Owner approval.

This request was submitted in AMPS on 09/18/2017 09:36:54 EDT.
No action is required from you at this time.

This task expires on 10/09/2017 13:48:31 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

16. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

After the External Authorizing Official approves the request, the status shows the SAAR has been forwarded to the Data Owner for approval.

A user can check SAAR listings in **Pending Requests** *to track the progress of any open SAAR.*

Note:

After a SAAR has been fully approved or rejected, AMPS moves this listing to the SAAR History table.

Data Owner Approval

The following procedure explains how to approve a role request by starting at the AMPS Home page.

This procedure applies to internal user and external user role requests.

1. After the Security Officer approves a role request, AMPS sends an email notification to the user with the request's status.

1

Sample User Notification: Status

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: The Security Officer has completed an approval for SAAR #106077.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After the Security Officer approves a role request, AMPS sends an additional email notification to the user indicating the approval of the request has been forwarded to the Data Owner.

2

Sample User Notification: Status

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: SAAR #106077 is awaiting Data Owner approval.

This request was submitted in AMPS on 09/14/2017 09:27:35 EDT.
No action is required from you at this time.
This task expires on 10/04/2017 13:04:52 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

3. After the Security Officer approves a role request, AMPS sends an email notification to the application's Data Owner, indicating that a SAAR has been submitted for the Security Officer's approval.

3

Sample Approver Notification

Subject: Action Required: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: SAAR #106077 - Request User Access for Teck, Rupert (DRT0021) (DFAS Columbus) has been submitted for approval.
This request for DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319 was submitted in AMPS on 09/14/2017 09:27:35 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/04/2017 13:04:52 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

4. In the AMPS banner, click your
    User ID to open the User ID
    dropdown menu, then click
    Inbox from the menu.

    *AMPS opens the **Approval Details**
    screen to the **My Tasks** tab
    (see Figure 204).*
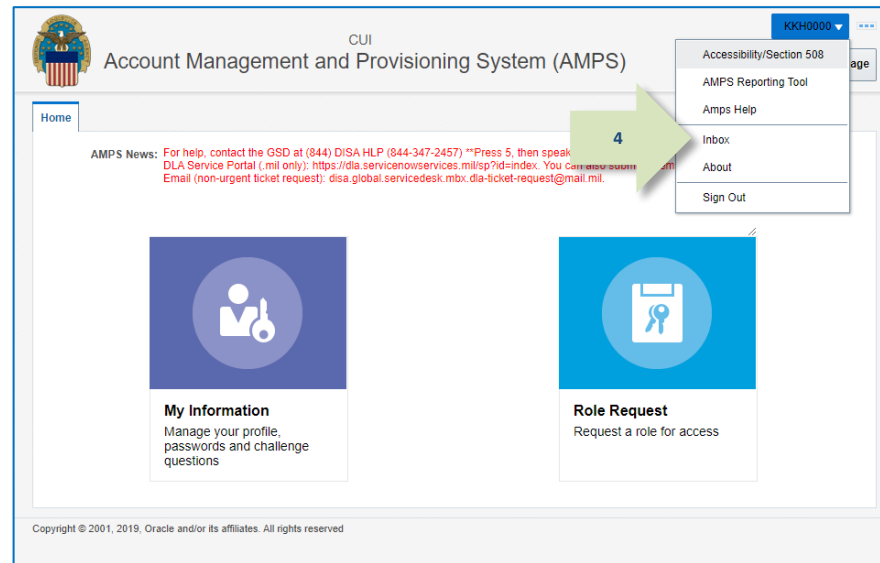
Figure 203: Inbox Command

5. On the **My Tasks** screen, click the
    SAAR number indicated in the
    email notification.

    *AMPS displays the **Data Owner
    Application Access Decision**
    screen for the SAAR
    (see Figure 205).*
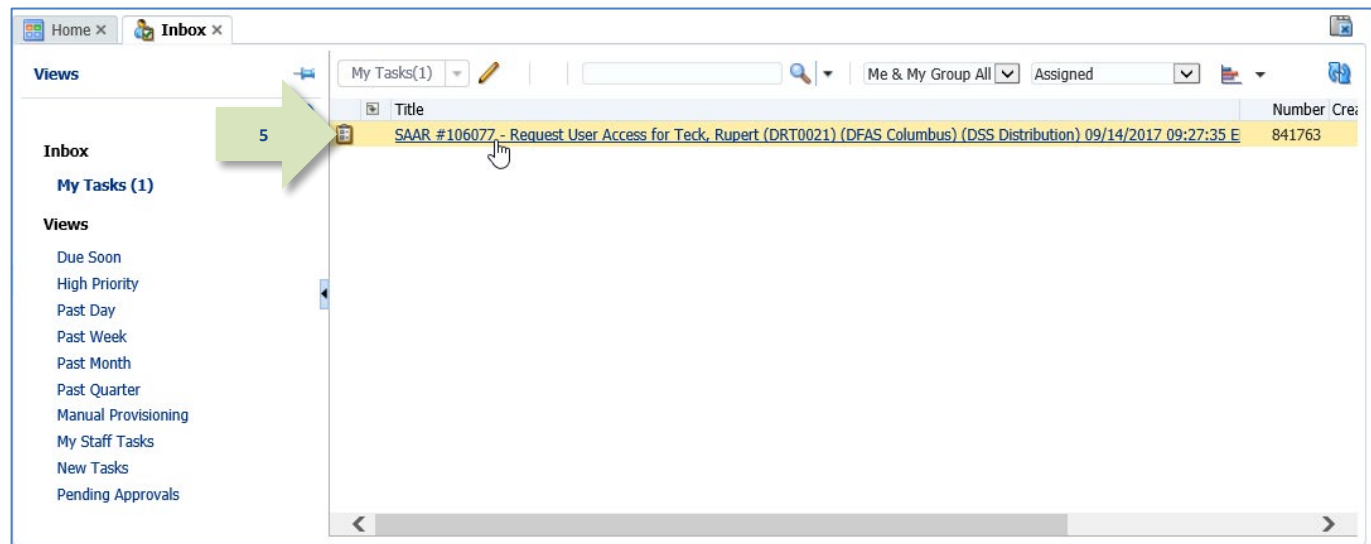
Figure 204: My Tasks

Data Owner Decision Screen and Tabs

Most approval screens for Data Owners have standard content as shown in the sample screen (see Figure 205). EBS Data Owners see a screen with an additional Segregation of Duties/Governance, Risk and Compliance (SOD/GRC) section that reports possible SOD conflicts. See **Appendix F: SOD/GRC Reports in the Role Request Approval Process** for more information.

6. In the **Data Owner Decision** screen, complete the entries for required fields.

   a. **Start Date (auto-filled):** Required entry. The **Start Date** must not be earlier than the current date.

   b. **End Date (auto-filled):** Required entry. Change this date, as needed. External User role assignments are limited to 365 days.

   c. **Comments:** As an option, enter comments to support the decision. Comments are not required for an approval, but AMPS passes them to the next approver when they are entered.

   Comments appear on the **Additional Information** *tab.*

7. Click the Additional Information tab.

   AMPS displays the **Additional Information** *screen (see Figure 206).*

Figure 205: Data Owner Approval Screen

8. As an option in the **Additional Information** tab, you can download and review any of the documents the user has included as supporting information.

   To view a document, click Download and Review Document.

   AMPS downloads the PDF file and automatically opens the document in Adobe Reader.

9. Click User Information.

   *AMPS displays the **User Information** tab (see Figure 207).*

Figure 206: Data Owner Decision Screen - Additional Information

10. In the **User Information** tab, review the user account, contact, organization, and supervisor information to help verify the correct user is requesting the role specified in the **Pending Requests** table (see bottom of screen, Figure 207).

As an option, enter supporting comments in the **Comments** text area.

Comments are not required for an approval but will be captured in the **Additional Information** *screen that is passed to the next approver.*

11. Click **Approve**.

AMPS automatically . . .

- *Sends the SAAR to the next approver, if applicable, and*
- *Removes the SAAR as assigned to the Data Owner from the* **My Tasks** *tab.*

Figure 207: Data Owner Decision Screen - User Information Tab

12. After the approval is submitted, AMPS sends an email notification to the user regarding the approval's status.
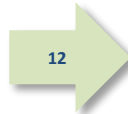
Sample User Notification: Status

Subject: Notification: SAAR #102046 - Request User Access for Simon Teck (DST9218) (DFAS Columbus) (DFAS SABRS) 08/01/2016 10:56:57 EDT

Body: The Data Owner has completed an approval for SAAR #106077.

12 → The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

13. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

If the role is a DLA role...

The status shows the SAAR is **TICKETED**. *This approved request is forwarded to the* ***application Provisioner*** *for action.*

If the role is a DFAS role...

The status shows the SAAR has been forwarded to the **Information Assurance Officer** *for approval.*

Note:

After a SAAR has been fully approved or rejected, AMPS moves this listing to the SAAR History table.

Information Assurance Officer Approval (DFAS users only)

The following procedure explains how to approve a role request by starting at the AMPS Home page. This procedure applies only to customer applications, such as DFAS applications that require an IAO approval.

Note:

DLA applications do not require IAO approval.

However, if a DLA user requests a DFAS role, an approval by a DFAS IAO is required.

---

1. After the DFAS Data Owner approves a Role Request, AMPS sends an email notification to the User indicating whether or not the request has been approved.

Sample User Notification: Status

Subject: Notification: SAAR #106077 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DSS Distribution) 09/14/2017 09:27:35 EDT

Body: The Data Owner has completed an approval for SAAR #106077.

> **1**

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

2. After the DFAS Data Owner approves a Role Request, AMPS sends an email notification to the user with the request's status.

Sample User Notification: Status

Subject: Notification: SAAR #106067 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DFAS SABRS) 09/12/2017 10:15:37 EDT

> **2**

Body: SAAR #102046 is awaiting Information Assurance Officer approval.

This request was submitted in AMPS on 08/01/2016 10:56:57 EDT.

No action is required from you at this time.

This task expires on 08/21/2016 14:03:43 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

3. After the DFAS Data Owner approves a Role Request, AMPS sends an email notification to the user's Information Assurance Officer (IAO), indicating that a SAAR has been submitted for the IAO's approval.

Sample Approver Notification

Subject: Action Required: SAAR #106067 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DFAS SABRS) 09/12/2017 10:15:37 EDT

> **3**

Body: SAAR #106067 - Request User Access for Teck, Rupert (DRT0021) (DFAS Columbus) has been submitted for approval.

This request for DFAS SABRS Prod - DFAS Systems Maint Team SABRS-020 was submitted in AMPS on 09/12/2017 10:15:37 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/04/2017 15:00:32 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

4. In the AMPS banner, click your User ID to open the User ID dropdown menu, then click **Inbox** from the menu.

   *AMPS displays the **Inbox** tab and automatically opens the standard **My Tasks** view for the currently logged in user (see Figure 209).*
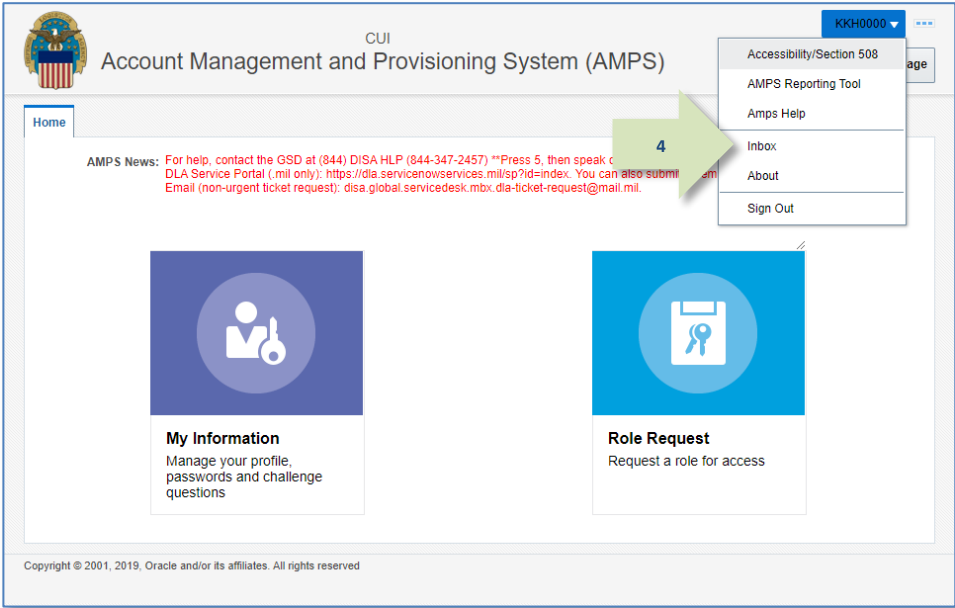
Figure 208: Inbox Command

5. In the **My Tasks** screen, click the SAAR number indicated in the email notification.

   AMPS displays the SAAR approval tab for the selected SAAR (see Figure 210).
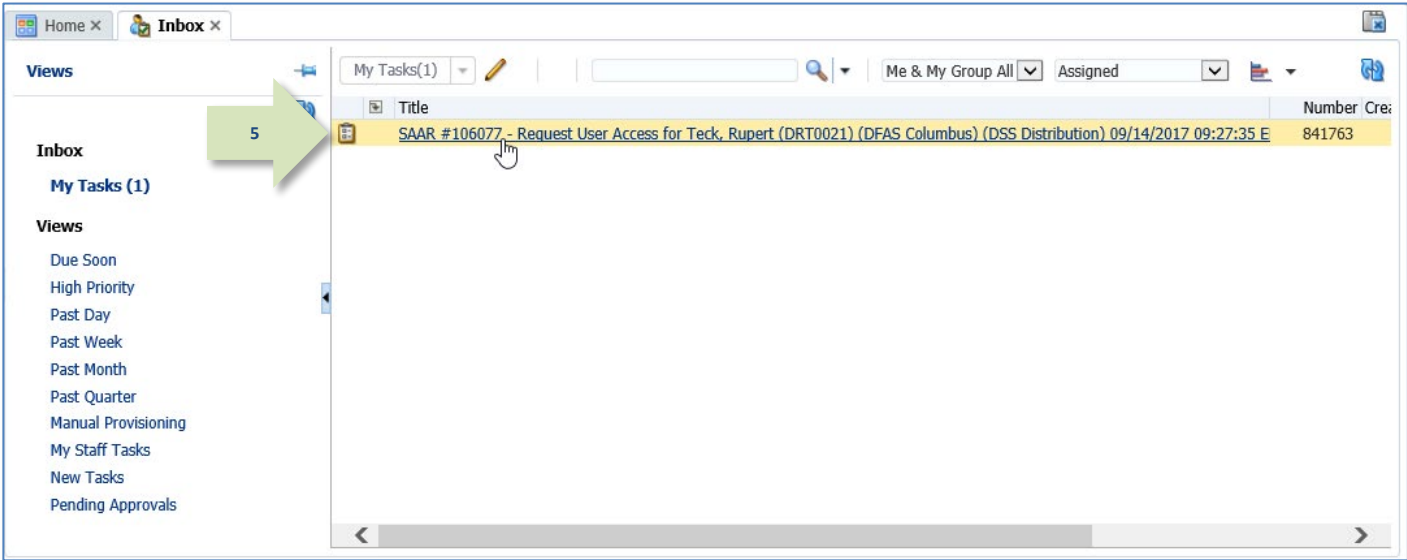
Figure 209: Approval Details - My Tasks

6. In the Information Assurance Officer Application Decision screen, fill in the required fields:

   - **Cyber Awareness Training Date (auto-filled from user record, if available):** Enter or select the correct date for the requestor's Cyber Awareness Training Date, as needed.

   - **DLA users only:** an IAO approval for role requests is not required.

7. Click Additional Information.

   *AMPS displays the **Additional Information tab (see Figure 211).***

Figure 210: Information Assurance Officer Decision Screen – Role Request Details Tab

8. As an option in the **Additional Information** tab, you can download and review any of the documents the user has included as supporting information.

    To view a document, click Download and Review Document.

    AMPS downloads the PDF file and automatically opens the document in Adobe Reader.

9. Click User Information.

    AMPS displays the User Information tab (see Figure 212).

Figure 211: Information Assurance Officer Decision - Additional Information Tab

10. In the **User Information** tab, review the user account, contact, organization, and supervisor information to help verify the correct user is requesting the role specified in the **Pending Requests** table (see bottom of screen).

11. As an option, enter supporting comments in the **Comments** text area.

   Comments are not required for an approval but will be passed to the next approver in the Additional Information screen.

12. Click **Approve**.

   AMPS automatically provides the customer's provisioning service per the application's service agreement with AMPS: either a provisioning ticket directed to application provisioners or automated provisioning through an AMPS-to-application connector.

Figure 212: Information Assurance Officer Decision - User Information Tab

13. AMPS sends an email notification to the user regarding the approval's status.

13

Sample User Notification: Status

Subject: Notification: SAAR #106067 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DFAS SABRS) 09/12/2017 10:15:37 EDT

Body: The Information Assurance Officer has completed an approval for SAAR #106067.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

14. AMPS displays information from a completed SAAR in the **Current Roles** and **Request History** tables of the user's **Applications & Roles** tab on the **My Information** screen. If, however, the access requires provisioning, the SAAR will still be in the **Pending Requests** table.

In the example (Figure 213) the listing shows the SAAR has been approved but not yet provisioned. The SAAR status is "TICKETED".

After the role is provisioned, the system name and account are listed in the Provisioned Accounts section.

See the section entitled What Comes After the Final Approval? (page 199) for more information.

14

Figure 213: Applications & Roles - Provisioned Accounts and Current Roles

What Comes After the Final Approval?

At this stage, the role approval process is complete. The next stage involves provisioning the role, which includes the following processes:

- Creating the user's account in the application.
- Assigning the appropriate permissions to the user's account, which enables the user to perform tasks in the application.

Provisioning methods vary by customer:

- If your application is set up for automated provisioning, AMPS will complete that process and notify you when your application account has been created based on the role you requested. As a user, you will be able to access your account approximately 20 minutes after AMPS sends the notification.

- Other customers prefer to perform provisioning themselves in one of two ways:
    - **Remedy Ticketing:** Receive a Remedy ticket, generated by AMPS, with provisioning data included in it.
    - **Total AMPS Ticketing:** Use an automatically generated AMPS ticket as a source of information for setting up the account. This process is called Total AMPS.

Total AMPS

The **Provisioning Process: Total AMPS** section in this *User's Guide* provides a description of the Total AMPS procedure for provisioning a role through a ticketing process. See page 204.

Role Request Approval Subprocesses

Role request approval subprocesses include alternate paths for handling role requests. The following table introduces a subprocess for alternate procedures described in this section.

This subprocess . . .	Enables an approver to . . .
Reject a Role Request	Deny a user a request for a role. The request rejection process occurs during the approval process itself, and any approver can reject a role request. AMPS requires the rejecting user to enter reasons for the rejection in the Comments field. The reasons entered may provide the basis for corrective action on the part of the user or other approvers.

How to Reject a Role Request

What you can do: In AMPS, any approver who has a valid reason to reject a role request can do so during the standard approval process. The procedures that follow illustrate the process in AMPS and explain the few steps required to bring up a role request approval form and select a rejection, rather than an approval, option.

- Follow this procedure if you are a **Supervisor** or other approver and you need to reject a user's role request.
- Follow this procedure **if you are NOT the user's Supervisor,** which means you are not authorized to approve the user's role request and, therefore, must reject the role request.

Where to start: To reject a role request, start on the **Home** page, and navigate to the **Approval Details** screen, which lists pending tasks.

If a user has requested an incorrect role, but the role has been fully approved and provisioned, a Role Removal procedure can remove the role from the user's account. See the section entitled *Role Removal*.

1. After a user submits a role request, AMPS notifies the Supervisor by email of a pending action.

1 ➡

Sample Approver Notification

Subject: Action Required: SAAR #106083 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (AMPS) 09/15/2017 14:15:50 EDT

Body:

SAAR #106083 - Request User Access for Teck, Rupert (DRT0021) (DFAS Columbus) has been submitted for approval.

This request for DFAS Prod - BI Publisher Developer DFAS-801 was submitted in AMPS on 09/15/2017 14:15:50 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/05/2017 14:15:58 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2. In the AMPS banner, click your User ID to open the User ID dropdown menu, then click **Inbox** from the menu.

   AMPS opens the **Inbox** *tab screen.*

   The SAAR is listed in the My Tasks list (see Figure 215).
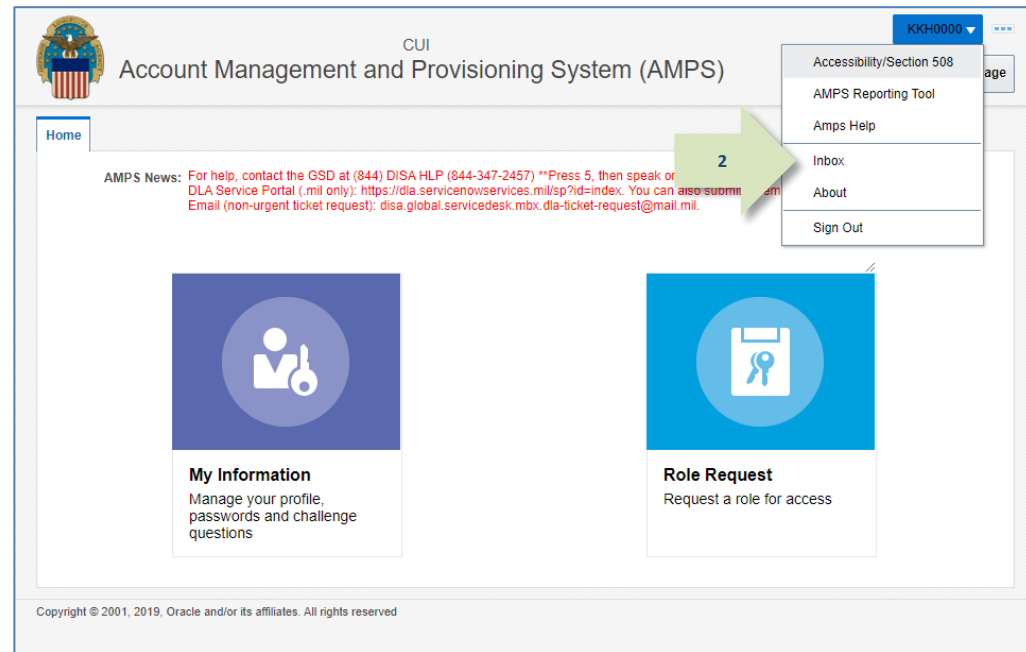
Figure 214: Inbox Command

3. In the **My Tasks** list, click the SAAR number indicated in the email notification.

   AMPS opens the **Approval Decision** *screen for the appropriate approver (see Figure 216).*

   In the example provided in this procedure, the approver's screen illustrated is the Supervisor Decision screen. However, the same steps apply to other approvers.
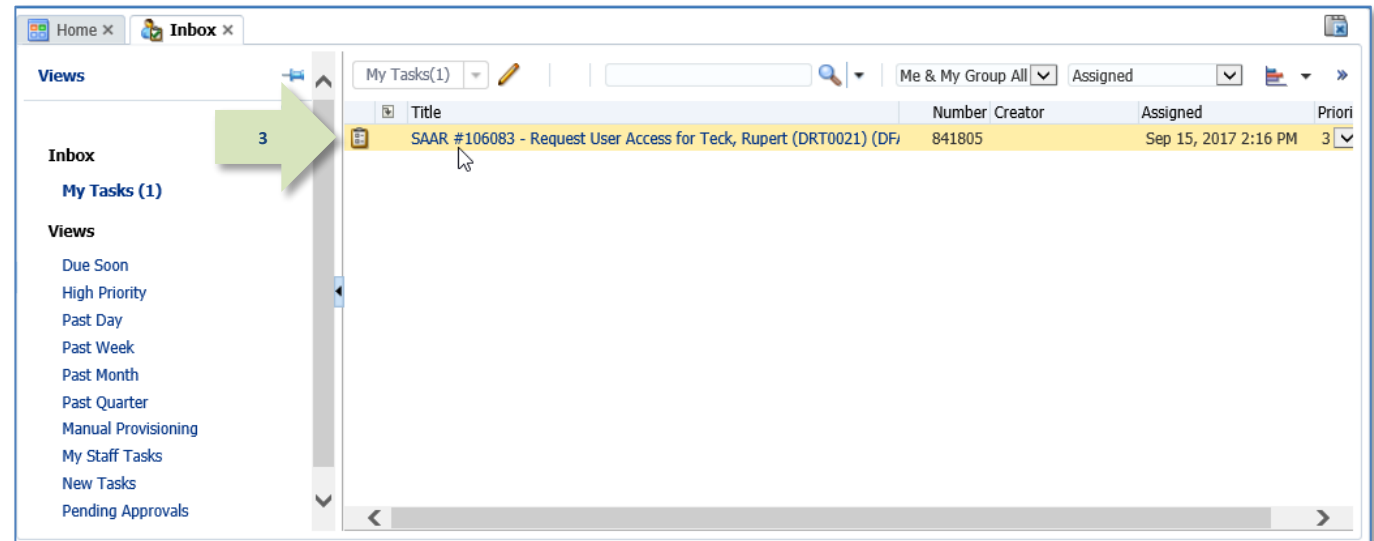
Figure 215: Inbox Tab - My Tasks List

4.　After making a determination to reject a role request, the approver must enter text to summarize the reasoning for the rejection.

This text goes in the **Comments** text area. Entering this text activates the **Reject** button.

AMPS saves these comments as part of the SAAR record.

Note:

The text in the Comments in Figure 216 is for illustrative purposes only. Please enter text relevant to the SAAR before clicking the Reject button.

Note:

An approver can also review data on the Additional Information or User Information tab before making the decision to reject the current role request.

5.　Click **Reject**.

AMPS displays a confirmation request (see Figure 217).

Figure 216: Approver's Decision Screen

6. AMPS displays a request for confirmation of the rejection action.

7. Click **OK** to confirm the rejection.

AMPS automatically . . .

- *Removes the SAAR as assigned to the current approver from the approver's **My Tasks** tab.*

- *Stores the number of the rejected SAAR and its information for display in the user's role status tab.*
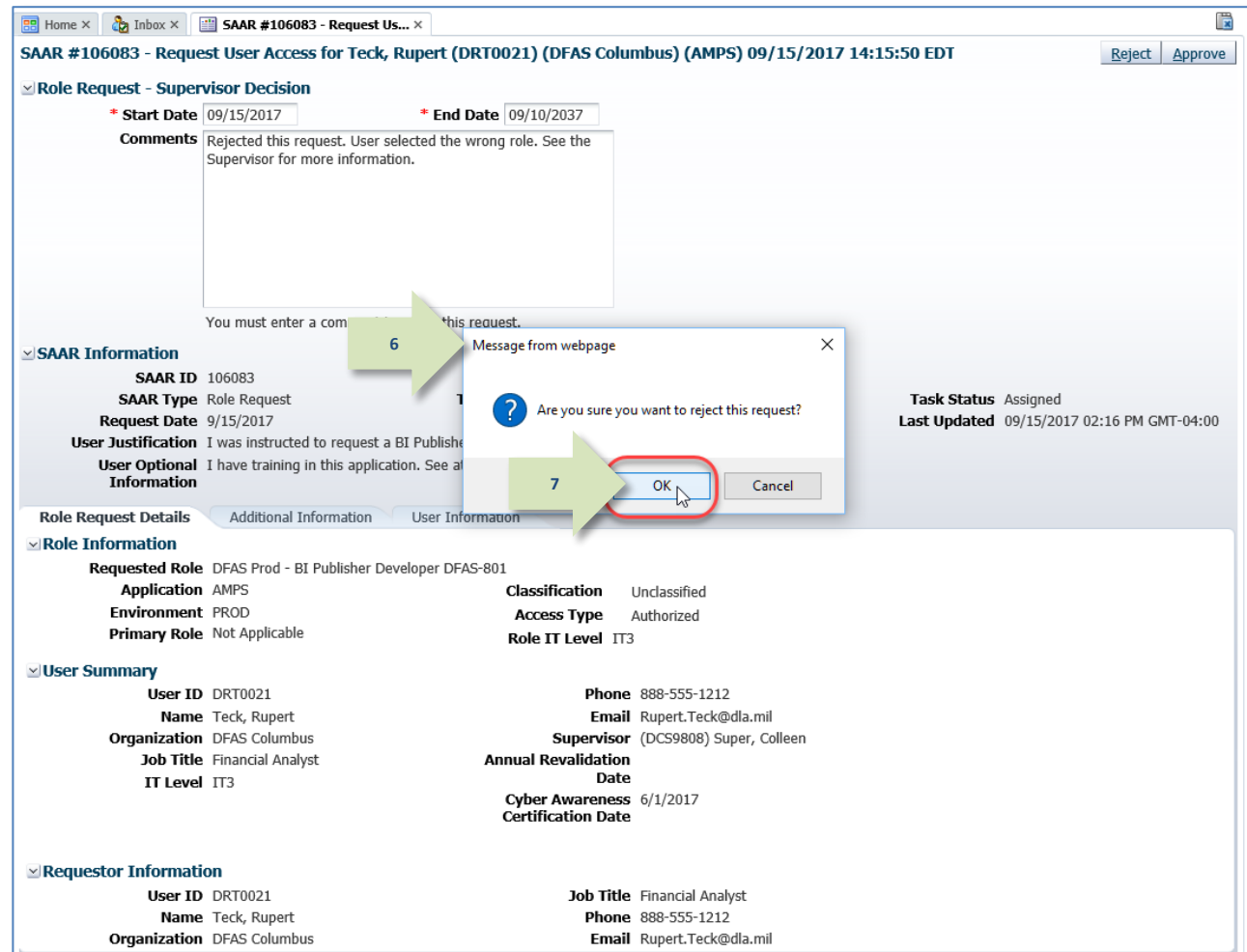
Figure 217: Confirmation of the *Reject* Request

8. AMPS sends an email notification to the user regarding the outcome of the request.

   Check with your Supervisor to correct any deficiency in your request and submit a new role request.

Sample User Notification: Rejection Notice

Subject: Notification: SAAR #106083 - Request User Access for Rupert Teck (DRT0021) (DFAS Columbus) (AMPS) 09/15/2017 14:15:50 EDT

Body: The Supervisor has completed an approval for SAAR #106083.

The outcome for this task is REJECT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Provisioning Process: Total AMPS

When a Provisioner for a user's organization receives a notification to assign a user to an application with a certain role, the request for that role has been approved. The Provisioner's task is to assign the user the requested role. Users should check with their Supervisors for more information about how provisioning tickets are handled for an application. This section discusses one ticket-handling method called "Total AMPS."

Total AMPS represents a ticketing method that provides an alternative to Remedy ticket procedures for customers who perform manual provisioning. The procedure in this section furnishes the steps a Total AMPS provisioner takes to perform the following tasks in AMPS:

- Open a Total AMPS ticket,
- Fill in comments to indicate work in progress, as needed, as well as work completed, and
- Complete the Total AMPS ticket.

A provisioner can open the ticket, enter comments, and save the commented ticket without completing it, if necessary, to document the provisioning process.

AMPS notifies the user through email when provisioning of the role is complete.

Note:

Manual provisioning takes place outside the AMPS provisioning process itself; completing a ticket within AMPS signals to the system that provisioning is complete. Records of completed Total AMPS tickets appear on AMPS reports.

How to Provision a Role through Total AMPS

1. AMPS sends the requesting user an email notification indicating the SAAR has been submitted for provisioning.

1

Sample User Notification

Subject: AMPS Application Processing for SAAR #106067

Body:

AMPS Application Processing request for SAAR 106067 has started.

```
Request For:
DLA Login: DRT0021
Name: Teck, Rupert
Phone: 888-555-1212
Email: Rupert.Teck@dla.mil
EDIPI/UPN: 1286972493

Access Information:
SAAR #: 106067
Effective Date: 09/12/2017
End Date: 09/07/2037

Add Job Role: DFAS SABRS Prod - DFAS Systems Maint Team SABRS-020

Applications and Access:
        Resource: DFAS Prod - SABRS
                Add: CICS$TST
                Add: M$SABSAT
                Add: M$SABSIT
                Add: MQ$SAT
                Add: ROSCOE$
                Add: SABRS-020 TKA#SAB1
                Add: TAK@CICS
                Add: TJOBS$
                Add: TKA$SAB1
                Add: TKA$SAB5
                Add: TKA$SABA
                Add: TPANUSR$
                Add: TSO$
```

Data Owner Comments: (none)

Justification: I need this role to perform my job tasks.

Optional Information: I have received training in this application. Certificate is attached.

Role Request SAAR requested by Rupert Teck on 09/12/2017

2. AMPS sends the application's
    Provisioner an email notification
    indicating a SAAR has
    been submitted
    for provisioning.

2

Note:

If the Data Owner added any
comment text to the Data Owner
approval screen, those comments are
included on the Total AMPS
provisioning ticket for a role request.

Sample Provisioner Notification

Subject: AMPS Application Processing for SAAR #106067 requires your attention.

Body:
AMPS Application Processing request for SAAR 106067 requires your attention.

```
Request For:
DLA Login: DRT0021
Name: Teck, Rupert
Phone: 888-555-1212
Email: Rupert.Teck@dla.mil
EDIPI/UPN: 1286972493


Access Information:
SAAR #: 106067
Effective Date: 09/12/2017
End Date: 09/07/2037


Add Job Role: DFAS SABRS Prod - DFAS Systems Maint Team SABRS-020

Applications and Access:
        Resource: DFAS Prod - SABRS
                Add: CICS$TST
                Add: M$SABSAT
                Add: M$SABSIT
                Add: MQ$SAT
                Add: ROSCOE$
                Add: SABRS-020 TKA#SAB1
                Add: TAK@CICS
                Add: TJOBS$
                Add: TKA$SAB1
                Add: TKA$SAB5
                Add: TKA$SABA
                Add: TPANUSR$
                Add: TSO$


Data Owner Comments: (none)


Justification: I need this role to perform my job tasks.


Optional Information: I have received training in this application. Certificate is attached.


Role Request SAAR requested by Rupert Teck on 09/12/2017
```

3. In the AMPS banner, click your User ID to open the User ID dropdown menu, then click **Inbox** from the menu.

   *AMPS displays the **My Tasks** view for the current Provisioner (see Figure 219).*

Figure 218: User ID Dropdown Menu – Inbox Command

4. The Provisioner checks the list of provisioning tickets listed in the **My Tasks** view.

5. The Provisioner clicks the number and title of the SAAR that corresponds to the notification.

   AMPS displays the Total AMPS provisioning ticket for the SAAR.

Tip:
At this point, the provisioner checks the ticket details (see Figure 220) and uses the information to provision the requested role for the user in the specified resource.
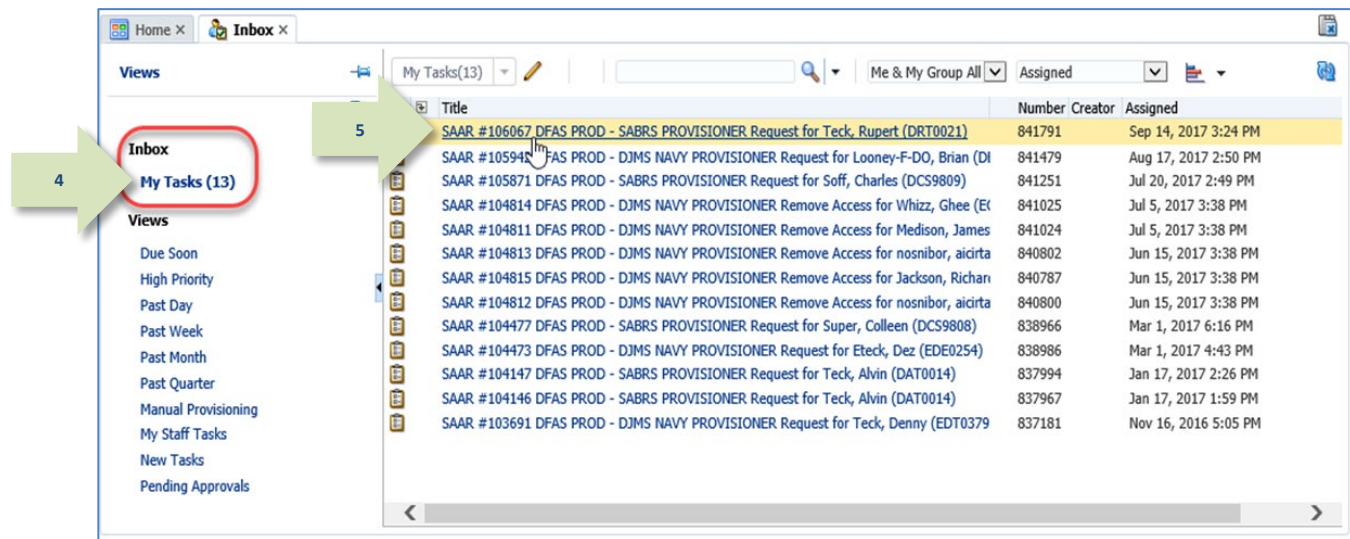
Figure 219: Sample Provisioner's Approval Details - My Tasks Tab

6. The Total AMPS ticket offers the provisioner these features. The provisioner can . . .

   a. Click the **Claim** button, and then enter comments and click **Save Comments** to preserve current work and maintain exclusive control over the ticket for three calendar days.

      AMPS saves and closes the request, enabling the provisioner to close and later reopen the incomplete ticket to perform the prescribed provisioning work.

   b. Enter comments and click **Save Comments** to preserve the Provisioning ticket. Reopen the ticket, as needed, to enter final comments in the required **Comments** text area.

   c. Click **Work is Complete** when provisioning is complete.

      AMPS closes the request.

      AMPS also moves a record into the user's **SAAR History** *indicating that the role has been provisioned to the user's account (see Figure 221).*

Figure 220: Sample Application Request Provisioning Ticket - Total AMPS

*AMPS completes the provisioning process by moving the role record from the user's **Pending Requests** table to the user's **Current Roles** table in the **Applications & Roles** tab of **My Information**.*

*AMPS lists the completed SAAR in **SAAR History**.*

Figure 221: Provisioned User's Applications & Roles Tab - Current Roles

7. AMPS sends the user an email confirmation indicating that administrative staff have completed provisioning of the role.

Sample User Notification: Confirmation of Role Provisioning

Subject: AMPS Application Processing for SAAR #106067

Body: Your request for role DFAS SABRS Prod - DFAS Systems Maint Team SABRS-020 with access to DFAS SABRS (SAAR 106067) has been fully approved and provisioned.

Your account has been set up with the permissions associated with the role you requested, and you can now access the application.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Role Maintenance

Role maintenance procedures enable you to perform the following tasks:

- Update additional role attributes.
- Remove a role from your AMPS account and the corresponding applications.

A Note on Attribute Change Requests...

Note that in past versions of AMPS, the system provided attribute changes through a vehicle called a "999 role." With the release of AMPS 17.2.0, the system no longer uses 999 roles.

Instead, users update additional role attributes through a sequence of screens similar to a role request.

How to Update Additional Attributes

AMPS captures a wide range of basic information in the My Profile areas of AMPS that is required by the resources it provisions. Some roles, however, require additional information, such as access codes, that pertain to resources. AMPS also captures this information in the form of Additional Role Attributes. To achieve this aim, AMPS must store and manage those attributes required by the various resources that it provisions. This information includes attributes such as name, telephone, email, etc., as well as the accesses required on the resources. In many cases the standard set of attributes provided by AMPS is not enough to satisfy the access provisioning requirements on an external system. As an example, consider an IT resource that provides users with access to data specific to a certain "Site ID." In these cases, the AMPS team can configure the system to collect additional custom attribute values from the user when they initiate a role request. These additional attributes are specific to the user and related to the role the user is requesting. Attribute values are also included in the role request approval process and are ultimately used to provision the user's access to IT resources.

After a user role request is approved and resource access is provisioned, access to these additional attribute values is available through the **Applications & Roles** screen, which a user can access within the **My Information** area of AMPS. AMPS enables users to request a modification of these attribute values without having to remove the existing role and request a new role. However, because modifying these attributes can affect a user's access to external IT resources, an attribute change request follows the same approval path as the original role request. The attribute update request also includes the same information as the original role request, such as user information, justification, and optional attachments.

Approval Paths for Attribute Update Requests

An attribute change requests follows the approval path for the original role request. However, if a group of roles share an attribute but have a different role path, AMPS uses the path shared by the most roles in the group.

DLA and DFAS agencies have different rules for some approvers, and these rules apply to attribute updates:

The following sequences illustrate Attribute Update approval paths:

User Category	Supervisor	Security Officer	External Authorizing Official	Data Owner	Information Assurance Officer
DLA *internal* user	Yes	Not required	N/A	Yes	Not required
DFAS *internal* user	Yes	Yes	N/A	Yes	Yes
DLA *external* user	Yes, external supervisor	Yes, external security officer	Yes, if the role requires an EAO review	Yes	Not required
DFAS *external* user	Yes, external supervisor	Yes, external security officer	Yes, if the role requires an EAO review	Yes	Yes
Vendor	N/A	N/A	N/A	Yes	N/A

- In the typical approval path for DLA attribute update requests, Security Officer approvals are not required. Security Officers have no knowledge of application-specific attributes; therefore, DLA does not require their approval.
- All DFAS attribute update requests for DFAS roles require approvals from a Security Officer.
- DLA attribute change requests, like other role requests, do not require an approval by an Information Assurance Officer.
- All DFAS attribute update requests for DFAS roles require an approval by an Information Assurance Officer.

Shared Attributes

Most users do not have two or more roles that share the same attribute. However, for those situations where roles have shared attributes, AMPS addresses attribute updates using these rules:

- If two or more roles share the same attribute, AMPS assumes all the roles with the same role path also share the attribute value. AMPS generates one SAAR for each set of roles to which the updated attributes belong.
- Some roles may have shared attributes along with non-shared attributes. In this case, AMPS groups the non-shared attributes together on the same SAAR associated with the role to which they belong.

Multiple Approvers: Data Owners or Information Assurance Officers

Some additional rules for attribute change requests affect how AMPS handles a SAAR with multiple Data Owners or, in the case of DFAS roles, multiple IAOs. If AMPS identifies multiple Data Owners for different roles with shared attributes, AMPS accepts the decision of the first Data Owner to submit a decision.

Similarly, if AMPS identifies multiple IAOs for a DFAS role attribute change request, AMPS accepts the decision of the first IAO to submit a decision.

Cross-organization Requests

In some cases, a DLA user or DLA external user may request a DFAS role that has attributes, or a DFAS user or DFAS external user may request a DLA role that has attributes. Such requests are called "Cross-organization requests." Refer to the section on Cross-organization Requests, on page 126 in the **AMPS User Guide**, for more information.

Attribute Role Requests: Special Circumstances

Because role requests and role attribute change requests occur on different SAARs, users may have situations in which they submit a role request or extension, and also find a need to update attributes for the role in a pending request. The following sections describe the conditions for these situations.

Role Request and Additional Role Attribute Updates

If a user submits a role request and decides to update attributes while the request is still pending approval, the user has two options:

- Cancel the role request and submit a new role request using the appropriate attribute values.
- Wait until the SAAR approval process is completed and submit an attribute update request.

In a different scenario, a user may have attributes set for one role in an application. If the user adds a request for a different role in the same application with the same attributes, and does so before the original role request is completed, AMPS must choose which attribute values to set. In this case, AMPS sets the attributes based on the last SAAR approved.

Role Extension and Additional Role Attribute Updates

If you have an expiring role with associated additional attributes, you can request an extension for the role, but you cannot update the attributes in the extension. However, you can submit a separate attribute update request while the role extension request is pending approval. The attribute update request is included in a SAAR that is approved separately from the role extension request.

External Users: Update and Approval of Role Attributes

External users have access to the attribute change process through the **My Information** screen. Beginning with AMPS release 17.2.0, AMPS presents the process of requesting an attribute update through a series of screens reviewed and filled in by the user. The following procedure explains how an external user completes and submits an attribute update request.

External Users: How to Request Attribute Changes

What you can do:	External users with CAC authentication, or authentication through External Certificate Authority (ECA) or Federal Bridge Certificate Authority (FBCA) open their AMPS accounts using a CAC or other authentication card, such as a PIV card.
	External users (non-certificate users): User registration, user ID, and password are required authentication credentials for non-certificate-enabled external users. Use your ID and password to log in to AMPS.
	You can update a role attribute if it is available for update through the **Request Attribute Changes** module. If it is not available, AMPS does not display the attribute. Discuss the requirement for an attribute change with your supervisor.
Where to start:	Start the latest version of Edge, Firefox, or Chrome.
	Authenticate your identity with the appropriate credentials and launch AMPS. The system opens the AMPS Home page automatically.

1. Log in to AMPS.

   AMPS displays the **Self Service Home** *page and identifies the logged-in user by ID.*

2. On the **Self Service Home** page, click the **My Information** tile.

   AMPS displays a **Privacy Act Statement** *appropriate to your organization (see* **Appendix E, Privacy Act Statements***). Read the statement and click* **Accept** *to proceed.*

   AMPS displays the **My Information** *screen (see Figure 223).*
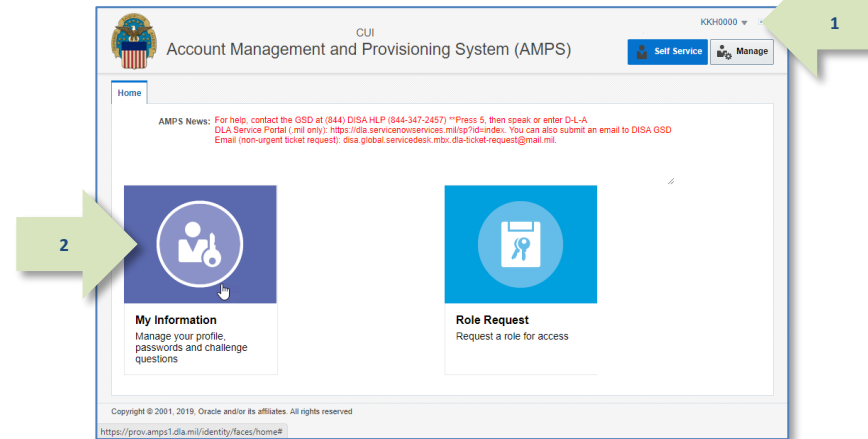
Figure 222: AMPS Self Service Home Page – My Information Tile

3. In the My Information screen, click the Applications & Roles tab.

   AMPS displays the **Applications & Roles** *tab (see Figure 224).*

Figure 223: My Information

4. Locate the Additional Role Attributes table.

   This table lists all the roles associated with additional attributes. Some of these attributes are updates from the user.

5. Click the **Edit Additional Attributes** button to proceed.

   *AMPS launches **Request Attribute Changes** (see Figure 225).*

Figure 224: Update Additional Attributes – Edit Button

6. You are no longer required to enter your Date of Birth.

    AMPS no longer collects this data.

    Note: External users who authenticate their access identity with a user ID and password are no longer required to enter the Social Security (SSN) number when an SSN field is displayed.

    These data fields, when displayed, contain non-editable faux data.

7. Click **Next** to proceed.

Figure 225: Update Additional Attributes – User Account Information

8. The Attribute Changes screen displays a drop-down box that enables you to select the application that includes the role or roles assigned to your account.

   To select an application, click the drop-down box and click the application name from the list.

   Wait for AMPS to refresh the screen.

   This action displays a table listing the attributes and their associated roles (see Figure 227).
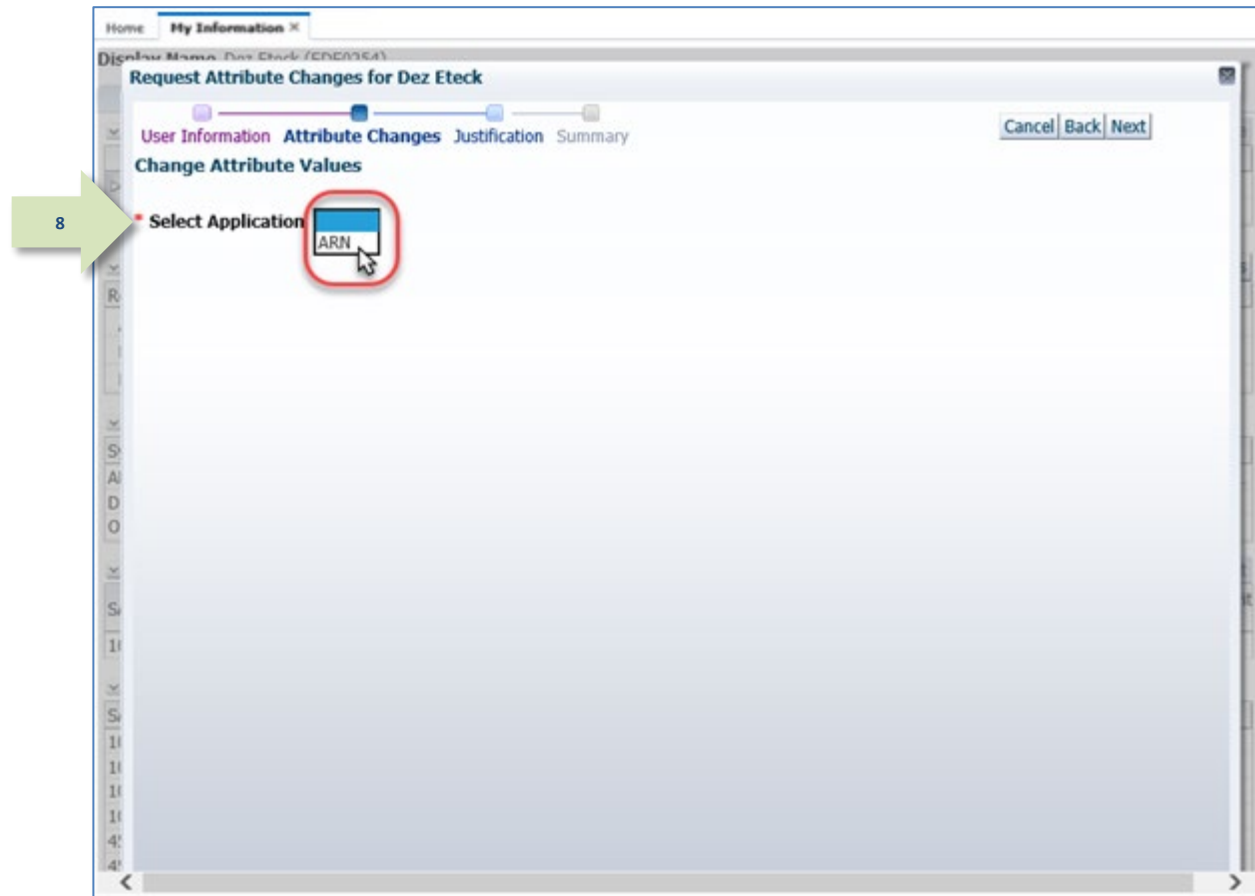
Figure 226: Update Additional Attributes – Select Application

9. Use the available screen tools to update the attribute.

AMPS displays a tool tip box that describes the purpose of the attribute.

Some attributes may have predefined values listed in a drop-down box. Figure 227 illustrates this type of attribute.

Other attributes may be displayed in modifiable text fields that enable you to enter updated values.

Figure 227: Update Additional Attributes – Select Attribute and New Value

10. After you select or enter the updated attribute value, click the **Next** button.

AMPS proceeds to the **Justification** *screen (see Figure 229).*

Figure 228: Update Additional Attributes – Selection Completed

11. The **Request Justification & Supporting Details** screen requires you to enter text reflecting a complete and thorough basis for the attribute change request.

    Enter this text in the required **Justification** text area.

12. As an option, you can add as many as three PDF attachments to support the justification.

    Click the Browse button to locate and attach a file. Repeat this action for additional files.

    Attachments must be PDF files, and each file can be no larger than two megabytes.

    Do not upload any files that contain PII.

13. To proceed, click the **Next** button.
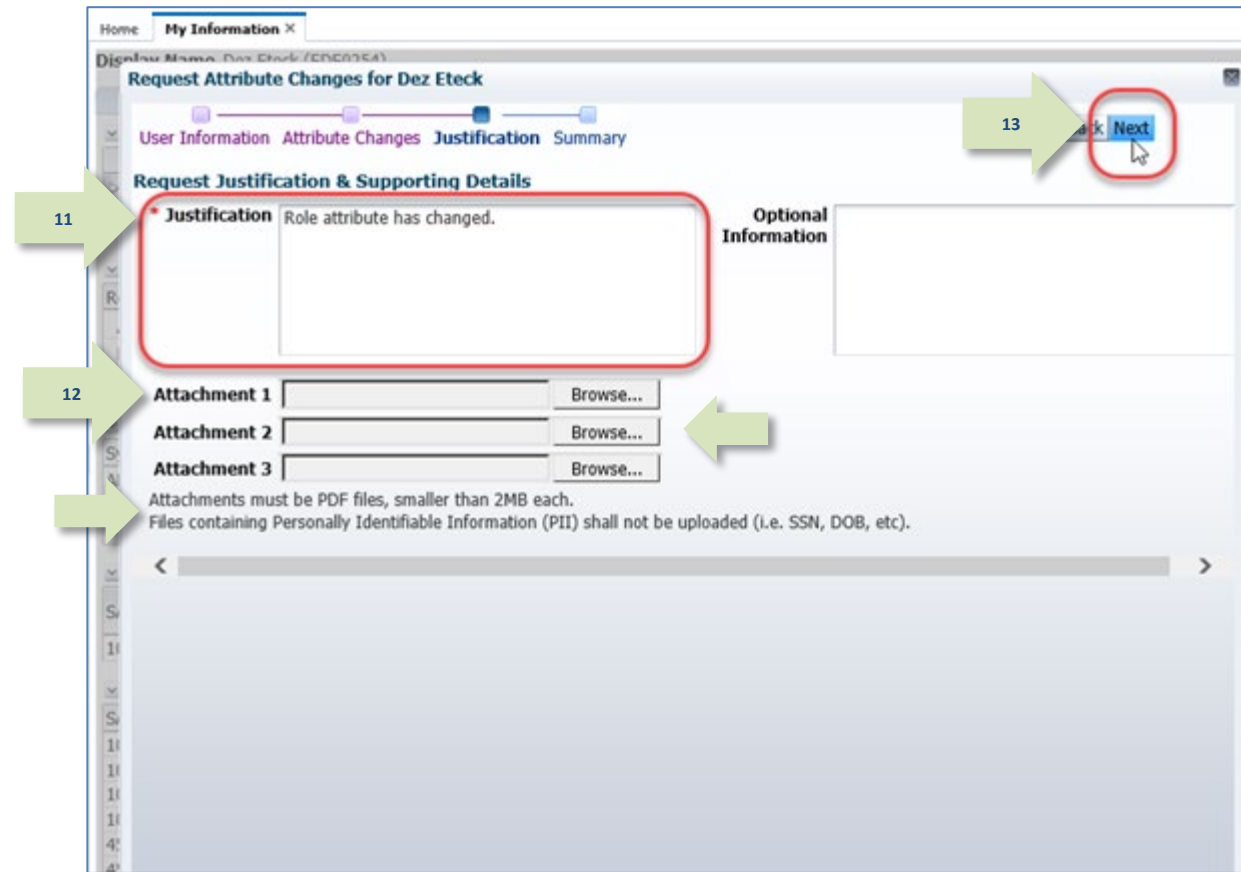
Figure 229: Request Update Changes – Justification

14. Review the **Summary** information for accuracy.

    *The **Role Request Summary** screen recaps the key information to be submitted for review and approval.*

    *The **Changed Attributes** table lists each new attribute value and shows which role or roles are associated with the attribute.*

    *If you need to correct any entries, click the **Back** button to return to previous screens.*

15. To proceed, click the **Submit** button.

    AMPS displays the Attribute Request Confirmation screen (see Figure 231).

Figure 230: Request Attribute Changes – Summary

16. Review the SAAR number, role name, and attributes listed on the confirmation screen and close the window by clicking on the close icon.

   AMPS adds the attribute change SAAR to the user's Pending Requests table.
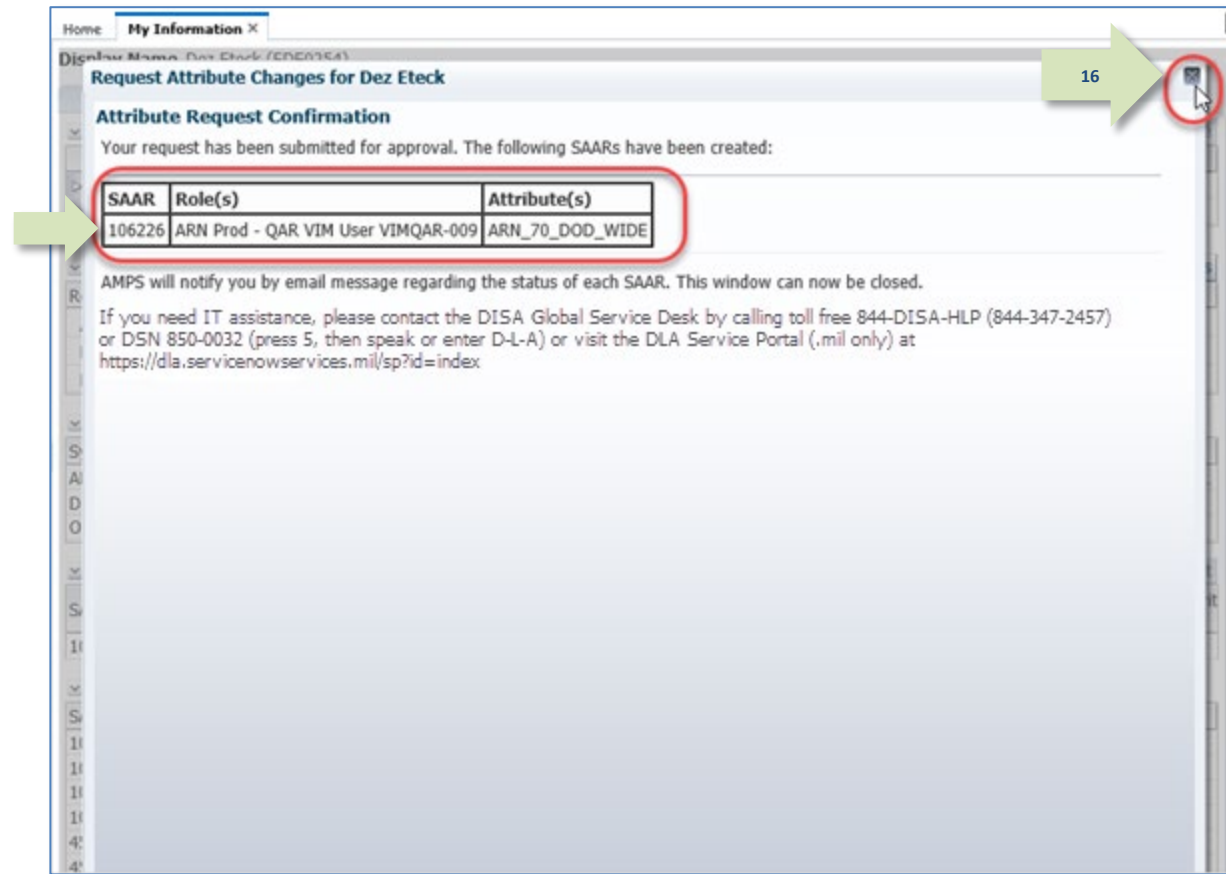
Figure 231: Attribute Request Confirmation

17. AMPS displays SAAR information and status in the user's Pending Requests table. (See How to Check Your Role Status on page 97).

   *The **Status** and **Current Approver** listings reflect the SAAR's approval stage.*

18. AMPS sends an email notification indicating that the SAAR has been submitted for approval.

At each stage of the approval process, AMPS continues to send email notifications of the SAAR's progress.

18

Sample User Notification: Confirmation

Subject: Notification: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT
Body: SAAR #106226 is awaiting External Supervisor approval.

This request was submitted in AMPS on 10/03/2017 08:54:02 EDT.
No action is required from you at this time.

This task expires on 10/23/2017 08:54:13 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

How to Approve a Role Attribute Update Request

Users:	This procedure explains how approvers handle an attribute update request. AMPS sends email notifications that alert the user about the status of the request. A user can check their **Pending Requests** table to monitor the progress of a request through the approval process.
Approvers:	This procedure outlines and describes the steps for reviewing and approving an attribute update request. After a user submits a request to update role attributes, AMPS submits request in the form of a SAAR to a standard approval process. AMPS notifies each approver by email message when a user submits a request for an attribute update. This procedure features sample email notifications to illustrate the timing and content of the email notification process.

External Supervisor Approval

1. After a user submits a request to update attributes, AMPS sends an email notification to the user's Supervisor, indicating that a SAAR awaits the Supervisor's approval action.

   Copy the AMPS URL provided in the email notification.

1

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT
Body: SAAR #106226 - Attribute Change Request for Eteck, Dez (EDE0254) (DLA External) has been submitted for approval.
This request was submitted in AMPS on 10/03/2017 08:54:02 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=3073%3A6iRnHaQYREAxOAYGtm1c6In7wgqZsCOGkjIZUkcAKu8%3D

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/23/2017 08:54:13 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2. Open a browser-Edge, Firefox, or Chrome-and paste the copied URL into the address field.

3. Press Enter or click the launch button that activates the URL search.

    If this occasion is the first time you have been tasked with an approval, AMPS displays an **Approver Information Update** *screen (see Figure 233).*

    Otherwise, AMPS opens the **Approval Work Queue** *(see Figure 234).*

Note:

If you have already entered this information on a previous approval for the requesting user, AMPS does not display the Approver Information Update screen.

Skip step 4 of this procedure if you have already entered this information, which AMPS associates with the requestor.

4. Enter your first name, last name, and phone number in the fields.

    Click the **Save** button.

    AMPS opens the **Approval Work Queue** *(see Figure 234).*

Figure 232: Main Menu - My Information Command

Figure 233: Approver Information Update

5. In the **Approval Requests** list, locate and click the SAAR listing that matches the SAAR number and requestor information in the email notification.

   For a first-time approver, AMPS opens the **Verify Approver** *screen (see Figure 235).*

Figure 234: Approval Requests - Open a SAAR

Note:

Skip step 6 if you have already verified that you are the AMPS Supervisor for this requestor.

Go to Step 7.

6. Click **Verify** if you are the AMPS Supervisor for the requestor identified on the **Verify Approver** screen.

   AMPS displays the **Attribute Change Request –External Supervisor Decision** *screen (see Figure 236.)*
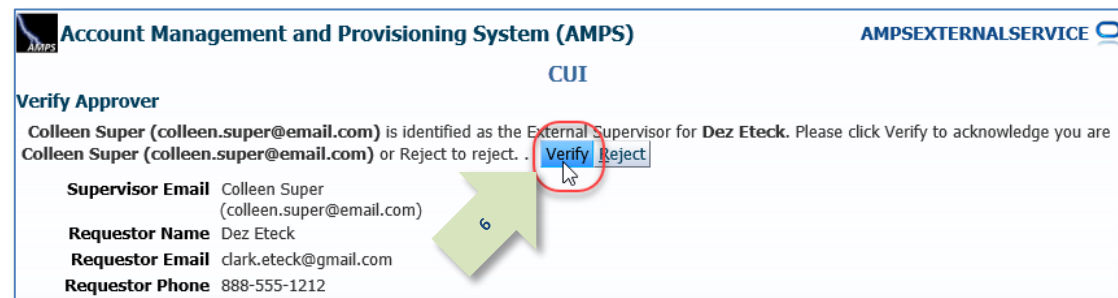
Figure 235: Supervisor's Approval Decision Screen – Verify Approver

7. Review the information on the **Attribute Change Request Details** screen.

   If you have an issue with any of the information, you can consult with the requestor to clarify the purpose or content of the information.

   The AMPS Supervisor can reject this request, if necessary, by following these steps:

   - *Enter the reason for the rejection in the* **Comments** *field. This action activates the* **Reject** *button.*

   Click the **Reject** *button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

8. Click the Additional Information tab.

   AMPS displays the **Additional Information** *tab on the decision screen (see Figure 237).*

Figure 236: External Supervisor Decision –Attribute Change Request Details

9. Review the SAAR Approval History table.

    Because the AMPS Supervisor is the first approver to handle the SAAR, AMPS has not recorded any approver actions yet.

    AMPS will fill in the details of the Supervisor's action after the Supervisor has completed an action on this decision screen. AMPS retains this information and displays it when the SAAR is reopened.

    The AMPS Supervisor can reject this request, if necessary, by following these steps:

    - *Enter the reason for the rejection in the* **Comments** *field. This action activates the* **Reject** *button.*
    - *Click the* **Reject** *button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

10. Click the User Information tab.

    AMPS displays the **User Information** *tab on the decision screen (see Figure 238).*

Figure 237: Attribute Change - Additional Information

11. Review the information provided in the **User Information** tab to finalize the decision.

As an option, the AMPS Supervisor can fill in comments that explain or justify the approval.

The AMPS Supervisor can also reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the* **Comments** *field. This action activates the* **Reject** *button.*

- *Click the* **Reject** *button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

12. To proceed, click the **Approve** button.

AMPS displays the **Task Completed** *message (see Figure 239).*

Figure 238: Attribute Change - User Information

13. In the **Task Completed** message, click the link to return to the **Approval Worklist**, also labeled as the **AMPS Approval Work Queue** (see Figure 240).
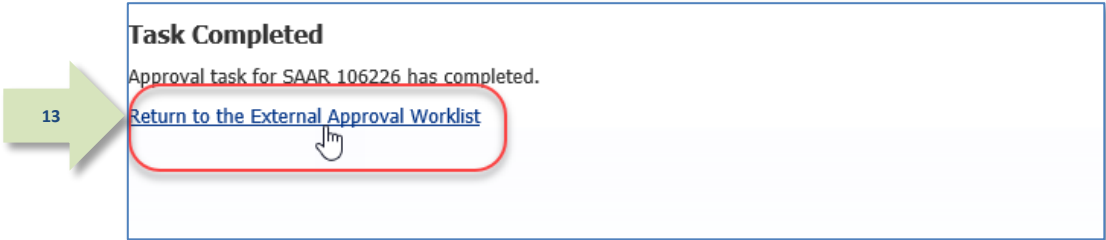
Task Completed

Approval task for SAAR 106226 has completed.

Return to the External Approval Worklist
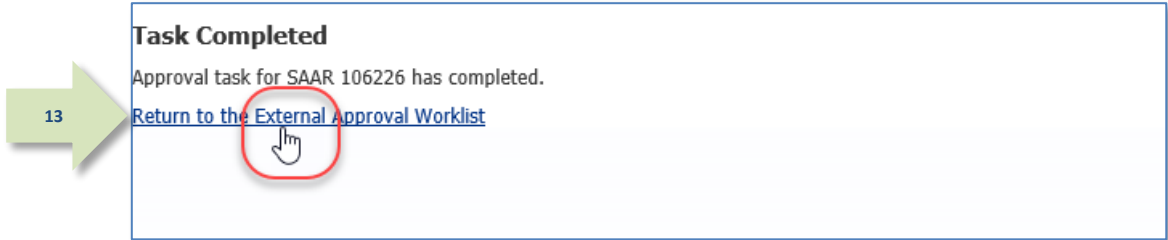
Figure 239: Confirmation of Completed Approval

14. If there are no approvals listed for action, or you have completed work with SAARs for the current session, click the **Logout** button.

*This action closes the **AMPS Approval Work Queue** and displays a logout confirmation message (see Figure 241).*

AMPS Approval Work Queue   Logout

CUI

Approval Requests

Approval Action		Approval Request Date	Approval Request Expires
There are no pending approvals awaiting your attention. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index			

Figure 240: AMPS Approval Work Queue – Logout

15. Click the close browser icon to close the message.
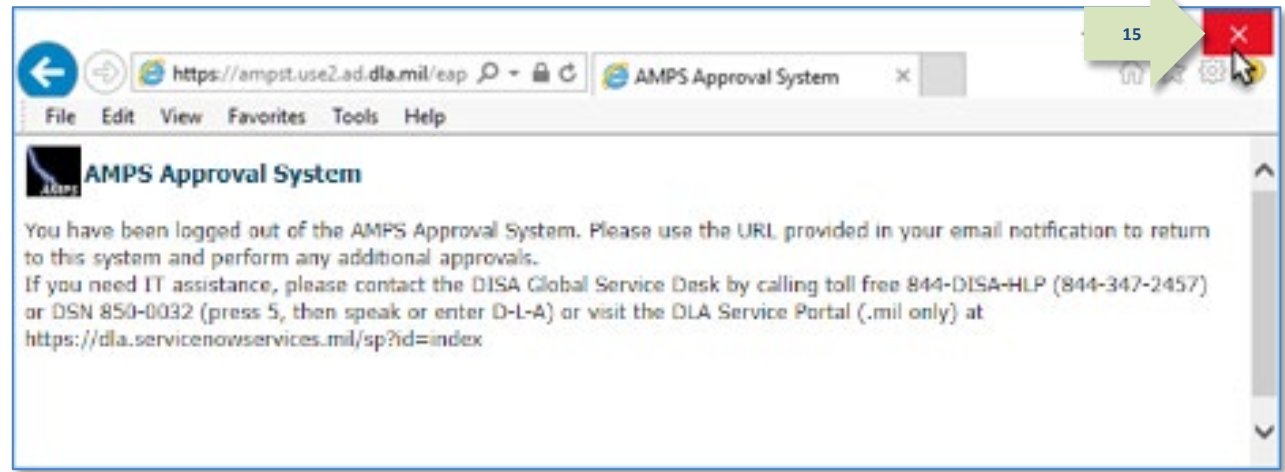
Figure 241: Logout Confirmed

16. After you complete an approval for an attribute update, AMPS sends an email notification to the user regarding the AMPS Supervisor decision.

Sample User Notification: Status

Subject: Notification: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: The External Supervisor has completed an approval for SAAR #106226.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

17. After you complete an approval for an attribute update, AMPS sends an email notification to the user regarding the status of the approval.

Sample User Notification: Next Approver

Subject: Notification: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: SAAR #106226 is awaiting External Security Officer approval.

This request was submitted in AMPS on 10/03/2017 08:54:02 EDT.

No action is required from you at this time.

This task expires on 10/23/2017 15:11:48 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

External Security Officer Approval

After a user submits a request to update attributes, AMPS sends an email notification to the user's external Security Officer, indicating that a SAAR awaits the Security Officer's approval action.

1. As the external Security Officer, copy the AMPS URL provided in the email notification.

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: SAAR #106226 - Attribute Change Request for Eteck, Dez (EDE0254) (DLA External) has been submitted for approval.

This request was submitted in AMPS on 10/03/2017 08:54:02 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=0503%3AcrYBrCN8%2BEm5SZ%2BfEsFhSCMWBzMiNt1U6Hf%2F4O%2BW9lg%3D

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/23/2017 15:11:48 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. Open a browser-Edge, Firefox, or Chrome-and paste the copied URL into the address field.

3. Press Enter or click the launch button that activates the URL search.

*If this occasion is the first time you have been tasked with an approval for the requesting user, AMPS displays an **Approver Information Update** screen (see Figure 243).*

*Otherwise, AMPS opens the **Approval Work Queue** (see Figure 244).*
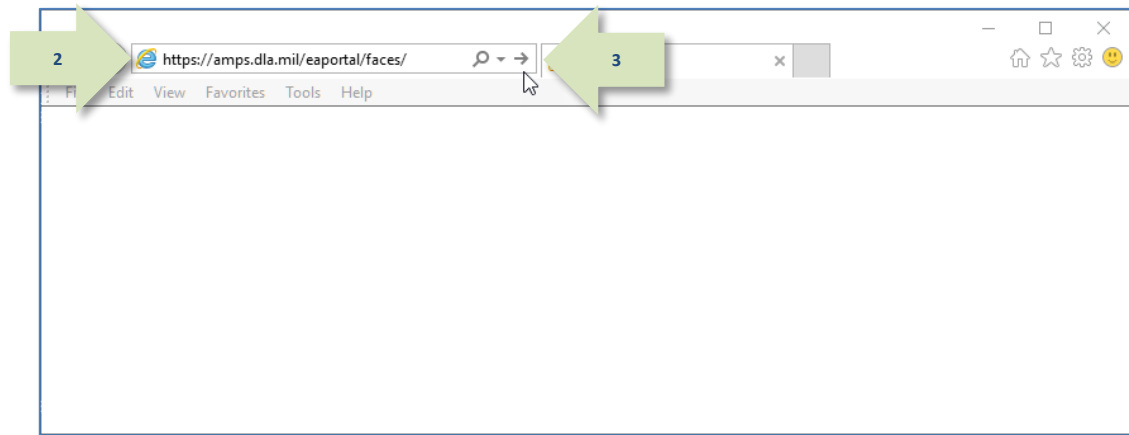
Figure 242: Main Menu - My Information Command

Note:

If you have already entered this information on a previous approval for the requesting user, AMPS does not display the Approver Information Update screen.

Skip step 4 in this procedure if you have already entered this information, which AMPS associates with the requestor.

AMPS opens the **Approval Work Queue** *(see Figure 244).*

Figure 243: Approver Information Update

4. Enter your first name, last name, and phone number in the fields.

    Click the **Save** button.

5. In the **Approval Requests** list, locate and click the SAAR listing that matches the SAAR number and requestor information in the email notification.

    For a first-time approver, AMPS opens the **Verify Approver** *screen (see Figure 245).*

Figure 244: Approval Requests - Open a SAAR

Note:

If you have already verified that you are the AMPS Supervisor for this requestor, AMPS does not display the Verify Approver screen again.

Skip step 6 and go to Step 7.

Figure 245: Supervisor's Approval Decision Screen – Verify Approver

6. Click **Verify** if you are the AMPS Security Officer for the requestor identified on the **Verify Approver** screen.

   *AMPS displays the **Attribute Change Request –External Security Officer Decision** screen (see Figure 246).*

7. Review the information on the **Attribute Change Request Details** screen.

    If you have an issue with any of the information, you can consult with the requestor to clarify the purpose or content of the information.

    The AMPS Security Officer can reject this request, if necessary, by following these steps:

    - *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

    - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

8. Click the Additional Information tab.

    *AMPS displays the **Additional Information** tab on the decision screen (see Figure 247).*

Figure 246: External Security Officer Decision –Attribute Change Request Details

9. Review the SAAR Approval History table.

    The External Security Officer sees the previous approver's comments if any have been added.

    AMPS will fill in the details of the Security Officer's action after the Security Officer has completed an action on this decision screen. AMPS retains this information and displays it when the SAAR is reopened.

    The External Security Officer can reject this request, if necessary, by following these steps:

    - *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*
    - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

10. Click the User Information tab.

    *AMPS displays the **User Information** tab on the decision screen (see Figure 248).*

Figure 247: Attribute Change - Additional Information

11. Review the information provided in the **User Information** tab to finalize the decision.

As an option, the External Security Officer can fill in comments that explain or justify the approval.

The Security Officer (SO) can also check the requestor's security information and update the Security Information fields, as needed. The Date of Birth field is displayed on this screen, but does not contain the user's DOB. This data is no longer collected by AMPS.

The External Security Officer can also reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

- *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

12. To proceed, click the **Approve** button.

*AMPS displays the **Task Completed** message (see Figure 249).*

Figure 248: Attribute Change - User Information

13. In the **Task Completed** message, click the link to return to the **Approval Worklist**, also labeled as the **AMPS Approval Work Queue** (see Figure 250).

Task Completed

Approval task for SAAR 106226 has completed.

13 → Return to the External Approval Worklist

Figure 249: Confirmation of Completed Approval

14. If there are no approvals listed for action, or you have completed work with SAARs for the current session, click the **Logout** button.

*This action closes the **AMPS Approval Work Queue** and displays a logout confirmation message (see Figure 251).*

AMPS Approval Work Queue　　　　　　　　　14 → Logout

CUI

Approval Requests

Approval Action		Approval Request Date	Approval Request Expires
There are no pending approvals awaiting your attention. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index			

Figure 250: AMPS Approval Work Queue – Logout

15. Click the close browser icon to close the message.
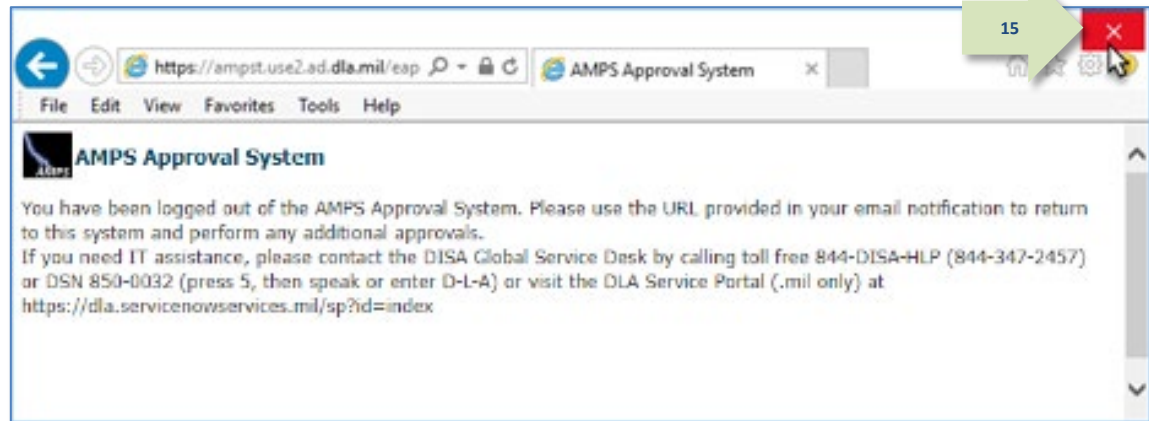
Figure 251: Logout Confirmed

16. After you complete an approval for an attribute update, AMPS sends an email notification to the user regarding the Security Officer decision.

Sample User Notification: Status

Subject: Notification: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: The External Security Officer has completed an approval for SAAR #106226.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

17. After you complete an approval for an attribute update, AMPS sends an email notification to the user regarding the approval.

Sample User Notification: Next Approver

Subject: Notification: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: SAAR #106226 is awaiting Data Owner approval.

This request was submitted in AMPS on 10/03/2017 08:54:02 EDT.

No action is required from you at this time.

This task expires on 10/24/2017 15:28:35 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Data Owner Approval: External and Internal Users

This procedure illustrates the steps an application Data Owner takes to approve a SAAR for a Total AMPS-enabled application.

1. After the previous approver approves a role request, AMPS sends an email notification to the application's Data Owner, indicating that a SAAR has been submitted for the Data Owner's approval.

1

Sample Approver Notification

Subject: Action Required: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: SAAR #106226 - Attribute Change Request for Eteck, Dez (EDE0254) (DLA External) has been submitted for approval. This request was submitted in AMPS on 10/03/2017 08:54:02 EDT.

Please visit AMPS at this URL:
https://amps.dla.mil/

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/23/2017 15:11:48 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. In the AMPS banner, the Data Owner clicks their User ID to open the dropdown menu, then clicks **Inbox** from the menu.

   AMPS opens the **Inbox** *screen to the My Tasks view (see Figure 253).*
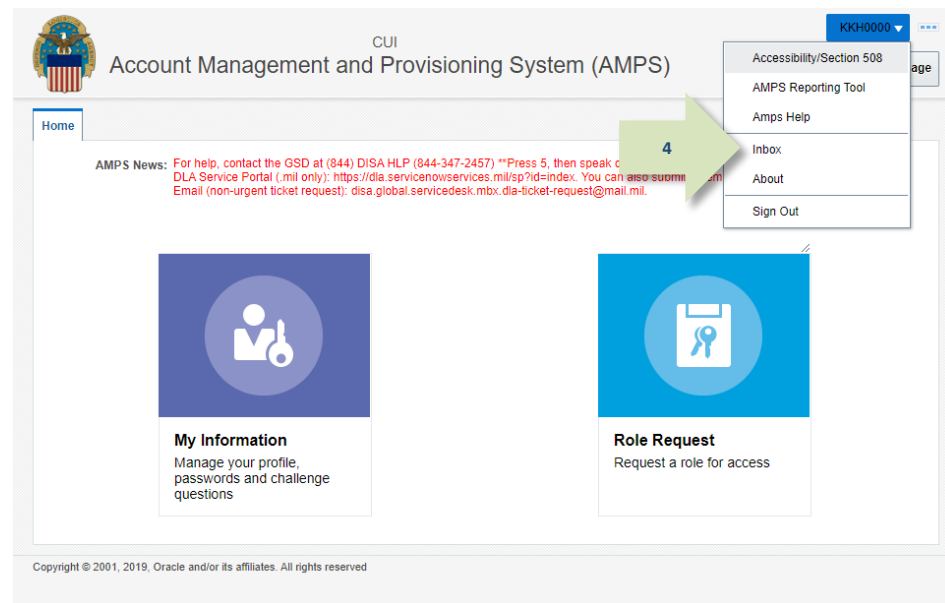
Figure 252: User ID Dropdown – Inbox Command

3. On the **My Tasks** screen, click the SAAR number indicated in the email notification.

   AMPS displays the **Attribute Change Request - Data Owner Decision** *screen for the SAAR (see Figure 254).*
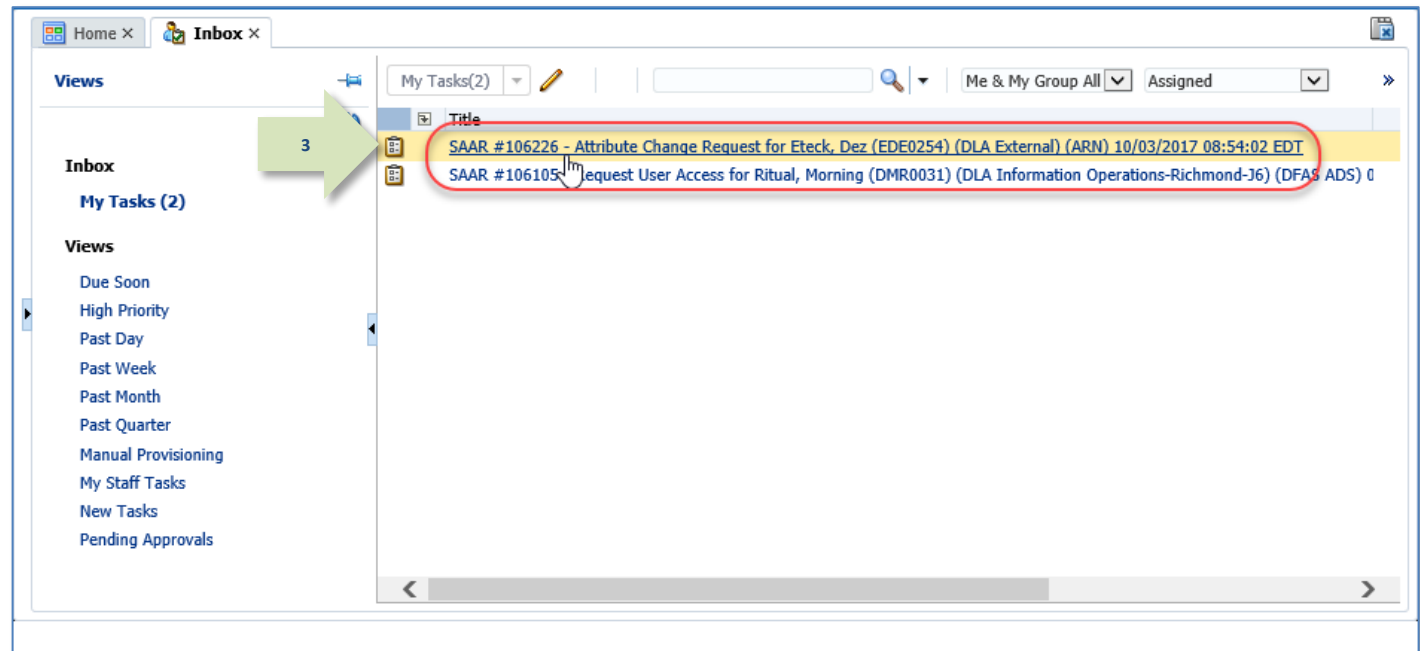
Figure 253: My Tasks

4. In the **Data Owner Decision** screen, review the SAAR information and change request details.

The AMPS Data Owner can reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

- *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

5. Click the Additional Information tab.

*AMPS displays the **Additional Information** screen (see Figure 255).*

Figure 254: Attribute Change Request – Details

6. In the **Additional Information** tab, review the SAAR Approval History, as needed.

    Any comments entered by previous approvers to support their decisions are listed in the SAAR Approval History table.

7. Click the User Information tab.

    AMPS displays the user's information.

Figure 255: Attribute Change Request – Additional Information Tab

8. In the **User Information** tab, you can review key information about the user's account, contact, and security information.

9. To proceed, click the **Approve** button.

AMPS automatically . . .

- *Closes the* **Data Owner Decision** *screen,*

- *Sends the SAAR to the next stage in the workflow, and*

- *Removes the SAAR as an* **Assigned** *item from the Data Owner's* **My Tasks** *tab.*

Figure 256: Attribute Change Request - User Information

10. After the approval is submitted, AMPS sends an email notification to the user regarding the approval's status.

10

Sample User Notification: Status

Subject: Notification: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT

Body: The Data Owner has completed an approval for SAAR #106226.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

11. In addition, AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

If the role is for a DLA application...

The status shows the SAAR is **TICKETED.**
AMPS forwards this approved DLA request to the **Provisioning** *process for action. No role requests or other requests require an approval by an Information Assurance Officer.*

If the role is a DFAS role...

The status shows the SAAR has been forwarded to the Information Assurance Officer *for approval.*

12. AMPS notifies the external user that processing for the attribute change request SAAR has begun.

   AMPS has forwarded the SAAR to the Provisioner's task list.

12

Sample User Notification:

Subject: AMPS Application Processing for SAAR #106226

Body:
AMPS Application Processing request for SAAR 106226 has started.

Request For:

DLA Login: EDE0254

Name: Eteck, Dez Phone: 888-555-1212

Email: clark.eteck@gmail.com

EDIPI/UPN: 1286972493

Access Information:
SAAR #: 106226

Attribute Change on Job Role: ARN Prod - QAR VIM User VIMQAR-009

Current Applications and Access:
          Resource: ARN PROD - ARN
                    Access: VIM account request for a DCMA QAR user (AMPS Role ID: VIMQAR-009)

Data Owner Comments: Approved by the Data Owner.

Justification: Role attribute has changed.

Optional Information: (none)

Attribute Change Request SAAR requested by Dez Eteck on 10/03/2017

Provisioner: How to Provision Attribute Updates

This procedure illustrates the steps a provisioner takes to complete a SAAR for a Total AMPS- enabled application.

For a Remedy-enabled application, AMPS sends this information to a Remedy system that produces a Remedy ticket for the provisioner.

Applications set up for automatic provisioning do not require manual provisioning

1. After all approvers have approved a SAAR for a Total AMPS role, AMPS forwards the SAAR to the provisioner group.

AMPS notifies the provisioner that the SAAR awaits action.

1
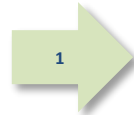
Sample Provisioner Notification: Total AMPS Ticket

Subject: Action Required: SAAR #106226 - Attribute Change Request for Dez Eteck (EDE0254) (DLA External) (ARN) 10/03/2017 08:54:02 EDT
Body:
AMPS Application Processing request for SAAR 106226 requires your attention.

Request For:
DLA Login: EDE0254
Name: Eteck, Dez
Phone: 888-555-1212
Email: clark.eteck@gmail.com
EDIPI/UPN: 1286972493

Access Information:
SAAR #: 106226

Attribute Change on Job Role: ARN Prod - QAR VIM User VIMQAR-009

Current Applications and Access:
        Resource: ARN PROD - ARN
                Access: VIM account request for a DCMA QAR user (AMPS Role ID: VIMQAR-009)

Data Owner Comments: Approved by the Data Owner.

Justification: Role attribute has changed.

Optional Information: (none)

Attribute Change Request SAAR requested by Dez Eteck on 10/03/2017

2. After you launch AMPS, the system opens the **Self Service Home** page. Click your User ID to open the dropdown menu, then click the **Inbox** command from the menu.

AMPS opens the logged-in provisioner's **My Task***s view.*
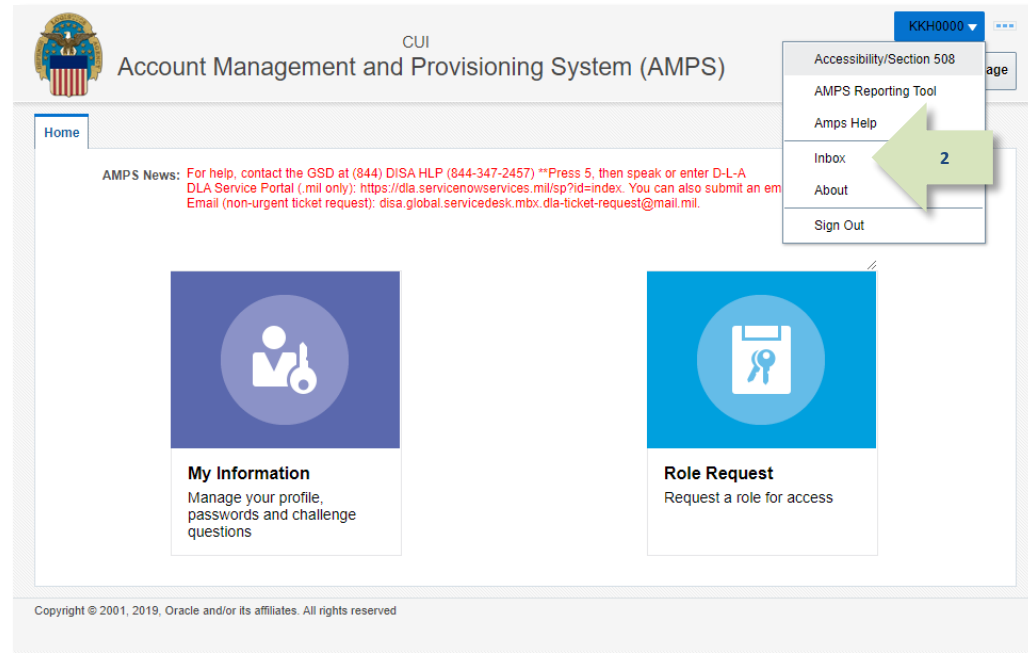
Figure 257: Self-Service Home Page – Inbox Command

3. In the My Tasks view, locate and click the SAAR in the provision notation.

AMPS opens the Total AMPS ticket for the **selected SAAR (see Figure 259).**
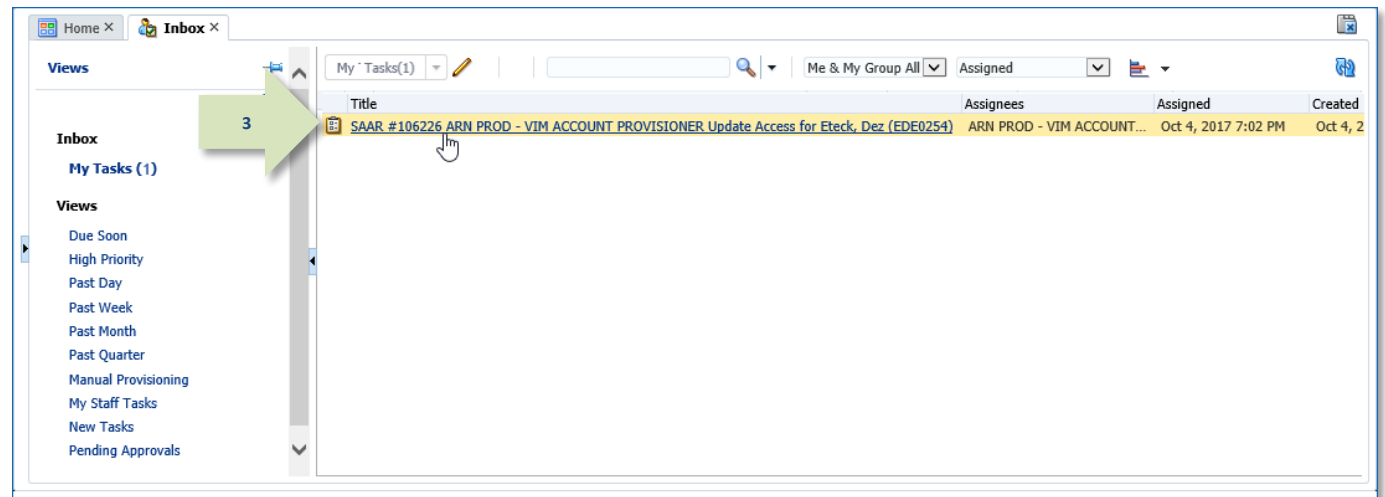
Figure 258: Provisioner's My Tasks View

4. Review the contents of the ticket.

The ticket contains the type of action required and the details of the approved change in the **Additional Role Attributes** table.

If you, as the provisioner, need more time to act on the request, you have the **Save Comments** *option.*

You can enter text in the **Comments** *area, click the* **Save Comments** *button, and close the ticket without completing it.*

The ticket remains in your **My Tasks** *list until you click the* **Work is Complete** *button.*

5. To signify ticket processing is finished, click the **Work is Complete** button.

This action closes the ticket and removes it from the provisioner's **My Tasks** *list in AMPS.*

Some customers may generate AMPS reports that list open tickets and ticket closures, which makes closing each Total AMPS ticket an important step in completing the approval process.

Figure 259: Completed Provisioning Ticket

6. The user can log on to his or her account and check the **Applications & Roles** tab to monitor the SAAR's approval progress.

   The example in Figure 260 shows that the current SAAR's status is COMPLETED. The updated attribute is displayed in the **Additional Role Attributes** *table.*

Figure 260: User's Applications & Roles - Additional Role Attributes

---

7. After provisioning is finished and the provisioner officially closes the ticket, AMPS notifies the user by email that the attribute update has been completed.

Sample Notification: Total AMPS Ticket Processing is Completed

Subject: AMPS Application Processing for SAAR #106226

Body: Your request to update attributes associated with your access to ARN (SAAR 106226) has been completed.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Internal Users: How to Request Attribute Changes

This procedure outlines and describes the steps taken by an internal user to edit role attributes.

1. Log in to AMPS.

   AMPS displays the **Self Service Home** *page and identifies the logged-in user by ID.*

2. In the main working area, click the **My Information** tile.

   AMPS displays a **Privacy Act Statement** *appropriate to your organization (see* **Appendix E, Privacy Act Statements***). Read the statement and click* **Accept** *to proceed.*

   AMPS displays the **My Information** *screen (see Figure 262).*
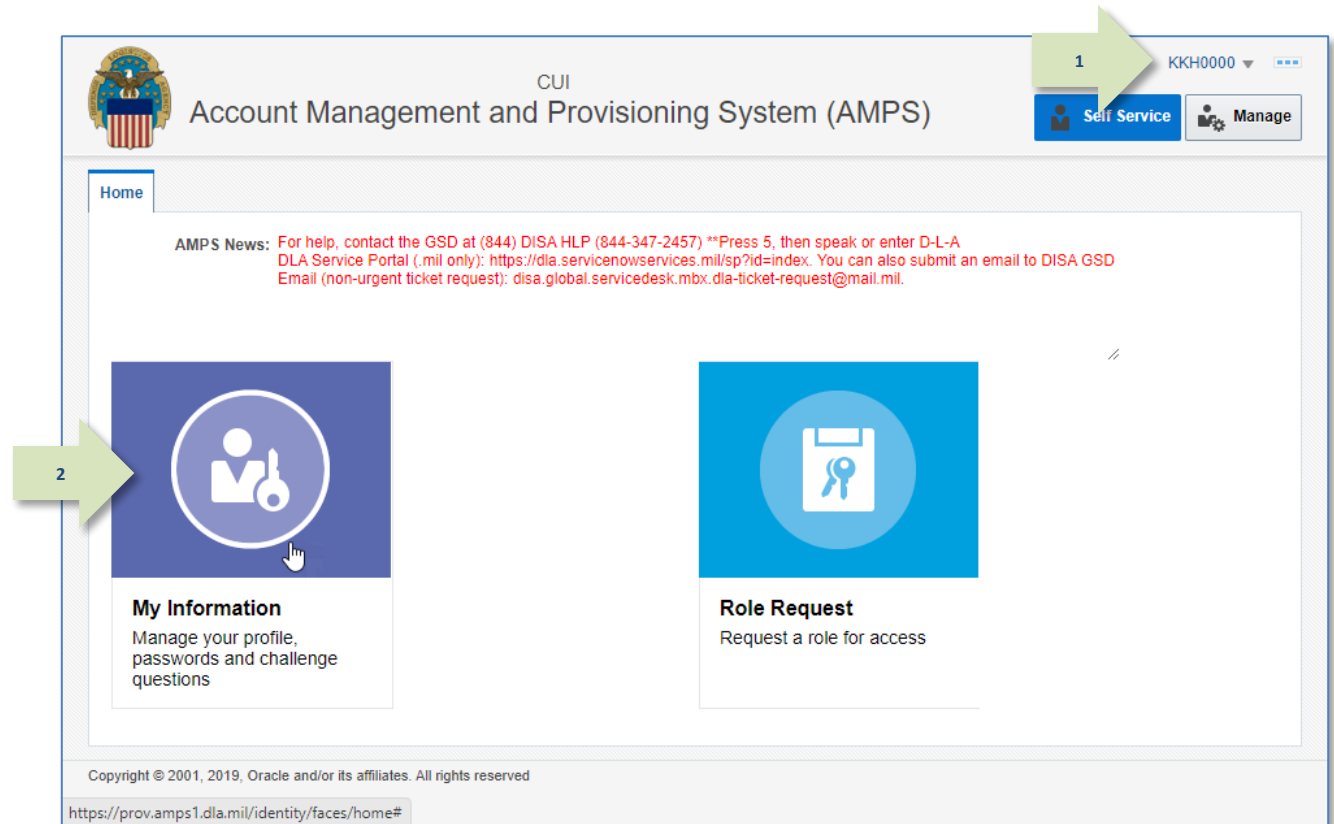
Figure 261: AMPS Self Service Home Page – My Information Tile

3. In the My Information screen, click the Applications & Roles tab.

AMPS displays the **Applications & Roles** *tab (see Figure 263).*

Figure 262: My Information

4. Locate the Additional Role Attributes table.

    This table lists all the roles associated with additional attributes. Some of these attributes are updates from the user.

5. Click the **Edit Additional Attributes** button to proceed.

    *AMPS launches **Request Attribute Changes** (see Figure 264).*

Figure 263: Update Additional Attributes – Edit Button

6. You no longer need to enter your Date of Birth.

    AMPS no longer collects this data.

    Also, external users who authenticate their access identity with a user ID and password must no longer need to enter the Social Security (SSN) number when an SSN field is displayed.

    This data cannot be entered or stored anywhere in AMPS.

7. Click **Next** to proceed.

Figure 264: Update Additional Attributes – User Information

8. The Attribute Changes screen displays a drop-down box that enables you to select the application that includes the role or roles assigned to your account.

    To select an application, click the drop-down box and click the application name from the list.

    Wait for AMPS to refresh the screen.

    This action displays a table listing the attributes and their associated roles (see Figure 266).

Figure 265: Update Additional Attributes – Select Application

9. Use the available screen tools to update the attribute.

AMPS displays a tool tip box that describes the purpose of the attribute.

Some attributes may have predefined values listed in a drop-down box. Figure 266 illustrates this type of attribute.

Other attributes may be displayed in modifiable text fields that enable you to enter updated values.

Figure 266: Update Additional Attributes – Select Attributes

10. After you select or enter the updated attribute value, click the **Next** button.

   AMPS proceeds to the **Justification** *screen (see Figure 268).*

Figure 267: Update Additional Attributes – Enter New Value

11. The **Request Justification & Supporting Details** screen requires you to enter text reflecting a complete and thorough basis for the attribute change request.

    Enter this text in the required **Justification** text area.

12. As an option, you can add as many as three PDF attachments to support the justification.

    Click the Browse button to locate and attach a file. Repeat this action for additional files.

    Attachments must be PDF files, and each file can be no larger than two megabytes.

    Do not upload any files that contain PII.

13. To proceed, click the **Next** button.

Figure 268: Request Update Changes - Justification

14. Review the **Summary** information for accuracy.

    *The **Role Request Summary** screen recaps the key information to be submitted for review and approval.*

    *The **Changed Attributes** table lists each new attribute value and shows which role or roles are associated with the attribute.*

    *If you need to correct any entries, click the **Back** button to return to previous screens.*

15. To proceed, click the **Submit** button.

Figure 269: Request Attribute Changes – Summary

16. Review the SAAR number, role name, and attributes listed in the confirmation and close the window by clicking on the close window icon.

AMPS adds the attribute change SAAR to the list of Pending Requests on your **My Information** *screen (see Figure 263).*

Figure 270: Attribute Request Confirmation

17. AMPS displays SAAR information and status in the user's Pending Requests table. (See **How to Check Your Role Status** on page 97).

The **Status** *and* **Current Approver** *listings reflect the SAAR's approval stage.*

18. AMPS sends an email notification indicating that the SAAR has been submitted for approval.

At each stage of the approval process, AMPS continues to send email notifications of the SAAR's progress.

18 →

Sample User Notification: Confirmation

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 is awaiting Supervisor approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

No action is required from you at this time.

This task expires on 10/25/2017 11:37:59 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Supervisor Approval

After a user submits a request to update attributes, AMPS sends an email notification to the user's Supervisor, indicating that a SAAR awaits the Supervisor's approval action.

1. Note the SAAR number in the email notification.

*This SAAR number appears in the Supervisor's **Inbox**, in the **My Tasks** view.*

1 →

Sample Approver Notification: Action Required

Subject: Action Required: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 - Attribute Change Request for Teck, Alvin (DAT0014) (DFAS Columbus) has been submitted for approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/25/2017 11:37:59 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. Launch AMPS in a browser: Edge, Firefox, or Chrome

    The login ID reflects the identity of the currently logged in user.

3. Click the User ID to open the dropdown menu, then click the **Inbox** command from the menu.

    *AMPS opens the **Inbox** screen (see Figure 272).*
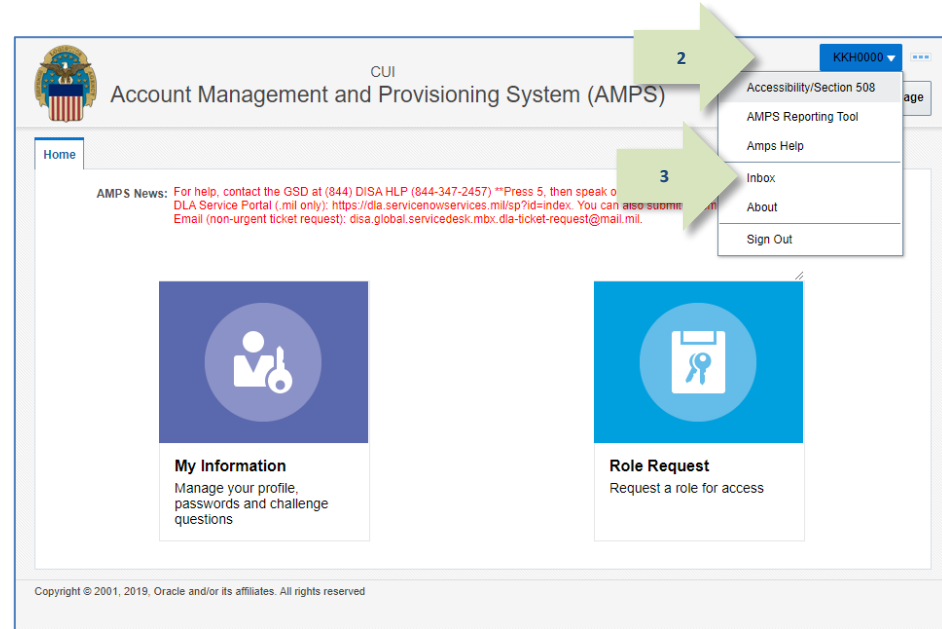
Figure 271: User ID Dropdown Menu – Inbox Command

4. In the **My Tasks** view, click the SAAR number indicated in the **Action Required** email notification.

    *AMPS opens a new tab and displays the **Attribute Change Request – Supervisor Decision** screen.*

    *In the **Supervisor Decision** screen, AMPS displays the **Attribute Change Request Details** tab by default (see Figure 273).*
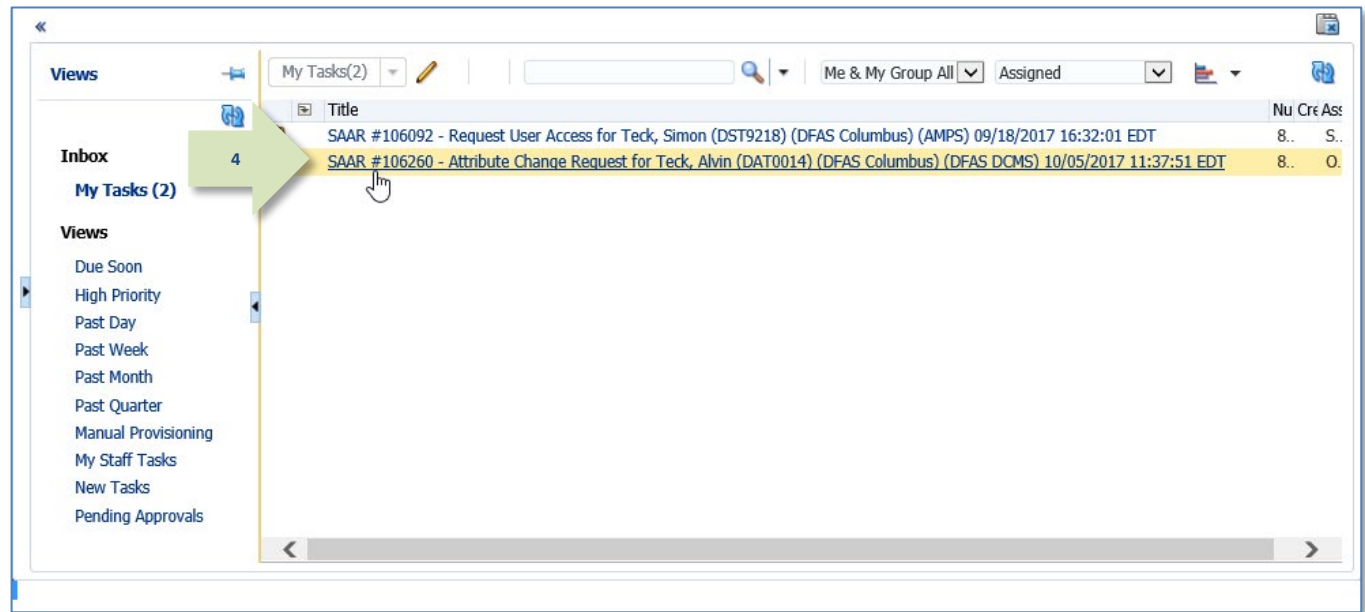
Figure 272: Approval Requests - Open a SAAR

5. Check the **Additional Role Attributes** section to review the attributes and values.

*The new value is shown in the **Additional Role Attributes** table.*

If you have an issue with any of the information displayed, you can consult with the requestor to clarify the purpose or content of the information.

The AMPS Supervisor can reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

- *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

6. To proceed, click the **Additional Information** tab.

*AMPS displays the **Additional Information** tab page (see Figure 274).*

Figure 273: Supervisor Decision - Attribute Change Request Details

7. Review the information in the **Additional Information** tab.

   *AMPS displays the **SAAR Approval History** on this screen.*

   Because the AMPS Supervisor is the first approver to handle the SAAR, AMPS has not recorded any approver actions yet.

   AMPS will fill in the details of the Supervisor's action after the Supervisor has completed an action on this decision screen. AMPS retains this information and displays it when the SAAR is reopened.

   The AMPS Supervisor can reject this request, if necessary, by following these steps:

   - *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*
   - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

8. To proceed, click the **User Information** tab.

   *AMPS displays the **User Information** tab on the decision screen (see Figure 275).*

Figure 274: Supervisor Decision –Additional Information

9. Review the information provided in the **User Information** tab to finalize the decision.

   As an option, the AMPS Supervisor can fill in comments that explain or justify the approval.

   The AMPS Supervisor can also reject this request, if necessary, by following these steps:

   - *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

   - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

10. To proceed, click the **Approve** button.

    *AMPS closes the decision screen and tab, and returns to the **Inbox** tab.*

Figure 275: Supervisor Decision – User Information

11. **OPTIONAL:** Follow these steps to view the completed request screen, as needed:

   a. In the **Search** field, enter the SAAR number for the decision you want to review.

   b. In the **Status** dropdown list, select either **Any** or **Completed**.

   AMPS automatically initiates a search based on the criteria entered.

   In this example, the system displays the SAAR because it also has a status of **Completed***.*

   c. Click the SAAR title to review the SAAR on screen (not shown).
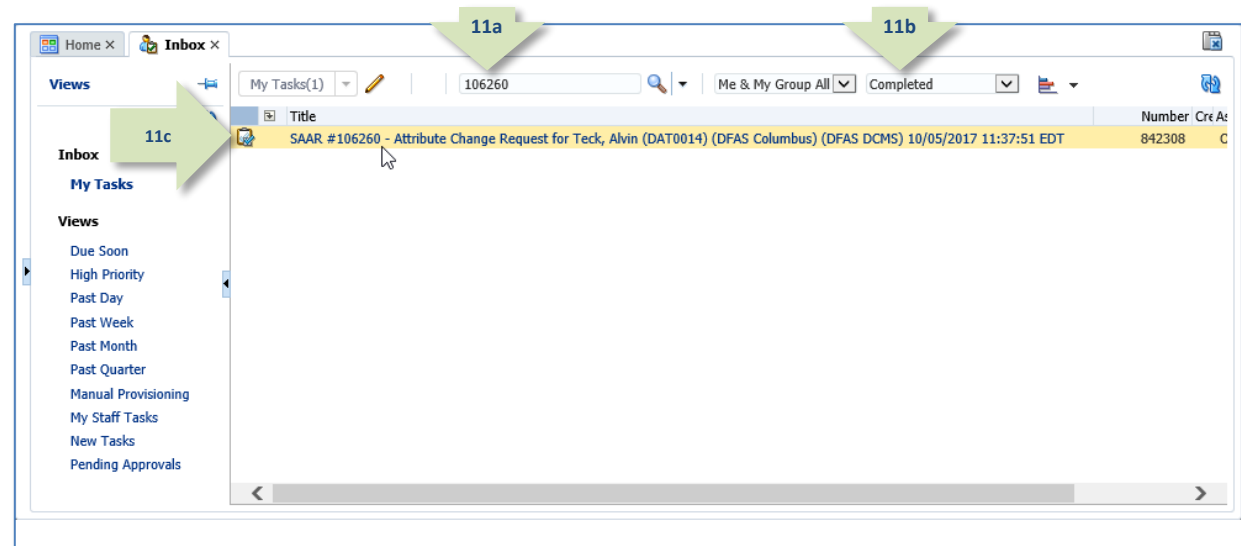
Figure 276: Inbox - My Tasks - Search for Completed SAAR

12. After you complete an approval for an attribute update, AMPS sends an email notification to the user regarding the AMPS Supervisor decision.

Sample User Notification: Status

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: The Supervisor has completed an approval for SAAR #106260.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

13. After you complete an approval for an attribute update, AMPS sends an email notification to the user regarding the approval.

Sample User Notification: Next Approver

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 is awaiting Security Officer approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

No action is required from you at this time.

This task expires on 10/25/2017 13:52:17 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Security Officer Approval

After a Supervisor completes an approval for an attribute update, AMPS sends an email notification to the next approver regarding an action required on a pending approval task.

A Security Officer approval for DLA requests may not be required if the request is bypassed or automatically approved. See the section entitled **Security Officer: Internal Users** in this user guide for more information.

1. Note the SAAR number in the **Action Required** email notification.

   The email message describes the type of SAAR submitted for review.

1

Sample Approver Notification: Next Approver

Subject: Action Required: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 - Attribute Change Request for Teck, Alvin (DAT0014) (DFAS Columbus) has been submitted for approval.
This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/25/2017 13:52:17 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. To begin the approval process, a Security Officer logs in to AMPS.

   *AMPS displays the **Self Service Home** page and identifies the logged in user by ID.*

3. Click the User ID to open the dropdown menu, then click the **Inbox** command from the menu.

   *AMPS displays the Security Officer's **My Tasks** view (see Figure 278).*
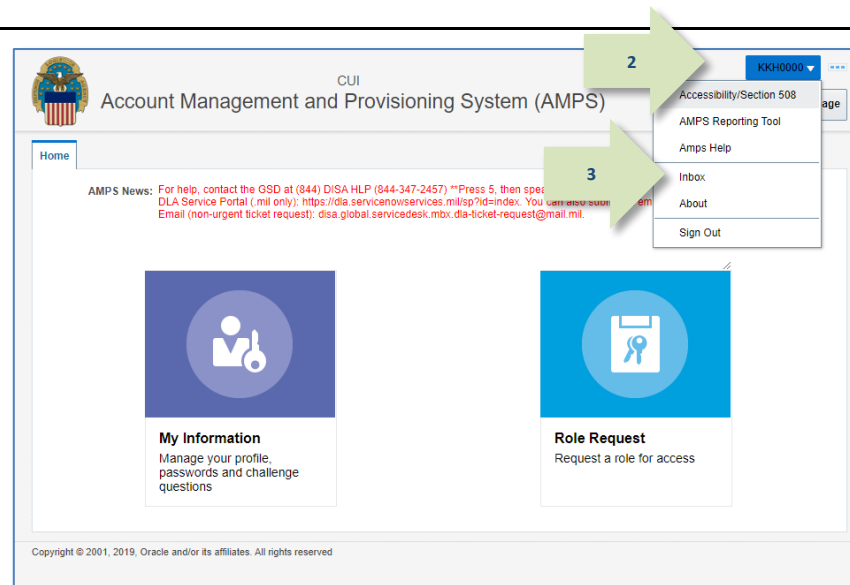
Figure 277: User ID Dropdown Menu – Inbox Command

4. From the **Title** column on the **My Tasks** view, click the SAAR identified in the **Action Required** notification.

AMPS opens the **Attribute Change Request Security Officer Decision** *screen (see Figure 279).*
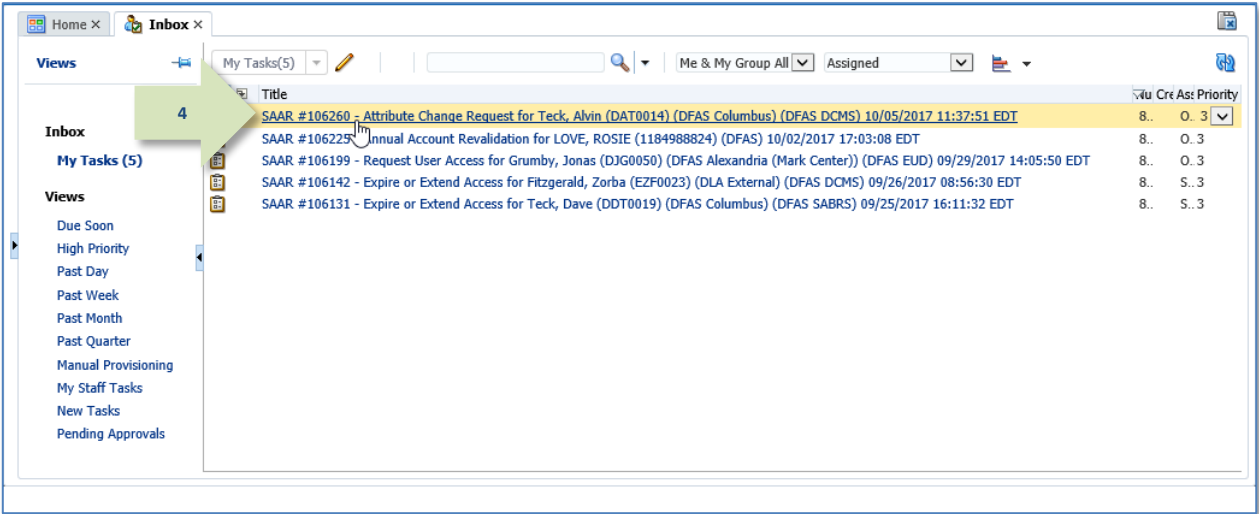
Figure 278: My Tasks - Security Officer

5. Review and update the **Security Information** at any time on the decision screen.

   SAAR attribute information is displayed on the Attribute Change Request Details tab.

   If you need more information about the user in order to update the Security Information section, review the User Information tab.

   If you have an issue with any of the information displayed, you can consult with the requestor to clarify the purpose or content of the information.

   Contact information for previous approvers is included on the Additional Information screen.

   The AMPS Security Officer can reject this request, if necessary, by following these steps:

   - *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*
   - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

6. Click the Additional Information tab.

   *AMPS displays the **Additional Information** tab screen (see Figure 280)*

Figure 279: Security Officer Approval Decision Screen

7. Review the SAAR Approval History table.

If the Supervisor has entered comments, AMPS displays them on this screen.

Contact information for previous approvers is also included.

8. Click the User Information tab.

*AMPS displays the **User Information** tab screen (see Figure 281).*

Figure 280: Attribute Change Request – Additional Information

9. Review the information provided in the **User Information** tab to finalize the decision.

As an option, the AMPS Security Officer can fill in comments that explain or justify the approval.

The AMPS Security Officer can also reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the **Comments** field. This action activates the Reject button.*

- *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

10. To proceed, click the **Approve** button.

AMPS closes the decision screen and tab, and returns to the Inbox tab.

Figure 281: Attribute Change Request - User Information

11. **OPTIONAL:** Follow these steps to view the completed request screen, as needed. Start on the **Inbox** tab - **My Tasks** view:

   a. In the search field, enter the SAAR number for the decision you want to review.

   b. In the status drop-down list, select either **Any** or **Completed**.

   c. Click the SAAR title to review the SAAR on screen (not shown).

   AMPS automatically initiates a search based on the criteria entered.

   *In this example, the system displays the SAAR because it also has a status of **Completed**.*
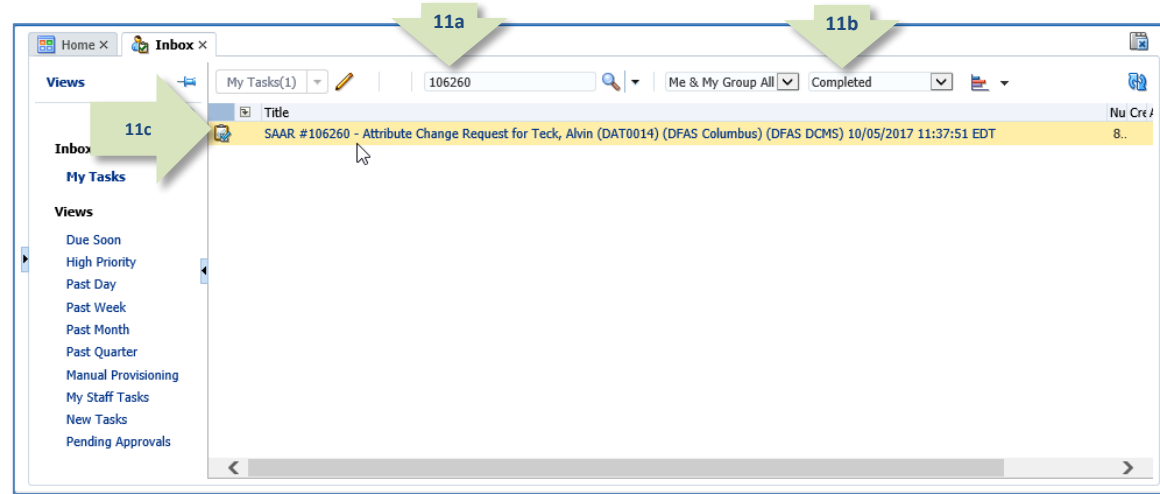
Figure 282: Inbox – Search for Completed SAAR

12. After a Security Officer completes an approval for an attribute update, AMPS sends an email notification to the user regarding the Security Officer's decision.

Sample User Notification: Status

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: The Security Officer has completed an approval for SAAR #106260.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

13. After a Security Officer completes an approval for an attribute update, AMPS sends an email notification to the user regarding the next step in the approval process.

Sample User Notification: Next Approver

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 is awaiting Data Owner approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

No action is required from you at this time.

This task expires on 10/25/2017 14:22:48 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Data Owner Approval

After a Security Officer completes the approval for an attribute update, AMPS sends an email notification to the next approver regarding an action required on a pending SAAR.

1. Note the SAAR number in the **Action Required** email notification.

   The email message describes the type of SAAR submitted for review.

1

Sample Approver Notification: Next Approver

Subject: Action Required: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 - Attribute Change Request for Teck, Alvin (DAT0014) (DFAS Columbus) has been submitted for approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/25/2017 14:22:48 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. To begin the approval process, a Data Owner logs in to AMPS.

   *AMPS displays the **Self Service Home** page and identifies the logged-in user by ID.*

3. Click the User ID to open the dropdown menu, then click the **Inbox** command from the menu.

   *AMPS displays the Data Owner's **My Tasks** screen (see Figure 284).*
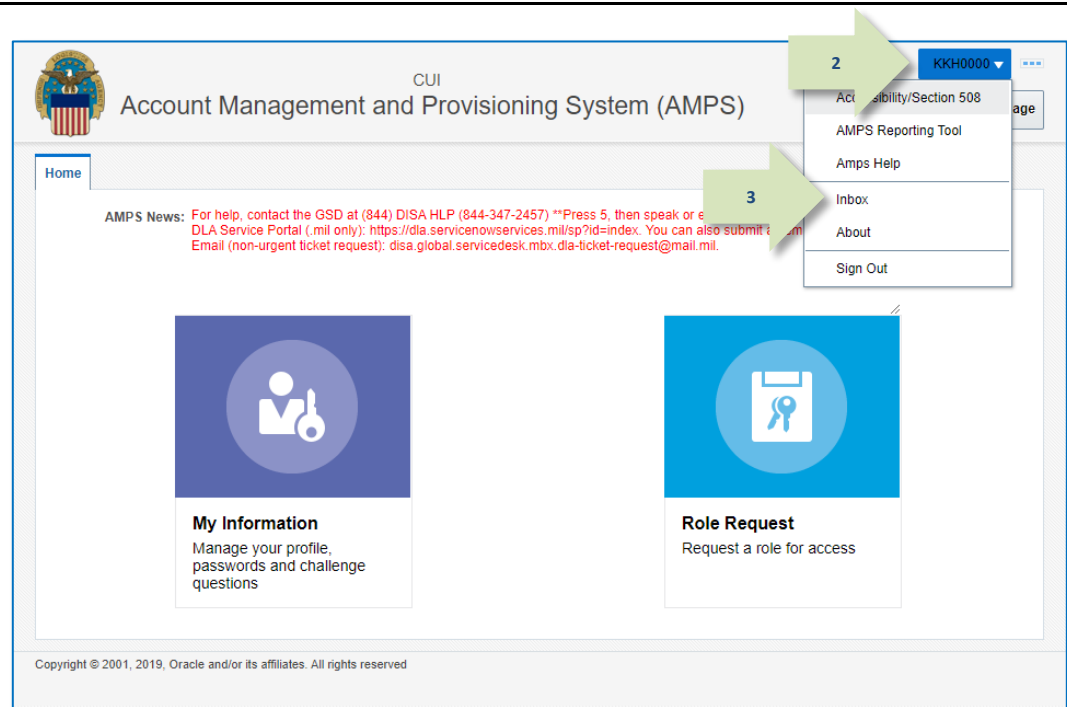
Figure 283: User ID Dropdown Menu – Inbox Command

4. In the **My Tasks** screen's **Title** column, click the SAAR identified in the **Action Required** notification.

   AMPS opens the **Attribute Change Request - Data Owner Approval Decision** *screen (see Figure 285).*
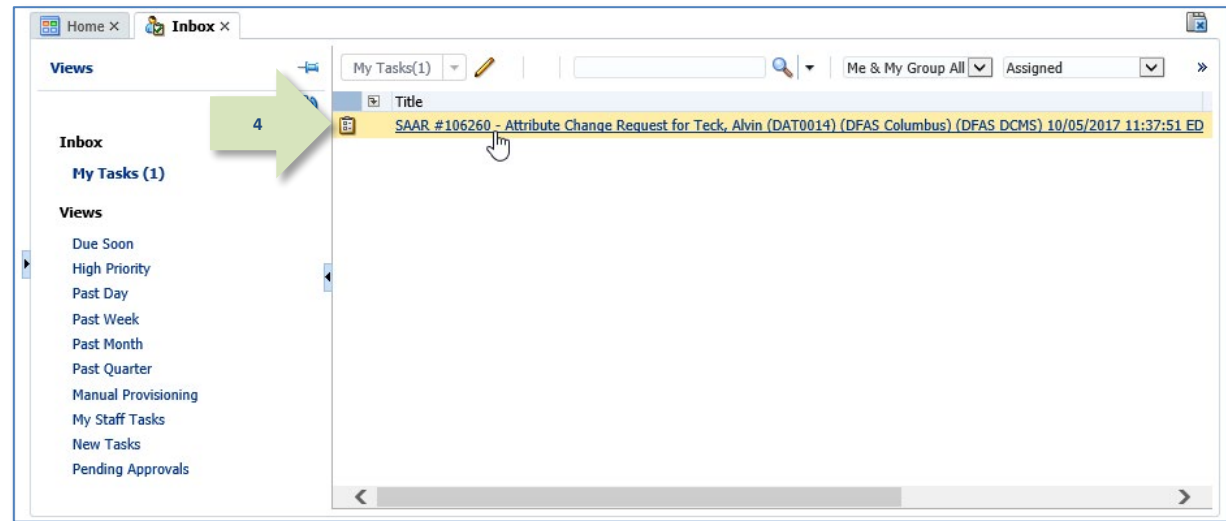
Figure 284: My Tasks - Data Owner

5. Review the SAAR information and SAAR attribute information on this screen.

If you have an issue with any of the information displayed, you can consult with the requestor to clarify the purpose or content of the information.

*Contact information for previous approvers is included on the **Additional Information** screen.*

The AMPS Data Owner can reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

- *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

6. Click the Additional Information tab.

AMPS displays the Additional Information screen (see Figure 286).

Figure 285: Data Owner Decision – Attribute Change Request Details
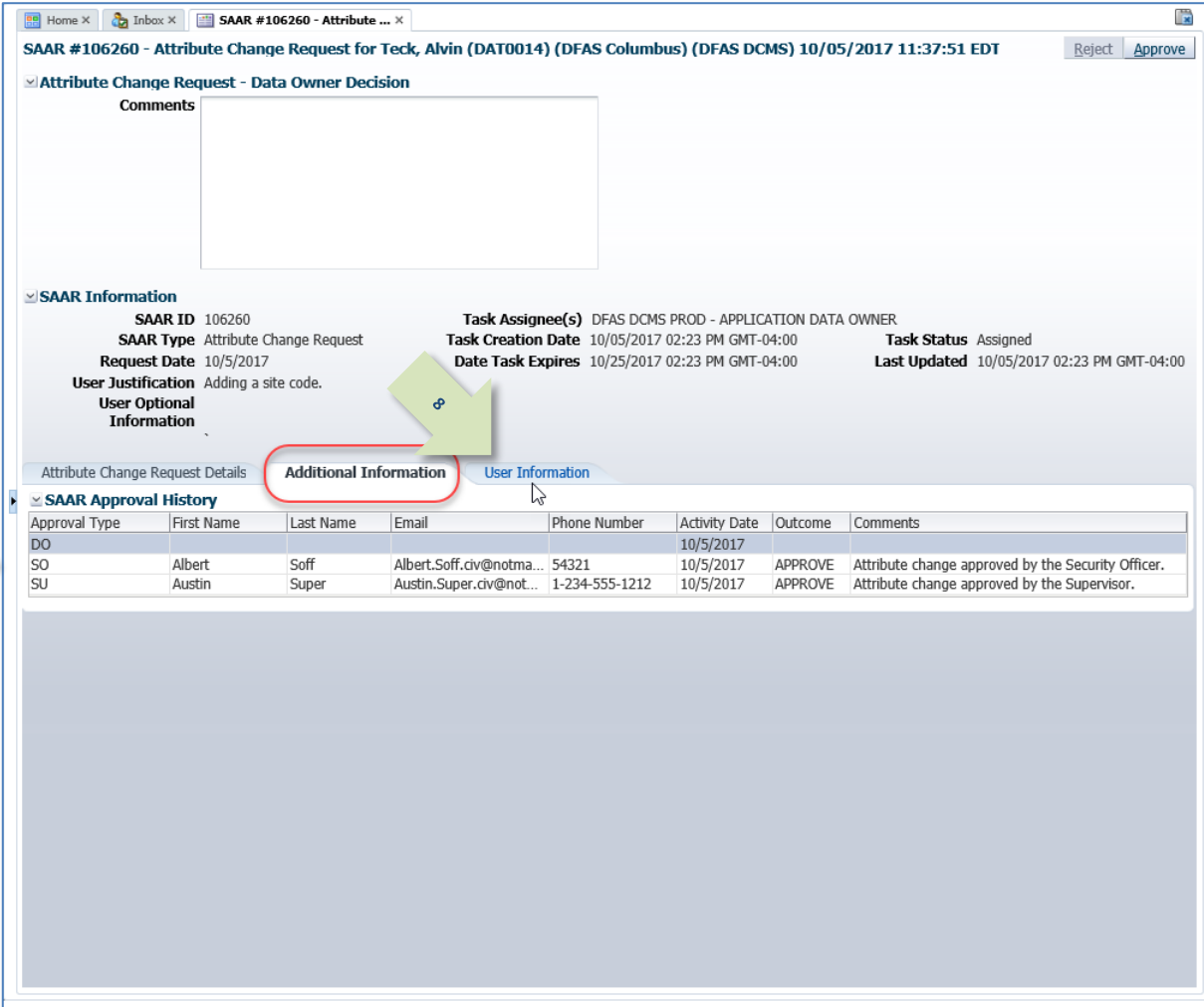
7. In the Additional Information screen, review the SAAR Approval History table.

    If the Supervisor or Security Officer has entered comments, AMPS displays them on this screen.

    Contact information for previous approvers is also included.

8. Click the User Information tab.

    AMPS displays the User Information tab (see Figure 287).

Figure 286: Attribute Change Request –Additional Information

9. Review the information provided in the **User Information** tab to finalize the decision.

    As an option, the application Data Owner can fill in comments that explain or justify the approval.

    The Data Owner can also reject this request, if necessary, by following these steps:

    - *Enter the reason for the rejection in the **Comments** field. This action activates the Reject button.*

    - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

10. To proceed, click the **Approve** button.

    *AMPS closes the decision screen and tab, and returns to the **Inbox** tab.*

Figure 287: Attribute Change Approval – User Information

11. **OPTIONAL:** Follow these steps to view the completed request screen, as needed. Start on the **Inbox** tab - **My Tasks** view:

   a. In the **Search** field, enter the SAAR number for the decision you want to review.

   b. In the **Status** dropdown list, select either **Any** or **Completed**.

   c. Click the SAAR title to review the SAAR on screen (not shown).

   AMPS automatically initiates a search based on the criteria entered.

   In this example, the system displays the SAAR because it also has a status of **Completed**.
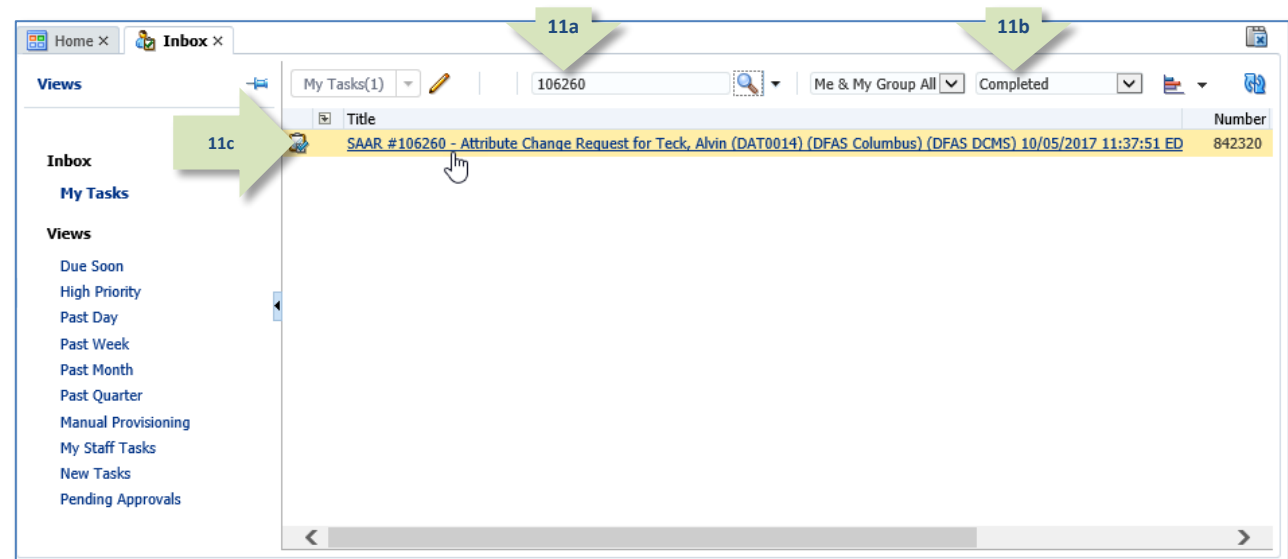
Figure 288: Search for Completed SAAR

12. After a Data Owner completes an approval for an attribute update, AMPS sends an email notification to the user regarding the Data Owner's decision.

Sample User Notification: Status

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: The Data Owner has completed an approval for SAAR #102799.

The Data Owner has completed an approval for SAAR #106260.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

13. After a Data Owner completes an approval for an attribute update, AMPS sends an email notification to the user regarding the next step in the approval process.

Sample User Notification: Next Approver

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 is awaiting Information Assurance Officer approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

No action is required from you at this time.

This task expires on 10/25/2017 14:35:32 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

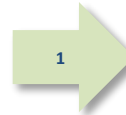## Information Assurance Officer (IAO) Approval (DFAS Roles Only)

After a Data Owner completes the approval for an attribute update, AMPS sends an email notification to the next approver regarding an action required on a pending SAAR.

Note:

DLA applications do not require an IAO review. If a DFAS user requests a DLA role, AMPS does not present the Information Assurance Officer Decision screens.

---

1. Note the SAAR number in the **Action Required** email notification.

   The email message describes the type of SAAR submitted for review.

1

Sample Approver Notification: Next Approver

Subject: Action Required: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: SAAR #106260 - Attribute Change Request for Teck, Alvin (DAT0014) (DFAS Columbus) has been submitted for approval.

This request was submitted in AMPS on 10/05/2017 11:37:51 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/25/2017 14:35:32 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

2. To begin the IAO approval process, an IAO logs in to AMPS.

   *AMPS displays the **Self Service Home** page and identifies the logged-in user by ID.*

3. Click the User ID to open the dropdown menu, then click the **Inbox** command from the menu.

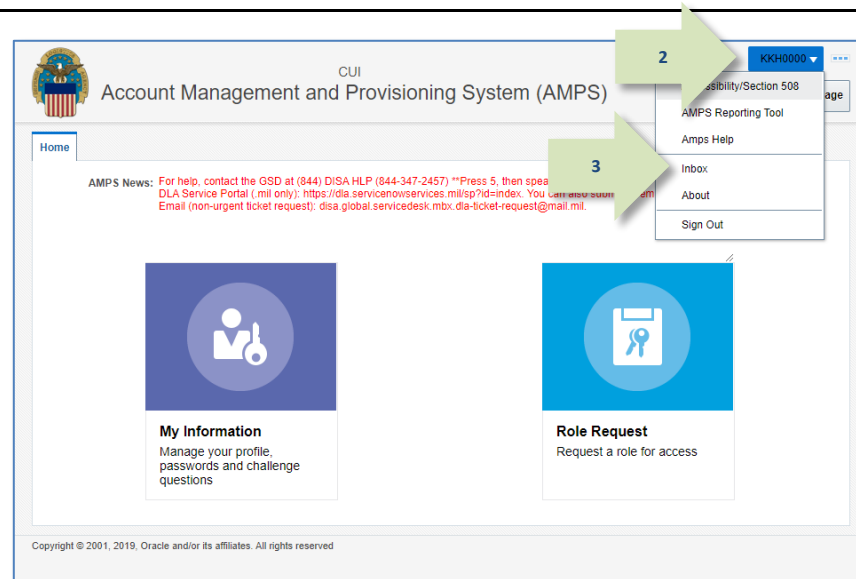   *AMPS displays the IAO's **My Tasks view** (see Figure 290).*

Figure 289: User ID Dropdown Menu – Inbox Command

4. In the **Title** column of the **My Tasks** view, click the SAAR identified in the **Action Required** notification.

AMPS opens the **Attribute Change Request - Information Assurance Officer Decision** *screen (see Figure 291).*
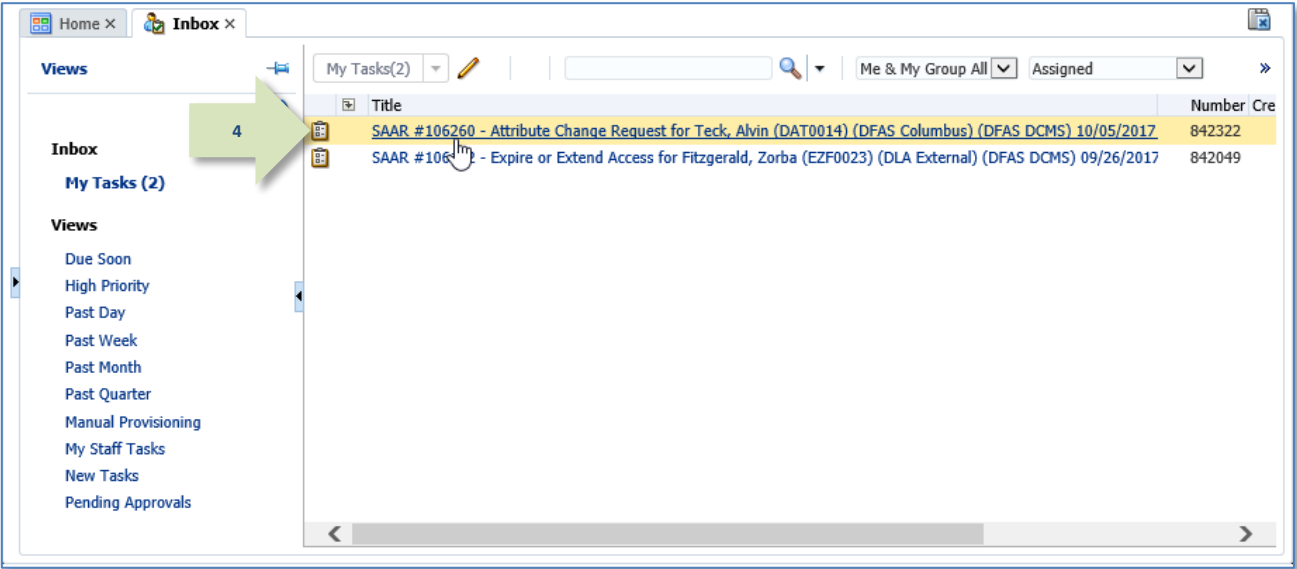

Figure 290: My Tasks - Information Officer

5. Review the SAAR information and SAAR attribute information on this screen.

    If you have an issue with any of the information displayed, you can consult with the requestor to clarify the purpose or content of the information.

    *Contact information for previous approvers is included on the **Additional Information** screen.*

    The AMPS Information Assurance Officer can reject this request, if necessary, by following these steps:

    - *Enter the reason for the rejection in the **Comments** field. This action activates the Reject button.*
    - *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

6. Click the Additional Information tab.

    AMPS displays the Additional Information screen (see Figure 292).

Figure 291: Attribute Change Request Details – Information Assurance Officer Decision

7. In the Additional Information screen, review the SAAR Approval History table.

    If the Supervisor, Security Officer, or Data Owner has entered comments, AMPS displays them on this screen.

    Contact information for previous approvers is also included.

8. Click the User Information tab.

    *AMPS displays the **User Information** tab (see Figure 293).*

Figure 292: Attribute Change Request – Information Assurance Officer – Additional Information

9. Review the information provided in the **User Information** tab to finalize the decision.

As an option, the Information Assurance Officer can fill in comments that explain or justify the approval.

The Information Assurance Officer can also reject this request, if necessary, by following these steps:

- *Enter the reason for the rejection in the **Comments** field. This action activates the **Reject** button.*

- *Click the **Reject** button. This action stops the approval process and notifies the requestor that the change request has been rejected by the approver for the stated reason.*

10. To proceed, click the **Approve** button.

*AMPS closes the decision screen and tab, and returns to the **Inbox** tab.*

Figure 293: Attribute Change Request-Information Assurance Officer – User Information

11. **OPTIONAL**: Follow these steps to view the completed request screen, as needed. Start on the **Inbox** tab - **My Tasks** view:

   a. In the search field, enter the SAAR number for the decision you want to review.

   b. In the status dropdown list, select either **Any** or **Completed**.

   c. Click the SAAR title to review the SAAR on screen (not shown).

   AMPS automatically initiates a search based on the criteria entered.

   In this example, the system displays the SAAR because it also has a status of **Completed**.
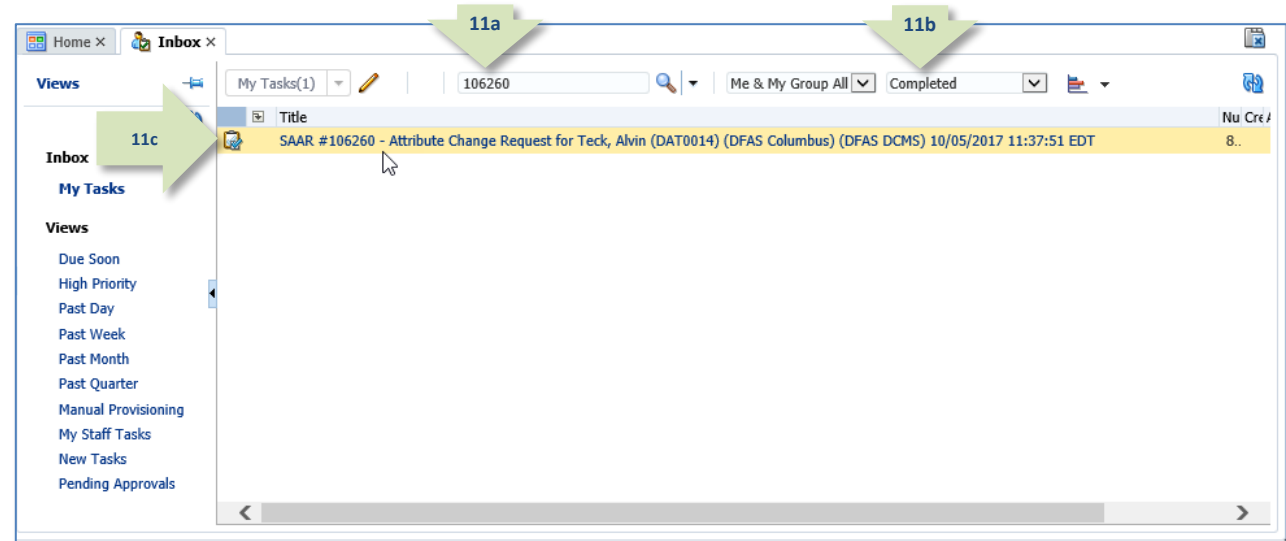
Figure 294: Inbox–My Tasks–Search for the Completed SAAR

12. After an Information Assurance Officer completes an approval for an attribute update, AMPS sends an email notification to the user regarding the IAO's decision.

Sample User Notification: Status

Subject: Notification: SAAR #106260 - Attribute Change Request for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS DCMS) 10/05/2017 11:37:51 EDT

Body: The Information Assurance Officer has completed an approval for SAAR #106260.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

13. After the IAO approval is completed, AMPS sends an email notification to the requestor indicating that the application provisioning has started.

13

Sample Provisioner Notification

Subject: AMPS Application Processing for SAAR #106260

Body: AMPS Application Processing request for SAAR 106260 has started.

Request For:
DLA Login: DAT0014
Name: Teck, Alvin
Phone: 888-555-1212
Email: Alvin.Teck@dla.mil
EDIPI/UPN: 0999999990

Access Information:
SAAR #: 106260

Attribute Change on Job Role: DFAS DCMS Prod - DSK Air Force Entry DE-DAO (380100) Profiles DSK-002

Current Applications and Access:
      Resource: DFAS PROD - DFAS DCMS
            Access: DSK-002 DSK Air Force Entry DE-DAO (380100) Profiles

Data Owner Comments: Attribute change approved by the Data Owner.

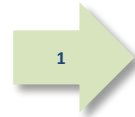Justification: Adding a site code.

Optional Information: (none)

Attribute Change Request SAAR requested by Alvin Teck on 10/05/2017

Provisioner Action

This procedure outlines and describes the procedure followed by a Total AMPS provisioner
for an application role defined for Total AMPS provisioning.

1. After the IAO approval is completed, AMPS sends the attribute update request by email to the Provisioner for final action.

1

Sample Provisioner Notification

Subject: AMPS Application Processing for SAAR #106260 requires your attention.

Body: AMPS Application Processing request for SAAR 106260 requires your attention.

Request For:
DLA Login: DAT0014
Name: Teck, Alvin
Phone: 888-555-1212
Email: Alvin.Teck@dla.mil
EDIPI/UPN: 0999999990

Access Information:
SAAR #: 106260

Attribute Change on Job Role: DFAS DCMS Prod - DSK Air Force Entry DE-DAO (380100) Profiles DSK-002

Current Applications and Access:
        Resource: DFAS PROD - DFAS DCMS
                Access: DSK-002 DSK Air Force Entry DE-DAO (380100) Profiles

Data Owner Comments: Attribute change approved by the Data Owner.

Justification: Adding a site code.

Optional Information: (none)

Attribute Change Request SAAR requested by Alvin Teck on 10/05/2017

2. To begin the provisioning process, a Provisioner logs in to AMPS.

   *AMPS displays the **Self Service Home** page and identifies the logged in user by ID.*

3. The Provisioner clicks the User ID, to open the dropdown menu, then clicks the **Inbox** command from the menu.

   *AMPS displays the Provisioner's **My Tasks** view (see Figure 296).*
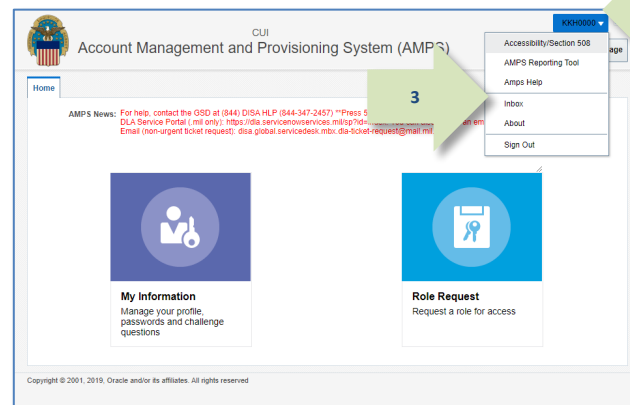
Figure 295: Main Menu – Provisioner

4. In the **My Tasks** view, the Provisioner clicks the SAAR identified in the **Action Required** notification.

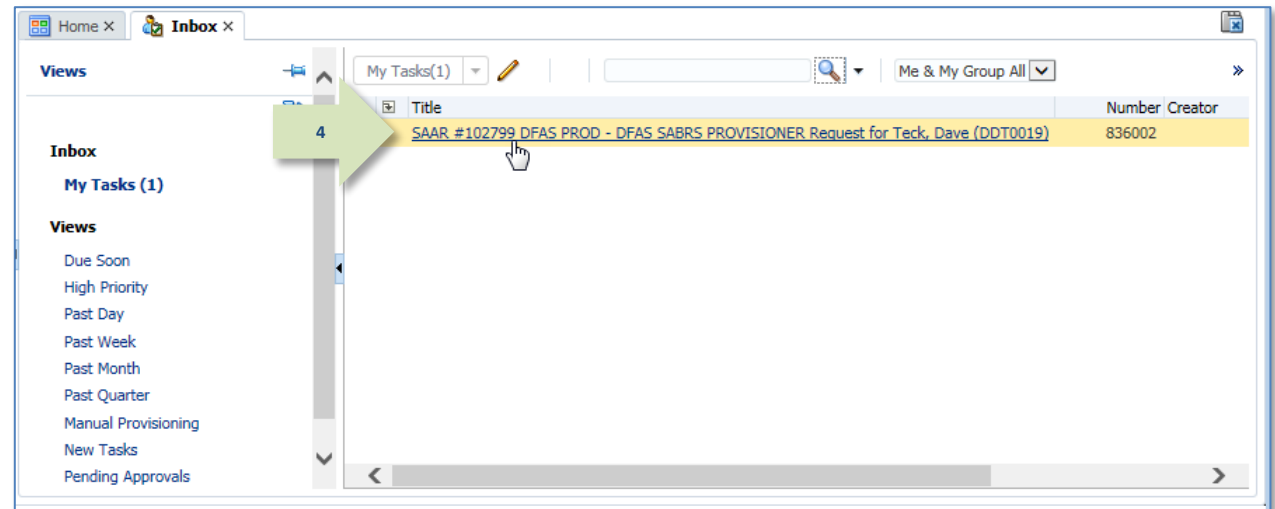   *AMPS opens the Provisioning ticket screen for the SAAR (see Figure 297).*

Figure 296: My Tasks – Provisioner

5. The Provisioner reviews the Work Details and other information on the Total AMPS ticket.

The Total AMPS ticket offers the provisioner these features. The provisioner can . . .

5a. Enter comments and click **Save Comments** to preserve the Provisioning ticket. Reopen the ticket, as needed, to enter final comments in the required **Comments** text area.

AMPS saves and closes the request, enabling the provisioner to close and later reopen the incomplete ticket to perform the prescribed provisioning work.

5b. Enter comments and click **Work is Complete** when provisioning is finished.

AMPS closes the provisioning ticket.

AMPS also moves a record into the user's SAAR History indicating that the role has been provisioned to the user's account.

Figure 297: Provisioner Ticket Screen

6. After the Provisioner completes the work specified in the ticket. AMPS sends a final approval notice to the user.

Sample User Notification: Status

Subject: AMPS Application Processing for SAAR #102799

Body: Your request for role DFAS SABRS Prod - Update Additional Attributes SABRS-999 with access to DFAS SABRS (SAAR 102799) has been fully approved and provisioned. Your account has been set up with the permissions associated with the role you requested, and you can now access the application.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Role Removal

What you can do:	All users can submit a role removal request by selecting a role from a list of currently held roles and submitting the selection as a removal request. AMPS notifies you at each stage of the role removal submission and approval process. **The Role Removal process submits each role set for removal to the appropriate deprovisioning process: either a Total AMPS ticket or Remedy ticket is issued for deprovisioning, or the role is automatically deprovisioned in applications that have automatic provisioning.** Note that if you are an administrative user with access to the Application Access Removal module, you can remove a role from your own account, but the role removal request still requires Supervisor approval. Refer to the section entitled **Application Access Removal** for more information on this module.
For additional information about removing roles:	AMPS provides a separate user interface and procedures for Data Owners to remove roles from users, remove users from roles, and to perform such tasks in bulk. Please see the section entitled **Application Access Removal** for a complete description and procedural instructions.
About removing *Primary Only* roles:	AMPS enables you to remove a **Primary Only** role using the procedure in this section, but it may not be necessary. If, for example, you change jobs and need a different **Primary Only** role, you can request the new **Primary Only** role. AMPS displays an **Information** message cautioning you that you already have a **Primary Only** role. Close the message and proceed with the request; AMPS creates a single SAAR for removing the existing role and adding the new role.
Where to start:	Begin at the AMPS Home page.

How to Request Removal of a Role

Users:	This role removal procedure gives you the capability to remove a role you no longer need. Your AMPS supervisor must approve all role removal requests.
Supervisors:	AMPS sends role removal requests submitted by your subordinates to you for approval.

1. Log in to AMPS.

    *AMPS displays the **Self Service Home** page and identifies the logged in user by ID.*

2. Click the **My Information** tile.

    *AMPS displays the **My Information** screen with access to two tabs: **User Information** and **Applications & Roles** (see Figure 299).*
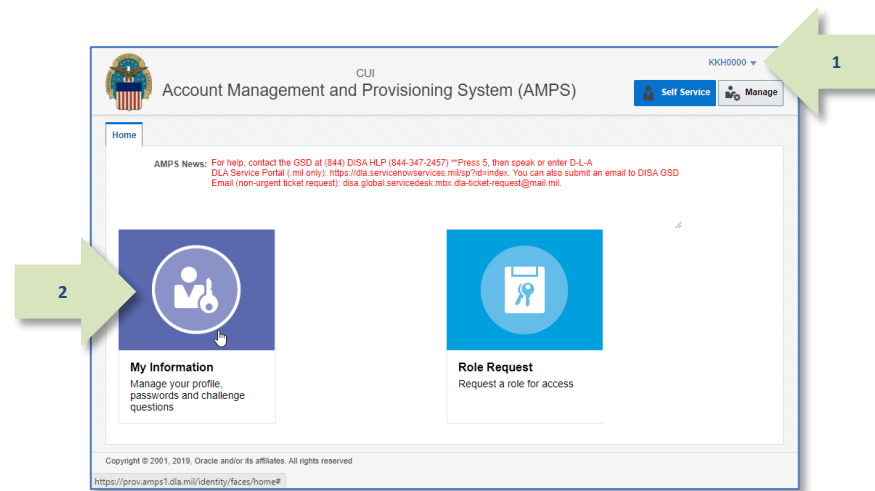

Figure 298: AMPS Home Page

3. Click the **Applications & Roles** tab to open this screen.

Figure 299: My Information

4. Click the name of a role from the **Current Roles** list to select it for removal.

5. Click the **Remove Role** button.

   AMPS displays the Request Role Removal *dialog box (see Figure 301).*

Figure 300: Select and Remove a Role

6. Enter text in the **Justification** text area to clarify the removal request for your supervisor. An entry in this text area is required.

7. Click **OK**.

   *AMPS displays an **Information** message to confirm the submission of the role removal request (see Figure 302).*

> ## Note:
> The Justification text featured in the sample screen is for demonstration purposes only. Please enter comments applicable to the current request.

Figure 301: Role Removal - Justification for Removal

8. In the **Information** message box, note the SAAR number and click **OK** to close the box.
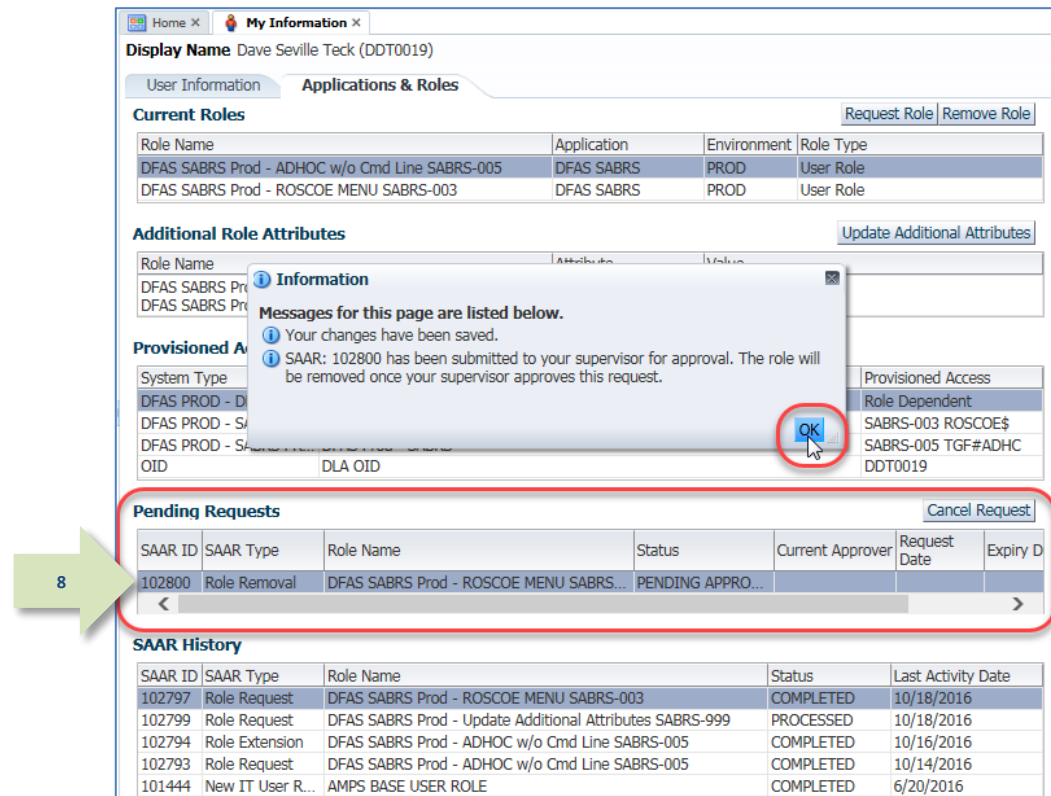
Figure 302: Role Removal - Information Message

9. To check the status of a role removal request see **How to Check Your Role Status** on page 97.

AMPS lists the SAAR for the role removal request and provides the Status, Current Approver, and date information for the SAAR.

From this data, you can determine that the SAAR awaits your Supervisor's approval, and that AMPS will discard your request after the specified Expiry Date. If the request expires, you must resubmit the request.

Figure 303: Role Removal – SAAR Information

Note:

Do not attempt to cancel a request with a status of TICKETED. A ticketed role request is in the provisioning stages and cannot be cancelled through AMPS. Contact the Service Desk (see page 9) if you need assistance cancelling a ticketed role request.

10. After you submit a role removal request, AMPS sends an email notification confirming the submission of a role removal request.

The email contains the SAAR number, SAAR Type, Removal Type, Role name, Justification, name, and User ID of the administrator requesting the removal and when the request was submitted.
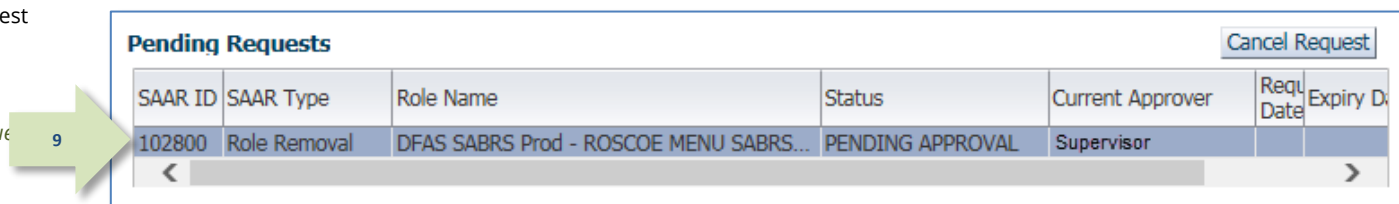
Note:

AMPS sends the email in HTML format, but it can also be viewed in plain text. The sample provided in Figure 304 is an image of the email viewed in HTML format.
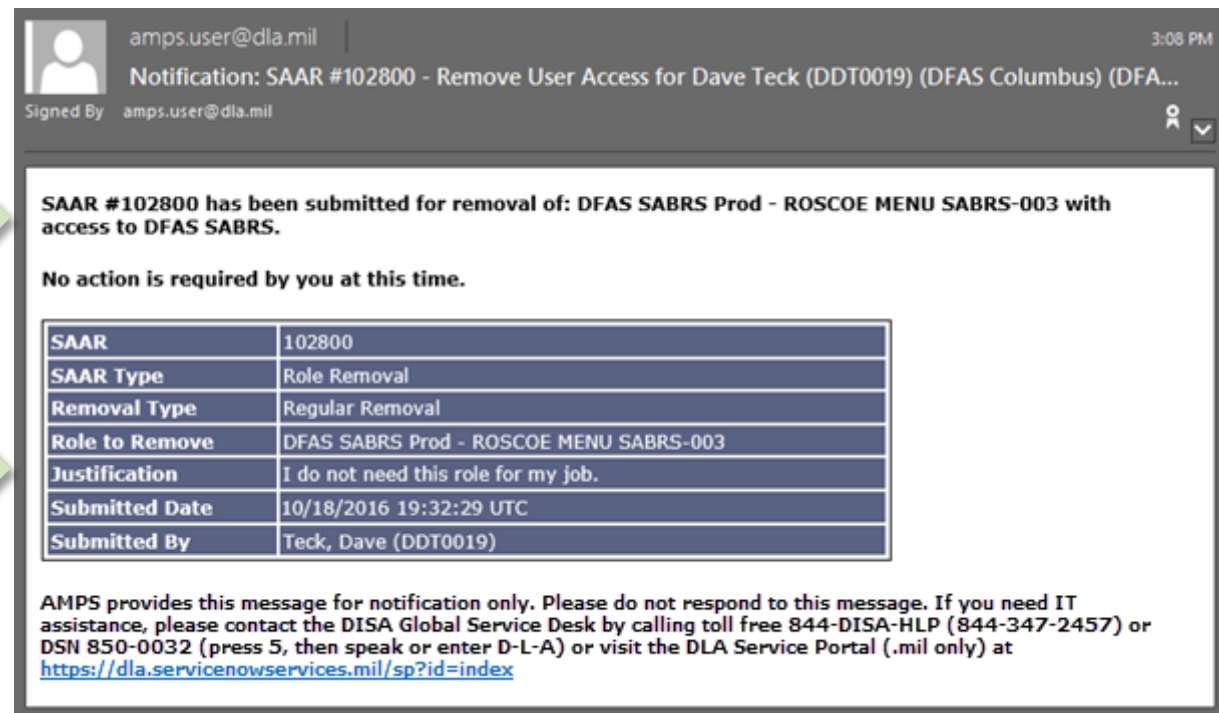
Sample User Notification: Confirmation

Figure 304: Sample User Notification - Role Removal Confirmation

11. After you submit a role removal request, AMPS also sends an email notification confirming the status of the role removal request.

11 →

Sample User Notification: Status

Subject: Notification: SAAR #102800 - Remove User Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 10/18/2016 12:32:29 UTC

Body: SAAR #102800 is awaiting Supervisor approval.

This request was submitted in AMPS on 10/18/2016 12:32:29 UTC.

No action is required from you at this time.

This task expires on 11/07/2016 11:32:35 UTC.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Next Steps . . .

As the notifications state, AMPS has received the role removal request, entered the request in the system, and assigned a SAAR number.

Next, AMPS notifies your Supervisor that an action on this request is pending. When the Supervisor completes this action, AMPS notifies you of the result.

How to Approve a Role Removal Request

Supervisors:	You must have the AMPS Supervisor role to approve a role removal request. A role removal is listed in your **Inbox** as a SAAR. Role removals come from three sources: • User submits a role removal request. The Supervisor must approve the removal request. • User's role expiration task expires, and the role is automatically submitted for removal. The Supervisor must approve the removal request. • Supervisor submits a role removal request on the user's behalf. AMPS automatically approves this type of request. See the section entitled: **How to Submit a Role Expiration Request.** Follow these steps to approve a role removal request starting at the **Inbox**.
Users:	After your Supervisor approves a role removal request, the request goes through a deprovisioning process. At that time, the role removal request is complete, and your access to the role's application and resources is cancelled. The role is removed from your account in AMPS.

1. After a user submits a role removal request, AMPS notifies the Supervisor by email of a pending action required.

1
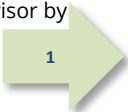
Sample Approver Notification

Subject: Action Required: SAAR #102800 - Remove User Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 10/18/2016 12:32:29 UTC

Body: SAAR #102800 - Remove User Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to remove DFAS SABRS Prod - ROSCOE MENU SABRS-0003 was submitted in AMPS on 10/18/2016 12:32:29 UTC.

 Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open the approal task. This task expires on 11/07/2016 11:32:35 UTC.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. Click the User ID to open the dropdown menu, then click the **Inbox** command from the menu.

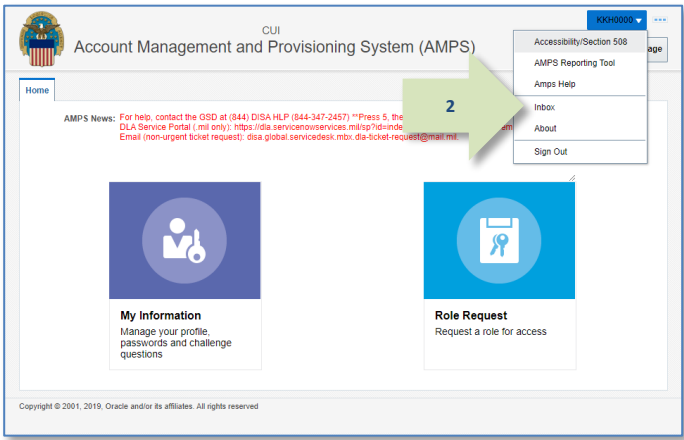   *AMPS displays the **My Tasks** view (see Figure 306).*

Figure 305: User ID Dropdown Menu – Inbox Command

3. In the **Title** column of the **My Tasks** view, click the SAAR number for the role removal request.

    AMPS displays a **Supervisor Application Access Decision** *screen (see Figure 307).*
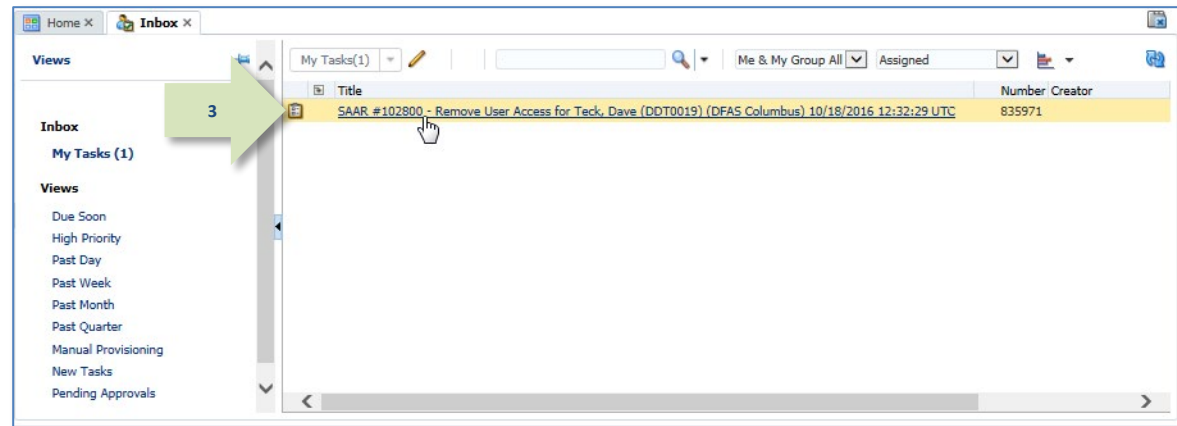

Figure 306: My Tasks List

4. Review the details, as needed, on the **Role Removal – Supervisor Decision** screen.

   Note that the SAAR number and Request Type are listed in SAAR Information. The Request Type identifies the SAAR as a request to remove a role.

5. Enter or select the required data.

   As an option, you can enter an explanation for your decision in the Comments area. AMPS saves this entry with the SAAR record.

6. Click **Approve**.

   *AMPS returns to the Supervisor's **My Tasks** tab. The approved SAAR is removed from the list of SAARs.*

> *Note:*
>
> The Comments text featured in sample screens is for demonstration purposes only. Please enter comments applicable to the current request.

Figure 307: Application Supervisor Approval Screen

7. After a Supervisor approves a role removal request, AMPS notifies the user by email of the result.

   AMPS advances the SAAR to the deprovisioning step.

Sample User Notification: Removal Approved

Subject: Notification: SAAR #102800 - Remove User Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 10/18/2016 12:32:29 UTC

Body: The Supervisor has completed an approval for SAAR #102800.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

8. After AMPS prepares the request for provisioning, AMPS sends the user an email notification informing them that the process of removing the role has started.

8

Sample User Notification: Role Deprovisioning Process Started

Subject: AMPS Application processing for SAAR #102800

Body: AMPS application processing for SAAR 102800 has started for DFAS SABRS.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

9. After the role is deprovisioned, or removed from the application, AMPS sends an email notification to the user indicating the role has been removed from the user's account in AMPS and in the application.

The email contains the SAAR number, SAAR Type, Removal Type, Role name, Justification, name, and User ID of the administrator requesting the removal and when the request was submitted.

Note:

AMPS sends the email in HTML format, but it can also be viewed in plain text. The sample provided in Figure 308 is an image of the email viewed in HTML format.

9

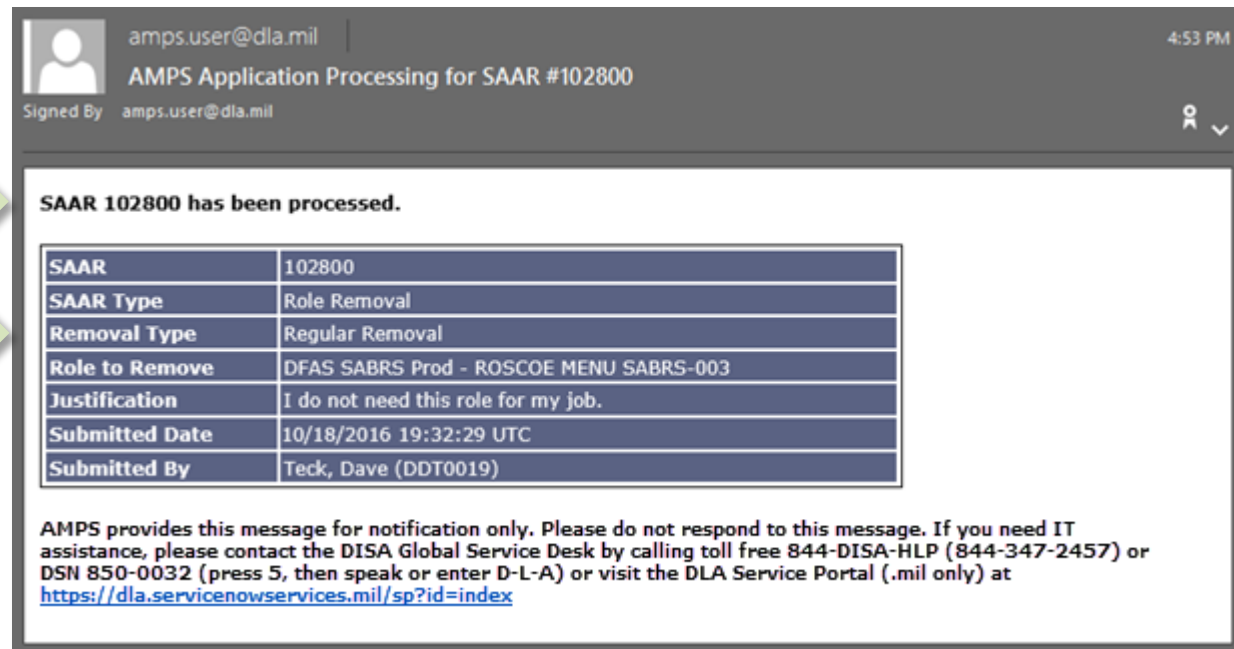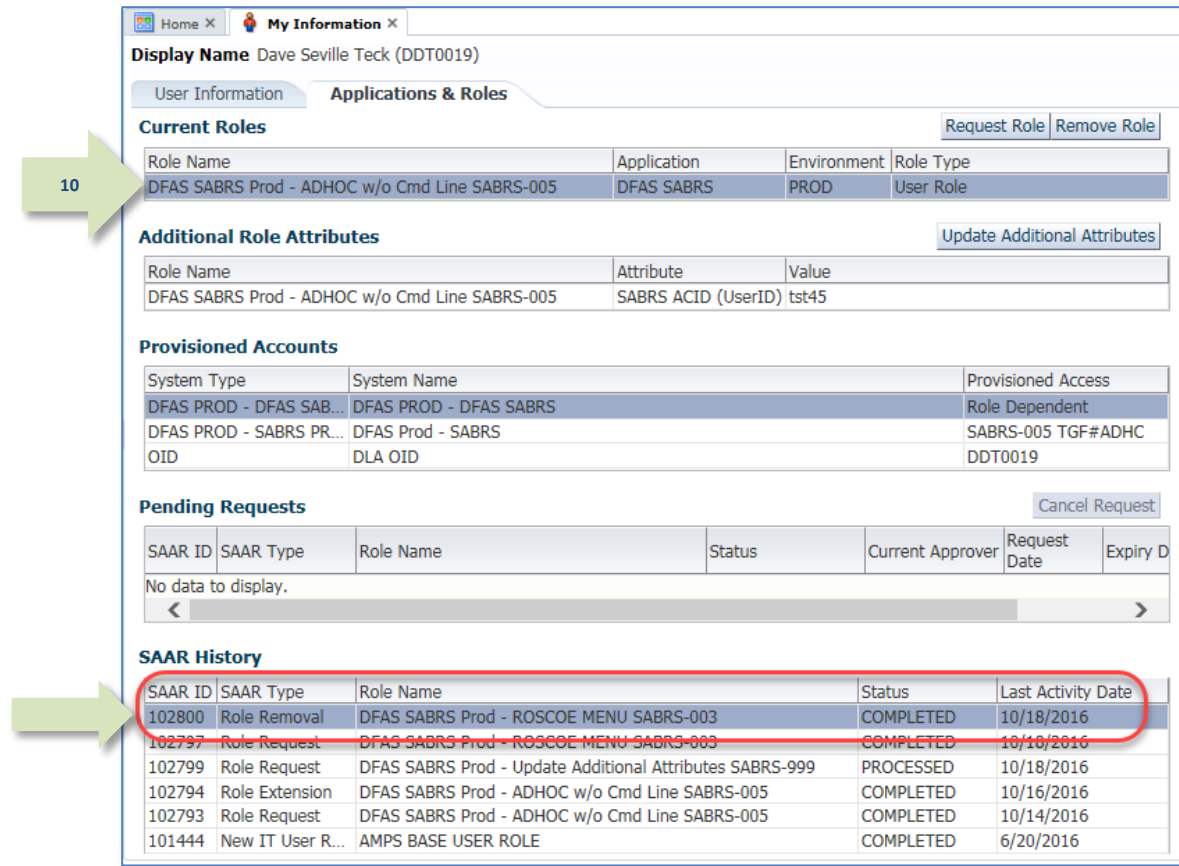## Sample User Notification: Role Removal Complete

Figure 308: Sample User Notification: Role Removal Complete

10. When the role has been deprovisioned, it is no longer listed in the user's **Current Roles** section of the **Applications & Roles** tab.

- The user's **Pending Requests** table lists the SAAR in **TICKETED** status if the role must be deprovisioned through a Total AMPS ticket or a Remedy ticket.
- After the provisioner has completed the deprovisioning process and closes the ticket, AMPS moves the SAAR record to SAAR History with a status of **COMPLETED**.
- The user's SAAR history lists the role removal SAAR as **COMPLETED** if the role is deprovisioned automatically.

Figure 309: User's Applications & Roles Screen - After Role Removal

Role Expiration and Extension

AMPS roles are assigned to users with start and end dates that determine the length of time a user retains the role before the assignment expires. The specification of start and end dates ensures that access to any application does not continue without the user being asked to confirm that the access rights are still needed. As an AMPS user, you can request either an expiration or an extension of a role assignment when AMPS notifies you that a role is about to expire. For a user who receives an email notification of an impending role expiration, AMPS presents the following three options:

- Submit a request for an expiration of the role, which confirms the upcoming expiration. AMPS submits this request to an expiration approval process.
- Allow the role to expire without submitting a request for expiration. AMPS submits this automatic expiration to the role removal process, notifies the user's Supervisor, and assigns a task to approve or deny the role expiration.
- Submit a request for an extension of the role. A role extension is limited to one year for all External User roles. AMPS submits role extension requests to the same approval process as the original role request.

Who Determines the Duration for a Role Assignment?

The role assignment terms for internal and external users are set by default, but certain approvers can modify the start and end dates.

- For **internal users**, the AMPS Supervisor and the application Data Owner determine the start and end dates of a role assignment. AMPS automatically calculates the term of a role assignment at approximately 20 years as each role request is submitted by the user to the approval process. When the Supervisor receives the role request for approval, he or she can adjust the start and end dates. Similarly, the application Data Owner can adjust the start and end dates as needed for an internal user.
- For **external users**, the application Data Owner determines the start and end dates of a role assignment. The default period for an external user is one year (365 days), but the Data Owner can shorten that period during the approval process.

Role Expiration

Role Expiration, also called "Role Expiry**,** refers to the withdrawal of a role assignment in AMPS from a user's AMPS account and to the associated deprovisioning of the role in the applications and resources associated with the role.

To automate the processing of role expiration, AMPS monitors the period during which each role is assigned to a user and detects impending role expirations using the role's expiration date. This date is set during the request approval process and is identified as the role's "End Date." During a role's assignment period, when the current date reaches 130 days before the specified end date, AMPS begins the role expiration process by sending an expiration

notification to the user. The notification is sent to the email address associated in AMPS with the user's account.

AMPS sends the email notification to the user every day until day 20 of the notification period. After the first role expiration notification is sent, the user is responsible for exercising either a role expiration or role extension request within the first 20 days. If the user does not respond to the email notification by midnight Eastern Time of the 20th day, AMPS submits a role expiration request to the Role Removal process. The Role Removal request that AMPS generates for the expiration task goes to the user's Supervisor for approval or other action. See the section entitled **How to Approve a Role Removal Request**.

Role Extension

Role extension refers to the extension of a role assignment to a new end date. When a user submits a request to extend a role assignment in response to the role expiration notification, AMPS submits the extension request to a predefined approval process.

When a role extension is approved in a timely manner during the role-extension approval process, the user's access to the role's application continues without interruption. However, a role extension request also carries an expiration date in the approval process, and if the extension request expires, the user's role may expire too.

The user is advised to monitor any role expiration or extension requests.

Role Extension and Attribute Change Request

Note that if you submit a request to extend a role with associated attributes, you cannot update any attributes within the extension request. However, you can submit a separate attribute change request while your extension request is pending approval.

Please see How to Update Additional Attributes on page 210 in the *AMPS User Guide* for more information.

Exemption from the Role Expiration Process

Some roles may be exempt from the role expiration process, in which case the role assignment will not expire. When AMPS detects a role that is exempt from the role expiration process, it skips the role, regardless of the **End Date** assigned to the role. The base AMPS user role is one such role, permanently exempt from expiration. Other roles may be placed on an exemption list by the application owner, as is the case with certain DFAS roles. However, most roles are subject to the **Annual Account Revalidation** (AAR) process, which requires the user's account to be re-verified on an annual basis (see page 385).

Role Expiration and Extension Procedures: All Users

A user with an expiring role can make a request to expire or extend the role. The following guidelines apply to internal and external users:

- An **internal user** can update profile information, update his or her Organization designation, update the current AMPS Supervisor designated for the user's account, and request approval for the expiration or extension of an AMPS-managed application role.
- An **external user** can update profile information, enter or change External Supervisor email address (if applicable to the User Type), enter or change an External Security Officer email address (if applicable to the User Type), enter or change an External Authorizing Official email address (if applicable to the User Type), and request the approval for the expiration or extension of an AMPS-managed application role.

Role Expiration and Extension Procedures: Approvers

The following subsections summarize procedures for role expiration and extension approvers.

Approving a Role Expiration Request

- **Time Limit for the Supervisor: 20 days**
- Reminder interval: Every day

A role expiration request needs only the approval of the user's Supervisor to be processed immediately. After AMPS records the approval, the system removes the role and, if necessary, generates a provisioning ticket to deprovision the role for the user.

If a user fails to respond to a role expiration notification, AMPS notifies the user's AMPS Supervisor who can recommend the appropriate action.

Approving a Role Extension Request

- **Time Limit for each Approver: 20 days**
- Reminder interval: Every day

A role extension request requires the same types of approvals as a new role request. The user's Supervisor, organizational Security Officer, application Data Owner, and organizational IAO address the role extension request and recommend approval or rejection.

- ➢ DLA systems do not require an IAO review.
- ➢ DLA roles may not require a Security Officer review if they meet specific criteria. Under the right circumstances, the review is not required, or the request is automatically approved.

A rejected role extension request results in the removal of the role from the user's AMPS account and the subsequent deprovisioning of the user's account from the corresponding application.

Note that role extension requests for external users are approved by External Supervisors and External Security Officers. These approvers do not have AMPS accounts.

Instead, AMPS provides access to an external approval system that displays the approval screen to the authenticated, authorized approver and enables that approver to complete a decision without logging in to AMPS.

How to Submit a Role Expiration Request

| What You Can Do	This procedure enables you to submit a request for role expiration on an expiring role.
	This procedure differs from Role Removal in that a user can submit a Role Removal request at virtually any time. However, a user must respond to a Role Expiration task or allow the expiring role to be removed without action on his or her part.
Where to Start	After reading the **Action Required** email notification, start by logging in to AMPS and checking your **Inbox** > **My Tasks** list.

How to Submit a Role Expiration Request: Internal Users

1. Read the extension notification and make note of the SAAR number.

   This number refers to the SAAR that requires a response from the user within 20 days.

   AMPS issues the user a reminder notification about a pending role expiration every day.
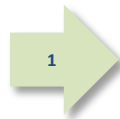
Sample User Notification: Expiration of a Role

Subject: Action Required: SAAR #106107 - Expire or Extend Access for Charles Soff (DCS9809) (DFAS Columbus) (DFAS SABRS) 09/21/2017 07:53:26 EDT

Body: SAAR #106107 - Expire or Extend Access for Soff, Charles (DCS9809) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - ROSCOE MENU SABRS-003 was submitted in AMPS on 09/21/2017 07:53:26 EDT.

 Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/11/2017 07:53:35 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

   *AMPS displays the **My Tasks** view on a separate tab (see Figure 311).*
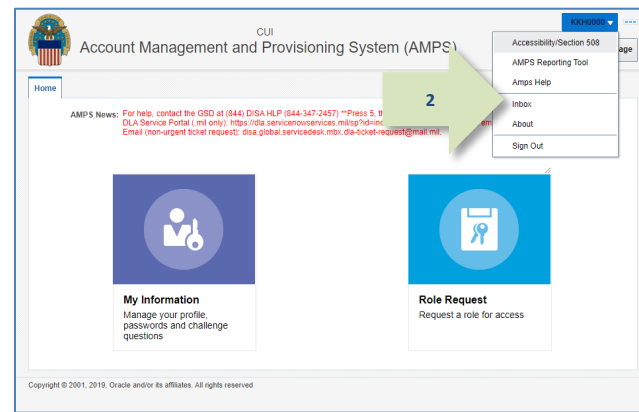
Figure 310: User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR number for the role expiration in the **Title** field.

    You can verify the correct SAAR by its number, information, and role name.

4. Click the SAAR's **Title** to start the **Expiration** request process.

    AMPS opens an Extend or Expire Role Access screen in a separate tab in AMPS (see Figure 312).
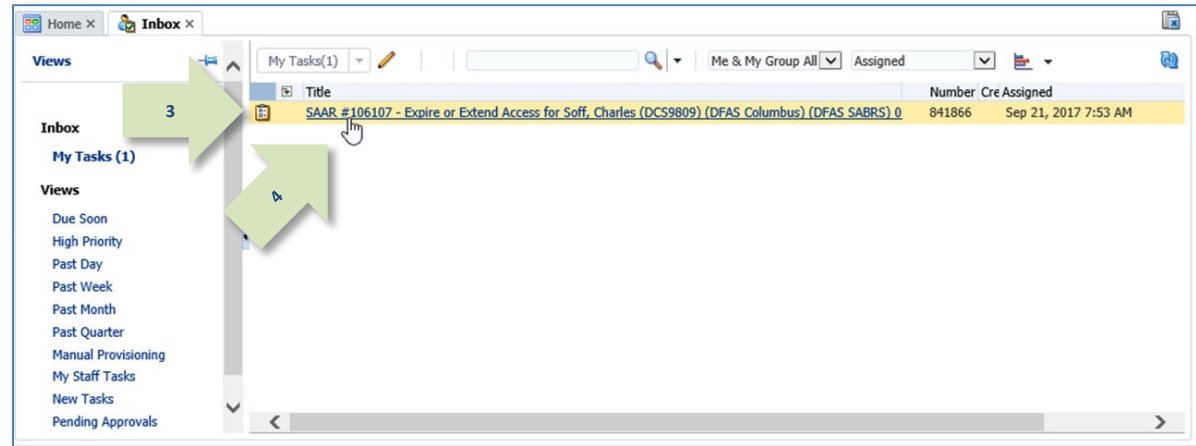
Figure 311: Inbox – My Tasks View

5. Review the **Role Information** section to verify the name of the role you want to submit for expiration.

6. Review and correct any **User Account Information** fields or **User Contact Information** fields.

Note:

AMPS uses this screen to submit an Expiration or an Extension request.
Your Date of Birth is no longer required for any request. The Date of Birth field is not editable.

AMPS saves any changes you make to your account along with the expiration request.

7. Review your AMPS **Supervisor** name, email address, and telephone number, as well as your **Organization,** to ensure AMPS sends your expiration request to the correct Supervisor.

*If the **Supervisor** name is incorrect, click the **Update** option to identify and select the correct Supervisor name. See the procedures in **How to Update the Supervisor** and **How to Update Organization Information** in this guide for instructions.*

*AMPS does not require an entry in the **Justification** text box for an expiration request.*

8. Click **Expire.**

AMPS displays a confirmation request message before it completes the expiration request (see Figure 313).

Figure 312: Role Expiration Request

9. Review the message and click the **OK** button to confirm the expiration request.

   *AMPS closes the **Expire or Extend** request screen and forwards email notifications to you as the user and to your Supervisor.*

   *The display is returned to the **Inbox** view (see Figure 314).*
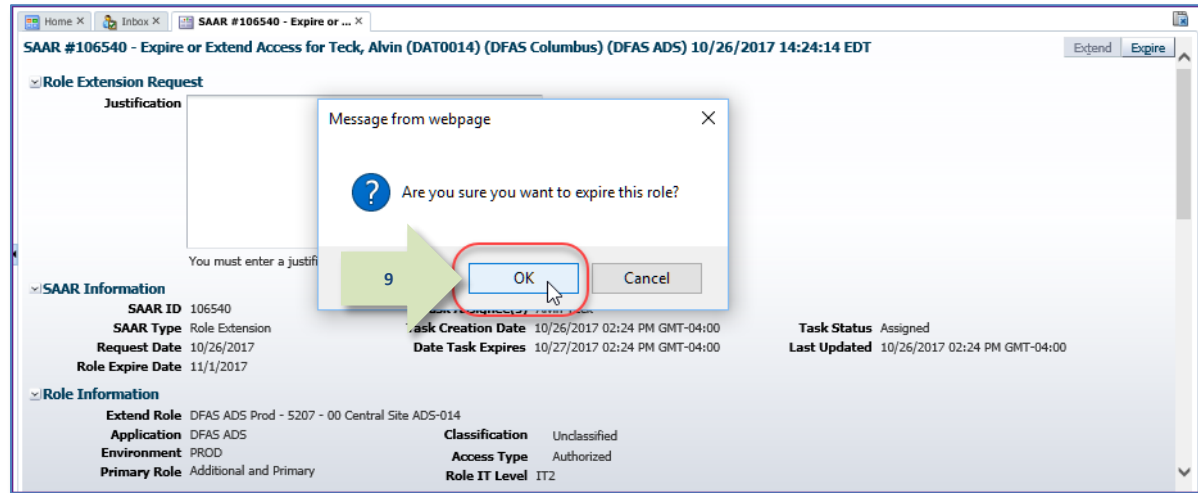
Figure 313: Expiration Message - Confirm the Expiration Request

10. In the screen, click the Refresh button to update the list and remove the completed task.

    *AMPS removes an **Assigned** task that has been processed and completed by the assignee.*
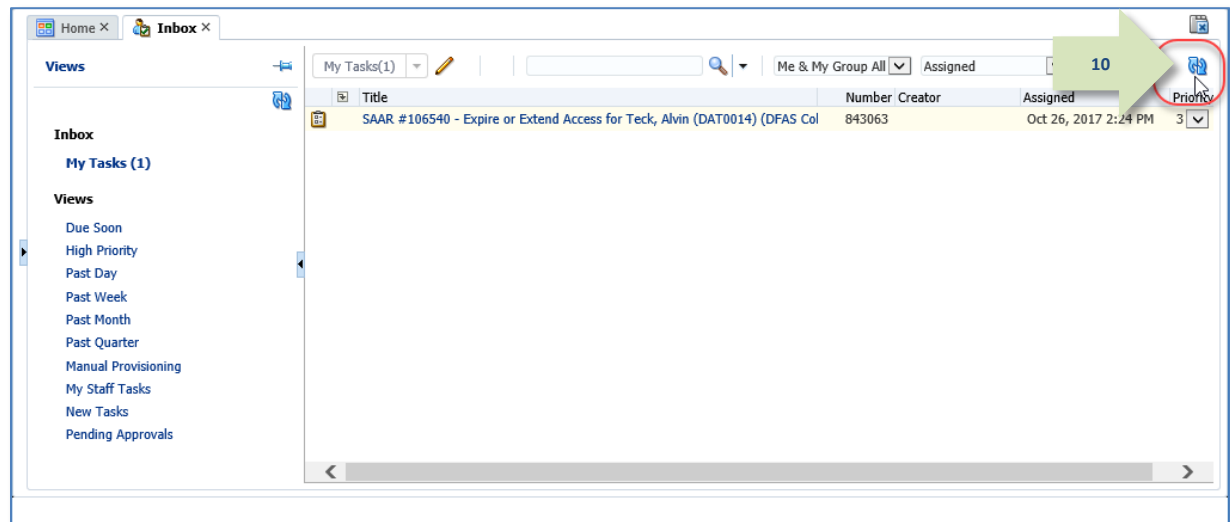
Figure 314: Inbox – My Tasks

11. **OPTIONAL:** Follow these steps to view the completed request screen, as needed:

   a. In the **Search** field, enter the SAAR number for the decision screen you want to review.

   b. In the **Status** dropdown list, select either **Any** or **Completed**.

   *AMPS automatically initiates a search based on the criteria entered. In this example, the system displays the SAAR because it also has a status of **Completed**.*

   *In the sample, AMPS displays the **Completed** task for **SAAR 106540**.*

   c. Click the SAAR title to review the SAAR on screen (not shown).
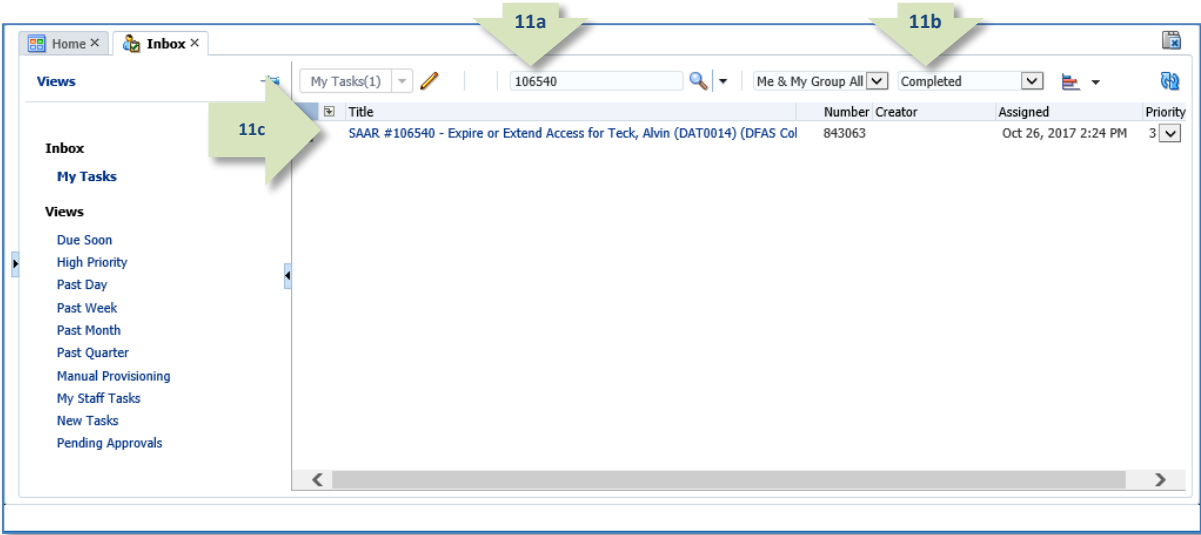
Figure 315: Pending Approvals - Completed Task List

12. AMPS notifies you that the expiration request has been submitted for Supervisor approval.

   *The SAAR number and related data in the email notification are also available in the user's **Pending Requests** table.*

Sample User Notification: Expiration Request Submitted

Subject: Notification: SAAR #106540 - Expire or Extend Access for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS ADS) 10/26/2017 14:24:14 EDT

Body:

SAAR #106540 is awaiting Supervisor approval.

This request was submitted in AMPS on 10/26/2017 14:24:14 EDT.

No action is required from you at this time.

This task expires on 11/15/2017 14:37:55 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

13. To monitor the status of your expiration request, check your **Pending Requests** table. (See **How to Check Your Role Status** on page 97.)

*Immediately after you submit a role expiration request, the SAAR for the request is listed in **Pending Requests** with its current status.*

This status changes as the role proceeds through the approval and deprovisioning process.

How to Submit a Role Expiration Request: External Users

1. Read the expiration notification and make note of the SAAR number.

   This number refers to the SAAR that requires a response from the user within 20 days.

   AMPS issues a reminder notification to the user about a pending role expiration every day.
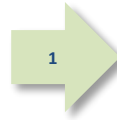
1

Sample User Notification: Expiration of a Role

Subject: Action Required: SAAR #106546 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 10/26/2017 15:52:19 EDT

Body: SAAR #106546 - Expire or Extend Access for Fitzgerald, Zorba (EZF0023) (DLA External) has been submitted for approval.

This request to extend DFAS DCMS Prod - DSK Air Force Entry Columbus (503000) Profiles DSK-006 was submitted in AMPS on 10/26/2017 15:52:19 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 11/15/2017 15:52:25 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

   AMPS displays the **Inbox** *screen in a separate tab (see Figure 317).*
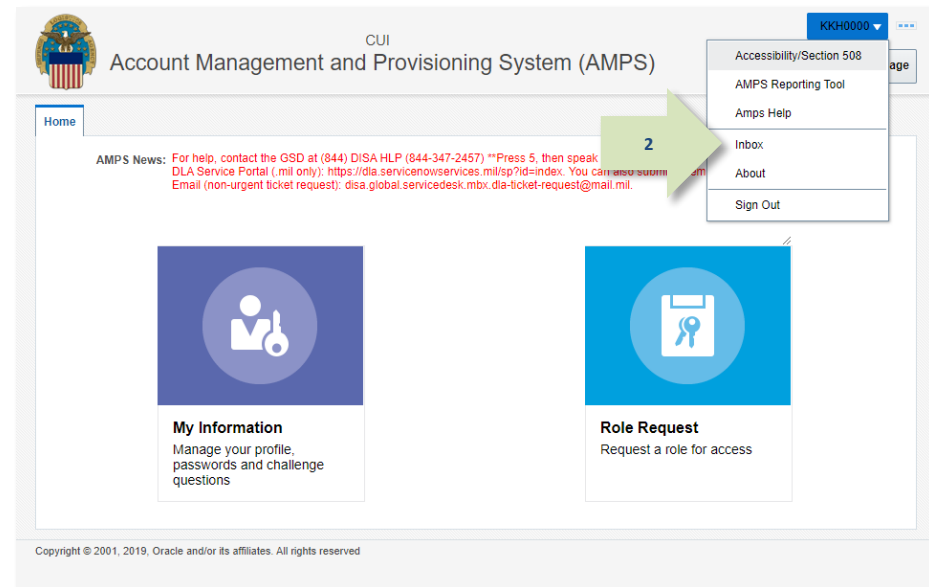
Figure 316: User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR number for the role expiration in the **Title** field.

   You can verify the correct SAAR by its number, information, and role name.

4. Click the SAAR's **Title** to start the **Expiration** request process.

   *AMPS opens an **Extend or Expire Role Access** screen in a separate tab.*
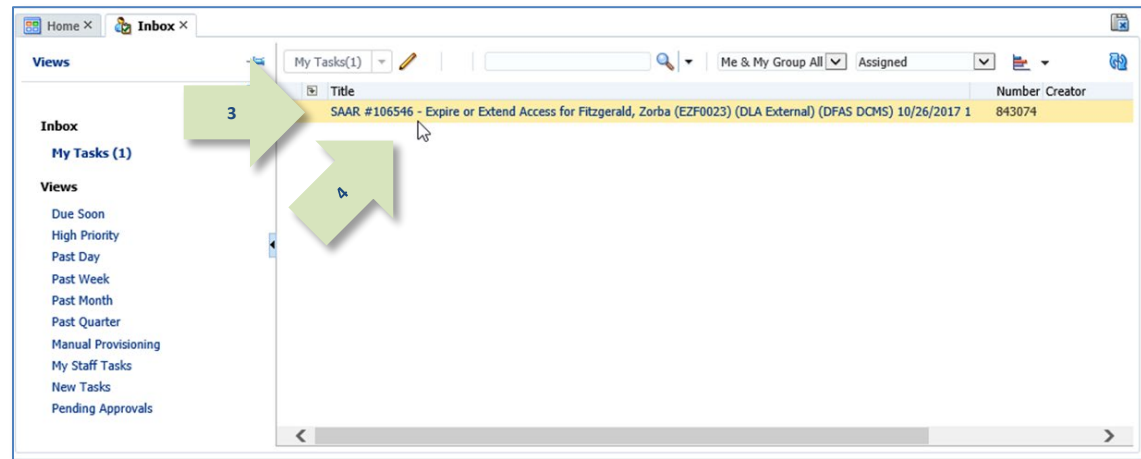
Figure 317: Inbox Screen – My Tasks

5. Review the **Role Information** section to verify the name of the role you want to submit for expiration.

6. Review and correct any **User Account Information** fields or **User Contact Information** fields.

   AMPS saves the changes to your account along with the expiration request. (AMPS no longer collects Date of Birth data. This field is not editable.)

7. Review your **External Supervisor** email address to confirm that AMPS will send your expiration request to the correct Supervisor.
   (It is also advisable to update the email addresses of your External Security Officer and External Authorizing Official as applicable.)

   *If the email address is incorrect, AMPS cannot send the expiration request to the correct recipient. Enter the correct data in the **Email** fields.*

   *AMPS does not require an entry in the **Justification** text area for an expiration request.*

8. Click **Expire.**

   AMPS displays a confirmation message (see Figure 319).

Figure 318: Role Expiration Request

9. Review the message and click the **OK** button to proceed.

*AMPS closes the **Expire or Extend Access** request screen and forwards email notifications to you as the user and to your Supervisor.*
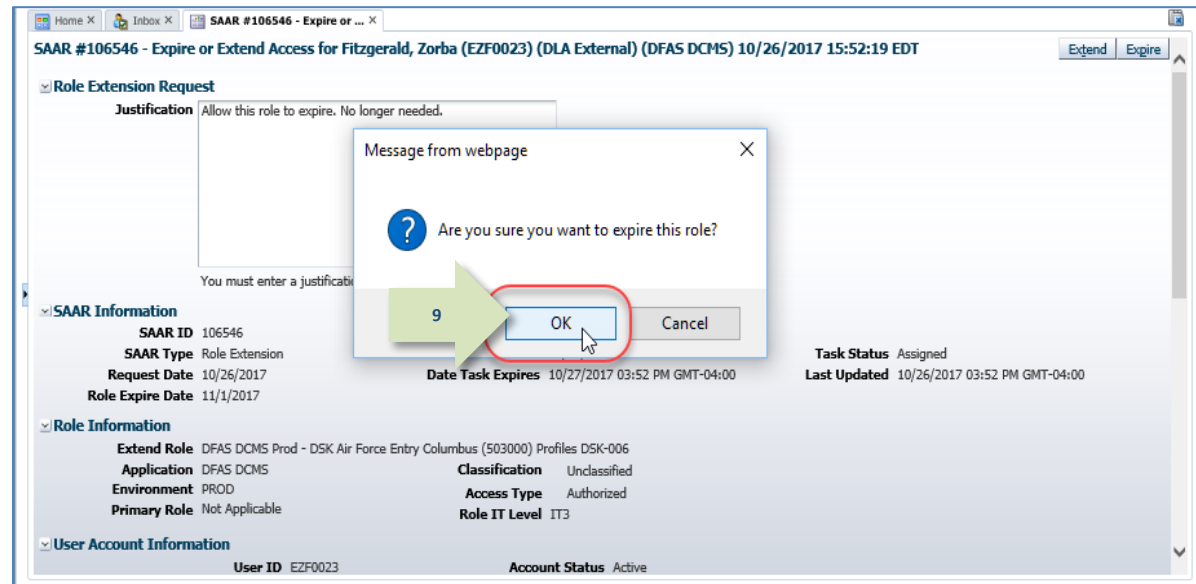
Figure 319: Expiration Request - Confirmation Message

10. In the **My Tasks** screen, click the Refresh button to update the list and remove the completed task.

*AMPS removes an **Assigned** task that has been processed and completed by the assignee.*
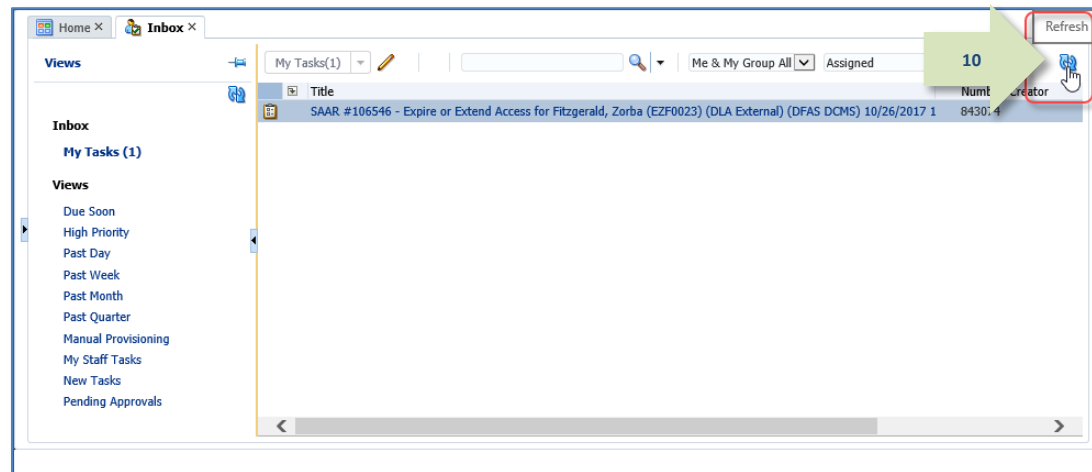
Figure 320: Inbox – My Tasks

11. **OPTIONAL:** Follow these steps to view the completed request screen, as needed:

   a. In the **Search** field, enter the SAAR number for the decision screen you want to review.

   b. In the **Status** dropdown list, select either **Any** or **Completed**.

   AMPS automatically initiates a search based on the criteria entered. In this example, the system displays the SAAR because it also has a status of **Completed***.*

   In the sample, AMPS displays the **Completed** *task for* **SAAR 106546***.*

   c. Click the SAAR title to review the SAAR on screen (not shown).
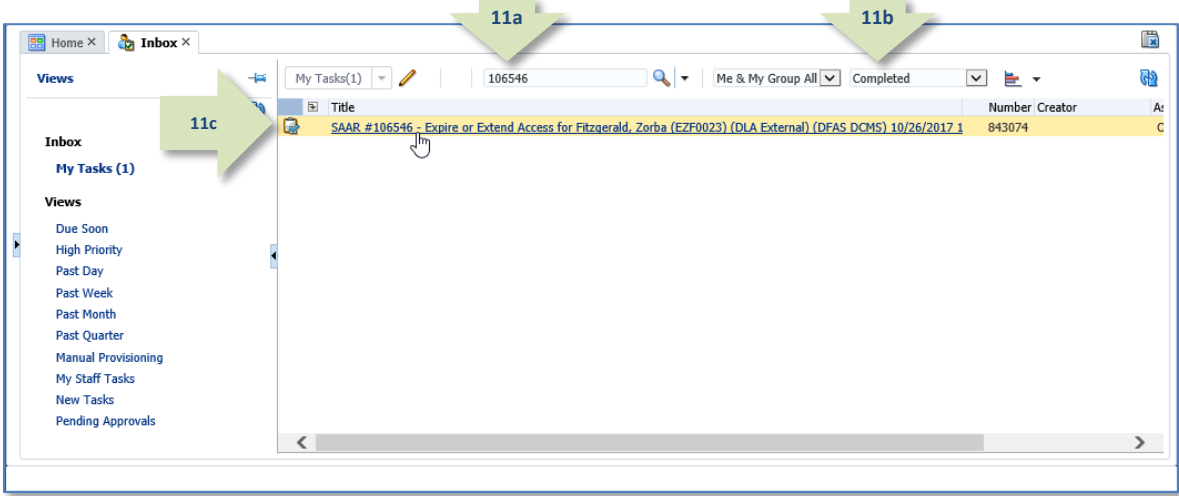
Figure 321: Inbox - Completed Task List

---

12. AMPS notifies you that the expiration request has been submitted for External Supervisor approval.

   The SAAR number and related data in the email notification are also available in the user's **Pending Requests** *table.*

Sample User Notification: Expiration Request Submitted

Subject: Notification: SAAR #106546 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 10/26/2017 15:52:19 EDT

Body:

SAAR #106546 is awaiting External Supervisor approval.

This request was submitted in AMPS on 10/26/2017 15:52:19 EDT.

No action is required from you at this time.

This task expires on 11/15/2017 15:06:31 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

13. To monitor the status of your expiration request, check your **Pending Requests** table. (See **How to Check Your Role Status** on page 97.)

   Immediately after you submit a role expiration request, the SAAR for the request is listed in **Pending Requests** *with its current status.*

   This **Current Approver** *changes as the role proceeds through the deprovisioning process.*

How to Approve a Role Expiration Request

An expiration request goes only to the user's Supervisor. After the user submits an expiration request, AMPS sends an email notification to the user's Supervisor with the SAAR number and data related to the expiration request, along with a link to the Supervisor's **My Tasks** list on the **Pending Approvals** screen. AMPS resends this notification every day for 20 days.

The approval decision screen for a role expiration request is similar to a role request approval and is submitted to an AMPS expiry/extend approval workflow, as follows:

- Submissions from all internal users go to their AMPS Supervisors for an **Expire** or **Extend** decision. If the role is confirmed by the Supervisor for expiration, the role is removed and role information is sent to the provisioning service for removal. The role is either automatically deprovisioned, or provisioners handle the deprovisioning tasks manually.

- Submissions from all external users with a User Type designation of Military, Civilian, or Contractor go to their AMPS Supervisors for an **Expire** or **Extend** decision. If the role is confirmed by the Supervisor for expiration, the role is removed and role information is sent to the provisioning service for removal. The role is either automatically deprovisioned, or a provisioner handles the deprovisioning tasks manually.

- Role expiration submissions from Vendors are automatically approved, and the information is sent to the provisioning service for removal. The role is either automatically deprovisioned, or a provisioner handles the deprovisioning tasks manually.

- Role expiration submissions from members of the Public are automatically approved, and the information is sent to the provisioning service for removal. The role is either automatically deprovisioned, or a provisioner handles the deprovisioning tasks manually.

Approving the Expiration Request: A Summary Table

The following table outlines the approval process for a role expiration request:

For This Process Phase...	The User Responsible is...
Approve the expiration request.	Supervisor.
Deprovision the user's role, if expiration is approved.	Application Provisioner, unless the application is subject to automated provisioning.

Supervisor Approval Procedure for Role Expiration: Internal Users

What You Can Do	This procedure enables you, as an AMPS Supervisor, to respond to the request of a direct report to approve the removal of a role in a role expiry procedure.
Where to Start	After reading the email notification, start by logging in to AMPS.

1. Read the expiration notification and make note of the SAAR number.

   This SAAR number refers to the SAAR that requires a response from the Supervisor within 20 days.

   AMPS issues an expiration or extension notification to the Supervisor immediately after the request is submitted by the user.

   AMPS also issues to the Supervisor a reminder notification about a pending role expiration every day.

Sample Approver Notification: Expiration of a Role

Subject: Action Required: SAAR #106540 - Expire or Extend Access for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS ADS) 10/26/2017 14:24:14 EDT

1

Body: SAAR #106540 - Expire or Extend Access for Teck, Alvin (DAT0014) (DFAS Columbus) has been submitted for approval. This request to extend DFAS ADS Prod - 5207 - 00 Central Site ADS-014 was submitted in AMPS on 10/26/2017 14:24:14 EDT.

 Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 11/15/2017 14:37:55 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

   *AMPS displays the **My Tasks** view on the **Inbox** page (see Figure 323).*
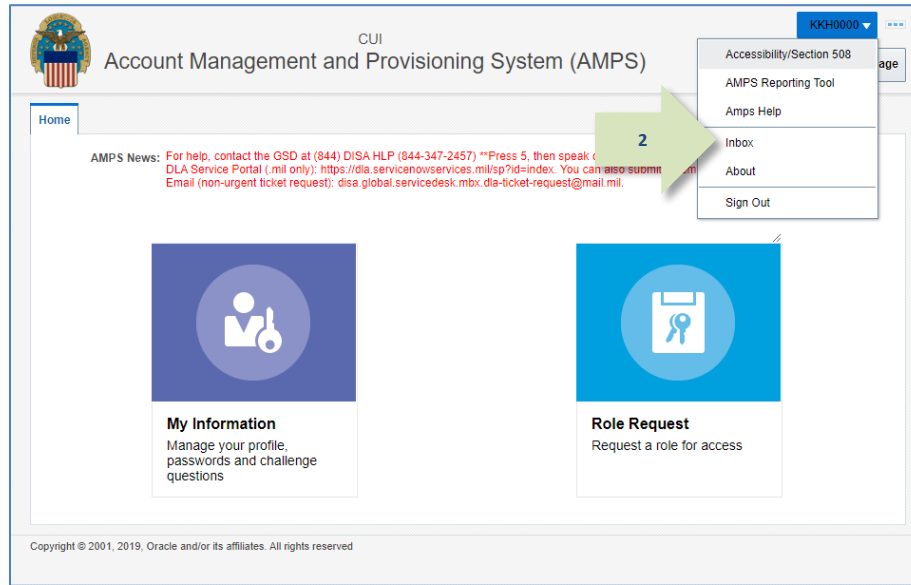
Figure 322: User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role expiration in the **Title** field.

   You can verify the correct SAAR by its number and user information.

4. Click the SAAR's **Title** to start the approval process.

   AMPS opens an approval screen in a separate tab (see Figure 324).
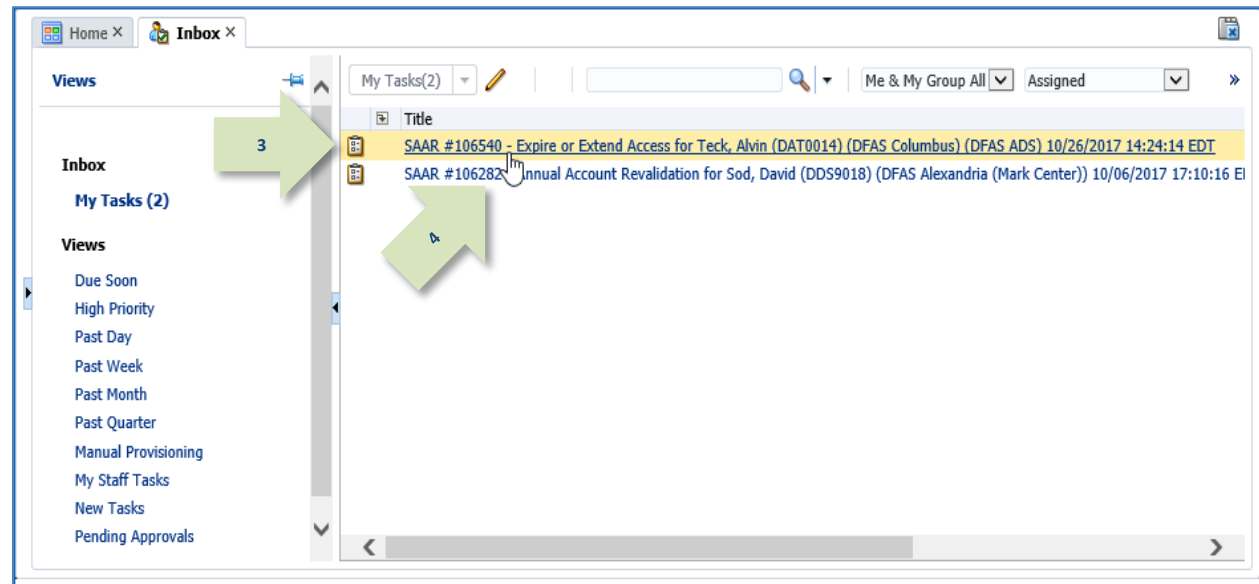
Figure 323: Inbox – My Tasks View

5. Review the **Supervisor Decision** data and **Role Extension Details**.

   a. Disregard the **End Date** in this screen.

   Both Expiration and Extension requests are handled on the same online form. **End Dates** *are not used in Expiration requests.*

   b. Review the **Role Information** section to verify the name of the role submitted for expiration.

   c. Review the **User Summary** for details about the user requesting the expiration of the role.

6. Click the **Additional Information** tab.

   AMPS displays the **Additional Information** *screen (see Figure 325).*

Figure 324: Role Expiration - Supervisor Decision – Role Extension Details Tab

7.　Review the **SAAR Approval History**.

*In **SAAR Approval History**, the Supervisor's contact information and decision information will be included in the SU (Supervisor) row of the table after the Supervisor decision has been completed.*

SAAR approval history is available in a SAAR report through BI Publisher.

8.　Click the **User Information** tab.

*AMPS displays detailed information about the requesting user in the **User Information** tab (see Figure 326).*

Figure 325: Role Expiration - Supervisor Decision - Additional Information Tab

9. In the **User Information** tab, AMPS displays key data about the requesting user:

    - *Account information*
    - *User Contact information*
    - *Supervisor contact information*
    - *Requesting User's organization*
    - *Requesting user's current roles*
    - *Requesting user's pending requests.*

10. After making a decision on your action, you have the option to fill in the **Comments** field explaining the review decision.

    You can enter comments to support the completion of the review. AMPS records these comments in the SAAR Approval History when the supervisor submits the completed review.

    ## Note:

    The Comments text shown in the sample screen is for demonstration purposes only. Please enter comments applicable to the current request.

11. To confirm the user's role expiration request, click the **Expire** button.

    AMPS displays a message requesting confirmation of the expiration request (see Figure 327).

Figure 326: Role Expiration - Supervisor Decision - User Information Tab

12. Click **OK**.

Clicking **OK** *allows the role expiration to proceed. The role assignment will expire in AMPS, and a provisioner will remove related system and associated access rights to the application.*

After you click **OK***, AMPS closes the decision screen and the message box.*
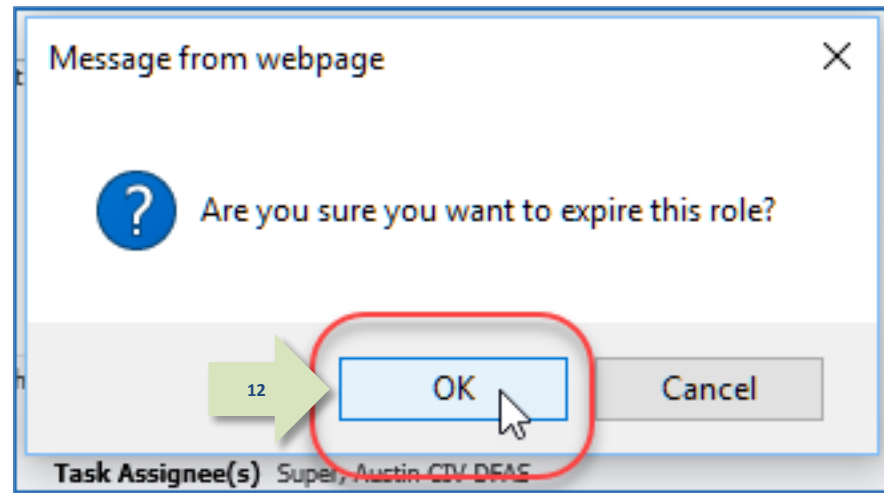
Figure 327: Role Expiration – Confirmation

13. In the **My Tasks** view, click the Refresh button to remove the completed SAAR from the **My Tasks** list.
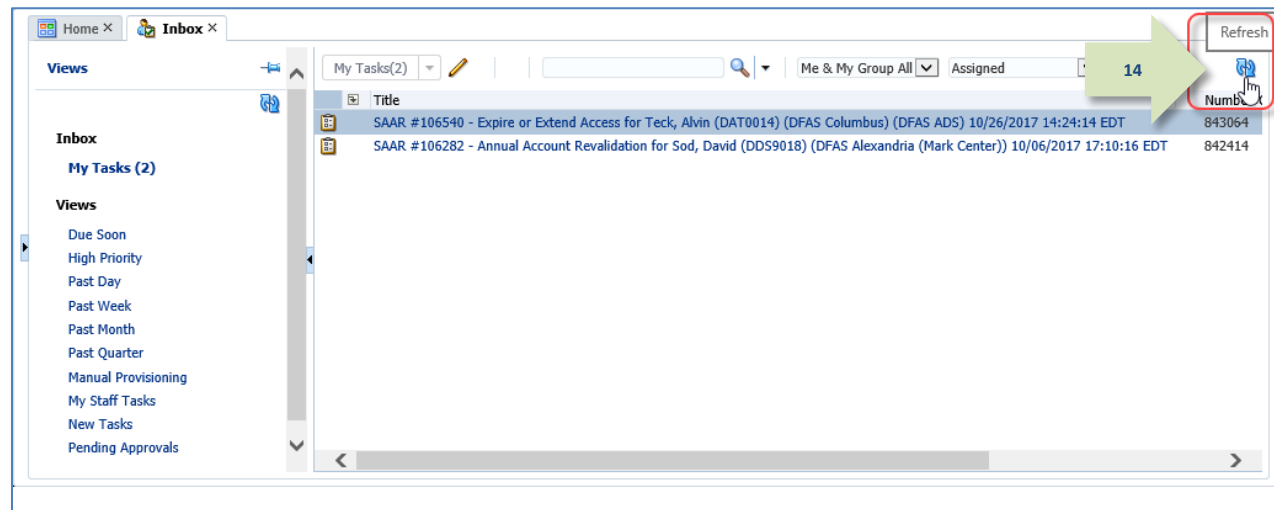
Figure 328: Inbox – My Tasks

14. **OPTIONAL:** Follow these steps to view completed request in the current task list view, as needed:

   a. In the **Search** field, enter the SAAR number.

   b. In the Status field, enter either **Completed** or **Any**.

      AMPS automatically searches for the specified SAAR. The result is displayed in the list area. In the sample, AMPS displays the **Completed** *task for* **SAAR 106546**.

   c. Click the SAAR title to view the SAAR decision screen again.

      You cannot change the decision, but you can review the decision information.
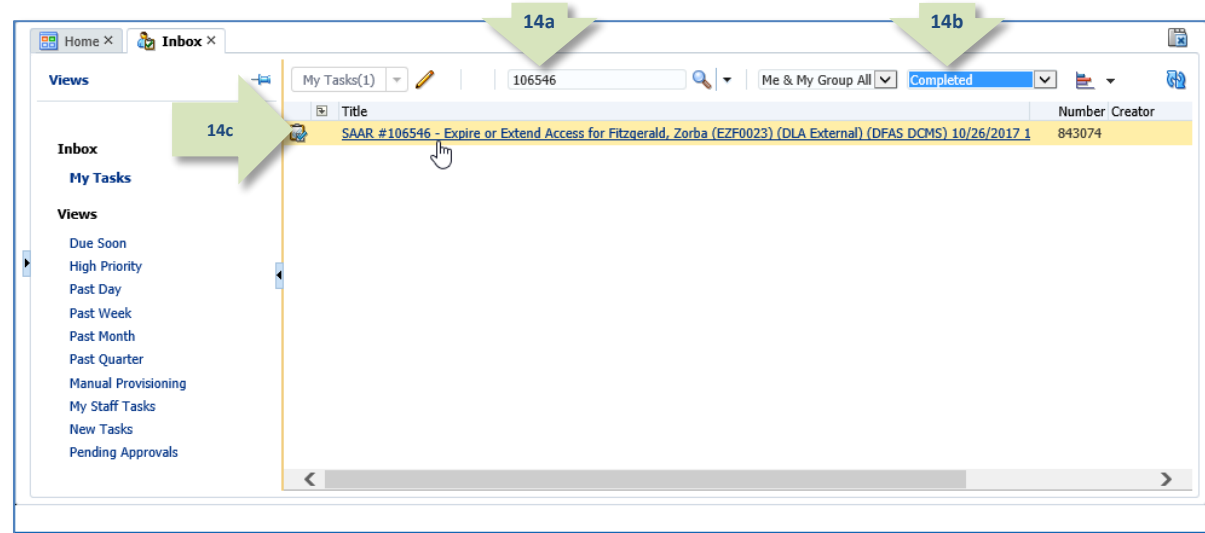
Figure 329: Inbox - Completed Task List

15. AMPS notifies the user that the expiration request has been completed.

   The SAAR number and related data in the email notification are also available on the user's **Pending Requests** *table.*

Note:

> The role expiration confirmation message does NOT mean that the approver rejected the expiration request.
> The message actually means the Supervisor approved the user's request to allow the role to expire immediately: that is, the Supervisor is "rejecting" the role for the user.

Sample User Notification: Expiration Request Completed

Subject: Notification: SAAR #106540 - Expire or Extend Access for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS ADS) 10/26/2017 14:24:14 EDT

Body:

The Supervisor has completed an approval for SAAR #106540.

The outcome for this task is REJECT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

16. The user can monitor the status of the expiration request during the approval process, by checking their **Pending Requests** table.
(See **How to Check Your Role Status** on page 97.)

If AMPS lists the expiration SAAR with a status of **TICKETED**, *this indicates the SAAR awaits the action of a provisioner to complete the removal of the role access privileges from the user's application account.*

17. After the Supervisor approves a request for a role expiration, AMPS also notifies the requestor that the role expiration request has been forwarded to an application provisioner for removal of access privileges.

After a role expiration request has been approved and the role removed from AMPS, the role's access privileges must be removed from the user's account through a deprovisioning process:

If an application role is provisioned through Total AMPS or Remedy, the **Status** *changes to* **TICKETED**. *This status remains in place until the provisioner closes the provisioning ticket to indicate the role has been removed.*

Note:

If your application is auto-provisioned, AMPS automatically handles the deprovisioning process and removes the role from your account.

17 →

Sample User Notification: Deprovisioning Notification of a Role

Subject: AMPS Application Processing for SAAR #106540

Body:

AMPS Application Processing request for SAAR 106107 has started.

Request For:
DLA Login: DAT0014
Name: Teck, Alvin
Phone: 888-555-1212
Email: Alvin.Teck@dla.mil
EDIPI/UPN: 1286972493

Access Information:
SAAR #: 106540

Remove Job Role: DFAS ADS Prod - 5207 - 00 Central Site ADS-014

Applications and Access:
        Resource: DFAS PROD - DFAS ADS
                Remove: Central site Disbursing personnel only. Print application auto-granted to sub-super and above.
Remove: Role ID:ADS-014

Justification: (none)

Optional Information: (none)

Role Expiration SAAR requested by AMPS on 10/26/2017

18. After the deprovisioning step is complete, AMPS delivers an email notification to advise you that the expiration request is complete.

18

Sample User Notification: Expiration of a Role – Final Notice

Subject: AMPS Application Processing for SAAR #106540

Body: The following application roles have expired and the removal of your access has been fully processed.

User: Alvin Teck

Request Type: 106640 - Request Extension of User Access for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS ADS) 10/26/2017 14:24:14 EDT

Application: DFAS ADS

Role: DFAS ADS Prod - 5207 - 00 Central Site ADS-014

Recommended Resolution: If you still need this role, consult with your Supervisor for recommendations on further action. You can also log in to AMPS and submit a new request for the role.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index
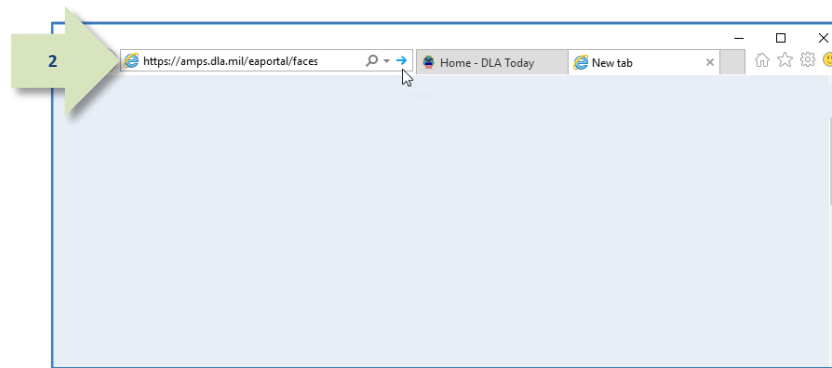
19. Check the SAAR History table on the **Applications & Roles** tab to monitor the final status of your expiration request.

When the role expiration request has been completely approved, AMPS shows the role's status as **REJECTED**.

This status indicates that the role expiration request was accepted, the role has been deprovisioned, and the user no longer has access to the application.

19

Figure 330: SAAR History - Role Expiration Request is Complete (Status: Rejected)

Supervisor Approval Procedure for Role Expiration: External Users

What You Can Do	This procedure enables you, as an External AMPS Supervisor, to respond to the request of a direct report to approve the removal of a role in a role expiry procedure.
	Note that an expiration requires an approval by the Supervisor ONLY. No other approvers are needed or notified to complete an expiration request.

Where to Start	Check email messages for a notification from AMPS regarding a pending action.

1. Read the expiration notifications and make note of the SAAR number.

   This SAAR number refers to a SAAR that requires a response from the Supervisor within 20 days.

   AMPS issues a standard expiration or extension notification to the Supervisor immediately after the request is submitted by the user.

   AMPS also issues to the Supervisor a reminder notification about a pending role expiration every day (not shown).

2. Copy and paste the URL into a browser URL address field and navigate to the associated screen.

   AMPS displays a Consent to Monitoring screen (not shown). Upon confirmation of assent, the system displays the **Approval Work Queue** *screen in the browser (see Figure 332).*

Sample Notifications: Action Required – Role Expiration Request

Subject: Action Required: SAAR #106546 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 10/26/2017 15:52:19 EDT

Body: SAAR #106546 - Expire or Extend Access for Fitzgerald, Zorba (EZF0023) (DLA External) has been submitted for approval.

This request to extend DFAS DCMS Prod - DSK Air Force Entry Columbus (503000) Profiles DSK-006 was submitted in AMPS on 10/26/2017 15:52:19 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=3819%3AjW%2BTewsFOqzT%2FIzDy40BglgAgqqLGtUDJ1MJzTs1QCQ%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 11/15/2017 15:06:31 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 331: Web Browser Instance - Enter the Approval URL in the URL Field

3. Locate the pending SAAR in the **Approval Action** column of the **Approval Work Queue** and click the SAAR Approval Action anywhere in that table cell.

   AMPS displays the **External Supervisor Decision** *screen (see Figure 333).*

Figure 332: External Supervisor Approval Work Queue

4. Review the **Role Expiration Details** on the **External Supervisor Decision** screen

    a. Disregard the **End Date**. This date is not used in Expiration requests.
    b. Review the **Expire Role** field to verify the name of the role submitted for expiration.

5. Click the **Additional Information** tab.

    AMPS displays the **Additional Information** *screen.*

Figure 333: Supervisor Decision – Role Expiration Details

6. In the **Additional Information** screen, note the **SAAR Approval History**.

   All approval details are saved in this screen to preserve the approval record. Any comments entered by the user will be displayed in this table.

7. Click the **User Information** tab.

   *AMPS displays the **User Information** screen.*

Figure 334: Supervisor Decision - Additional Information

8. In the **User Information** screen, review the user's account, contact, External Security Officer, and External Supervisor information.

9. Note the **Pending Requests** table, which lists all outstanding role requests.

    The current request is included in the **Pending Requests** *list.*

10. Enter text in the **Comments** area to clarify the decision and activate the **Expire** button.

    As the screen advises, you must enter comments to activate the **Expire** *button and complete the decision to allow the expiration to proceed.*

11. Click the **Expire** button.

    AMPS displays a message requesting confirmation of the decision (see Figure 336).

Note:

If you click the Expire button, you are affirming the user's request to allow the role to expire.

Selecting Expire sends the role expiration request to the provisioning process so that the role can be removed from the user's account.

Figure 335: Supervisor Decision - User Information

12. In the Message dialog, click **OK**.

    The role expiration confirmation message asks the Supervisor to confirm that the user should be granted the request to allow the role to expire immediately.

    *Clicking **OK** allows the role expiration to proceed, and the role to expire and be deprovisioned from the user's account.*
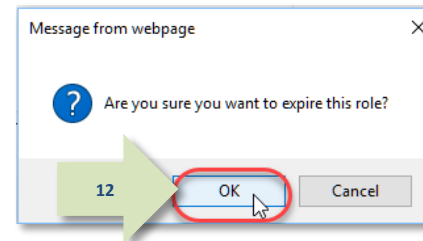

Figure 336: Expiration Message - Confirm the Expiration of the Role

13. Click the link **Return to the External Approval Worklist.**

    *AMPS displays the **Approval Work Queue** dialog (see Figure 338).*
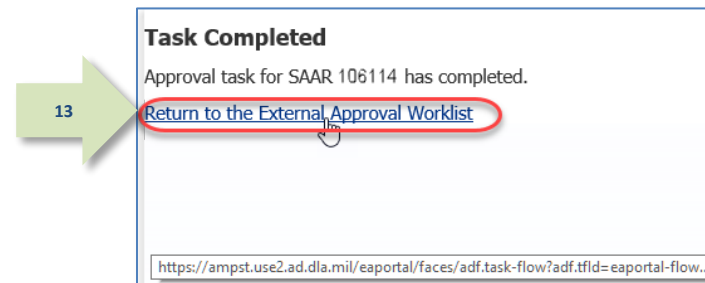
Figure 337: Approval Completed – Supervisor's Approval for External User Expiration Request is Complete

14. To exit the **Approval Work Queue**, click the **Logout** button.

    *AMPS closes the **Approval Work Queue** dialog.*

    To reopen this dialog, return to the next notification of a pending action and follow the instructions in Step 3.
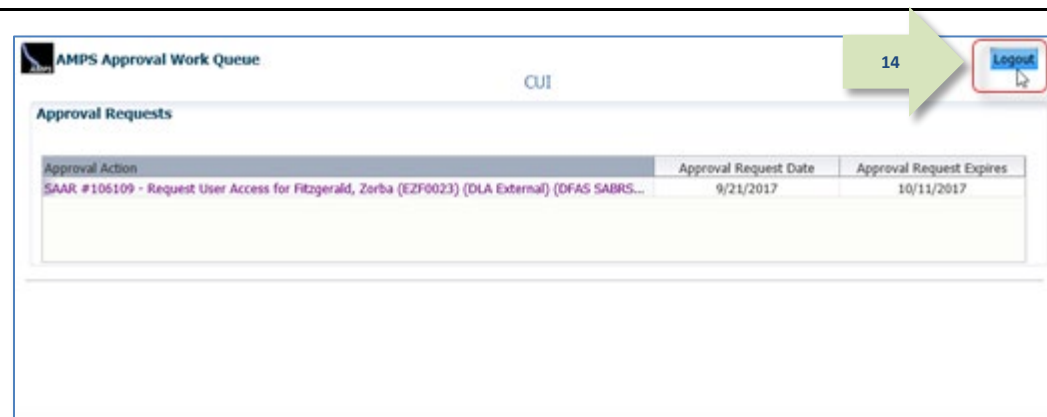
Figure 338: AMPS Approval Work Queue

15. After you log out of the AMPS Approval System for external approvers, the system displays a logout confirmation message.

    Use the Close Browser button shown in Figure 339 to close the browser.
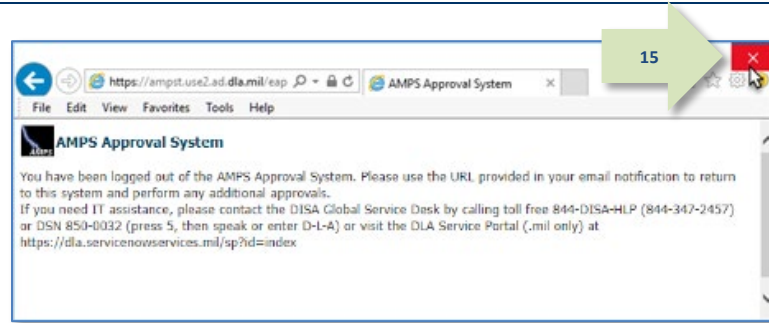
Figure 339: AMPS Approval System for External Approvers - Logout Confirmed

16. After the Supervisor approval is finished, AMPS sends a notification to the user explaining the outcome of this step in the role expiration process.

Sample User Notification

Subject: Notification: SAAR #106546 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 10/26/2017 15:52:19 EDT

Body: The External Supervisor has completed an approval for SAAR #106546.
The outcome for this task is REJECT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

17. AMPS then notifies the user that the expiring role is to be deprovisioned by an application provisioner.

Sample Provisioning Notification: To the User

Subject: AMPS Application Processing for SAAR #106546

Body: AMPS Application Processing request for SAAR 106546 has started.

Request For:
DLA Login: EZF0023
Name: Fitzgerald, Zorba
Phone: 888-555-1212
Email: zfitz@mail.com
EDIPI/UPN: 1286972493

Access Information:
SAAR #: 106546

Remove Job Role: DFAS DCMS Prod - DSK Air Force Entry Columbus (503000) Profiles DSK-006
Applications and Access:
         Resource: DFAS PROD - DFAS DCMS
                 Remove: DSK-006 DSK Air Force Entry Columbus (503000) Profiles

Justification: Allow this role to expire. No longer needed.
Optional Information: (none)
Role Expiration SAAR requested by AMPS on 19/26/2017

18. The user can monitor the progress of the expiration request during the approval process, by checking their **Pending Requests** table.
    (See **How to Check Your Role Status** on page 97.)

How to Process a Provisioning Ticket for an Expiring Role

What You Can Do

This procedure is provided for a Total AMPS ticket provisioner. Similar information for Remedy-enabled applications is also delivered to a provisioner through email.

As the provisioner, you can identify a Total AMPS provisioning ticket for a role that has expired and is to be deprovisioned.
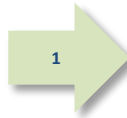
This procedure applies to requests from internal users and external users.

Where to Start

After reading the email notification, start by logging in to AMPS.

1. Read the provisioning notification and make note of the SAAR number.

   This SAAR number refers to the SAAR that requires a response from the Provisioner.

Sample Provisioning Notification

Subject: AMPS Application Processing for SAAR #106107 requires your attention.

Body:
AMPS Application Processing request for SAAR 106540 requires your attention.

Request For:
DLA Login: DAT014
Name: Teck, Alvin
Phone: 888-555-1212
Email: Alvin.Teck@dla.mil
EDIPI/UPN: 1286972493

Access Information:
SAAR #: 106540

Remove Job Role: DFAS ADS Prod - 5207 - 00 Central Site ADS-014

Applications and Access:
       Resource: DFAS PROD – DFAS ADS
           Remove: Central site Disbursing personnel only. Print application auto-granted to sub-super and above.
           Remove: Role ID:ADS-014

Justification: (none)

Optional Information: (none)

Role Expiration SAAR requested by AMPS on 10/26/2017

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

   *AMPS displays the **My Tasks** view (see Figure 341).*
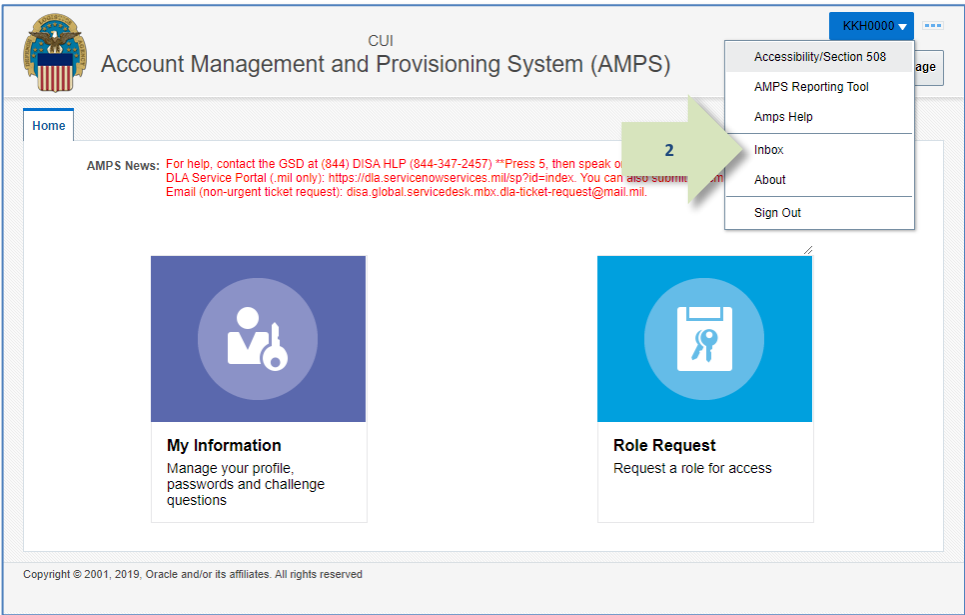
Figure 340: User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role expiration in the **Title** field.

   You can verify the correct SAAR by its number, information, and role name.

4. Click the SAAR's **Title** to start the provisioning process.

   AMPS opens an approval screen in a separate window.
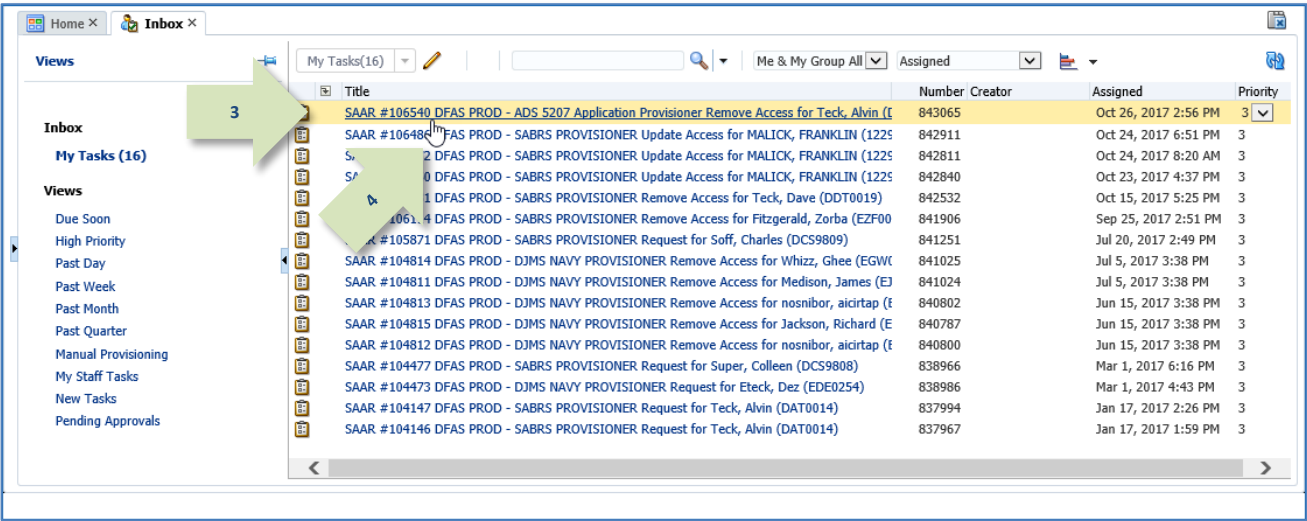
Figure 341: Inbox – My Tasks

5. Check the **Work Details** section for instructions about the provisioning request.

    In the sample screen, the **Work Details** *indicate the provisioner is to remove the specified role currently assigned to the* **Requestor**.

6. Enter text in the **Comments** area to clarify the current action taken.

    Comments *text is required, but since a provisioning ticket can be opened, closed, and reopened before it is complete, you can enter progress notes or other appropriate text to clarify the status of the provisioning task.*

    To save comments and reopen the ticket later, click **Save Comments**. *Reopen the ticket from the* **My Tasks** *view in your* **Inbox**.

7. When the deprovisioning tasks are complete, click **Work is Completed.**

    AMPS closes the provisioning ticket screen.

    AMPS then notifies the user that the deprovisioning actions are complete and the user's application access privileges have been removed.

Figure 342: Role Expiration – Provisioning Request

8. In the **My Tasks** screen, click the Refresh button to remove the completed provisioning task from the **My Tasks** list.
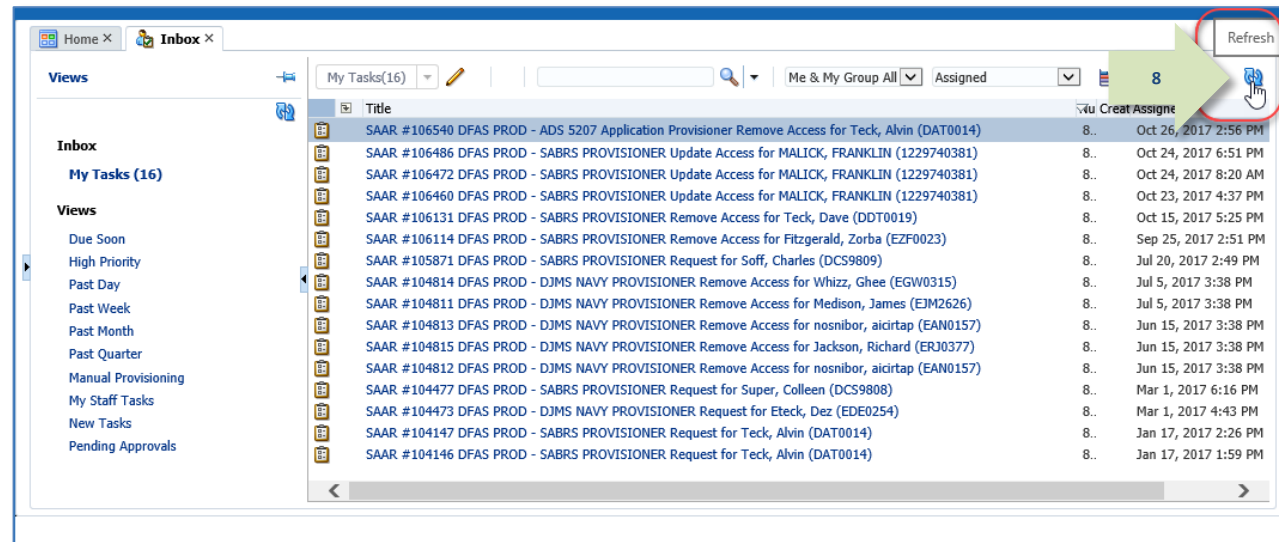
Figure 343: Inbox – My Tasks

9. **OPTIONAL:** Follow these steps to view the completed provisioning task, as needed:

   a. In the **Search** field, enter the SAAR number for the provisioning ticket you want to review.

   b. In the **State** dropdown list, select either **Any** or **Completed**.

   *AMPS automatically displays one or more tasks having a **State** that matches the search criteria.*

   c. Click the SAAR title to view the SAAR provisioning ticket again.

   *You cannot change the ticket after you have clicked **Work is Completed**, but you can review the provisioning information.*
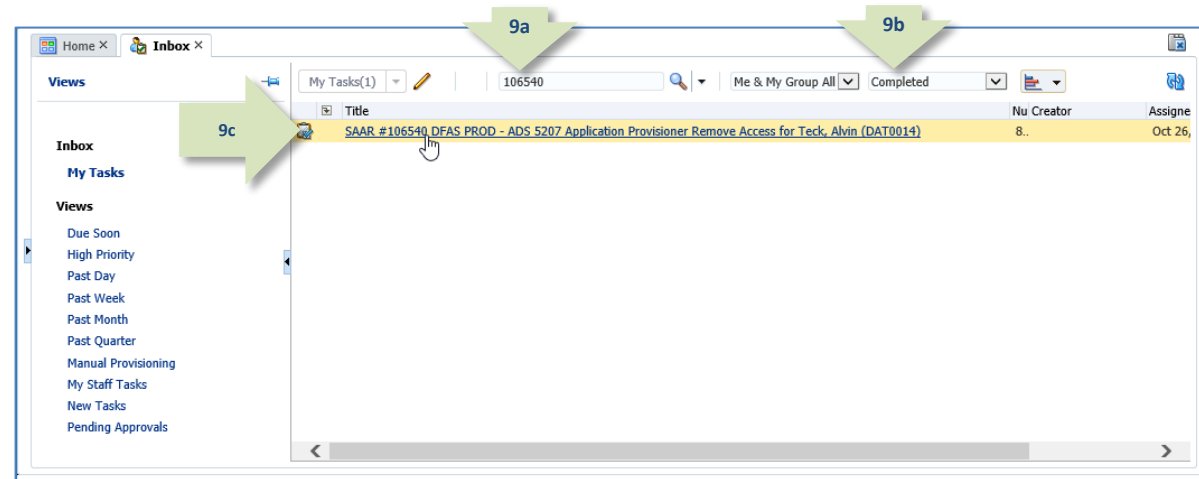
Figure 344: Inbox - Completed Task List

10. After deprovisioning is completed, AMPS notifies the user that the expiration request has been completed.

The SAAR number and related data in the email notification are also available on the **Applications & Roles** *tab of the* **My Information** *screen.*

10 →

Sample User Notification: Expiration Request Submitted

Subject: AMPS Application Processing for SAAR #106540

Body: The following application roles have expired and the removal of your access has been fully processed.

User: Alvin Teck

Request Type: 106540 - Request Extension of User Access for Alvin Teck (DAT0014) (DFAS Columbus) (DFAS ADS) 10/26/2017 14:24:14 EDT

Application: DFAS ADS

Role: DFAS ADS Prod - 5207 - 00 Central Site ADS-014

Recommended Resolution: If you still need this role, consult with your Supervisor for recommendations on further action. You can also log in to AMPS and submit a new request for the role.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

11. The user can check **SAAR History** in the **Applications & Roles** tab on the **My Information** screen to view the final status of the expiration request.

In this example, AMPS displays the expiration SAAR with a status of **REJECTED**.

This status indicates that the role has expired and that administrative personnel have completed deprovisioning work.

Figure 345: My Information - Applications & Roles Screen

How to Submit a Role Extension Request

What You Can Do | This procedure enables you to submit a request to extend a role that would otherwise expire and be removed from your account.
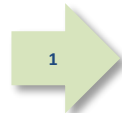
Where to Start | After reading the email notification, start by logging in to AMPS.

How to Submit a Role Extension Request: Internal User

1. Read the expiration notification and make note of the SAAR number.

    This SAAR number refers to a role expiration SAAR that requires a response from the user within 20 days.

    AMPS issues to the user a reminder notification about a pending role expiration every day.

Sample User Notification: Expiration of a Role

Subject: Action Required: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 - Expire or Extend Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - DFAS General User SABRS-014 was submitted in AMPS on 09/25/2017 18:04:31 EDT.

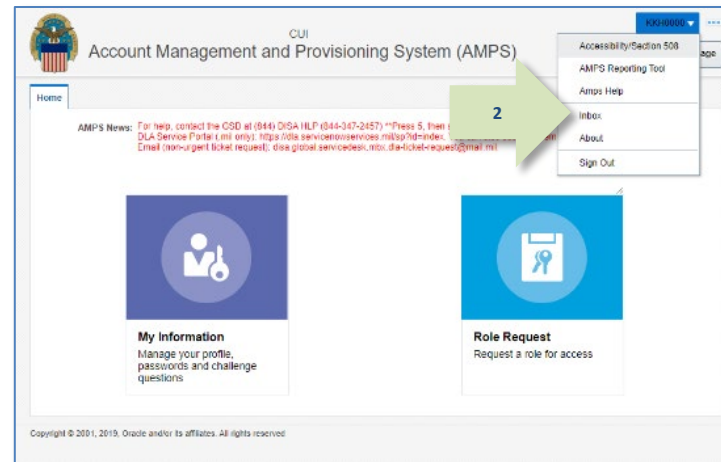Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/15/2017 18:04:37 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

    *AMPS displays the **My Tasks** view (see Figure 347).*
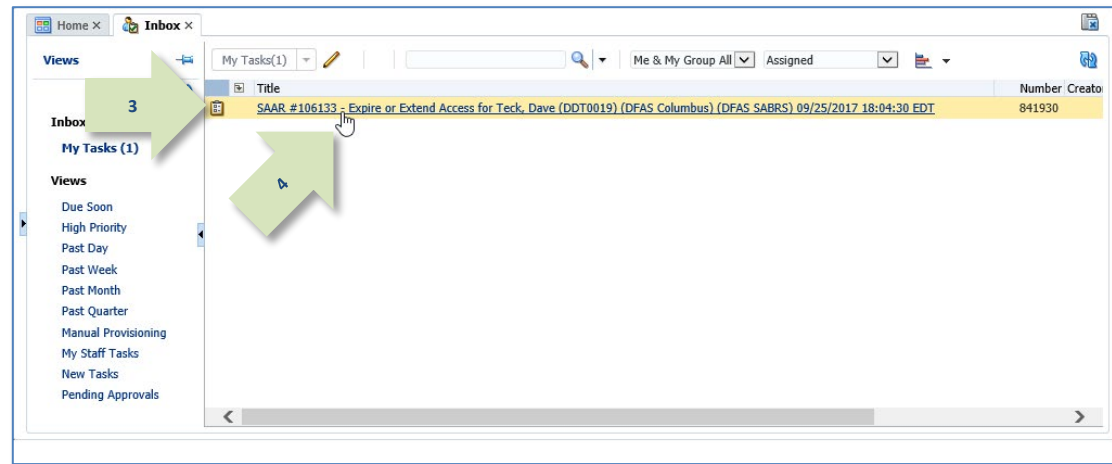

Figure 346: User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role extension in the **Title** field.

    You can verify the correct SAAR by its number.

4. Click the SAAR's **Title** to start the **Extension** request process.

    AMPS opens the Extension request screen in a new tab.

Figure 347: Inbox – My Tasks List

5. Verify the following information:

   5a. In the SAAR Information section, the SAAR number must match the SAAR indicated in the email notification.

   5b. In the Role Information section, the Role Name of role to be extended should be accurate.

6. Enter the reason for requesting the role extension in the **Justification** text area.

> *Note:*
>
> The text provided in the sample screen is for illustration purposes only. Please enter complete text appropriate for your extension request.

7. Check the **Organization** name, to verify the correct Organization is identified for your account.

   If the **Organization Name** *is incorrect, click* **Update Organization** *to search for and select a new Organization.*

8. Check the **Supervisor** name, identifying data, and contact information to verify the correct AMPS Supervisor is identified for your account.

   If the **Supervisor** *information is incorrect, click* **Update Supervisor** *to search for and select a new AMPS Supervisor.*

> *Note:*
>
> If you do not identify the correct Organization and Supervisor, AMPS cannot send the extension request approval to the correct approvers.

9. Click **Extend**.
   AMPS closes the **Expire or Extend** *screen and submits the request to the approval process.*

Figure 348: Expire or Extend – Internal User Extension Request Screen

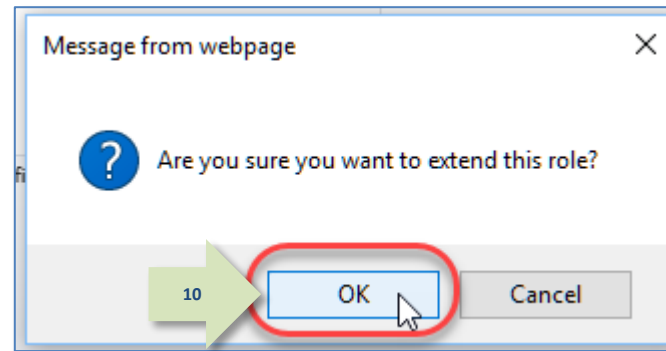10. To confirm the submission of an extension request, click the **OK** button.

Figure 349: Extension Request Confirmation

11. In the **My Tasks** list, you can search for and view the Extension request again, as needed. Follow these steps:

    a. Enter the SAAR number in the Search field.

    b. Change the **Status** selection to **Any** or **Completed**. After you select a different status, AMPS automatically initiates the search and displays the resulting SAARs.

    c. Click the SAAR **Title** to reopen the Extension request screen.

    AMPS lists the extension task in the **My Tasks** *list. Click* **Cancel** *in the Extension request to close the screen.*
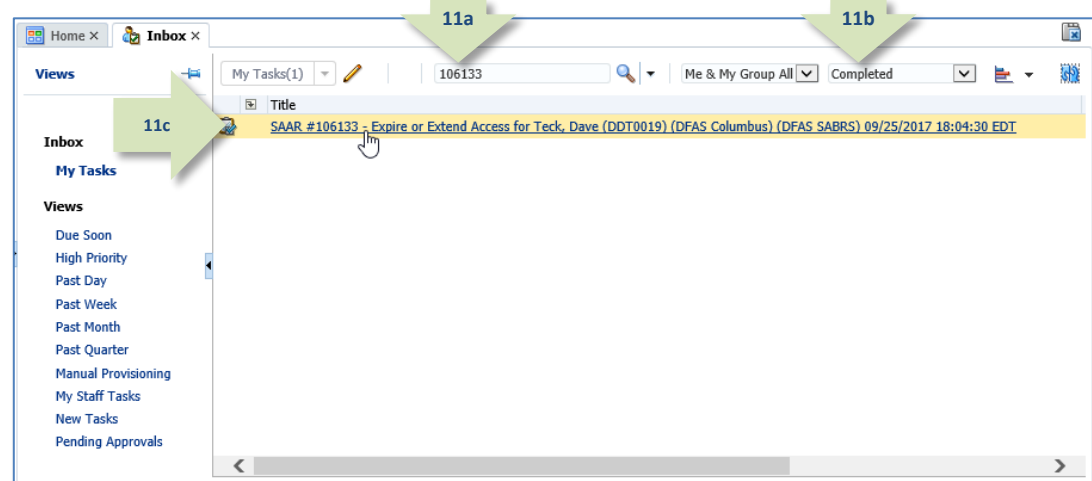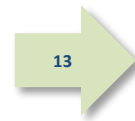

Figure 350: Inbox - My Tasks List – Updated

12. To monitor the progress of your extension request during the approval process, check your **Pending Requests** table.
    (See **How to Check Your Role Status** on page 97.)

13. After the extension request is submitted, AMPS sends an email message indicating the SAAR extension request is waiting for Supervisor approval.

    (A sample is shown at right.)

13

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 - Expire or Extend Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - DFAS General User SABRS-014 was submitted in AMPS on 09/25/2017 18:04:31 EDT.

Please visit AMPS at this URL

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/15/2017 18:04:37 EDT.
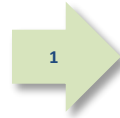
AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

How to Submit a Role Extension Request: External User

1. Read the expiration notification and make note of the SAAR number.

   This SAAR number refers to a role expiration SAAR that requires a response from the user within 20 days.

   AMPS issues to the user a reminder notification about a pending role expiration every day.

1 →

Sample User Notification: Expiration of a Role

Subject: Action Required: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: SAAR #106142 - Expire or Extend Access for Fitzgerald, Zorba (EZF0023) (DLA External) has been submitted for approval.

This request to extend DFAS DCMS Prod - DSK Air Force Approval DE-DAO (380100) Foreign National DSK-027 was submitted in AMPS on 09/26/2017 08:56:31 EDT.

 Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/16/2017 08:56:34 EDT.

---

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

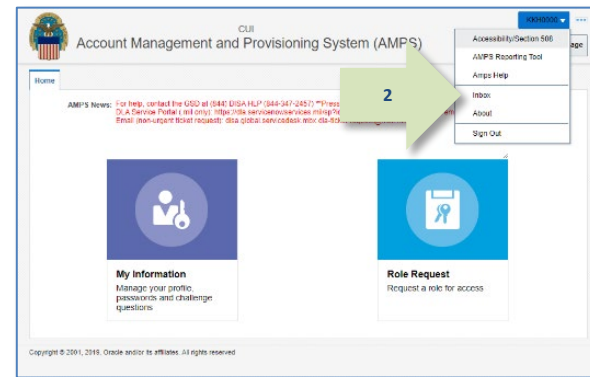   *AMPS displays the **My Tasks view** (see Figure 352).*

Figure 351: User ID Dropdown Menu - Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role extension in the **Title** field.

   You can verify the correct SAAR by its number.

4. Click the SAAR's **Title** to start the **Extension** request process.

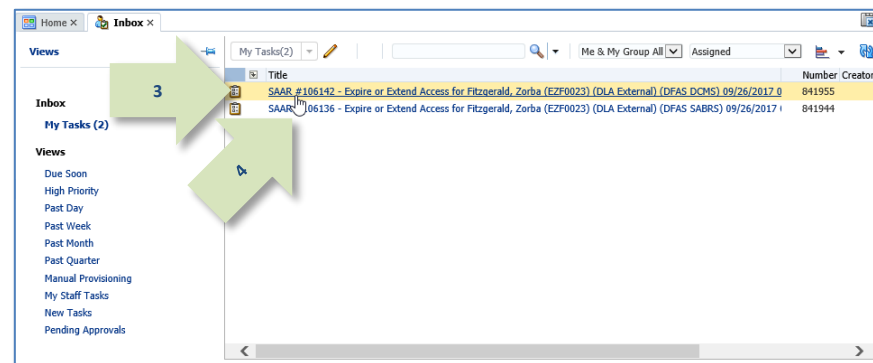   *AMPS launches the **Extension** request process in a separate tab.*

Figure 352: Inbox - My Tasks List

5. In the **SAAR Information** section screen, verify the following information:

    5a. SAAR number must match the SAAR indicated in the email notification.

    5b. Role Name of role that is expiring.

6. Enter the reason for requesting the role extension in the **Justification** text area.

> ### Note:
>
> The text provided in the sample screen is for illustration purposes only. Please enter complete text appropriate for your extension request.

7. You no longer need to enter your Date of Birth.

    AMPS no longer collects this data. This field is not editable and contains faux data only.

8. Check the **Supervisor** email address to verify the correct External Supervisor is identified for your account.
    If the information is incorrect, correct it as needed.

9. Check the **External Security Officer** email address to verify the correct External Security Officer is identified for your account.
    If the information is incorrect, correct it as needed.

10. Check the **External Authorizing Official** email address to verify the correct External Authorizing Official is identified for your account.

    If the information is incorrect, correct it as needed. Must be different from the ESU and ESO.

11. Click **Extend**.

    *AMPS closes the **Expire or Extend** screen and submits the extension request to the approval process.*

Figure 353: Expire or Extend – Internal User Extension Request Screen

12. Click the **OK** button in the extension confirmation message to proceed.
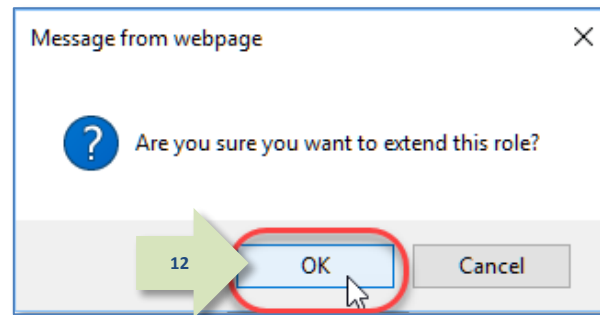

Figure 354: Extension Request Confirmation

13. **Optional:** In the **My Tasks** list, you can search for and view the Extension request again, as needed. Follow these steps:

   a. Enter the SAAR number in the Search field.

   b. In the Status drop-down box, select either **Completed** or **Any**.

   c. In the search results, click the SAAR **Title** to reopen the Extension request screen.

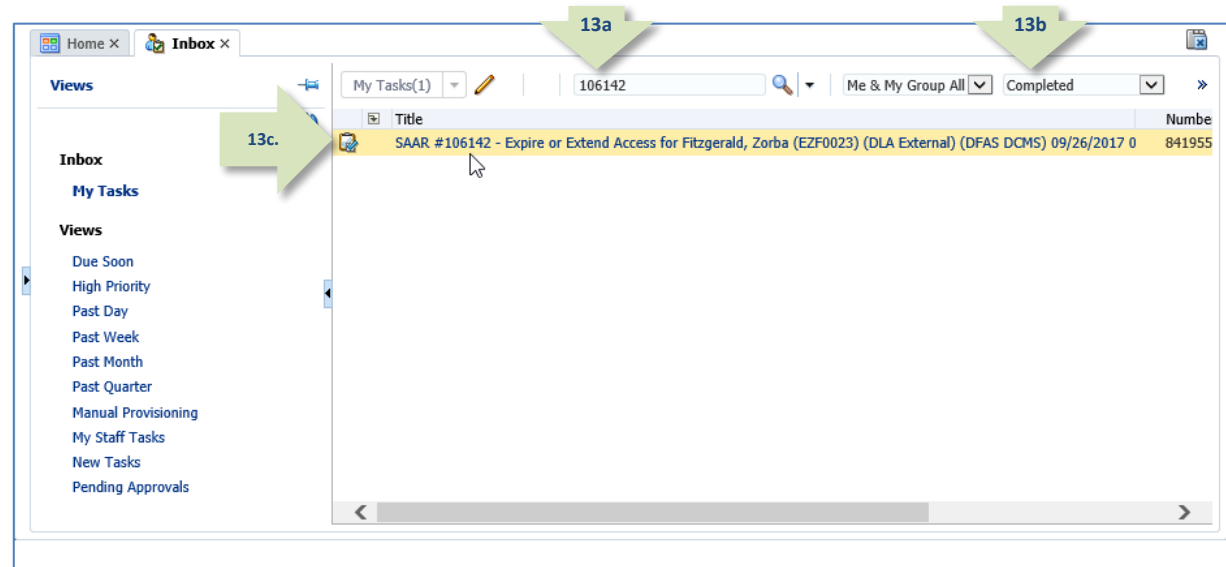   *Click* **Cancel** *in the Extension request to close the screen.*

Figure 355: My Tasks List – Updated

14. To monitor the progress of your extension request during the approval process, check your **Pending Requests** table.
(See **How to Check Your Role Status** on page 97.)

   If AMPS displays a **Privacy Statement** *screen (not shown), read the content and click* **Accept** *to proceed.*

15. After the extension request is submitted, AMPS sends an email message to the user indicating the SAAR extension request is waiting for Supervisor approval.

    (A sample is shown at right.)

14

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: SAAR #106142 is awaiting External Supervisor approval.

This request was submitted in AMPS on 09/26/2017 08:56:31 EDT.

No action is required from you at this time.

This task expires on 10/17/2017 14:50:45 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

How to Approve a Role Extension Request

An extension request goes to the same set of approvers as an initial role request. Approvers may include the following officers and staff:

Approver	Time Limit	Responsibility
AMPS Supervisor:	20 days (reminders sent every day)	The user's designated Supervisor in AMPS. External users identify their External Supervisor by email address; External Supervisors do not hold AMPS accounts.
Security Officer:	20 days (reminders sent every day)	The group of Security Officers designated by an organization to review each requestor's security information. DLA requests may not require a Security Officer approval if the request is eligible for a bypass or an automated approval. See **Security Officer: Internal Users** in this user guide for more information. External users identify their External Security Officers by email address; External Security Officers do not hold AMPS accounts.
Data Owner:	20 days (reminders sent every day)	The group of application staff members appointed to oversee the security and integrity of an application's data.
Information Assurance Officer:	20 days (reminders sent every day)	The group of IAOs designated by an agency to review each requestor's Cyber Awareness Training certification date to ensure the requestor's training is up to date. **DLA systems do not require an IAO review.** See the section entitled **Information Assurance Officer (IAO)** in this user guide for more information.

After an internal user submits an extension request, AMPS sends an email notification to the user's Supervisor with the SAAR number and data related to the extension request, along with a link to the Supervisor's **My Tasks** list on the **Inbox** screen. When an external user submits an extension request, AMPS sends an email notification to the user's External Supervisor through the email address supplied by the external user in his profile.

As the extension proceeds through the approval process, the Security Officer or External Security Officer, Data Owner, and Information Assurance Officer see the extension request approval in sequence and choose the option appropriate for the approval decision. AMPS notifies each approver and resends this notification every day for 20 days. If the approver fails to act on the extension request, AMPS submits the user's role to the role removal process.

Automatic Security Officer Approvals

AMPS can apply an automatic Security Officer approval to an extension request that meets specific criteria. The automatic approval speeds the approval process for requests that present no specific content requiring an immediate security review.

For role expiries and extensions, AMPS can automatically apply an approval for a Security Officer, if all of the following conditions are met:

- The user has not selected an option to retain any IT1- or IT2-level role. If so, the IT level of the requested role cannot exceed the user's IT level.

- The user has a value recorded for the four clearance-related fields that AMPS tracks, including the following fields:
  - Security Clearance
  - IT Level, or Position Sensitivity
  - Background Investigation Type
  - Last Investigation Date
- The user's recorded IT level satisfies one of the following conditions:
  - If the user's IT level is IT1 or IT2, the date of the user's investigation must be less than 5 years old, or . . .
  - If the user's IT level is IT3, the date of the user's investigation must be less than 10 years old.
- The user is not flagged for review by a Security Officer.
- The user is a member of the DLA organization or any organization under DLA.

When an automatic approval occurs, AMPS logs the automatic approval with the following data:

- The approver's user ID, normally reported in the audit logs, will be blank.
- The Status recorded in the audit logs will be "AUTOAPPROVE."

Note

AMPS reports all timestamps in the audit log in Eastern Time: Eastern Standard Time or Eastern Daylight Time, depending on the time of year.

- AMPS enters the following statement to this effect, subject to government change and approval:

  "This request has been automatically approved by AMPS, per the conditions specified by Kathy Cutler Account Management Policy – Signed 6 Nov 2014. <URL to eWorkplace location>"

Approver Decision Screens: Extend, or Expire

The approval decision screen for a role extension request is similar to a role request approval. The following sections list and describe the options available to each approver.

Supervisor Decision Options

The actions a Supervisor can perform on a role extension request approval screen include the following options:

- **Cancel** closes the approval decision screen without action (external approver only).
- **Extend** sends the role extension request to the next approver. The Supervisor must enter text in the Comments area to activate the **Extend** option. Otherwise, the Supervisor cannot approve the role extension request.
- **Expire** executes a role removal procedure in AMPS and notifies the user that the role has been removed from his or her account.

Security Officer and Data Owner Decision Options

The actions a Security Officer or Data Owner can perform on a role extension request approval screen include the following options:

- **Cancel** closes the approval decision screen without action (external approver only).
- **Approve** sends the role extension request to the next approver.
- **Reject** ends the role extension task. The user's role is submitted for removal, and AMPS sends the user an email notification indicating the role extension request was rejected.

IAO Decision Options (Not Applicable to DLA Approvals)

- **Cancel** closes the approval decision screen without action (external approver only).
- **Approve** ends the role extension approval process. The role assignment is renewed for the time period designated by the Supervisor or Data Owner.
- **Reject** ends the role extension task. The user's role is submitted for removal, and AMPS sends the user an email notification indicating the role extension request was rejected.

User Types

The role **extension** request is submitted to the AMPS approval workflow, as follows:

- Submissions from all **internal users** go their AMPS Supervisors for extension or expiration.
- Submissions from all **external users** with a **User Type** designation of **Military, Civilian, or Contractor** go their AMPS External Supervisors for extension or expiration.
- Submissions from **Vendors** (for a vendor role) go to the role application Data Owner for approval or rejection.
- Submissions from members of the **Public** (or for a vendor with a public role) are automatically approved with no intervening approver.

The following sections focus on internal and external users with the **User Type** of **Military, Civilian, or Contractor.** Data Owners handle all requests with the same procedure.

Supervisor Approval: Internal User's Extension Request

1. Read the extension notification and make note of the SAAR number.

   This SAAR number refers to the SAAR that requires a response from the Supervisor within 20 days.

   AMPS issues a reminder notification about a pending role extension task to the Supervisor every day (not shown).

1
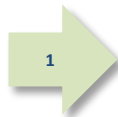
Sample Supervisor Notification: Action Required – Expire or Extend Access Role

Subject: Action Required: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 - Expire or Extend Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - DFAS General User SABRS-014 was submitted in AMPS on 09/25/2017 18:04:31 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/15/2017 18:04:37 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After you log in to AMPS, locate and click the **Inbox command** from the User ID dropdown menu.

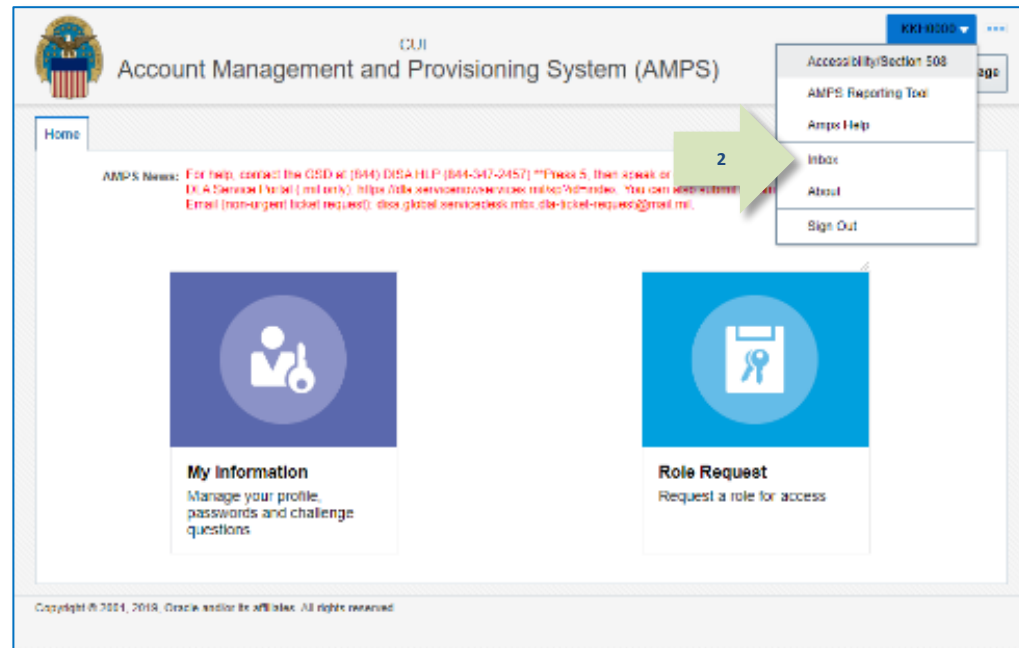   *AMPS displays the **Inbox** tab and the **My Tasks** view.*

Figure 356: User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role extension in the **Title** column.

   You can verify the correct SAAR by its number.

4. Click the **Title** of the SAAR to start the approval process.

   *AMPS launches the **Role Extension Supervisor Decision** screen in a separate window (see Figure 358).*
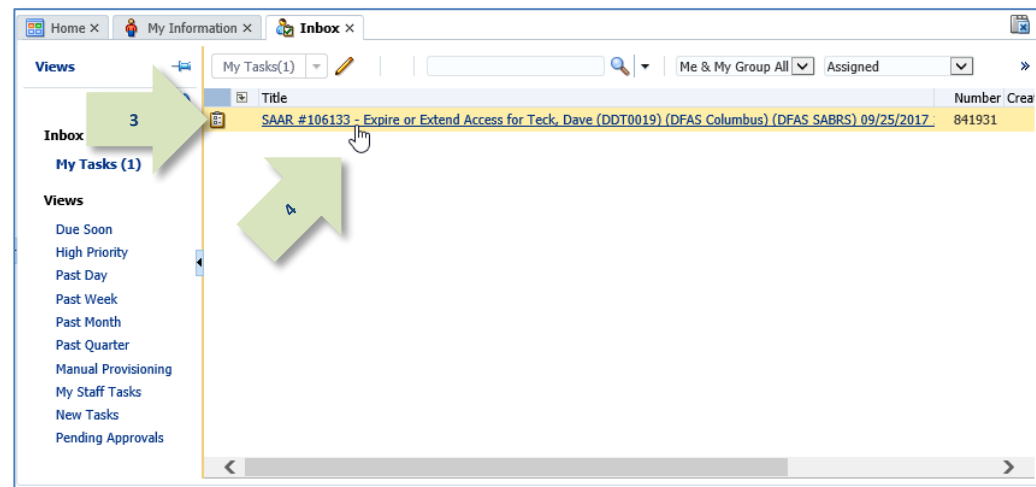
Figure 357: Inbox – My Tasks

5. Review and correct the **End Date**, as needed.

   *Change the **End Date** to the appropriate date for the user and role.*

6. Click the **Additional Information** tab.

   *AMPS displays the **Additional Information** screen (see Figure 359).*

Figure 358: Role Extension - Supervisor Decision – Role Expiration Details

7. On the **Additional Information** screen, note the **SAAR Approval History**.

    *This portion of the **Supervisor Decision** screen stores a record and all comments for the user and all approvers. AMPS adds comments and other information after each approval step is completed.*

8. Click the **User Information** tab.

    *AMPS displays the **User Information** screen (see Figure 360).*

Figure 359: Role Extension - Supervisor Decision - Additional Information

9. In the **User Information** screen, review the user's account, contact, organization, and supervisor information. **Current Roles** and **Pending Requests** are provided for additional review.

10. As an option, enter text in the **Comments** area.

    Comments are not required to extend a role. Text in the **Comments** *area is required ONLY to activate the* **Expire** *button if you want to allow this user's access to expire.*

    However, AMPS maintains a record of approver comments in the **SAAR Approval History** *table, located on the* **Additional Information** *screen, after each approval stage is completed.*

11. Click **Extend** to send the SAAR to the Security Officer for approval of the extension request.

    AMPS saves the response to the SAAR record, closes the decision screen, and returns the display to the **My Tasks** *tab.*

Note:

The comment provided is for illustration purposes only. Please enter specific content related to the AMPS Supervisor role extension decision.

Figure 360: Role Extension - Supervisor Decision - User Information

12. **OPTIONAL:** Follow these steps to view the completed decision screen, as needed:

   a. In the **Search** field, enter the SAAR number for the decision screen you want to review.

   b. In the **Status** drop-down box, click either **Completed** or **Any**.

   AMPS automatically searches for and displays the matching SAAR.

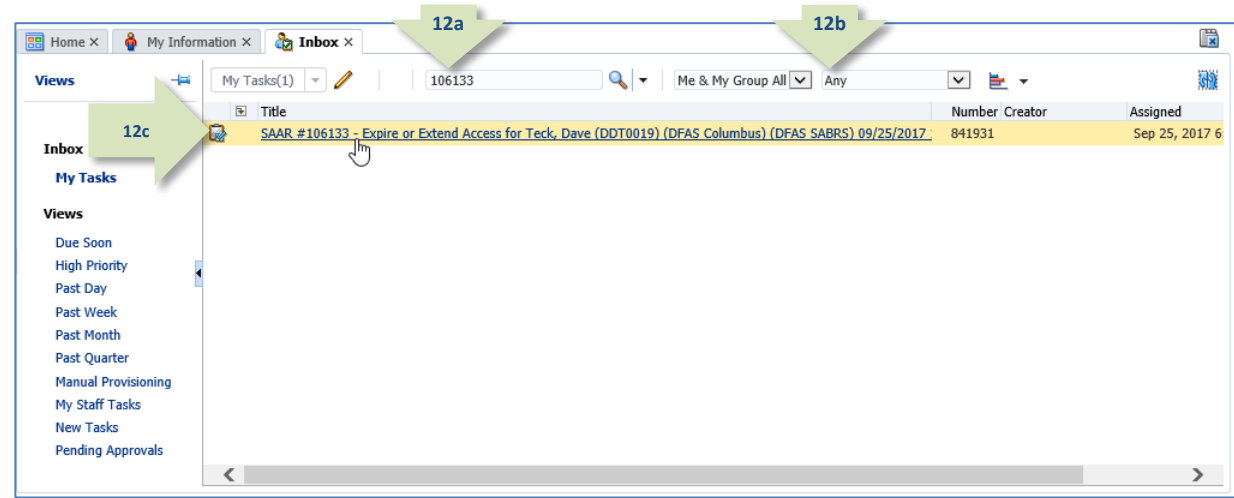   c. Click the SAAR title to review the SAAR decision screen (not shown).

Figure 361: My Tasks - Completed Role Extension SAAR

13. Following the Supervisor's approval of an extension request, the user receives an email notification indicating the outcome of the Supervisor's decision.

   (A sample is shown at right.)

   Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

   Body: The Supervisor has completed an approval for SAAR #106133.

   The outcome for this task is APPROVE.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

14. Following the Supervisor's approval of an extension request, the user also receives an email notification indicating that AMPS has forwarded the role extension request to the Security Officer, and the request awaits a decision from a Security Officer.

   (A sample is shown at right.)

   Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

   Body: SAAR #106133 is awaiting Security Officer approval.

   This request was submitted in AMPS on 09/25/2017 18:04:31 EDT.

   No action is required from you at this time.

   This task expires on 10/15/2017 20:55:34 EDT.

   AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

External Supervisor Approval: External User's Extension Request

1. Read the extension notification and make note of the SAAR number.

   This SAAR number refers to the SAAR that requires a response from the Supervisor within 20 days.

   AMPS issues a reminder notification about a pending extension task to the Supervisor every day.

Note:

The URL provided in the sample notification is a sample link. To ensure the correct result, obtain the correct URL from the actual email message.

Sample Supervisor Notification: Extension of a Role

Subject: Action Required: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: SAAR #106142 - Expire or Extend Access for Fitzgerald, Zorba (EZF0023) (DLA External) has been submitted for approval.

This request to extend DFAS DCMS Prod - DSK Air Force Approval DE-DAO (380100) Foreign National DSK-027 was submitted in AMPS on 09/26/2017 08:56:31 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=6304%3A7U10WnXUR3X8BtmFlAluMulsl%2FGv5Tk9vlJfYWH1z3Y%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/16/2017 14:50:45 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

2. **Copy the URL** from the email notification to a browser and press **Enter**.

   *Acknowledge the **Consent to Monitoring** if it is displayed (not shown).*

   *AMPS displays the **AMPS Approval Work Queue**. This screen lists all approval tasks currently assigned to the specific Supervisor (see Figure 363).*
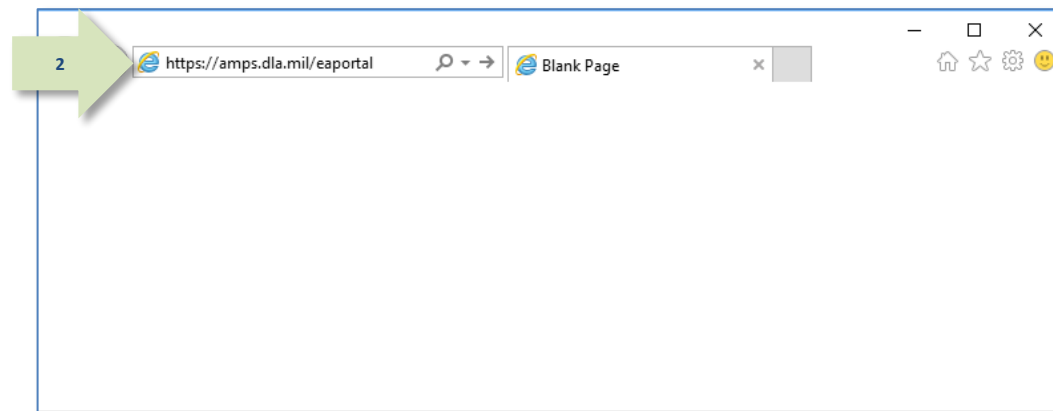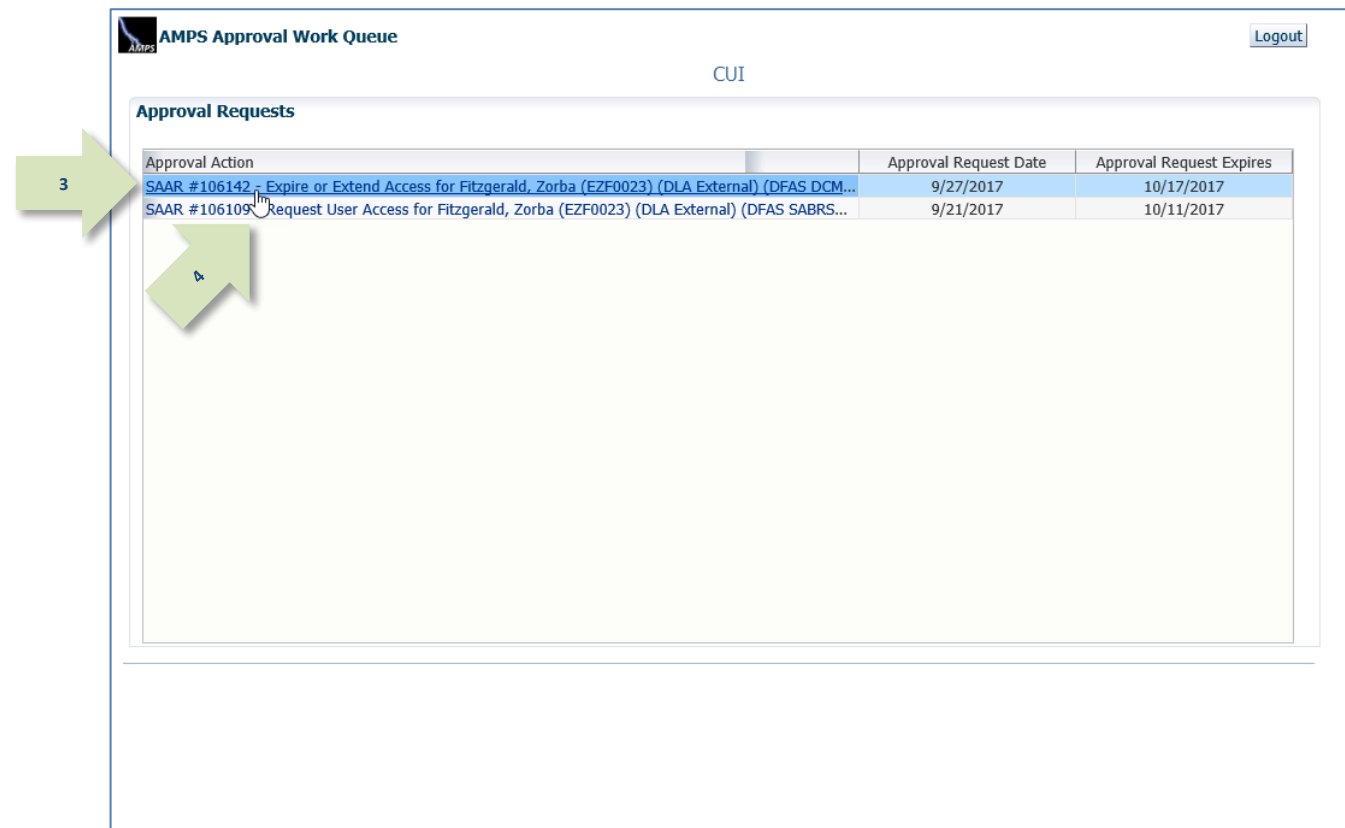
Figure 362: External Role Extension Approval – Email Link

3. In the **Approval Action** column, locate the SAAR for the role extension identified in the email notification.

    You can verify the correct SAAR by its number and user data.

4. Click the SAAR entry to start the approval process.

    *AMPS launches the **Supervisor Decision** screen (see Figure 364).*

Figure 363: Role Extension Approval – Approval Work Queue

5. Ensure the **End Date** has the appropriate extension period defined. Alter this date as needed, up to 365 days from the current date.

   If you enter a date more than 365 days from the current date, AMPS will alert you with an error message. You will not be able to submit the approval until the date in this field is within the 365-day limit.

6. Click the **Additional Information** tab.

   *AMPS displays the **Additional Information** screen (see Figure 365).*

Figure 364: Role Extension – External Supervisor Decision – Role Extension Details

7. On the **Additional Information** screen, note the **SAAR Approval History**.

    *This portion of the **External Supervisor Decision** screen stores a record and all comments for the user and all approvers. AMPS adds comments and other information after each approval step is completed.*

8. Click the **User Information** tab.

    *AMPS displays the **User Information** screen (see Figure 366).*

Figure 365: Role Extension – External Supervisor Decision - Additional Information

9. In the **User Information** screen, check the user's **Current Roles** and **Pending Requests**.

10. As an option, enter text in the **Comments** text area to clarify the extension decision.

    Comments are not required to extend a role. Text in the **Comments** *area is required ONLY to activate the* **Expire** *button, if you want to allow this user's access to expire.*

    However, AMPS maintains a record of approver comments in the **SAAR Approval History** *table, located on the* **Additional Information** *screen, after each approval stage is completed.*

    Note:

    The comment provided is for illustration purposes only. Please enter specific content related to the AMPS Supervisor role extension decision.

11. Click **Extend** to send the SAAR to the next approver.

    AMPS saves the response to the SAAR record, closes the decision screen, and displays a completion message (see Figure 367).

Figure 366: Role Extension – External Supervisor Decision – User Information

12. In the **Task Completed** screen, click the following link: **Return to the External Approval Worklist**.

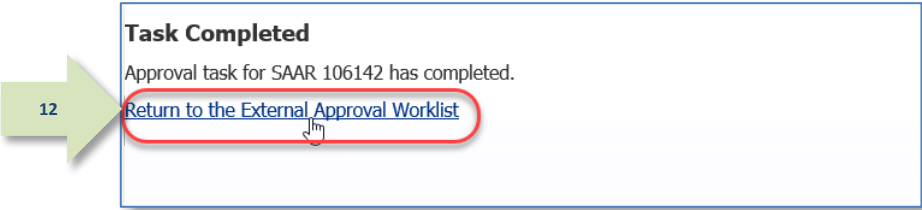*AMPS returns to the* **Approval Work Queue** *(see Figure 368).*

Figure 367: Role Extension Message – Approval Completed

13. If no further approvals are listed or you have completed the session for the time being, click the **Logout** button.

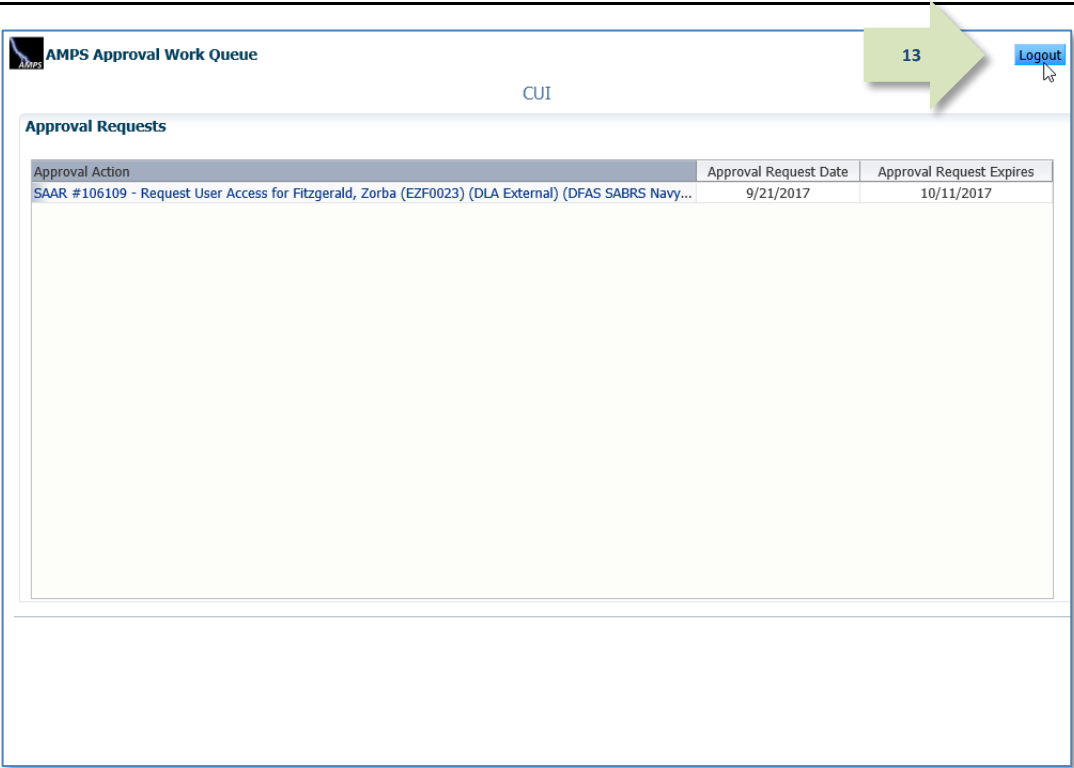*AMPS displays a logout confirmation message (see Figure 369).*

Figure 368: Approval Work Queue – Logout

14. After viewing the logout confirmation, you can close the browser. The Supervisor's approval step is complete.
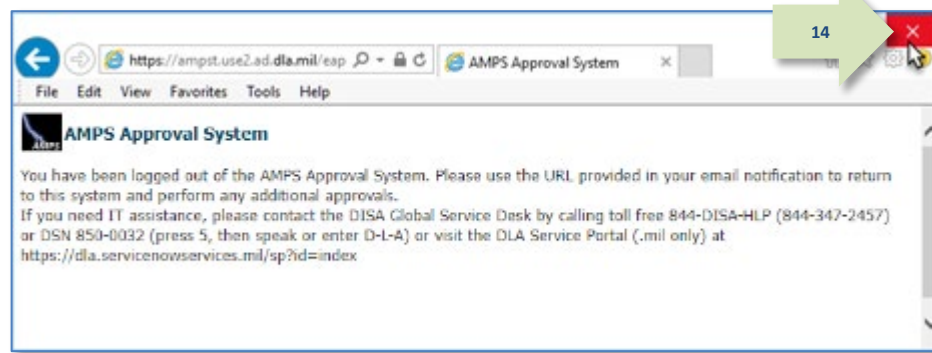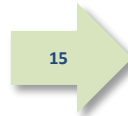

Figure 369: AMPS Approval System - Logout Confirmed

15. Following the Supervisor's approval of an extension request, the user receives an email notification indicating the outcome of the Supervisor's decision.

    (A sample is shown at right.)

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: The External Supervisor has completed an approval for SAAR #106142.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

16. Following the Supervisor's approval of an extension request, the user also receives an email notification indicating that AMPS has forwarded the role extension request to the Security Officer, and the request awaits a decision from the External Security Officer.

    (A sample is shown at right.)

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: SAAR #106142 is awaiting External Security Officer approval.

This request was submitted in AMPS on 09/26/2017 08:56:31 EDT.

No action is required from you at this time.

This task expires on 10/16/2017 16:01:04 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Security Officer Approval: Internal User's Extension Request

The Security Officer approval of an extension is required for each DFAS request. Some DLA requests may require a Security Officer approval, but most are either bypassed or automatically approved. See the section entitled **Security Officer: Internal Users** in this user guide for more information.

1. Read the extension notification and make note of the SAAR number.

    This SAAR number refers to the SAAR that requires a response from the Security Officer within 20 days.

    AMPS issues a reminder notification about a pending role extension task to the Security Officer every day.

1

Sample Security Officer Notification: Extension of a Role

Subject: Action Required: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 - Expire or Extend Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - DFAS General User SABRS-014 was submitted in AMPS on 09/25/2017 18:04:31 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/15/2017 20:55:34 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2.   After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

    *AMPS displays the **Inbox** screen and the **My Tasks** view for the current user (see Figure 371).*
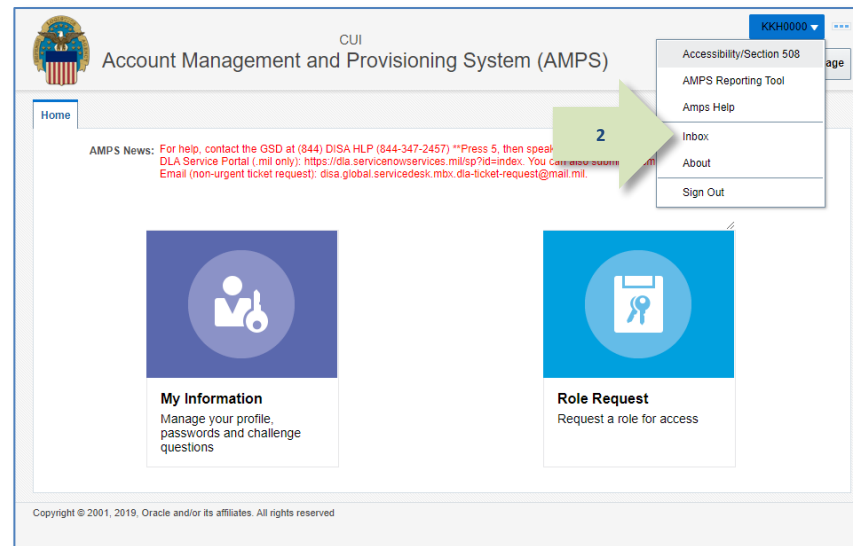
Figure 370: Role Extension Approval – User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role extension in the **Title** field.

    You can verify the correct SAAR by its number.

4. Click the SAAR **Title** to start the decision process.

    *AMPS opens the **Role Extension Security Officer Decision** screen (see Figure 372).*
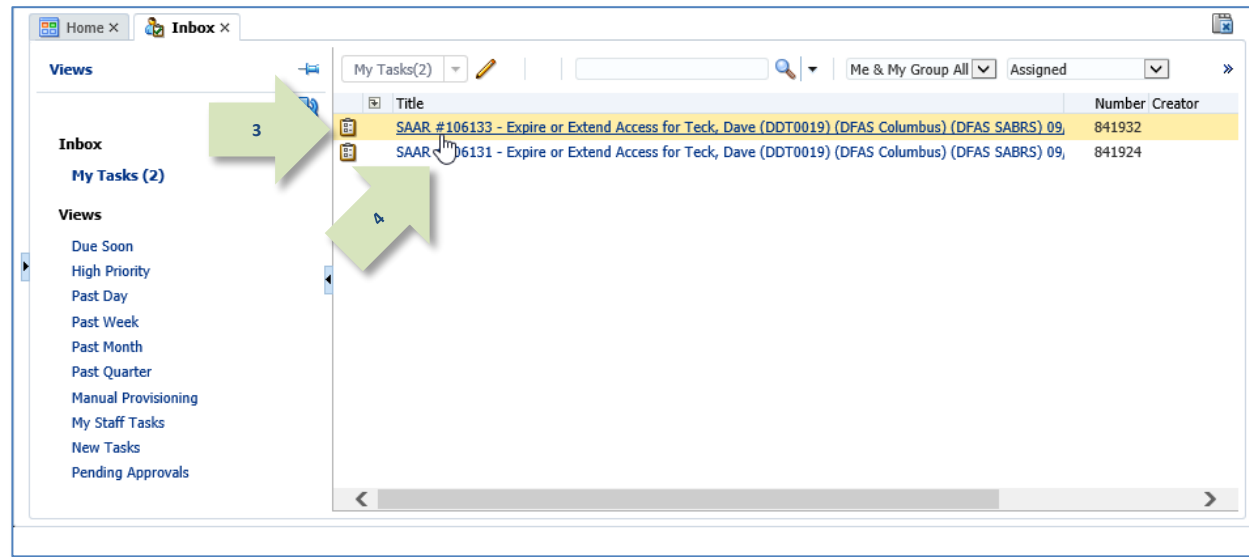

Figure 371: Role Extension Approval – Inbox – My Tasks

5. Enter or select data in the following areas:

    a. **IT Level:** select the user's IT level.

    b. **Clearance Level:** select the user's current Clearance Level.

    c. **Type of Investigation:** select the most recent investigation type applicable to the current Clearance Level.

    d. **Date of Investigation:** enter or select the user's most recent clearance investigation date.

    e. **Security Review Flag:** change this option to Flagged for Review if you do not want any requests from a DLA user to bypass the Security Officer. This flag does not affect DFAS users.

6. Click the **Additional Information** tab.

    AMPS displays the **Additional Information** *screen (see Figure 373).*

Figure 372: Role Extension Approval – Security Officer Decision – Role Expiration Details

7. On the **Additional Information** screen, note the **SAAR Approval History**.

    *This portion of the **Security Officer Decision** screen stores a record and all comments for the user and all approvers.*

8. Click the **User Information** tab.

    *AMPS displays the **User Information** screen (see Figure 374).*

Figure 373: Role Extension Approval – Security Officer Decision – Additional Information

9. In the **User Information** screen, review the user's account, contact, organization, and supervisor information. **Current Roles** and **Pending Requests** are provided for additional review.

10. As an option, enter text in the **Comments** area.

    *Comments are not required to extend a role. Text in the **Comments** area is required ONLY to activate the **Expire** button if you want to allow this user's access to expire.*

    *However, AMPS maintains a record of approver comments in the **SAAR Approval History** table, located on the **Additional Information** screen, after each approval stage is completed.*

11. Click **Extend** to send the SAAR to the Data Owner for approval of the extension request.

    *AMPS saves the response to the SAAR record, closes the decision screen, and returns the display to the **My Tasks** tab.*

    *The SAAR just approved is removed from the **My Tasks** list.*

    ### Note:

    The comment provided is for illustration purposes only. Please enter specific content related to the Security Officer role-extension decision.

Figure 374: Role Extension Approval – Security Officer Decision – User Information

12. **OPTIONAL:** Follow these steps to view the completed decision screen, as needed:

    a. In the **Search** field, enter the SAAR number for the decision screen you want to review.

    b. In the **Status** dropdown list, select either **Any** or **Completed**.

    c. Click the SAAR title to review the SAAR decision screen (not shown).
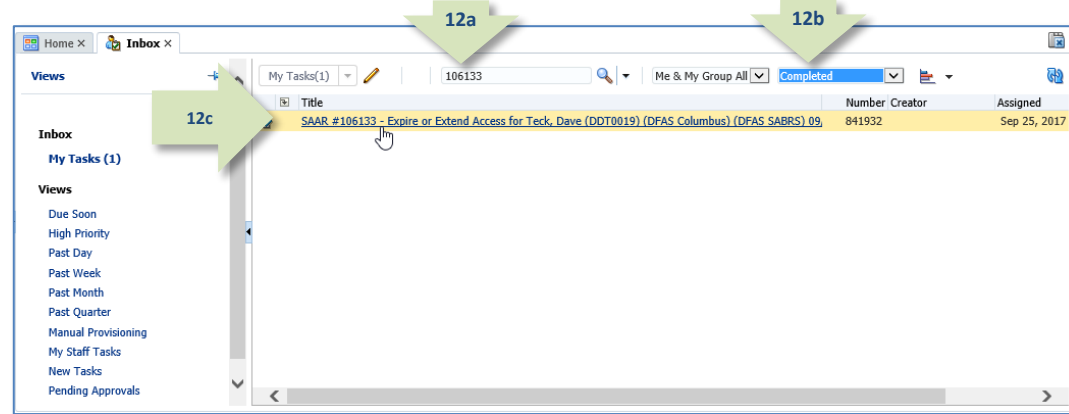
Figure 375: Role Extension Approval – Security Officer Post-decision

---

13. Following the Security Officer's approval of an extension request, the user receives an email notification indicating the outcome of the Security Officer's decision.

(A sample is shown at right.)

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: The Security Officer has completed an approval for SAAR #106133.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

14. Following the Security Officer's approval of an extension request, the user also receives an email notification indicating that AMPS has forwarded the role extension request to the application Data Owner, and the request awaits a decision from the Data Owner.

(A sample is shown at right.)

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 is awaiting Data Owner approval.

This request was submitted in AMPS on 09/25/2017 18:04:31 EDT.

No action is required from you at this time.

This task expires on 10/15/2017 17:55:02 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

External Security Officer Approval: External User's Extension Request

1. Read the extension notification and make note of the SAAR number.

   This SAAR number refers to the SAAR that requires a response from the Security Officer within 20 days. AMPS issues a reminder notification about a pending role expiration task to the Security Officer every day.

   ### Note:

   The URL provided in the sample notification is a sample link. To ensure the correct result, obtain the correct URL from the actual email message.

   → 1

   ### Sample Security Officer Notification: Extension of a Role

   Subject: Action Required: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

   Body: SAAR #106142 - Expire or Extend Access for Fitzgerald, Zorba (EZF0023) (DLA External) has been submitted for approval.

   This request to extend DFAS DCMS Prod - DSK Air Force Approval DE-DAO (380100) Foreign National DSK-027 was submitted in AMPS on 09/26/2017 08:56:31 EDT.

   Please visit AMPS at this URL:

   https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=0004%3A2N%2FYyFSdZu2S5h14Hu10Jm6en2G1no4LJ8Fyp8s%2BqJs%3D

   Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/16/2017 16:01:04 EDT.

   AMPS provides this message for notification only. Please do not respond to this message If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. Copy the URL from the extension notification to a browser and press **Enter**.

   Acknowledge the Consent to Monitoring *if it is displayed (not shown).*

   AMPS displays the **AMPS Approval Work Queue**. *This screen lists all currently assigned approval tasks by SAAR number (see Figure 377).*

   → 2

   Figure 376: External Role Extension Approval – Email Link

3. In the **Approval Action** column, locate the SAAR for the role extension identified in the email notification.

    You can verify the correct SAAR by its number.

4. Click the SAAR entry to start the approval process.

    *AMPS may display a **Verify Approver** screen (see Figure 187), unless you have already confirmed you are the user's Security Officer during a previous approval procedure.*

    *Otherwise, AMPS displays the **External Security Officer Decisio**n screen (see Figure 378).*

Figure 377: Approval Work Queue - Approval Action

5. Ensure the following fields have the appropriate entries:

    - **IT Level:** select the user's IT level.
    - **Clearance Level:** select the user's current Clearance Level.
    - **Type of Investigation:** select the most recent investigation type applicable to the current Clearance Level.
    - **Date of Investigation:** enter or select the user's most recent clearance investigation date.
    - **Not Flagged for Review:** leave this option as is to implement the Security Officer bypass for a DLA user; change this option to **Flagged for Review** if you do not want any requests from a DLA user to bypass the Security Officer. This flag does not affect DFAS users; all DFAS role requests are submitted for Security Officer review.

6. Click the **Additional Information** tab.

    AMPS displays the **Additional Information** *screen (see Figure 379).*

Figure 378: Role Extension – External Security Officer Decision – Role Extension Details

7. On the **Additional Information** screen, note the SAAR Approval History.

   *This portion of the **External Security Officer Decision** screen stores a record and all comments for the user and all approvers.*

8. Click the **User Information** tab.

   *AMPS displays the **User Information** screen (see Figure 380).*

Figure 379: Role Extension – External Security Officer Decision – Additional Information

9. In the **User Information** screen, review the user's account, contact, organization, and supervisor information. **Current Roles** and **Pending Requests** are provided for additional review.

10. As an option, enter text in the **Comments** area.

   *Comments are not required to extend a role. Text in the Comments area is required ONLY to activate the **Expire** button, if you want to allow this user's access to expire.*

   *However, AMPS maintains a record of approver comments in the **SAAR Approval History** table, located on the **Additional Information** screen, after each approval stage is completed.*

11. Click **Extend** to send the SAAR to the Data Owner for approval of the extension request.

   *AMPS saves the response to the SAAR record, closes the decision screen, and displays a **Task Completed** message (see Figure 381).*

Note:

The comment provided is for illustration purposes only. Please enter specific content related to the Security Officer role-extension decision.

Figure 380: Role Extension – External Security Officer Decision – User Information

12. Click the following link: **Return to the External Approval Worklist.**

*AMPS closes the message and displays the **Approval Work** Queue (see Figure 382).*

Task Completed

Approval task for SAAR 106142 has completed.

Return to the External Approval Worklist
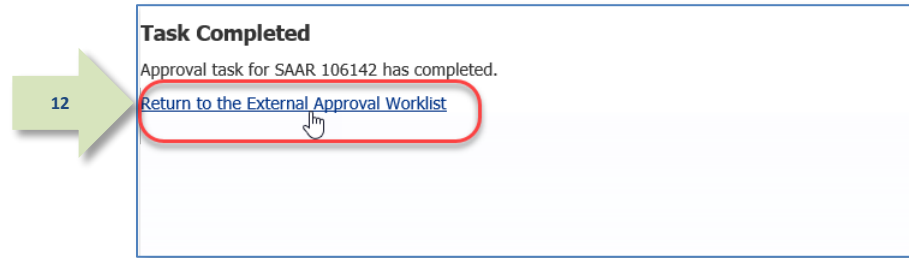
Figure 381: Message - Approval Completed

13. If no further approvals are listed or you have completed the session for the time being, click the **Logout** button.

AMPS displays a logout confirmation message (see Figure 383).

AMPS Approval Work Queue

CUI

Approval Requests

Approval Action		Approval Request Date	Approval Request Expires
There are no pending approvals awaiting your attention. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index			

Figure 382: Approval Work Queue - No Pending Approvals

14. After viewing the logout confirmation, you can close the browser. The Security Officer's approval step is complete.

AMPS Approval System

You have been logged out of the AMPS Approval System. Please use the URL provided in your email notification to return to this system and perform any additional approvals.
If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 383: AMPS Approval System - Logout Confirmation

15. Following the Security Officer's approval of an extension request, the user receives an email notification indicating the outcome of the Supervisor's decision.
(A sample is shown at right.)

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: The External Security Officer has completed an approval for SAAR #106142.

[15] The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

16. Following the Security Officer's approval of an extension request, the user also receives an email notification indicating that AMPS has forwarded the role extension request to the External Authorizing Official, and the request awaits a decision from the External Authorizing Official.
(A sample is shown at right.)

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

[16] **Body:** SAAR #106142 is awaiting External Authorizing Official approval.

This request was submitted in AMPS on 09/26/2017 08:56:31 EDT.
No action is required from you at this time.

This task expires on 10/16/2017 19:01:51 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

External Authorizing Official: External Users Only

Option for Certain Roles

AMPS requires all external users to enter the email address of an External Authorizing Official (EAO). The EAO is responsible for reviewing requests for roles or extensions of roles that require this extra approval step.

If you are an EAO, AMPS notifies you by email that a request awaits your action. Follow the steps in this section to review the role extension request and either approve or reject the request.

1. Read the extension notification and make note of the SAAR number.

This SAAR number refers to the SAAR that requires a response from the External Authorizing Official within 20 days.

AMPS issues a reminder notification about a pending role expiration task to the EAO every day.

Note:

The URL provided in the sample notification is a sample link. To ensure the correct result, obtain the correct URL from the actual email message.

2. Copy the URL from the extension notification to a browser and press **Enter**.

*Acknowledge the **Consent to Monitoring if** it is displayed (not shown).*

*AMPS displays the **AMPS Approval Work Queue**. This screen lists all currently assigned approval tasks by SAAR number (see Figure 385).*

1

Sample Security Officer Notification: Extension of a Role

Subject: Action Required: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: SAAR #106142 - Expire or Extend Access for Fitzgerald, Zorba (EZF0023) (DLA External) has been submitted for approval.

This request to extend DFAS DCMS Prod - DSK Air Force Approval DE-DAO (380100) Foreign National DSK-027 was submitted in AMPS on 09/26/2017 08:56:31 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/eaportal/faces/adf.task-flow?adf.tfId=eaportal-flow&adf.tfDoc=/WEB-INF/eaportal-flow.xml&ApprovalID=0004%3A2N%2FYyFSdZu2S5h14Hu10Jm6en2G1no4LJ8Fyp8s%2BqJs%3D

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/16/2017 16:01:04 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2

Figure 384: External Role Extension Approval – Email Link

3. In the **Approval Action** column, locate the SAAR for the role extension identified in the email notification.

    You can verify the correct SAAR by its number.

4. Click the SAAR entry to start the approval process.

    *AMPS may display a **Verify Approver** screen (see Figure 196), unless you have already confirmed you are the user's External Authorizing Official during a previous approval procedure.*

    *Otherwise, AMPS displays the **External Authorizing Official** Decision screen (see Figure 386).*

Figure 385: Approval Work Queue - Approval Action

5. Review the SAAR information and Role Extension Details.

6. Click the **Additional Information** tab.

    *AMPS displays the **Additional Information** screen (see Figure 379).*

Figure 386: Role Extension – External Security Officer Decision – Role Extension Details

7. In the **Additional Information** screen, note the **SAAR Approval History**.

    This portion of the External Security Officer Decision screen stores a record of all basic identifying information, outcome, and comments for the user and all approvers to date.

8. Click the **User Information** tab.

    AMPS displays the User Information screen (see Figure 388).

Figure 387: Role Extension – External Security Officer Decision – Additional Information

9. In the **User Information** tab, review the user's account, contact, organization, and supervisor information. **Current Roles** and **Pending Requests** are provided for additional review.

10. As an option, enter text in the **Comments** area.

    Comments are not required to extend a role. Text in the **Comments** *area is required ONLY to activate the* Expire *button, if you want to allow this user's access to expire.*

    However, AMPS maintains a record of approver comments in the **SAAR Approval History** *table, located on the* **Additional Information** *screen, after each approval stage is completed.*

    ## Note:

    > The comment provided is for illustration purposes only. Please enter specific content related to the EAO role extension decision.

11. Click **Extend** to send the SAAR to the Data Owner for review of the extension request.

    AMPS saves the response to the SAAR record, closes the decision screen, and displays a **Task Completed** *message (see Figure 389).*

Figure 388: Role Extension – External Security Officer Decision – User Information

12. Click the following link: **Return to the External Approval Worklist.**

AMPS closes the message and displays the **Approval Work Queue** *(see Figure 390).*

Task Completed

Approval task for SAAR 106142 has completed.

Return to the External Approval Worklist
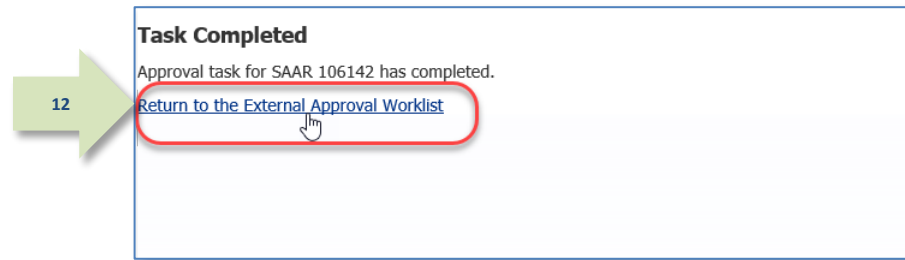
Figure 389: Message - Approval Completed

13. If no further approvals are listed or you have completed the session for the time being, click the **Logout** button.

AMPS displays a logout confirmation message (see Figure 391).

AMPS Approval Work Queue

Logout

CUI

Approval Requests

Approval Action	Approval Request Date	Approval Request Expires
There are no pending approvals awaiting your attention. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index		

Figure 390: Approval Work Queue - No Pending Approvals

14. After viewing the logout confirmation, you can close the browser. The External Authorizing Official's approval step is complete.

https://amps.dla.mil/   AMPS Approval System

AMPS Approval System

You have been logged out of the AMPS Approval System. Please use the URL provided in your email notification to return to this system and perform any additional approvals.
If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 391: AMPS Approval System - Logout Confirmation

15. Following the EAO's approval of an extension request, the user receives an email notification indicating the outcome of the EAO's decision.

(A sample is shown at right.)

15

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: The External Authorizing Official has completed an approval for SAAR #106142.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

16. Following the EAO's approval of an extension request, the user also receives an email notification indicating that AMPS has forwarded the role extension request to the Data Owner, and the request awaits a decision from an application Data Owner.

(A sample is shown at right.)

16

Subject: Notification: SAAR #106142 - Expire or Extend Access for Zorba Fitzgerald (EZF0023) (DLA External) (DFAS DCMS) 09/26/2017 08:56:31 EDT

Body: SAAR #106142 is awaiting Data Owner approval.

This request was submitted in AMPS on 09/26/2017 08:56:31 EDT.
No action is required from you at this time.

This task expires on 10/16/2017 07:44:12 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Data Owner Approval: Internal and External Users

1. Read the extension notification and make note of the SAAR number.

    This SAAR number refers to the SAAR that requires a response from the Data Owner within 20 days.

    AMPS issues to the Data Owner a reminder notification about a pending role expiration task every day.
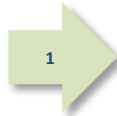
Sample Data Owner Notification: Extension of a Role

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 - Expire or Extend Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - DFAS General User SABRS-014 was submitted in AMPS on 09/25/2017 18:04:31 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/15/2017 17:55:02 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2.   After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

    AMPS displays the **My Tasks** *view and list for the current user (see Figure 393).*
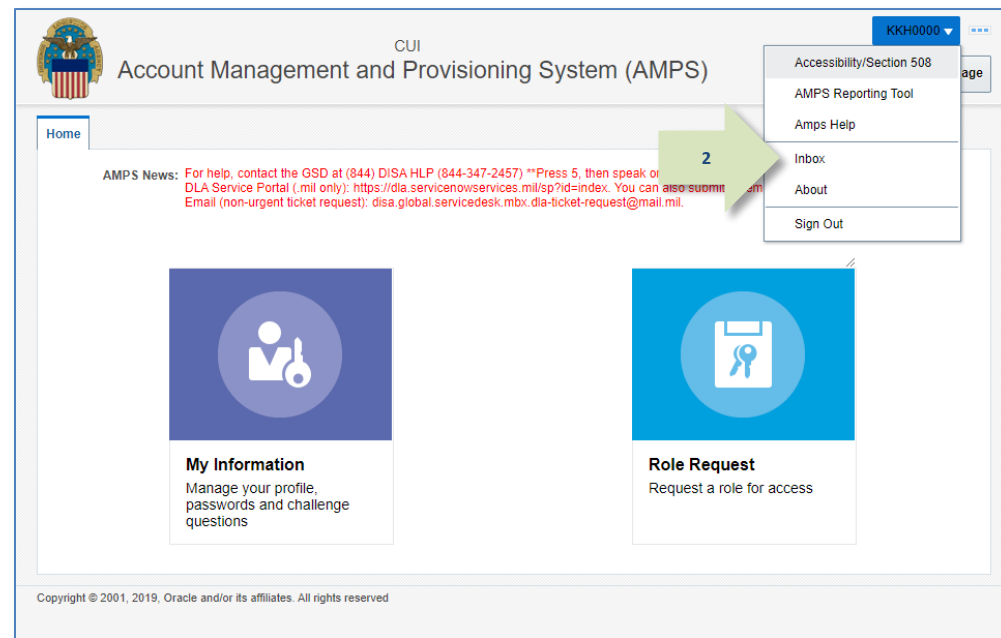
Figure 392: Role Extension Approval – User ID Dropdown Menu – Inbox Command

3.	In the **My Tasks** list, locate the SAAR for the role extension in the **Title** field.

4.	Click the SAAR **Title** to start the decision process.

AMPS launches the **Role Extension – Data Owner Decision** *screen in a separate window (see Figure 394).*
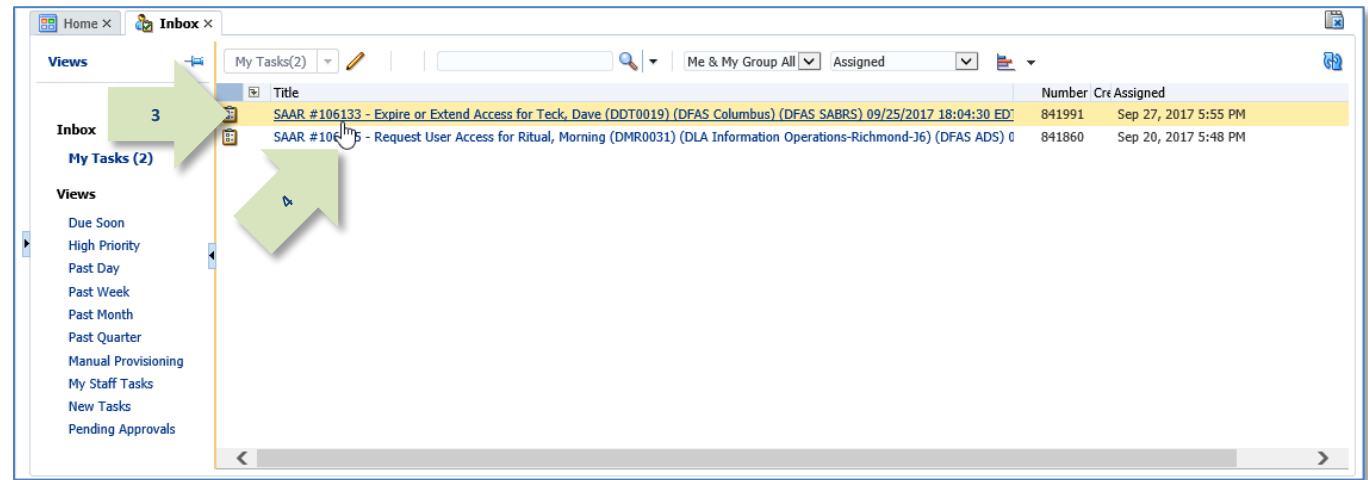
Figure 393: Role Extension Approval – Inbox – My tasks

5. In the **Role Extension – Data Owner Decision** screen, check the **End Date** and modify it, as needed.

   This field has an extension period defined by default. Change this date, as needed.

   For external user extension requests: *If you enter a date more than 365 days from the current date, AMPS will alert you with an error message. You will not be able to submit the approval until the date in this field is within the 365-day limit.*

6. Click the **Additional Information** tab.

   *AMPS displays the **Additional Information** screen (see Figure 395).*

Figure 394: Role Extension Approval – Data Owner Decision – Role Expiration Details

7. The **Additional Information** screen displays SAAR information related to the extension request.

   Also note the **SAAR Approval History**, which lists previous approvers, their email addresses, and their comments, if any.

   This portion of the Data Owner Decision screen stores an approver record, along with all comments entered by the user and approvers.

8. Click the **User Information** tab.

   AMPS displays the User Information screen (see Figure 396).

Figure 395: Role Extension Approval – Data Owner Decision – Additional Information

9. In the **User Information** tab, review the user's account, contact, organization, and supervisor information. **Current Roles** and **Pending Requests** are provided for additional review.

10. As an option, enter text in the **Comments** area.

    Comments are not required to extend a role. Text in the **Comments** *area is required ONLY to activate the* **Expire** *button if you want to allow this user's access to expire.*

    However, AMPS maintains a record of approver comments in the **SAAR Approval History** *table, located on the* **Additional Information** *screen, after each approval stage is completed.*

11. Click **Extend** to send the SAAR to the next stage in the approval process.

    ▪ DFAS requests go to the Information Assurance Officer.

    ▪ DLA requests are considered complete after the Data Owner's extension approval is complete.

    AMPS saves the response to the SAAR record.

    AMPS removes the SAAR just approved from the **My Tasks** *list after you click the* **Refresh** *button on the* **My Tasks** *tab page.*

    Note:

    The comment provided is for illustration purposes only. Please enter specific content related to the Data Owner role extension decision.

Figure 396: Role Extension Approval – Data Owner Decision – User Information

12. **OPTIONAL:** Follow these steps to view the completed decision screen, as needed:

    a. In the **Search** field, enter the SAAR number for the decision screen you want to review.

    b. In the **Status** dropdown list, select either **Any** or **Completed**.

        AMPS automatically searches for and displays the specified SAAR that matches the search criteria.

    c. Click the SAAR title to review the SAAR decision screen (not shown).

Figure 397: Role Extension Approval – Data Owner Post-decision

13. Following the Data Owner's approval of an extension request, the user receives an email notification indicating the outcome of the Data Owner's decision.

    (A sample is shown at right.)

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: The Data Owner has completed an approval for SAAR #106133.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

14. Following the Data Owner's approval of an extension request, DFAS users also receives an email notification indicating that AMPS has forwarded the role extension request to the Information Assurance Officers, and the request awaits a decision from an IAO.

    (A sample is shown at right.)

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 is awaiting Information Assurance Officer approval.

This request was submitted in AMPS on 09/25/2017 18:04:31 EDT.

No action is required from you at this time.

This task expires on 10/15/2017 13:04:32 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

NOTE:

DLA systems do not require an IAO review. After a DLA Data Owner approves a role extension request, the request is considered fully approved.

IAO Approval: Internal and External Users

Note:

DLA system requests do not require an IAO review for internal users.

---

1. Read the extension notification and make note of the SAAR number.

   This SAAR number refers to the SAAR that requires a response from the Information Assurance Officer within 20 days.

   AMPS issues to the Information Assurance Officer a reminder notification about a pending role expiration task every day.
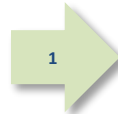
Sample Information Assurance Officer Notification: Extension of a Role

Subject: Action Required: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: SAAR #106133 - Expire or Extend Access for Teck, Dave (DDT0019) (DFAS Columbus) has been submitted for approval.

This request to extend DFAS SABRS Prod - DFAS General User SABRS-014 was submitted in AMPS on 09/25/2017 18:04:31 EDT.

Please visit AMPS at this URL:

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/15/2017 13:04:32 EDT.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at
https://dla.servicenowservices.mil/sp?id=index

2. After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

   *AMPS displays the **Inbox** and the **My Tasks** view for the current user (see Figure 399).*

Figure 398: Role Extension Approval – User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** list, locate the SAAR for the role extension in the **Title** field.

4. Click the SAAR **Title** to start the decision process.

    AMPS displays the **Role Extension - Information Assurance Officer Decision** *screen in a separate tab screen (see Figure 400).*
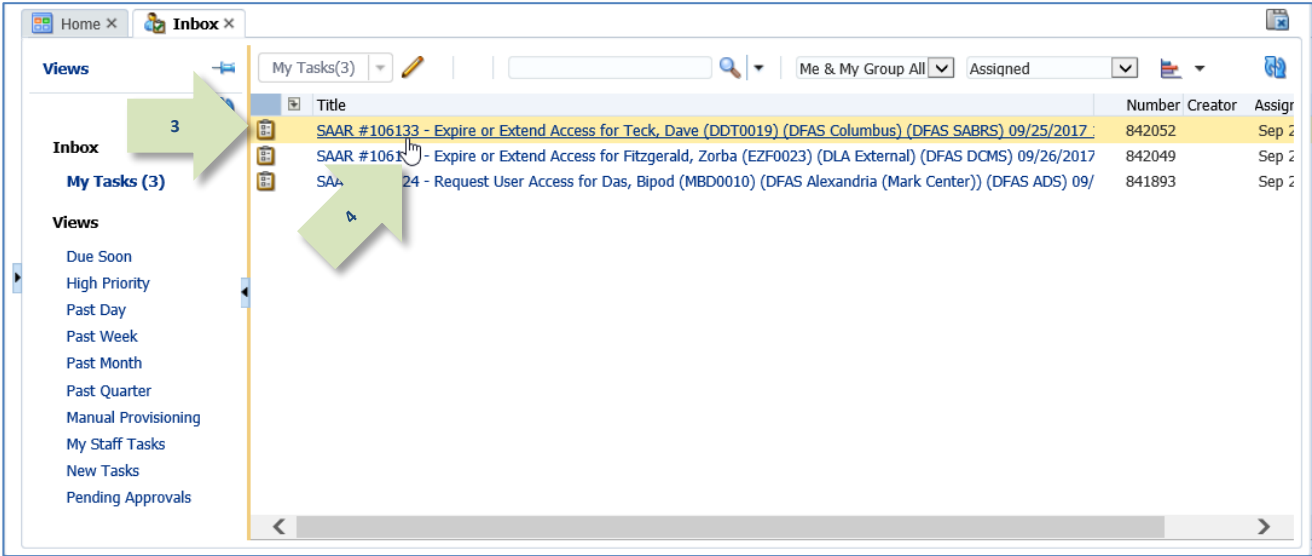
Figure 399: Role Extension Approval – Information Assurance Officer – My Tasks

5. Enter the user's latest **Cyber Awareness Certification Date**, as needed.

   DLA users: an IAO approval is not required.

6. Click the **Additional Information** tab.

   *AMPS displays the **Additional Information** screen (see Figure 401).*

Figure 400: Role Extension Approval – IAO Decision – Role Expiration Details

7. On the **Additional Information** screen, note the **SAAR Approval History**.

    *This portion of the **IAO Decision** screen stores a record of comments by the user and by all approvers after their task submission.*

8. Click the **User Information** tab.

    *AMPS displays the **User Information** screen (see Figure 402).*
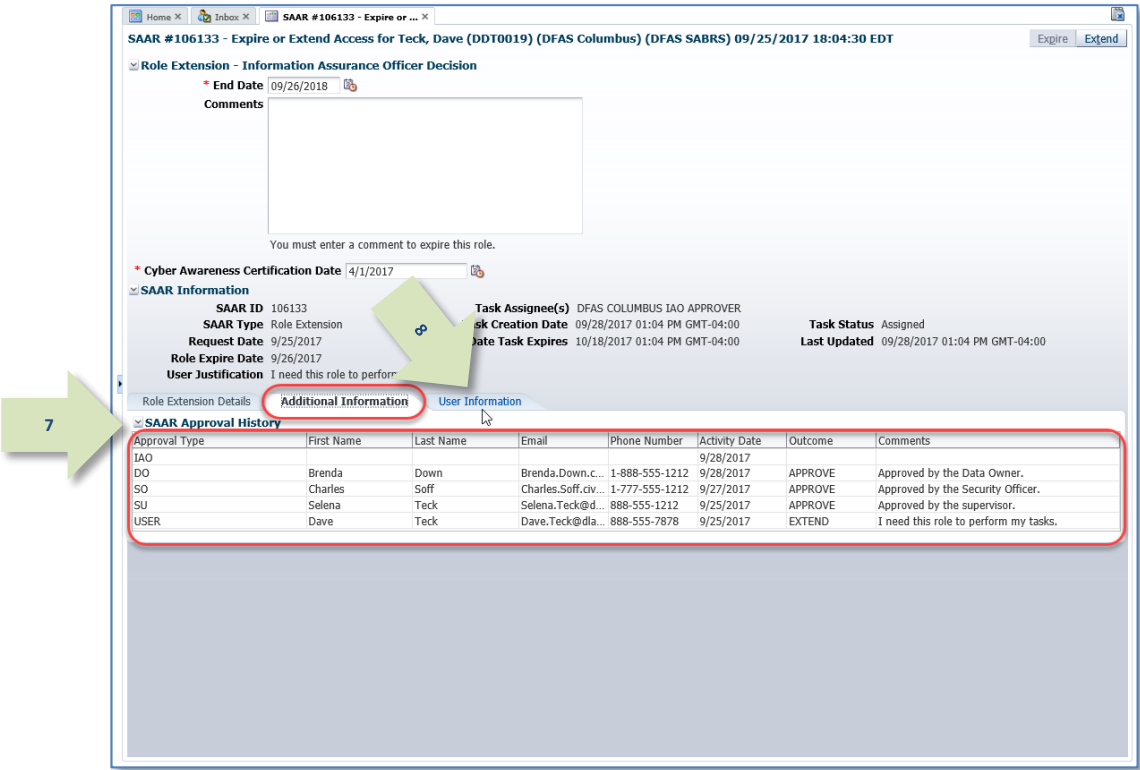
Figure 401: Role Extension Approval – IAO Decision –Additional Information

9. In the **User Information** screen, review the user's account, contact, organization, and supervisor information. **Current Roles** and **Pending Requests** are provided for additional review.

10. As an option, enter text in the **Comments** area.

   *Comments are not required to extend a role. Text in the Comments area is required ONLY to activate the **Expire** button if you want to allow this user's access to expire.*

   *However, AMPS maintains a record of approver comments in the **SAAR Approval History** table, located on the **Additional Information** screen, after each approval stage is completed.*

11. Click **Extend** to complete the SAAR approval process.

   AMPS saves the response to the SAAR record.

   *You can remove the completed SAAR from the **My Tasks** list by clicking the Refresh button on the **My Tasks** screen.*

Note:

The comment provided is for illustration purposes only. Please enter specific content related to the IAO role extension decision.
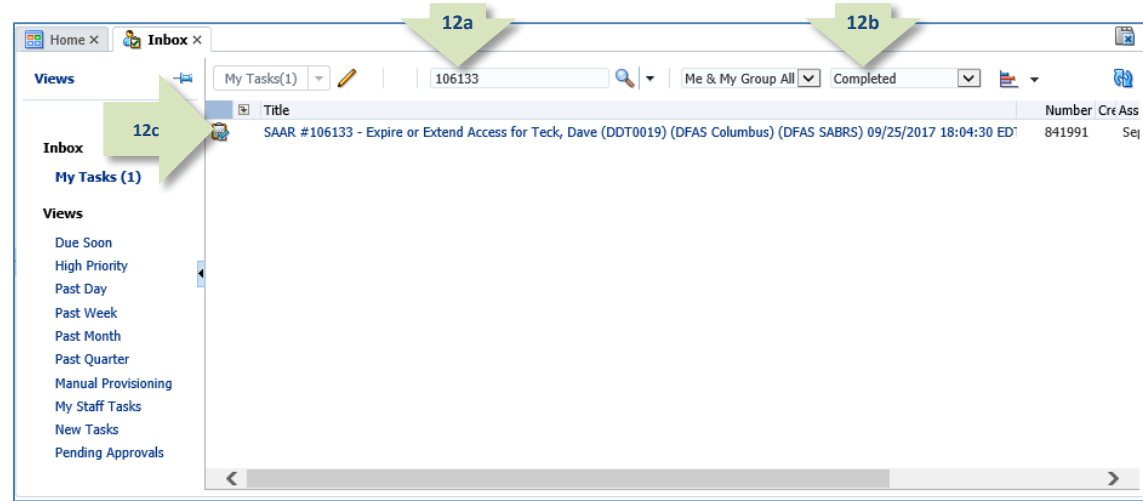

Figure 402: Role Extension Approval – IAO Decision – User Information

12. **OPTIONAL:** Follow these steps to view the completed decision screen, as needed:

    a. In the **Search** field, enter the SAAR number for the decision screen you want to review.

    b. In the **Status** dropdown list, select either **Any** or **Completed**.

    *AMPS automatically displays the specified SAAR in the **Title** column.*

    c. Click the SAAR title to review the SAAR decision screen (not shown).
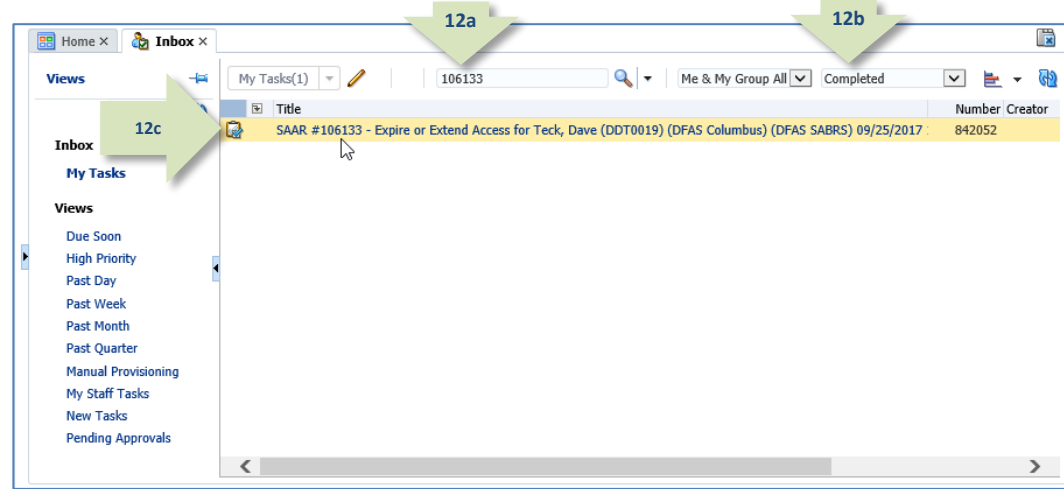
Figure 403: Role Extension Approval – Information Assurance Officer Post-decision

13. Following the Information Assurance Officer's approval of an extension request, the user receives an email notification indicating the outcome of the Information Assurance Officer's decision.
    (A sample is shown at right.)

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: The Information Assurance Officer has completed an approval for SAAR #106133.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

14. Following the Information Assurance Officer's approval of an extension request, the user also receives an email notification indicating that the role extension request approval process is complete.
    (A sample is shown at right.)

    The role has been extended, and no further action is required.

Subject: Notification: SAAR #106133 - Expire or Extend Access for Dave Teck (DDT0019) (DFAS Columbus) (DFAS SABRS) 09/25/2017 18:04:31 EDT

Body: Your request to extend role DFAS SABRS Prod - DFAS General User SABRS-014 with access to DFAS SABRS (SAAR 106133) has been processed.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Annual Account Revalidation

DLA management has established a requirement for AMPS to provide a function to support the revalidation of accounts on a yearly basis. DLA's AMPS team introduced this function in release 17.2.0. The AMPS function that supports the revalidation business process is called Annual Account Revalidation (AAR). DLA's AMPS team can extend the practice of Annual Account Revalidation through AMPS to organizations other than DLA, such as DFAS, which have applications managed in AMPS.

Using account data, AMPS automates the process of revalidating all of a user's accounts: AMPS and application accounts are included in the revalidation request. Revalidation of application accounts requires participation by all civilian employees, military personnel attached to an AMPS-participating organization, contractors working for these organizations, and any other users who have accounts in an organization's Active Directory (AD) domain.

The following users are exempt from annual revalidation:

- External users who do not have an Active Directory account with an AMPS-participating organization are exempt by definition.
- DFAS users who hold DLA accounts and roles are exempt from the DLA portion of the annual account revalidation process.

The following sections describe the annual account revalidation process and the concepts that support it.

Account Revalidation Requests

The process of requesting revalidation of an account in AMPS is referred to as the **Account Revalidation Request Process** (ARRP). This process refers to the issuance of an Annual Revalidation Request (ARR) and to the approval of that request through an approval subprocess. The process requires the user's Supervisor and an organizational Security Officer to review and approve the request.

Annual revalidation of each user's account is triggered by an Annual Revalidation Date (ARD), which is defined at account setup in AMPS. The initial ARD occurs approximately one year from each user's start date, and is updated based on the completion date of a successful AAR.

At 70 days in advance of the ARD, AMPS creates a revalidation SAAR and sends the SAAR information inside the first email notification to you, the account holder. The notification tells you to log in to AMPS and check the **Inbox** screen for a revalidation task.

The revalidation request submitted by the user in AMPS contains the following data:

- **User identification data:** the user's ID, name, DoD Identification Number (or EDIPI), and other data associated with the user's identity.
- **User Information:** the data found in the user's **My Information** page.
  - **Contact Information:** the same modifiable and required fields as those included in the AMPS **My Information** screen.
  - **Supervisor:** modifiable with a Supervisor selection utility.
  - **Organization:** modifiable with an Organization selection utility.

A user can modify most of this information. As a rule, the same data that is modifiable in the **My Information** screen's **User Information** tab is also modifiable in the user's revalidation request.

The revalidation request further provides a list of roles currently held by the user. **The user does not need to provide any action to retain roles currently held.** However, the user can select one or more roles for removal if they are no longer needed. When the user submits the revalidation request, AMPS takes the following actions on roles:

- Automatically submits the currently held roles with the revalidation request to the Supervisor for approval of retention. AMPS does not generate a provisioning task for retained roles. The submission of the approved revalidation request is confirmation that the roles should be retained, and no additional approvals are necessary.
- Generates deprovisioning tasks (including tickets) as necessary for roles the user selected for removal if removal is approved.

Time Limits

AMPS imposes time limits that determine how long an annual revalidation request can remain current before the system halts the request process and removes the user's application roles due to inaction on the part of the user or an approver. These time limits prevent a request from remaining current without action for an indefinite period. The options for user and approver actions expire due to these time limits, and the system terminates the account revalidation request.

Standard Revalidation Period: 70 Days

The initial ARR notification starts the standard revalidation period of 70 days. This 70-day period covers the amount of time allotted to a user to submit a revalidation request, plus the amount of time allotted to each approver who must process the request and revalidate the user's account. During this period, either a revalidation request moves forward to the end of the approval process or AMPS terminates the request due to inaction.

User's Time Limit

You, as an AMPS user, are allotted 20 days from the date of the initial email notification to respond to a revalidation request. However, if you do not act on your revalidation request within the 20-day period, AMPS forwards the request to your AMPS Supervisor.

User's Options

During the user's 20-day response period, the user has the following options:

With this option ...	The User ...
Submit a revalidation request.	Sends the revalidation request to the Approval process, in which the Supervisor and Security Officer review and act on the request: • If the Supervisor and the Security Officer approve the request, AMPS revalidates the account. • If the request is approved by the Supervisor and qualifies for an automated Security Officer approval, AMPS revalidates the account.
Allow a revalidation request to lapse after 20 days.	Takes no action: • AMPS sends the revalidation request to the user's AMPS Supervisor for action. • The Supervisor may approve the request or allow the request approval task to lapse.

Supervisor's Time Limit

A Supervisor has 20 days to respond to an ARR. During this time, the Supervisor has the following options:

- Before the 20-day period expires, the Supervisor can approve the request.
- Before the 20-day period expires, the Supervisor can reject the request.
- The Supervisor can allow the request approval task to time out.

If the Supervisor fails to act within 20 days, AMPS takes the following actions:

- Removes all the application roles in the user's AMPS account,
- Generates role removal tasks and tickets for all currently held roles,
- Marks the request as "rejected,"
- Leaves the AMPS account active and the AMPS Base User role intact,
- Updates the annual revalidation date on this account to 365 days from the current date.

Security Officer's Time Limit

A Security Officer has 20 days to respond to an ARR. During this time, the Security Officer has the following options:

- Before the 20-day period expires, the Security Officer can approve the request.
- Before the 20-day period expires, the Security Officer can reject the request.
- The Security Officer can allow the request approval task to time out.

If the Security Officer fails to act within 20 days, AMPS takes the following actions:

- Removes all application roles in the user's AMPS account,
- Generates role removal tasks and tickets for all currently held roles,
- Marks the request as "rejected,"
- Leaves the AMPS account active and the AMPS Base User role intact,
- Updates the annual revalidation date on this account to 365 days from the current date.

Approver's Options During the Revalidation Process

During the 20-day approval period, each approver has the following options when they receive a user's revalidation request:

With this option ...	The Supervisor ...	The Security Officer ...
Approve	Selects the **Approve** option to forward the request to the Security Officer, unless the request qualifies for an automated SO approval.	Selects the **Approve** option to revalidate the user's accounts.
Reject	Selects the **Reject** option to reject the request and begin the role removal process.	Selects the **Reject** option to reject the request and begin the role removal process.
Close	Closes the current revalidation request task without action.	Closes the current revalidation request task without action.
[No Action]	After 20 days have elapsed, AMPS automatically creates deprovisioning tasks to remove all roles assigned to the user and updates the ARD on the account.	After 20 days have elapsed, AMPS automatically creates deprovisioning tasks to remove all roles assigned to the user and updates the ARD on the account.

Note:

Some Security Officer revalidation approvals are subject to either a Security Officer bypass or an automated approval. See the sections entitled Security Officer Approval on page 165 or Security Officers: Internal and External SO Review Requirements on page 124 for more information.

Security Officer Automated Approval

For DLA roles, AMPS can apply an automatic Security Officer approval to a request that meets specific criteria. The automatic approval speeds the approval process for role requests that present no specific content requiring an immediate security review.

AMPS can automatically apply an approval for a Security Officer, if all of the following conditions are met:

- The IT level of roles requested for retention do not exceed the current IT level of the user.
- The user has a value recorded for the four clearance-related fields that AMPS tracks, including the following fields:
  - Security Clearance
  - IT Level, or Position Sensitivity
  - Background Investigation Type
  - Last Investigation Date
- The user's recorded IT level satisfies one of the following conditions:
  - If the user's IT level is IT1 or IT2, the date of the user's investigation must be less than 5 years old, or . . .
  - If the user's IT level is IT3, the date of the user's investigation must be less than 10 years old.
- The requestor is a member of the DLA organization or any organization under DLA.

When an automatic approval occurs, AMPS logs the automatic approval with the following data:

- The approver's user ID, normally reported in the audit logs, will be blank.
  - The Status recorded in the audit logs will be "AUTOAPPROVE."
  - AMPS enters the following statement to this effect, subject to government change and approval:

    "This request has been automatically approved by AMPS, per the conditions specified by the DLA CIO (the Designated Approving Authority (DAA)) per the DLA Account Management Policy signed 6 Nov 2014."

AMPS tests each request for a combination of these conditions. Those requests that meet the conditions are assigned an automatic Security Officer approval, because all conditions for an approval have been met.

About SIPR and NIPR Roles in Annual Account Revalidation

AMPS does not differentiate between a user with SIPR roles and a user with NIPR roles. When a Supervisor or Security Officer allows an AAR to lapse, AMPS removes all application roles from the user's AMPS account, but leaves the AMPS account active and leaves the Base User Role intact. The User's account remains in AMPS until the Offboarding process removes it.

Only the Offboarding process is used to delete a user's AMPS account. During a successfully completed revalidation SAAR, AMPS removes only application access roles that are submitted for removal by the user or subsequent approvers.

How to Submit a Revalidation Request

Each revalidation request begins with an email notification sent to the user. The notification in Step 1 provides a sample.

The recipient follows the procedure outlined in this section to perform the following tasks in response to this notification within 20 days of receiving it:

- Launch AMPS.
- Open the revalidation request listed in **Inbox** (see Figure 405).
- Respond to the request by identifying roles that should be removed, if any.
- Submit the response to the annual revalidation request approval process.

This procedure applies to . . .	All AMPS internal DLA users. (External user accounts are not subject to the revalidation requirement.)
What You Can Do	This procedure enables **you, as an AMPS end user**, to submit a request to revalidate your AMPS account and all managed accounts in other systems.
BEFORE You Begin . . .	**Ensure your Cyber Awareness Certification training is up to date. You must have completed Cyber Awareness training within one year of the current date. If you have not met this requirement, *STOP* and obtain the certificate before you begin the revalidation process.**
Where to Start	70 days before your annual revalidation date, AMPS automatically notifies you that your account must be revalidated. **If you do not respond by submitting a revalidation request, AMPS submits the AAR to your Supervisor for a decision.**

1. Read the email notification regarding your pending **Annual Account Revalidation** (**AAR**) action, and follow the instructions listed.

   After you log in to AMPS, the system displays the **Self Service Home** *page, which displays the appropriate clickable tiles (see Figure 404).*
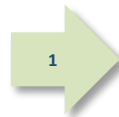
Sample Annual Account Revalidation (AAR) Notification

Subject: Action Required: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body:

Your AMPS and system access accounts are due for annual revalidation. A revalidation request in SAAR 106325 was automatically submitted on 10/11/2017 13:52:01 UTC to your AMPS account for your attention. You have 20 days to review and submit your Annual Revalidation Request (ARR).

To complete your Annual Revalidation Request task, please visit AMPS at this URL: https://amps.dla.mil/.

1. Log in to AMPS and open the AMPS Inbox screen.
2. Review AMPS Inbox to locate and open the revalidation SAAR.
3. Read the SAAR information. If the SAAR lists roles you no longer require, you can choose one or more roles to be removed from your accounts.
4. Click the Submit button to send your Annual Revalidation Request to your Supervisor for approval.

NOTE: This task expires on 10/31/2017 12:52:07 UTC If you do not take action on or before this date, your Supervisor will be notified and your accounts and roles may be disabled.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

AMPS issues reminder notifications periodically if you do not respond to the initial notification within one day.

Sample AAR Reminder Notification

Subject: Reminder Notifications: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body: Your AMPS and system access accounts are due for annual revalidation. A revalidation request in SAAR 106282 was automatically submitted on 10/06/2017 17:10:16 UTC to your AMPS account for your attention. You have 20 days to review and submit your Annual Revalidation Request (ARR).

To complete your Annual Revalidation Request task, please visit AMPS at this URL: https://amps.dla.mil/.

1.　Log in to AMPS and open the AMPS Inbox screen.

2.　Review AMPS Inbox to locate and open the revalidation SAAR.

3.　Read the SAAR information. If the SAAR lists roles you no longer require, you can choose one or more roles to be removed from your accounts.

4.　Click the Submit button to send your Annual Revalidation Request to your Supervisor for approval.

NOTE: This task expires on 11/05/2017 16:10:37 UTC If you do not take action on or before this date, your Supervisor will be notified and your accounts and roles may be disabled.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2.　After you log in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

*AMPS displays the **Inbox** and the **My Tasks** view, which lists tasks for the current user (see Figure 405).*
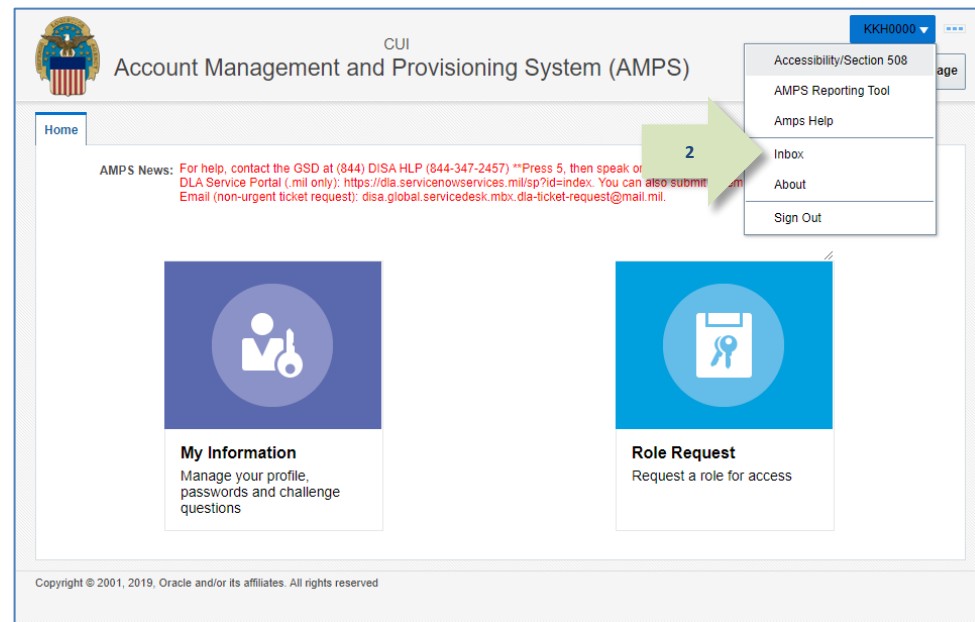
Figure 404: Annual Account Revalidation – *Inbox* Command

3.　In the **My Tasks** view, locate the SAAR for the annual revalidation in the **Title** field.

4.　Click the SAAR **Title** to start the revalidation process.

If this occasion is your first annual revalidation request, AMPS displays the **Standard Mandatory DoD Notice and Consent Agreement**. *See the next step in this procedure for more information.*
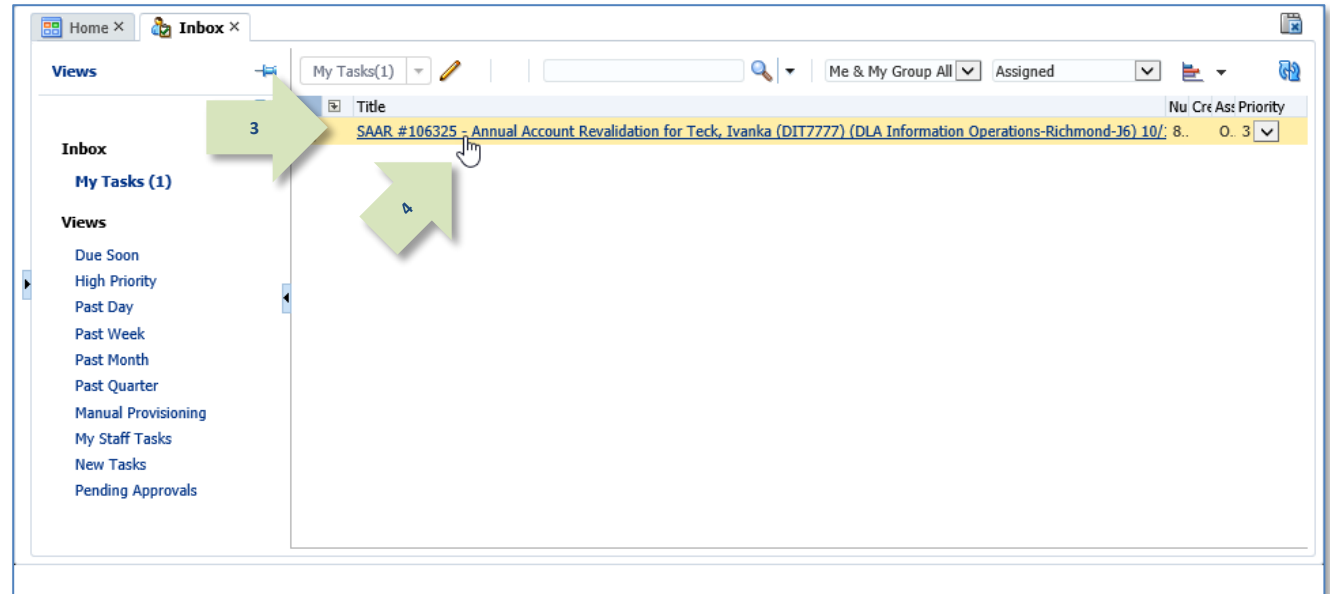

Figure 405: Annual Account Revalidation – Inbox, My Tasks

5. Conditional Step:
    If AMPS displays the **Standard Mandatory DoD Notice and Consent Agreement**, read the agreement first.

    As an option, you can print the page and retain a hard copy of the agreement by clicking the Print button.

6. Conditional Step:

    After reading the agreement, click the **I Accept** button to acknowledge the conditions and agree to comply with them.

    See the **AMPS User Guide, Appendix A,** *to read and review the full text of the* **Standard Mandatory DoD Notice and Consent Agreement** *(also called the* **Consent to Monitoring** *or CTM).*

    AMPS maintains a record of the date you accept the terms of this agreement.

    After you click **I Accept***, AMPS displays the* **General Rules of Behavior** *screen.*

Figure 406: Consent to Monitoring

7. Conditional Step:

    If AMPS displays the **General Rules of Behavior** (GROB), read the agreement first.

    As an option, you can print the page and retain a hard copy of the agreement by clicking the Print button.

8. Conditional Step:

    After reading the agreement, click the **I Accept** button to acknowledge the rules and agree to comply with them.

    See the **AMPS User Guide, Appendix A,** *to read and review the full text of the* **General Rules of Behavior**.

    AMPS maintains a record of the date you accept the terms of this agreement.

    After you click **I Accept***, AMPS displays the* **Annual Revalidation Request** *screen (see Figure 408).*

Figure 407: General Rules of Behavior

9. Note the SAAR ID, SAAR Type, and other information to verify you have opened the Annual Revalidation request.

   *Note the optional **Comments** text area. You can enter text to support or clarify the revalidation request, especially to explain a request to remove a role.*

   If you need to close the request temporarily and return to it later, click the tab close icon (X).

10. Check the **User Account Information** and **User Contact Information** sections to ensure all required fields have correct entries. Modify the required fields, as needed.

    a. *Required fields are marked with an asterisk (***). If any required field lacks an entry, AMPS displays an error message when you try to submit the request.*

    b. *The **Cyber Awareness Certification Date** is a nonmodifiable field. If the **Cyber Awareness Certification Date** exceeds one year past the current date, AMPS displays an error message when you try to submit the revalidation request. Ensure your Cyber Awareness training is up to date **before** you request a revalidation.*

    c. *You are no longer required to enter your date of birth in the **Date of Birth** field. AMPS no longer collects this information.*

Figure 408: AMPS Annual Revalidation Request Screen

11. Review the list of current roles in the **Revalidate User Roles** section to see all roles assigned to you (see Figure 409). As an option, follow these steps to request removal of any role you no longer use or need:

   - Select any application role you want to remove from your account.

   - Click the right arrow (→) button (a.k.a. Add button) to move the role name to the **Roles to Remove** list.

     If you move a role by mistake, select the role in the **Roles to Remove** list and use the left arrow (←) button (a.k.a. Remove button) to return the role name to the **Current Roles** list.

12. Click **Submit** (see Figure 408).

   *AMPS closes the revalidation request and returns to the **My Tasks** list.*

   AMPS submits the revalidation request to the approval process and notifies you of its progress.
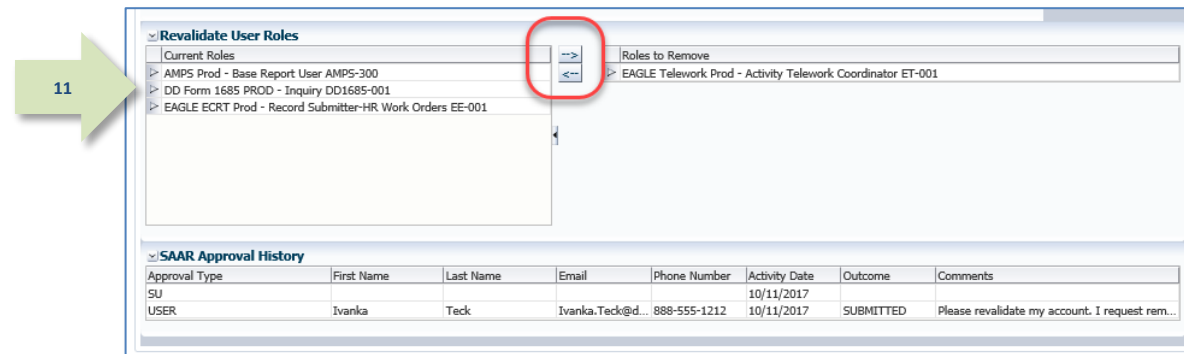
Figure 409: Annual Revalidation Request - Revalidate User Roles

13. On the **My Tasks** view of your Inbox, the SAAR for the annual revalidation will still be listed after you finish submitting the revalidation.

   To remove the SAAR from the list, click the Refresh icon on the **My Tasks** command bar.
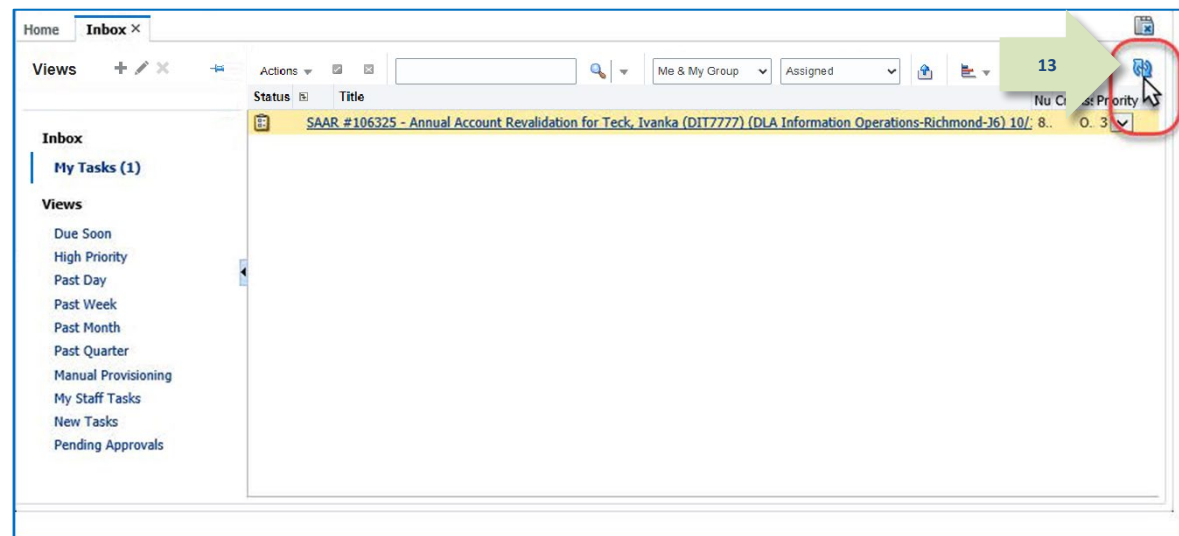
Figure 410: My Tasks - Refresh Button

14. Check email notifications to determine the progress of the revalidation request in the approval process.

    (A sample is shown at right.)

Note:

AMPS notifies the user through email of the following events:

- The revalidation request SAAR awaits Supervisor approval.

- The revalidation request SAAR has been approved by the Supervisor.

- The revalidation request SAAR awaits Security Officer approval, if a security information review is required.

- The revalidation request SAAR has been approved by the Security Officer.

- The revalidation request has been fully approved, and the account has been revalidated.

Subject: Notification: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body:

SAAR #106325 is awaiting Supervisor approval.

This request was submitted in AMPS on 10/11/2017 13:52:01 UTC.

No action is required from you at this time.

This task expires on 10/31/2017 14:01:59 UTC.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

How to Approve a Revalidation Request

AMPS Supervisor: Approval Procedure

This procedure applies to . . .	The requestor's AMPS Supervisor. If your request requires a Security Officer review, AMPS forwards the request to the appropriate Security Officer group following the Supervisor's approval. Review and approval instructions for the Security Officer are also provided in this section.
What You Can Do	This procedure enables you, as an AMPS Supervisor, to perform these tasks: • Submit an approval decision for a revalidation request submitted by an AMPS direct report. • Allow the revalidation approval task to lapse, thus beginning the process of removing roles from the account.
Where to Start	70 days before the user's annual revalidation date, AMPS automatically notifies the user that his or her account must be revalidated. After the user submits an account revalidation request, AMPS automatically submits the request to an approval process that starts with the user's AMPS Supervisor. AMPS notifies the Supervisor that an approval action is pending. The Supervisor has 20 days to respond to a pending AAR action. The Supervisor first opens and reads the email notification before proceeding. **If you allow the revalidation request to lapse (you take no action during the 20-day revalidation approval period), the user's roles and application account accesses will be removed. The user whose roles are removed through this process must submit new requests for roles.** **Do NOT allow the revalidation request to lapse unless the user does not need the access privileges provisioned through the application roles. The user's AMPS account is not disabled or deleted. A user's account is deleted ONLY during the Offboarding process, which takes place when a user leaves employment.**

1. Read the email notification regarding a pending **Annual Account Revalidation** (**AAR**) approval action, and log in to AMPS.

   *AMPS displays the **Self Service Home** page with the appropriate clickable tiles (see Figure 411).*

Sample Annual Account Revalidation Notification

Subject: Action Required: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

1

.... #106325 - Annual Account Revalidation for Teck, Ivanka (DIT7777) (DLA Information Operations-Richmond-J6) has been submitted for approval.

This request was submitted in AMPS on 10/11/2017 13:52:01 UTC.

Please visit AMPS at this URL

https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the approval task. This task expires on 10/31/2017 14:01:59 UTC.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After logging in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

    AMPS displays the **My Tasks** *view, which lists requests assigned to you (see Figure 412).*

Figure 411: Annual Account Revalidation – User ID Dropdown Menu – Inbox Command

3. In the **My Tasks** view, locate the SAAR for the annual revalidation in the **Title** field.

4. Click the SAAR **Title** to open the revalidation approval task.

    AMPS displays the **Annual Revalidation – Supervisor Decision** *screen (see Figure 413).*
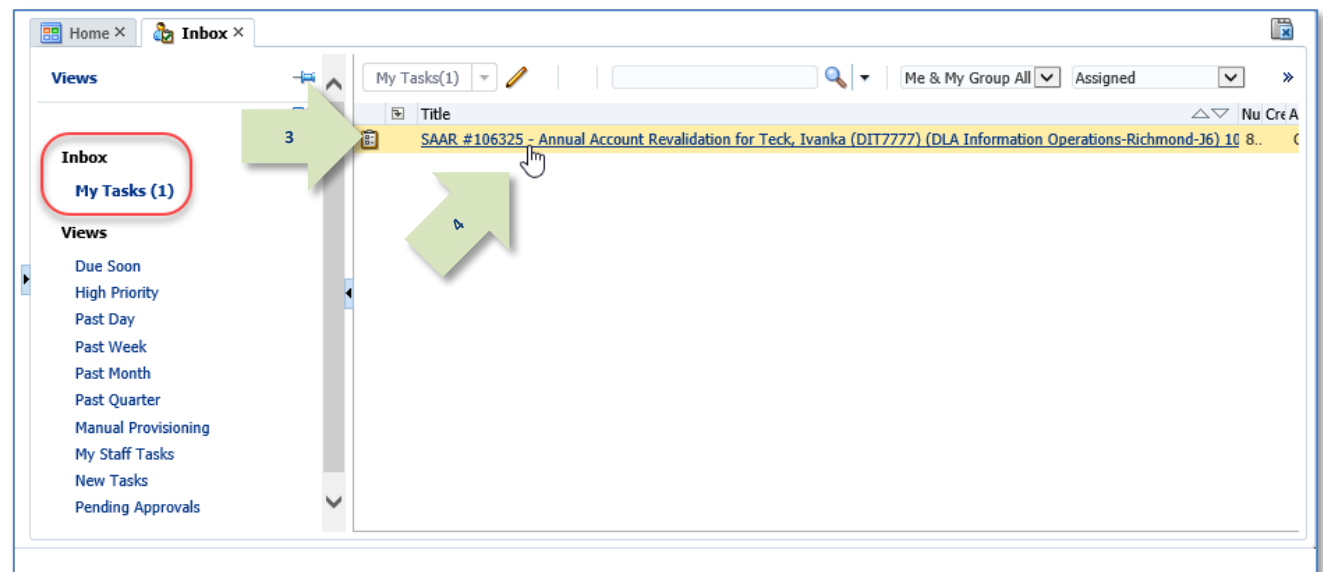
Figure 412: Annual Account Revalidation – Inbox, My Tasks

5. In the **Annual Revalidation Details** section, review the **User Summary** data.

6. Check the **Revalidate User Roles** section to ensure current roles are appropriate and any role request removal is justified:

   - In the **Current Roles** list, check each role to ensure the user should retain the role as assigned. If a role should be removed from the user's account, follow these steps:
     a. Click the role name to select it.
     b. Click the right arrow (→) button to move the role to the **Roles to Remove** list. After the approval is complete, this action generates tasks to remove the roles selected for removal.

   - In the **Roles to Remove** list, check roles, if any are listed, to ensure the roles should be removed from the user's account. If a role *should not* be removed, follow these steps:
     a. Click the role name to select it.
     b. Click the left arrow (←) button to move the role back to the **Current Roles** list.

7. Click the **Additional Information** tab.

   AMPS displays a **SAAR Approval History** *table (see Figure 414).*

Figure 413: Annual Revalidation Request - Supervisor Decision- Annual Revalidation Details

8. In the **Additional Information** tab, review the **SAAR Approval History**.

   Comments added by the user appear in the **Comments** *column of the approval history table.*

9. Click the **User Information** tab.

   AMPS displays the following data:
   - *User's account information*
   - *User's contact information*
   - *User's Organization and Supervisor*
   - *User's current roles and pending role requests*

   See Figure 415 for a sample.

Figure 414: Annual Revalidation - Supervisor Decision - Additional Information

10. In the **User Information** tab, review the information.

11. To add a comment to the SAAR record, enter text in the **Comments** text area. A comment is not required to approve the request. You must enter a comment if you want to reject the request.

    When you enter a comment, AMPS activates the Reject button.

12. Submit your decision by performing one of the following actions:

    a. Click the **Approve** button to send the revalidation request to the next step in the process.

    AMPS closes the approval screen, notifies the user of your decision, and forwards the request to the Security Officer as necessary.

    b. Click the **Reject** button to reject the revalidation request.

    AMPS closes the approval screen, marks the request as "rejected," and starts the role-removal process.

Figure 415: Annual Revalidation - Supervisor Decision - User Information

After the Supervisor completes an approval task for a revalidation request, AMPS sends an email notification to the user indicating that the Supervisor approval has been completed.

The outcome for the Supervisor's decision is included in this notification.

For DLA internal user requests, a Security Officer must review a revalidation request when any of the following conditions are met:

- *The requestor's account is flagged for Security Officer review.*
- *The requestor's position sensitivity level is IT2 or IT1, and any current role's level exceeds the requestor's IT level.*
- *The requestor's record is missing values for any of the security clearance fields that AMPS tracks (see Figure 418 for a sample view of the value fields).*
- *The requestor's last investigation date is more than five years old, if the requestor's IT level is IT1 or IT2.*
- *The requestor has one or more DFAS roles. The DFAS Security Officer must review and approve the role request.*

If the revalidation request must undergo a review by a Security Officer, AMPS also sends an email notification to the user indicating that the revalidation request SAAR awaits Security Officer approval.

Sample ARR Approval Notifications to the User

Subject: Notification: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body:

The Supervisor has completed an approval for SAAR #106325.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Subject: Notification: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body:

SAAR #106325 is awaiting Security Officer approval.

This request was submitted in AMPS on 10/11/2017 13:52:01 UTC.

No action is required from you at this time.

This task expires on 10/31/2017 14:22:31 UTC.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

AMPS Security Officer: Approval Procedure

What You Can Do	This procedure enables you, as an AMPS Security Officer, to submit an approval decision for a revalidation request submitted by an AMPS end user. You can conduct a review of the user's security-related information and make the changes necessary to update the user's account.
Where to Start	70 days before the user's annual revalidation date, AMPS automatically notifies the user that his or her account must be revalidated.
	After the user submits an account revalidation request, AMPS automatically submits the request to an approval process that starts with the user's AMPS Supervisor.
	After the Supervisor approves an account revalidation request, AMPS automatically submits the request to a Security Officer in the approval process.
	AMPS notifies the Security Officer that an approval action is pending. The Security Officer has 20 days to respond to a pending AAR action.
	The Security Officer first opens and reads the email notification before proceeding.

1. Read the email notification regarding a pending **Annual Account Revalidation** (**AAR**) approval action, and log in to AMPS.

1

Sample Annual Account Revalidation Notification

Subject: Action Required: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body: SAAR #106325 - Annual Account Revalidation for Teck, Ivanka (DIT7777) (DLA Information Operations-Richmond-J6) has been submitted for approval.

This request was submitted in AMPS on 10/11/2017 13:52:01 UTC.

Please visit AMPS at this URL

https://amps.dla.mil/

Review your Pending Approvals to locate the SAAR and complete the approval task. This task expires on 10/31/2017 14:22:31 UTC.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

2. After logging in to AMPS, locate and click the **Inbox** command from the User ID dropdown menu.

   AMPS displays the **My Tasks** *view for the current Security Officer (see Figure 417).*
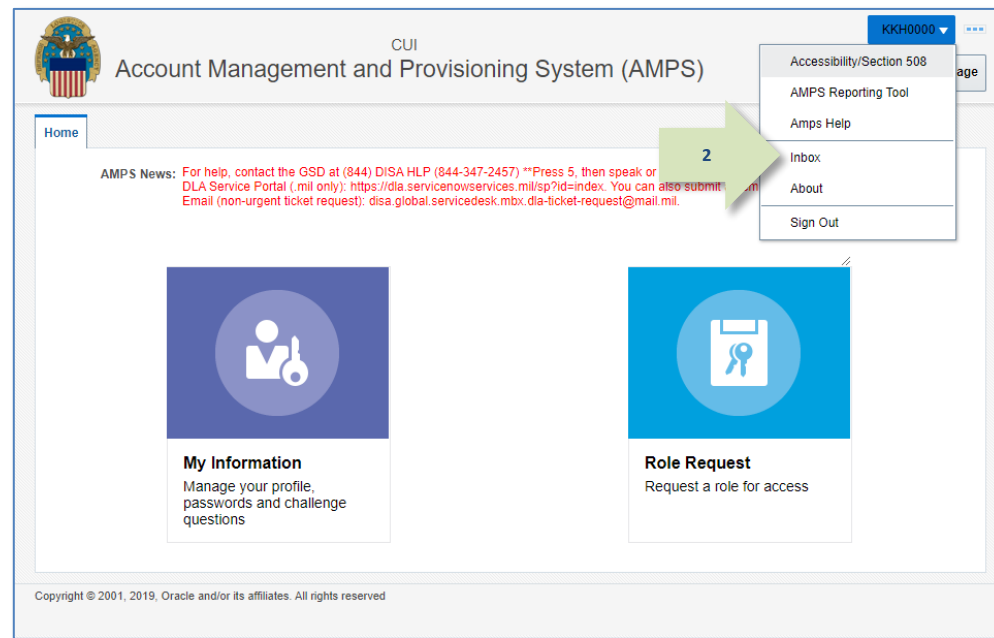
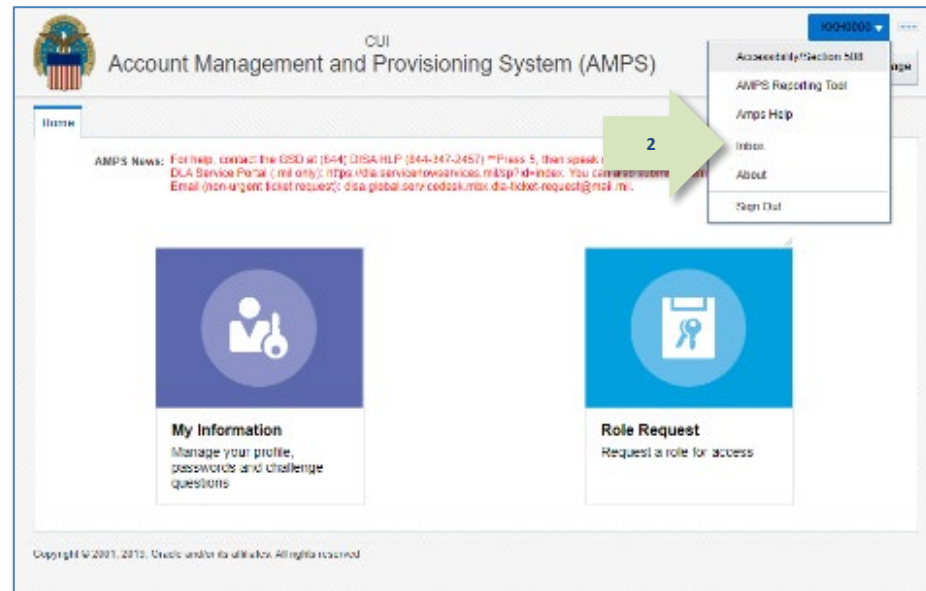**Figure 416: Annual Account Revalidation – User ID Dropdown Menu – Inbox Command**

3. In the **My Tasks** view, locate the SAAR for the annual revalidation in the **Title** field.

4. Click the SAAR **Title** to open the revalidation approval task.

   *AMPS displays the* **Annual Revalidation – Security Officer Decision** *screen (see Figure 418).*
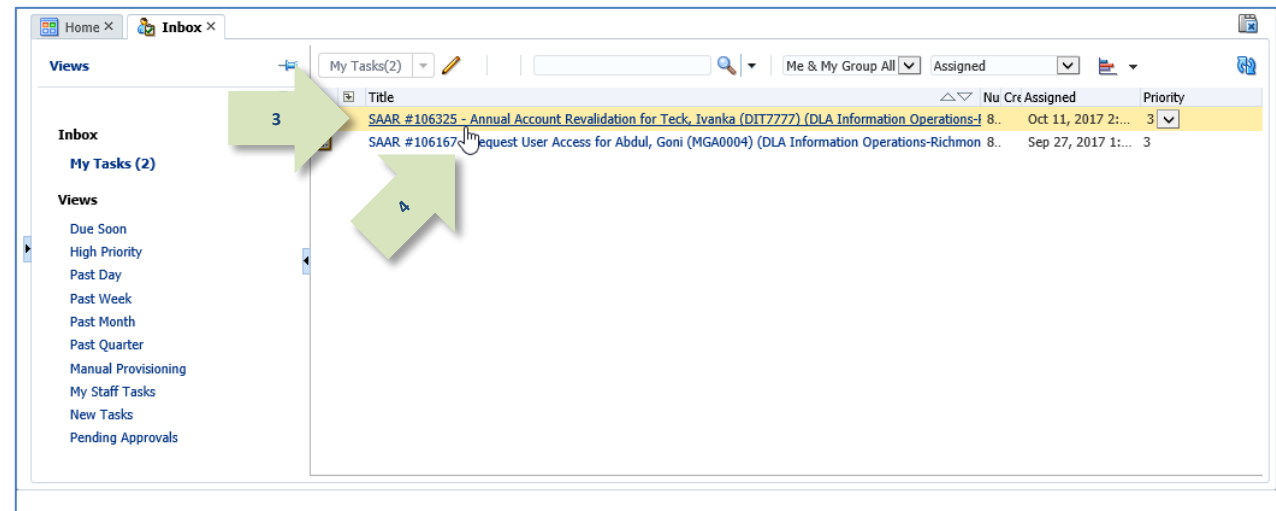
Figure 417: Annual Account Revalidation – Inbox, My Tasks

5. In the **Security Information** section, review the required fields and enter or update data, as needed.

6. Check the **Revalidate User Roles** section to ensure current roles are appropriate and any role request removal is justified:
   - In the **Current Roles** list, check each role to ensure the user should retain the role as assigned. If a role should be removed from the user's account, follow these steps:
     a. Click the role name to select it.
     b. Click the right arrow (→) button to move the role to the **Roles to Remove** list. AMPS will remove roles selected for removal from the user's account after the revalidation request has been fully approved.
   - In the **Roles to Remove** list, check roles, if any are listed, to ensure the roles should be removed from the user's account. If a role *should not* be removed, follow these steps:
     a. Click the role name to select it.
     b. Click the left arrow (←) button to move the role back to the **Current Roles** list.

   AMPS stores all entries and updates to the user's account record after the Security Officer **Approves** *the revalidation request.*

   AMPS does NOT save entries and updates if the Security Officer **Cancels** *the revalidation request.*

7. Click the **Additional Information** tab.

   AMPS displays the SAAR Approval History (see Figure 419).

Figure 418: Annual Revalidation - Security Officer Decision Screen

8. In the **Additional Information** tab, review the **SAAR Approval History**.

   *Comments added by the user and supervisor appear in the **Comments** column of the approval history table.*

9. Click the **User Information** tab.

   AMPS displays the following data:
   - *User's account information*
   - *User's contact information*
   - *User's Organization and Supervisor*
   - *User's current roles and pending role requests*

   See Figure 420 for a sample.

Figure 419: Security Officer Decision - Additional Information - SAAR Approval History

10. In the **User Account Information** section, review the user's personal, contact, organizational, and supervisor information.

    You can also review the user's **Current Roles** *and* **Pending Requests**.

11. To add a comment to the SAAR record, enter text in the **Comments** text area. A comment is not required to approve the request. You must enter a comment if you want to reject the request.

    When you enter a comment, AMPS activates the Reject button.

12. Submit your decision by performing one of the following actions:

    a. Click the **Approve** button to validate the account.

    AMPS resets the user's annual revalidation date to 365 days from the current date.

    If any roles are listed for removal on the **Annual Revalidation Details** *tab, AMPS generates the appropriate action to have the roles removed: either a removal ticket for ticketed-type roles is generated, or AMPS automatically deprovisions the role directly.*

    b. Click the **Reject** button to reject the revalidation request.

    AMPS closes the approval screen, marks the request as "rejected," and starts the role-removal process.

Figure 420: Security Officer Decision - User Information

AMPS sends the user an email notification indicating the Security Officer has completed the revalidation request.

The outcome of the Security Officer's decision is included in this notification.

Sample ARR Approval Notifications to the User

Subject: Notification: SAAR #106325 - Annual Account Revalidation for Ivanka Teck (DIT7777) (DLA Information Operations-Richmond-J6) 10/11/2017 13:52:01 UTC

Body:

The Security Officer has completed an approval for SAAR #106325.

The outcome for this task is APPROVE.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

---

AMPS sends the user an email notification indicating the request for removal of a role has been forwarded to an application provisioner for action.

*The user's new revalidation date is listed on the **My Information** screen for the user's account.*

Subject: AMPS Application Processing for SAAR #106325

Body:

AMPS application processing for SAAR 106325 has started for AMPS.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Total AMPS Provisioner: Role Removal

This procedure is for . . .	Total AMPS Provisioners who are deprovisioning the selected roles of users requesting revalidation or of users whose revalidation requests have timed out and are marked as "rejected."
What You Can Do	This procedure enables you, as a Total AMPS Provisioner, to remove one or more roles the user has specified for removal during an annual revalidation process.
Where to Start	70 days before the user's annual revalidation date, AMPS automatically notifies the user that his or her account must be revalidated. After the user submits an account revalidation request, AMPS automatically submits the request to an approval process that starts with the user's AMPS Supervisor. After the Supervisor and, optionally, the Security Officer have completed their approvals, AMPS notifies the application provisioners of any provisioning action that is pending. Total AMPS provisioning tickets do not have an expiration date. The Total AMPS provisioner should first open and read the email notification before processing the task.

1. AMPS sends the application's Provisioner an email notification indicating a SAAR has been submitted for (de)provisioning.

   The notification identifies the action as a role removal and identifies the resource and the role name.

Sample Provisioner Notification

Subject: AMPS Application Processing for SAAR #106325 requires your attention.

Body:

1

AMPS Application Processing request for SAAR 106325 requires your attention.

Please visit AMPS at this URL:
https://amps.dla.mil/

Open your inbox to locate the SAAR. Click the SAAR title to open and complete the task.

Task Details:
Request For:
DLA Login: DIT7777
Name: Teck, Ivanka
Phone: 888-555-1212
Email: Ivanka.Teck@dla.mil
EDIPI/UPN: 9999999999

Access Information:
SAAR #: 106325
Remove Job Role: EAGLE Telework Prod - Activity Telework Coordinator ET-001

Applications and Access:
        Resource: EAGLE Telework PROD - EAGLE Telework
                Remove: EAGLE Telework Prod - Activity Telework Coordinator

Justification: Please revalidate my account. I request removal of one role.
Optional Information: (none)
Annual Revalidation SAAR requested by AMPS on 10/11/2017

2. The Provisioner logs in to AMPS and clicks the **Inbox** command from the User ID dropdown menu.

   AMPS displays the **My Tasks** *view for the current Provisioner (see Figure 422).*
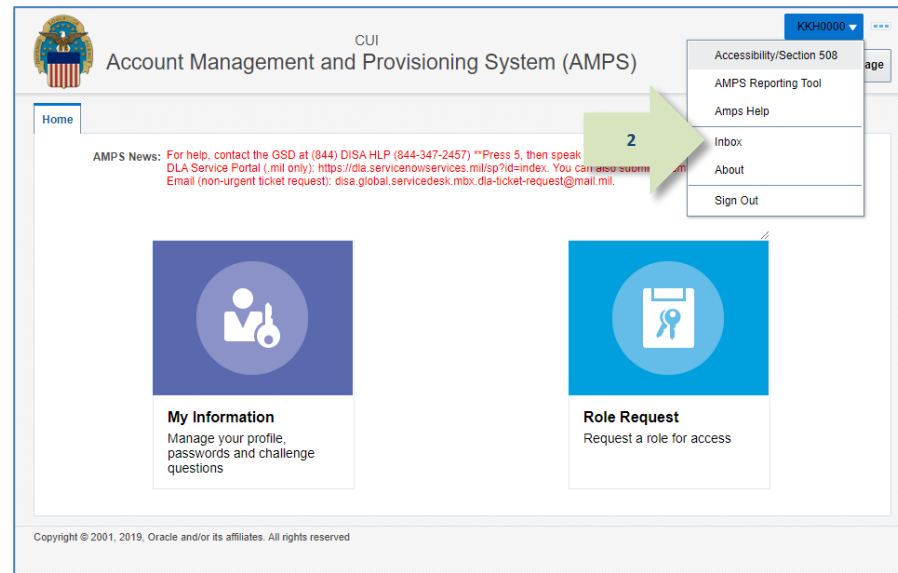
Figure 421: User ID Dropdown Menu – *Inbox* Command

3. The Provisioner checks the list of provisioning tickets listed in the **My Tasks** view.

4. The provisioner clicks the title of the SAAR that corresponds to the notification.

   AMPS displays the Total AMPS provisioning ticket for the SAAR.

Tip:
At this point, the provisioner checks the ticket details and uses the information to perform the requested provisioning or deprovisioning action.
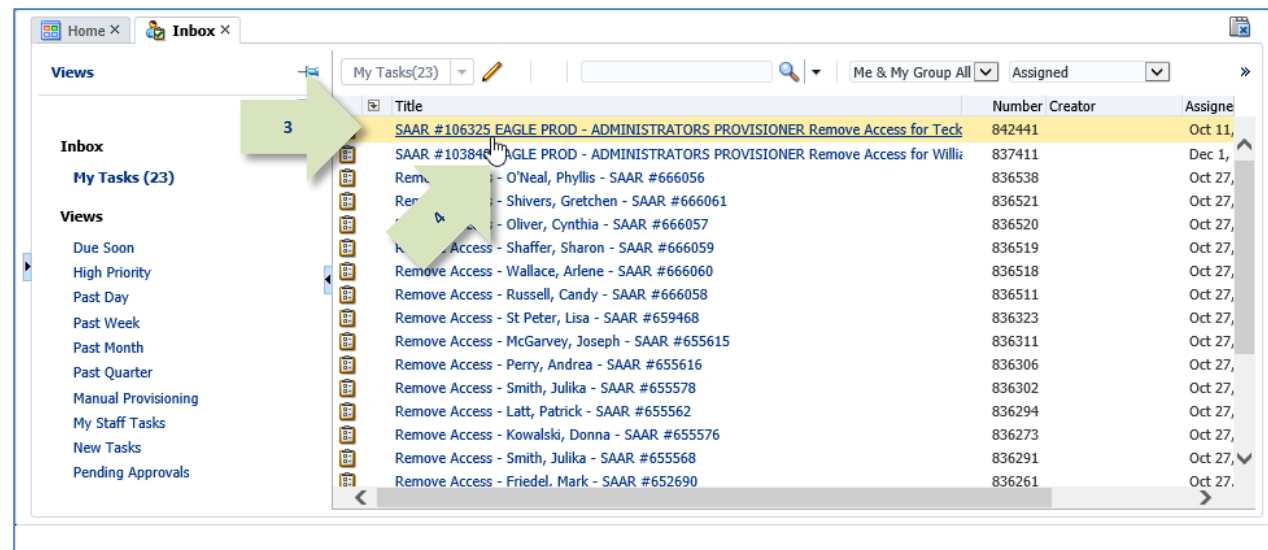
Figure 422: Sample Provisioner's Approval Details - My Tasks View

5. The Total AMPS ticket offers the provisioner these features. The provisioner can . . .

   a. Click the **Claim** button, and then enter comments and click **Save Comments** to preserve current work and maintain exclusive control over the ticket for three calendar days.

      AMPS saves and closes the request, enabling the provisioner to close and later reopen the incomplete ticket to perform the prescribed provisioning work.

   b. Enter comments and click **Save Comments** to preserve the Provisioning ticket. Reopen the ticket, as needed, to enter final comments in the required **Comments** text area.

   c. Click **Work is Complete** when provisioning is complete.

      AMPS closes the request.

      AMPS also moves a record into the user's **SAAR History** *indicating that the requested action is completed (see Figure 424).*

Figure 423: Sample Application Request Provisioning Ticket - Total AMPS

*AMPS lists the completed SAAR in the user's **Request History**.*

Figure 424: Provisioned User's Applications & Roles Tab – Request History

6. AMPS sends the user an email confirmation indicating that administrative staff have completed deprovisioning of the role.

Sample User Notification: Confirmation of Role Provisioning

Subject: AMPS Application Processing for SAAR #106325

Body:

Your Annual Revalidation Request (SAAR 106325) is now complete. All access specified for removal has been removed.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Supervisor's Tasks for Subordinates' Requests

Supervisors can monitor the role status of each "direct report" (also called a "subordinate") assigned to them in AMPS. The feature that enables Supervisors to monitor their direct reports is available through the **My Information** screen. When a Supervisor opens the **My Information** screen, AMPS displays a tab that provides access to a list of direct reports. From this tab, a Supervisor can perform the following tasks:

- See a list of direct reports.
- Click a direct report's User ID to view **Direct Report Details**.
- See the direct report's **User Information** in the **Direct Report Details** window.
- See the direct report's **Applications & Roles** tab.

Performing Tasks for Subordinates

The following subsections explain the procedures available to the Supervisor for performing the following tasks on behalf of a direct report:

- Submit a role request.
- Submit a request to update **Additional Attributes** for a specific role.
- Cancel a pending role request.
- Submit a request to remove a role from a subordinate's Current Roles.

How to View a Direct Report's Information

Users:	This procedure gives your Supervisor the capability to view your **User Information** and **Applications & Roles** screens.
Supervisors:	AMPS enables you to view a list of direct reports, view each user's role information and status, and submit certain requests on behalf of each direct report. Your direct reports, along with links to their user and role information, are listed on the **My Information** screen in the **Direct Reports** tab.

1. Log in to AMPS.

   *AMPS displays the **Self Service Home** screen and identifies the logged in user by ID.*

2. Click the **My Information** tile.

   *If this selection is your first request for **My Information** during the current session, AMPS displays a **Privacy Act Statement** appropriate for your organization (see **Appendix E, Privacy Act Statements**). Click **Accept** to proceed (not shown).*

   *AMPS displays the AMPS Supervisor's **My Information** screen with access to three tabs (see Figure 426: **My Information**):*

   - **User Information**
   - **Applications & Roles**
   - **Direct Reports**
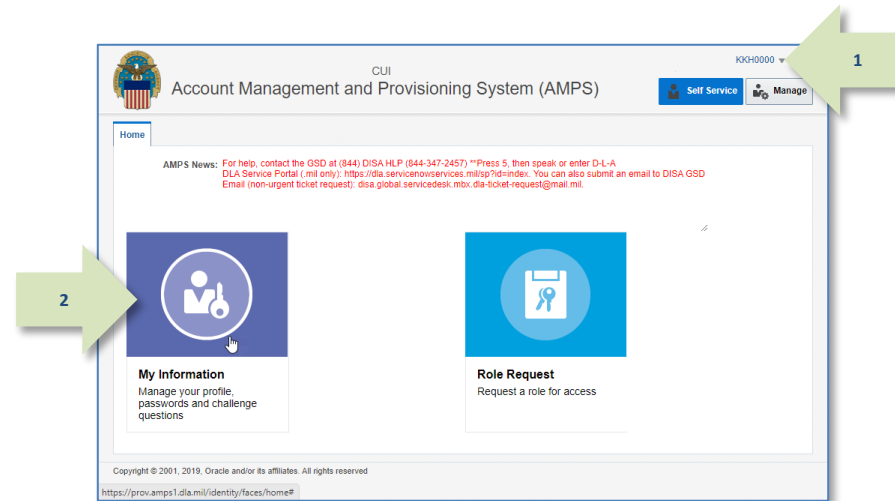
Figure 425: Self Service Home Page – *My Information* Tile

3. Click the **Direct Reports** tab.

    AMPS opens a tab that displays a table of all the direct reports assigned to the current Supervisor in AMPS (see Figure 427).

Figure 426: My Information

4. In the **Direct Reports** list, click the **User ID** of the direct report whose information you want to view.

    AMPS displays the **View Direct Report Details** *screen containing three tabs:*

    - **User Information**
    - **Applications & Roles**
    - **Direct Reports**

Figure 427: Direct Reports - Select a Direct Report

5.   Click the Applications & Roles tab.

*AMPS displays the user's **Applications & Roles** screen containing current and pending requests, as well as provisioned resources and SAAR history (see Figure 429).*

Figure 428: View Direct Report Details - User Information

The subordinate user's **Applications & Roles** *tab also provides the following functions to the user's Supervisor:*

- *Request a role for the subordinate.*
- *Remove a role for the subordinate.*
- *Edit additional role attributes for the subordinate.*
- *Cancel a request for the subordinate.*

The following sections outline and describe the procedures for these functions:

- How to Request a Role for a Direct Report.
- How to Cancel a Subordinate Role Request.
- How to Edit a Subordinate's Additional Attributes.
- How to Remove a Subordinate's Role.

Figure 429: Direct Reports - Applications & Roles Tab

How to Request a Role for a Direct Report

Users:	This role request procedure gives your Supervisor the capability to submit a role request on your behalf.
Supervisors:	AMPS enables you, a Supervisor, to request one or more roles for a subordinate who reports directly to you in AMPS. Your direct reports, along with links to their user and role information, are listed on the **My Information** screen in the **Direct Reports** tab.
	The process of requesting a role for a direct report follows the same sequence of screens as you follow when requesting a role for yourself. You have the same features available for requesting one or more roles, changing Primary Roles, adding optional information and up to three PDF file attachments to the request, and the same approval sequence. If you attach one or more documents, the attachments may not contain Personally Identifiable Information (PII). Notifications of the role request are sent to the user, rather than to you. However, you will receive the normal Supervisor notifications during the approval process.

1. In the **View Direct Report Details** screen, open the direct report's **Applications & Roles** tab.

2. In the **Current Roles** section, click the **Request Role** button.

   AMPS displays a **Privacy Act Statement** *appropriate to your organization (see* **Appendix E, Privacy Act Statements***). Read the statement and click* **Accept** *to proceed.*

   AMPS then displays the first in the sequence of role request screens, **User Information** *(see Figure 431).*
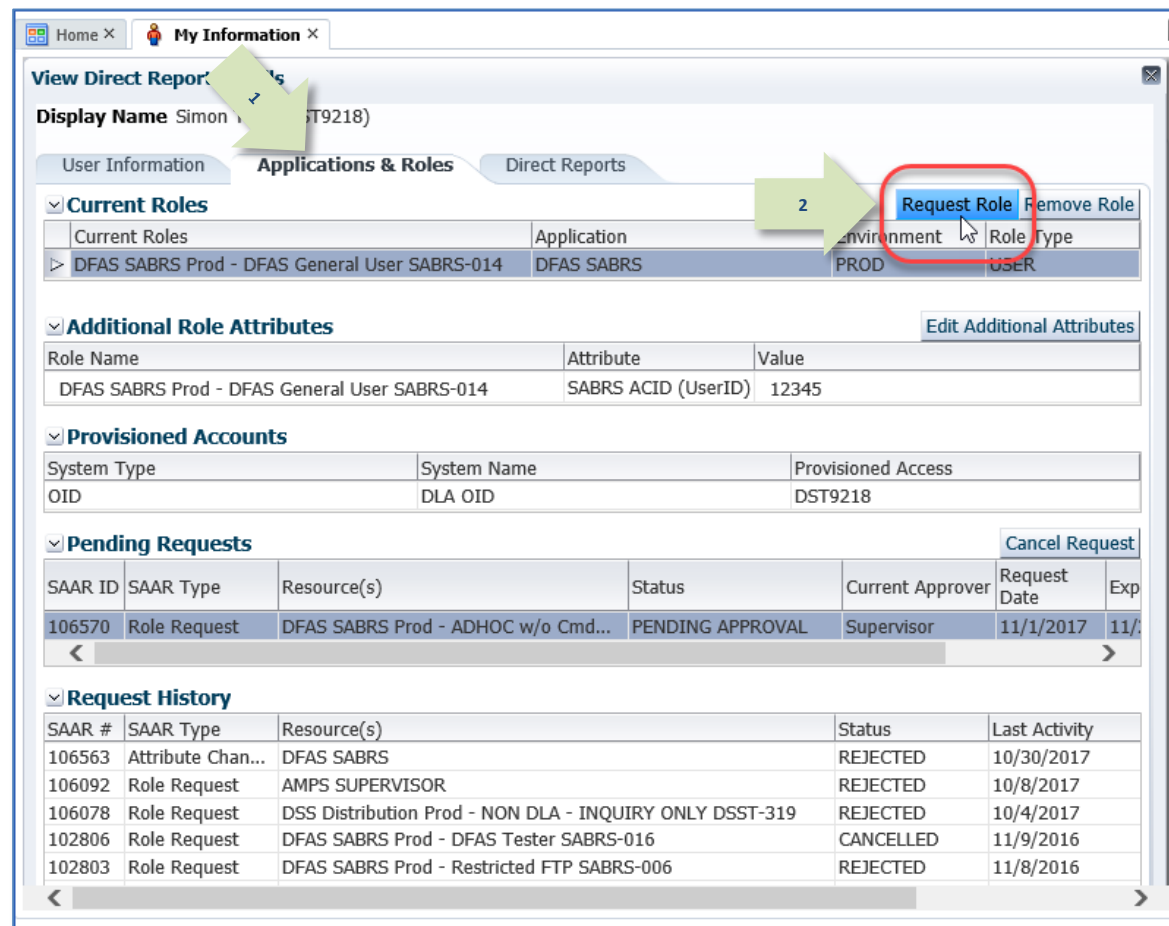
Figure 430: Subordinate's Applications & Roles Tab

3. In the **User Information** page of the **Request Role** screen, ensure that all required fields have entries.

   You no longer need to include the user's date of birth. AMPS no longer collects this data.

   Note that this screen is a nested screen, and it may not display the contents completely.

   ➢ *To correct the display, close the* **Request Role** *screen, and zoom out to approximately 85 percent.*

   ➢ *Then, click the* **Request Role** *button again.*

   ➢ *The contents of the resulting screen should fit correctly inside the nested screen area.*

   Required fields are marked with an asterisk (*****).

4. Click **Next** to proceed.

   If this request is the first in the current session, AMPS displays the Privacy Statement screen (not shown, see Appendix A).

   Click **Accept** *to proceed.*

   AMPS displays the **Select Roles** *screen (see Figure 432).*

Figure 431: Request Subordinate Role - User Information

5. In the **Select Roles** screen, use the search or browse features to locate and select a role.

6. Click on the role you want to select for the user and click the right arrow (→) button (a.k.a. the Add button) to move the role entry from the **Role Name** list to the **Selected Roles** list.

    You can repeat steps 5 and 6 to add more roles to this request. AMPS creates a SAAR for each role you identify in the Selected Roles list.

7. Click **Next** to proceed.

    *AMPS displays the **Justification** screen (see Figure 433).*

Figure 432: Request Subordinate Role - Select Roles

8. In the **Justification** screen, enter the appropriate text to justify the role request.

> **Note:**
> Comments shown in the sample screen are for illustration purposes only. Please enter information relevant to a specific request.

9. **Optional:** click the Browse button to search for and locate a supporting document to upload.

   Each attached document must be a PDF that is smaller than two megabytes in size.

   A supervisor can attach as many as three PDF documents that support the role request. However, none of these documents may contain any Personally Identifiable Information (PII).

10. Click **Next** to proceed.

    *AMPS displays the **Summary** screen (see Figure 434).*

Figure 433: Request Subordinate Role – Justification

11. In the **Summary** screen, review all entries for accuracy.

    *Use the **Back** button or the screen name links in the train to return to previous screens and make corrections, as needed.*

12. Click **Submit** to start the approval process for this request.

Figure 434: Request Subordinate Role – Summary

13. In the **Role Request Confirmation** screen, AMPS displays the SAAR number for the role request just submitted, along with the Role name and submission status.

You can note the SAAR number for reference, as needed for tracking purposes.

AMPS sends email notifications to the user advising the user of the request's status, and to each approver indicating an approval action is required.

14. Click **OK** to finish the role request.

Request a Role for Simon Teck

Role Request Confirmation

Your request has been submitted for approval. The following SAARs have been created:

SAAR   Role
106571 DFAS SABRS Prod - DFAS Tester SABRS-016

AMPS will notify you by email message regarding the status of each SAAR.

If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

OK

Figure 435: Request Subordinate Role - SAAR and Request Confirmation

15. After you click **OK** in the **Confirmation** screen, AMPS returns to the beginning of the role request process.

If you are finished with this process, click the **Close** button (**X** icon) in the upper right corner of the role request screen.

AMPS closes the role request screen and returns to the subordinate's **Applications & Roles** *tab in the* **View Direct Report Details** *screen.*

Figure 436: Request a Subordinate Role - Close the Role Request Screen

How to Cancel a Subordinate Role Request

Users:	This role cancellation procedure gives your Supervisor the capability to cancel a role request on your behalf.
Supervisors:	a subordinate who reports directly to you in AMPS. Your direct reports, along with links to their user and role information, are listed on the **My Information** screen in the **Direct Reports** tab.
AMPS enables you, the Supervisor, to remove one or more roles from	*Note:* You cannot cancel a request after it has entered the provisioning phase. (In this phase, the status field indicates the request is "TICKETED").
Where to Start:	Begin by logging in to AMPS, opening the **My Information** screen, and displaying the **Direct Reports** screen

1. In the **Direct Reports** list, click the **User ID** of the subordinate user whose information you want to view.

   AMPS displays the **View Direct Report Details** *screen containing three tabs:*

   - **User Information**
   - **Applications & Roles**
   - **Direct Reports**
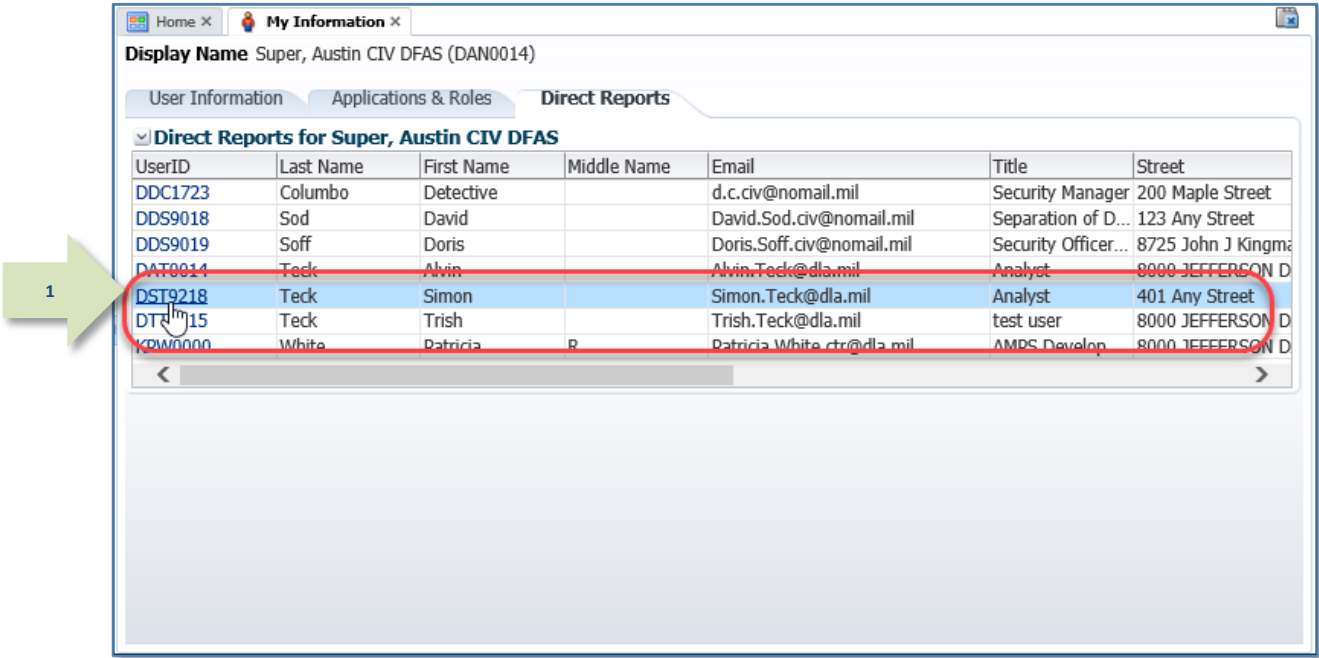
Figure 437: Direct Reports - Select a Direct Report

2. Click the Applications & Roles tab.

   AMPS displays the subordinate user's **Applications & Roles** *screen containing current and pending requests, as well as provisioned resources and SAAR history.*

3. In the **Pending Requests** table, locate and click the SAAR you want to cancel.

   AMPS highlights the SAAR record in **Pending Requests**.

4. Click Cancel Request.

   AMPS displays a confirmation message (see Figure 439).

Figure 438: View Direct Report Details - User Information

5.	To confirm the request cancellation request, click the **Yes** button.

AMPS displays an **Information** *message indicating the selected SAAR has been cancelled (see Figure 440).*

Figure 439: Cancel a Subordinate Role Request - Confirm the Cancellation

6. In the **Information** message box, click **OK** to acknowledge and close the message.

View Direct Report Details							

Display Name Simon Teck (DST9218)

User Information | **Applications & Roles** | Direct Reports

Current Roles   Request Role | Remove Role

Current Roles	Application	Environment	Role Type
▷ DFAS SABRS Prod - DFAS General User SABRS-014	DFAS SABRS	PROD	USER

Additional Role Attributes   Edit Additional Attributes

Role Name
DFAS SABRS Prod - DFAS General User SABRS-014

ⓘ **Information**

SAAR: 106570 has been cancelled.

OK   6

Provisioned Accounts

System Type	System Name	Provisioned Access
OID	DLA OID	DST9218

Pending Requests   Cancel Request

SAAR ID	SAAR Type	Resource(s)	Status	Current Approver	Request Date	Expire Date	Last Activity Date
106571	Role Request	DFAS SABRS Prod - DFAS Tester SABRS-016	PENDING APPRO...	Supervisor	11/1/2017	11/2/2017	11/1/2017

Request History

SAAR #	SAAR Type	Resource(s)	Status	Last Activity
106570	Role Request	DFAS SABRS Prod - ADHOC w/o Cmd Line SABRS-005	CANCELLED	11/1/2017
106563	Attribute Chan...	DFAS SABRS	REJECTED	10/30/2017
106092	Role Request	AMPS SUPERVISOR	REJECTED	10/8/2017
106078	Role Request	DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319	REJECTED	10/4/2017
102806	Role Request	DFAS SABRS Prod - DFAS Tester SABRS-016	CANCELLED	11/9/2016
102803	Role Request	DFAS SABRS Prod - Restricted FTP SABRS-006	REJECTED	11/8/2016
102808	Role Removal	DFAS SABRS Prod - DFAS Systems Maint Team SABRS-020	COMPLETED	10/20/2016
102807	Role Request	DFAS SABRS Prod - Update Additional Attributes SABRS-999	PROCESSED	10/20/2016
102804	Role Request	DFAS SABRS Prod - DFAS General User SABRS-014	COMPLETED	10/19/2016
102788	Role Request	DFAS SABRS Prod - ROSCOE MENU SABRS-003	COMPLETED	10/12/2016
102125	Role Request	DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319	REJECTED	9/27/2016
102130	Role Request	DFAS SABRS Prod - DFAS General User SABRS-014	REJECTED	9/27/2016
102046	Role Request	DFAS SABRS Prod - DFAS Systems Maint Team SABRS-020	COMPLETED	8/1/2016

Figure 440: Cancel a Subordinate Role Request - SAAR is Cancelled

7. Note that AMPS has removed the cancelled SAAR from the subordinate's **Pending Requests** table and moved it to the **Request History** table.

*The **Request History** entry saves the cancellation date of the SAAR for future reference.*

Figure 441: Cancel a Subordinate Role Request - Pending Requests is Updated

How to Edit a Subordinate's Additional Attributes

Users:	This update procedure gives your Supervisor the capability to update a role's Additional Attributes, such as DoDAACs or other required or optional codes and dates. Some roles share the same attribute, but AMPS requires you to change the attribute value only once. Other roles may have multiple values; for these roles, AMPS enables you to enter, change, or remove attributes as needed.
Supervisors:	This procedure is limited to internal Supervisors. (External Supervisors do not have AMPS accounts and, therefore, do not have access to a Direct Reports screen.) AMPS enables you to update Additional Attributes for a subordinate user who reports directly to you in AMPS. Your direct reports, along with links to their user and role information, are listed on the **My Information** screen in the **Direct Reports** tab.
Where to start:	A Supervisor begins this process by viewing the user's **Applications & Roles** screen: follow steps 1-4 of the section entitled **How to View a Direct Report's Information.**

1. If the user has more than one role with additional attributes, click the **Role Name** to select the role for update purposes.

   If the user has two or more roles that share the same attribute, select all the roles having that attribute.

2. Click the **Edit Additional Attributes** button to proceed.

   AMPS starts the Request Attribute Changes module (see Figure 443).
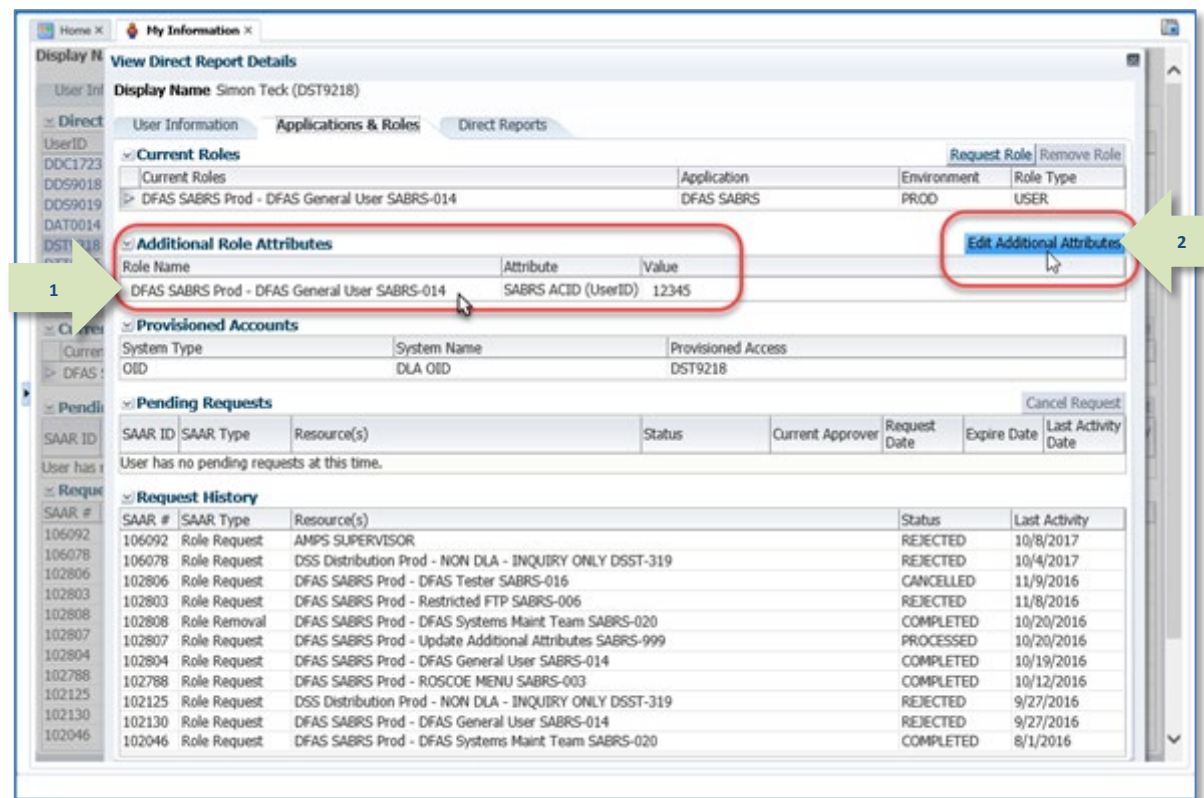
Figure 442: Additional Role Attributes – Edit Additional Attributes

3. In the **User information** screen, make sure all required fields have entries.

    The Supervisor is no longer required to enter the user's date of birth. AMPS no longer collects this data.

4. Click the **Next** button.

    AMPS displays the **Attribute Changes** *screen.*

Figure 443: Request Attribute Changes – User Information

5. In the **Attribute Changes** screen, locate and click the Select Application button.

    AMPS displays a drop-down list containing the names of all applications with roles having modifiable attributes.
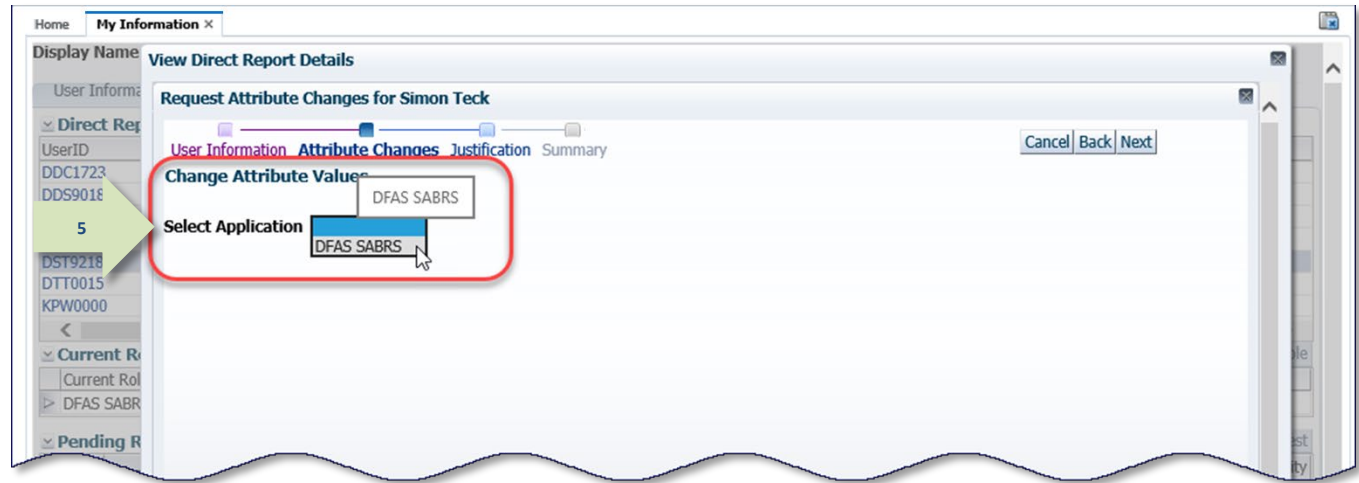
Figure 444: Change Attribute Value – Select Application

6. From the drop-down list, select the application having the role with attributes that must be edited.

    *AMPS displays an **Attributes** table that lists each attribute and the role with which it is associated.*
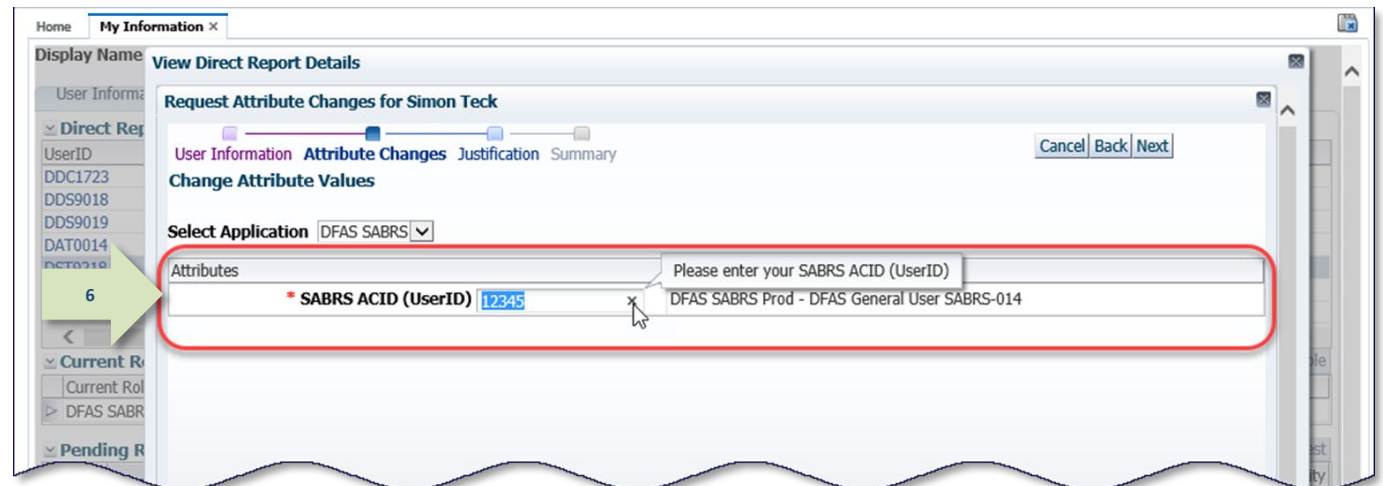
Figure 445: Change Attribute Value – Select or Enter New Value

Subsitue a New Value

7. Enter or select one or more values to edit the attribute.

   AMPS provides different methods for entering or selecting new attribute values:

   - *Free-form text field: enter a character string in the text field to replace an existing value with a new value.*

   - *Drop-down box: select a predefined value to replace an existing value with a new value.*

8. Click the **Next** Button.

Figure 446: Request Attribute Changes – Complete Selection of New Value

9. Enter text in the **Justification** field.

   This text must contain a complete and thorough explanation for the attribute change.

10. Click the **Next** button.

   *AMPS displays the **Summary** screen.*

Figure 447: Request Attribute Changes – Justification

11. Click the **Submit** button to proceed.

AMPS displays a confirmation message indicating a SAAR has been submitted to the approval process to complete the new attribute entry.

If you enter more than one change, AMPS creates a separate SAAR for each change entry.

Figure 448: Request Attribute Changes – Summary

12. In the **Attribute Request Confirmation** screen, AMPS displays a table containing the following information:

    - *SAAR number assigned to the attribute change request.*
    - *Name of the role affected by the attribute change.*
    - *New attribute value.*

13. Click the Close icon to close the **Request Attribute Changes** screen.

    *AMPS closes the screen and returns the display to the user's **Applications & Roles** screen.*
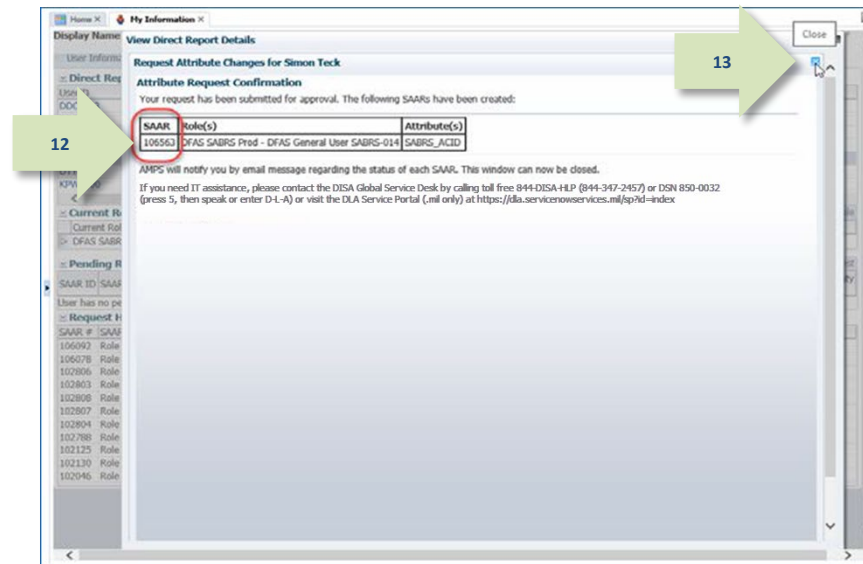
Figure 449: Update Additional Attributes - SAAR Submitted

14. AMPS refreshes the user's **Applications & Roles** tab to reflect the newly added entry in the **Pending Requests** table:

    *The existing attributes are listed in the **Additional Role Attributes** table, until after the SAAR has been fully approved.*

15. Click the **Close** icon.

    *This action closes the **View Direct Report Details** screen and returns the display to the supervisor's **Direct Report** screen.*
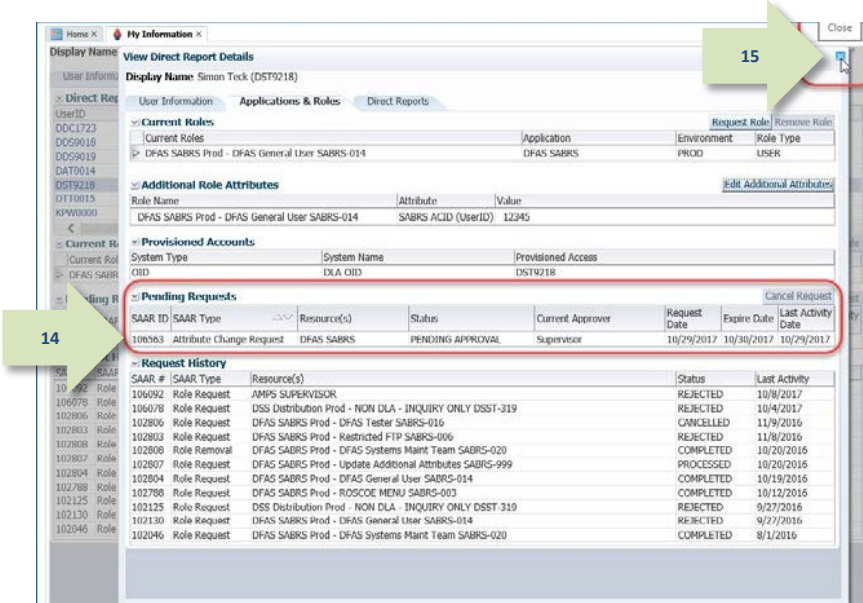
Figure 450: Update Additional Attributes - Update Completed

How to Remove a Subordinate's Role

Users:	This role removal procedure gives your Supervisor the capability to remove a role you no longer need. This capability provides the same capability available to the user to remove roles. The user can find this capability on the **Application & Roles** page of the user's **My Information** screen.
Supervisors:	AMPS enables you to remove one or more roles from a subordinate who reports directly to you in AMPS. Your direct reports, along with links to their user and role information, are listed on the **My Information** screen in the **Direct Reports** tab.

1. Begin on **the Direct Reports** screen and locate the name of the user whose records you want to view.

Note:

You can perform a role removal for the selected user on this screen, as well as on the View Direct Report Details screen mentioned in Step 2. To remove a role, follow the instructions provided in Step 3 and following.

2. Click the ID of the user whose records you want to view.

   AMPS opens the **View Direct Report Details** *screen for the selected user.*

Figure 451: Subordinate's List – Select Direct Report

3. Click the **Role Name** of the role to be removed.

*AMPS highlights the role record in the **Current Roles** table.*

3

Figure 452: Subordinate's Application & Roles Tab - Selected Role to Remove

4. With the role selected, click the **Remove Role** button.

*AMPS displays a **Request Role Removal** dialog (see Figure 454).*

Figure 453: Applications & Roles - Remove Role Button

5. Enter explanatory comments in the **Justification** text area.

    *AMPS requires an entry in the **Justification** window. AMPS stores the information with the SAAR that it creates for the subordinate role removal. This information is also directed to the provisioners of applications that employ ticketing services, such as Total AMPS (see Figure 457).*

> **Note:**
> Comments shown in the sample screen are for illustration purposes only. Please enter information relevant to each request.

6. Click **OK**.

    *AMPS creates a SAAR for the subordinate role removal request, closes the **Justification** window, and displays a confirmation message that includes the request's SAAR number (see Figure 455).*

Figure 454: Request Role Removal – Justification

7. Read the **Information** message containing the SAAR number assigned to the removal request.

8. Click **OK** to close the **Information** message box.

- *Because the Supervisor submitted the role removal request, AMPS assumes the approval is implicit and proceeds with the role removal.*

- *If the role is for an application that AMPS automatically provisions, AMPS proceeds with the corresponding deprovisioning action to complete the role removal.*

Figure 455: Role Removal Confirmation - SAAR Number

Total AMPS Provisioner: Steps to Complete the Role Removal

To complete the role removal task, an application or system provisioner must remove the user's access rights as detailed in the provisioning ticket.

For a Total AMPS ticketed application, AMPS performs the following tasks:

- Notifies the application resource provisioners,
- Lists the ticketing task in the provisioners' **My Task** list (see Figure 456), and
- Issues a provisioning ticket (see Figure 457).

1. Log in to AMPS, open the **Inbox** from the User ID dropdown menu, and locate the SAAR indicated in the email notification.

2. Click the SAAR title to start the provisioning process.

   AMPS opens the Total AMPS ticket in a separate window.
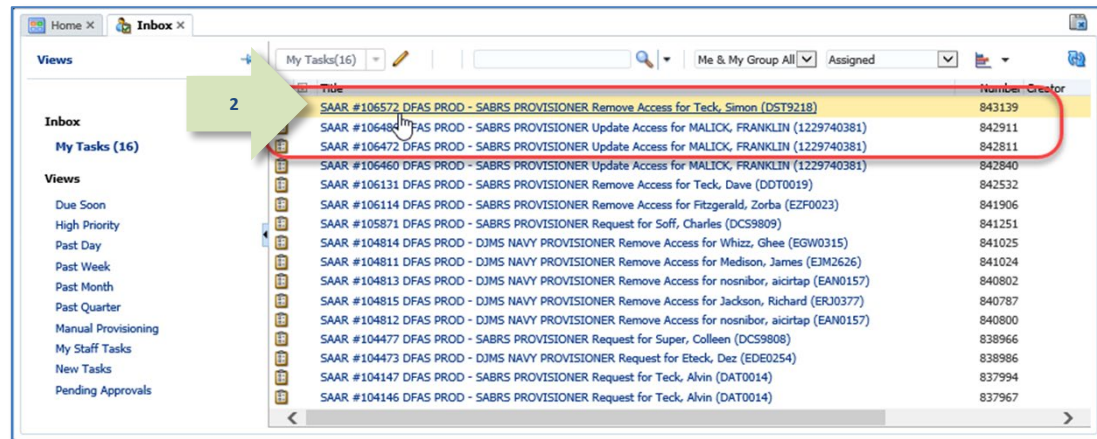
Figure 456: Provisioner's Sample Task List

3. Check the **Work Details** section for instructions about the provisioning request.

    In the sample screen, the **Work Details** *indicate the provisioner is to remove the specified role currently assigned to the* **Requestor***.*

4. Enter text in the **Comments** area to clarify the current action taken.

    Since a provisioning ticket can be opened, closed, and reopened before it is complete, you can enter progress notes or other appropriate text in the **Comments** *area to clarify the status of the provisioning task.*

    To save comments and reopen the ticket later, click **Save Comments***. Reopen the ticket from your* **My Tasks** *list.*

5. When the deprovisioning tasks are complete, click **Work is Completed.**

    AMPS closes the provisioning ticket screen.

    AMPS then notifies the user that the deprovisioning actions are complete and the user's application access privileges have been removed.

Figure 457: Remove Job Role - Total AMPS Ticket

Supervisors...

When the provisioner completes the deprovisioning process and closes the ticket, AMPS removes the role from the user's list of Current Roles.

AMPS also enters the role name and removal information in the user's SAAR History.

Figure 458: User's SAAR History - Role Removal Completed

Administrative Users' Utilities

AMPS Administrative Users have utilities available to them for account maintenance and troubleshooting purposes. Administrative users must have the appropriate role, as specified in the following sections, to get access to the utilities.

They include the following utilities:

- User Search
- User Security Maintenance

User Search

Prerequisites	**To employ the User Search screen, you must request the *AMPS Security Officer* role.** After your request for this role is approved, AMPS automatically provisions your account with this role and adds the **User Search** tile to the Manage Home page.

What You Can Do:	A Security Officer may have a number of reasons to check a user's record. AMPS stores a range of data for each user. In AMPS, a Security Officer can perform these tasks:
	    • Search for an individual user.
	    • View the user's User Information, Contact Information, Organization, and Supervisor assignment.
	    • View and modify a User's Security Information.
	    • Select and remove a user's role.

Where to Begin:	After you have received email confirmation that the AMPS Security Officer role you requested has been assigned to your account, launch AMPS and check the **Manage Home** page.

Access to the **User Search** screen is available from the AMPS Manage Home page:

1. After you launch AMPS, click the **Manage** button in the AMPS banner to open the **Manage Home** page.

2. Click the **User Search** tile.

    *AMPS opens the **User Search** screen (see a sample of this screen in Figure 460).*
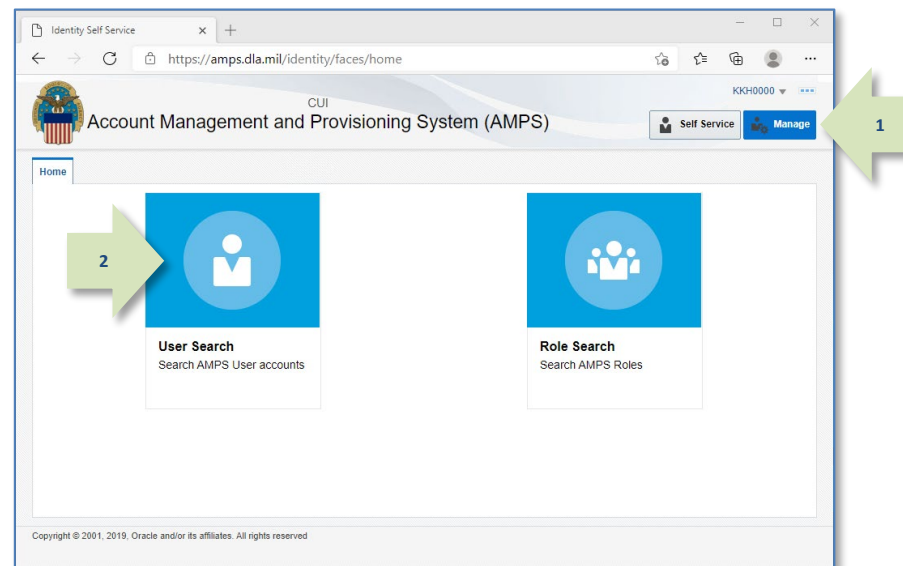
Figure 459: AMPS Manage Home Page – User Search Tile

The User Search screen contains two main areas:

A. Search

- Select an option to search on *All* or *Any* field criteria you enter or select.
    - o *All:* displays only records that match ALL criteria.
    - o *Any:* displays records with any matching criteria in the return.
- Use dropdown lists to select a different operation from among the available choices:
    - o **Starts with:** initial characters
    - o **Ends with:** final characters
    - o **Equals:** exact character match
    - o **Does not equal:** excludes results with a matching character string.
    - o **Contains:** contains the character string somewhere in the search field.
    - o **Does not contain:** excludes results that contain a matching character string.
    - o **Is blank:** includes results that have a blank entry in the specified field.
    - o **Is not blank:** includes results that do not have a blank entry in the specified field.

Note:

The search criteria are NOT case sensitive.

B. Search Results

- Verify the identity of the user whose record you need to review.
- Click the **User Login** entry for the record you want to review. Each User Login field is a link to the user's **User Information** and **Applications & Roles** screens.

Figure 460: Sample User Search Screen

How to Search for, View, and Maintain a User's Security Information

1. Choose an option for including or limiting how the search criteria are combined.

2. Enter one criterion or a combination of multiple search criteria.

   *For example, the screen in Figure 461 contains criteria for two fields. Because the user has selected **All** as the **Match** option, AMPS displays only items that match all of the search criteria.*

3. Click **Search**.

   *AMPS displays records with matching characters in the **Search Results** table.*

   *In the example shown, AMPS displays records for all users whose **Last Name** begins with the specified character string and whose **EDIPI** starts with the numeral **1**.*

   *Not included are users whose EDIPI begins with any numeral but **1**, even though their names may begin with **Soff.***

4. Click the **User Login** entry for the user whose record you want to review.

   *AMPS may display a **Privacy Act Statement** appropriate for your organization. Click **Accept** to proceed (see **Appendix A** in this user guide for more information on the **Privacy Act Statement**).*

   AMPS then displays the user's identity and role information (see Figure 462).

Figure 461: Sample User Search Screen

5. Add or change the following entries in the Security Information section:

    --Position Sensitivity
    --Date of Investigation
    --Clearance Type
    --Background Investigation Type
    --Security Officer Review Flag
    --Security Officer Review Comments

    The Security Officer Review Flag has two valid entries for selection:

    --Not Flagged for Review: The user's security information does not require a security review with every role request. This option is not applicable to DFAS users' requests, which always require a Security Officer review.

    --Flagged for Review: The user's security information requires a security review with every role request. DLA user requests for IT3 roles do not require a Security Officer review; for these types of role requests, AMPS disregards the flag setting.

6. Click **Save**.

    AMPS displays an **Information** *message to confirm changes have been saved (see Figure 463).*

Figure 462: User Search Result - User Information

7. Click **OK** to close the **Information** message.

8. As an option, click **Return to Search Results** to pick another record or create a new list of search results.
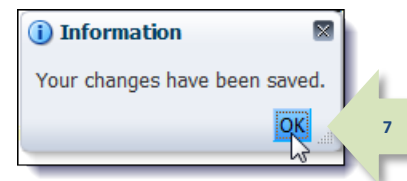
Figure 463: Information Message - Changes Saved

How to Remove a User's Role

A Security Officer who has the ***AMPS Security Officer*** role can remove roles from users' accounts through the **User Search** utility. Follow these steps to search for a user, select a role currently assigned to the user, and submit a role removal request.

The role removal process is completed when the application provisioner completes the work identified on the AMPS provisioning ticket. AMPS sends email notifications to the user and to the provisioner at each stage of the role removal process after the Security Officer submits the removal request

Access to the **User Search** screen is available from the AMPS Main Menu:

1. After you launch AMPS, click the **Manage** button in the AMPS banner to open the **Manage Home** page.

2. Click the **User Search** tile.

    AMPS opens the **User Search** *screen (see a sample of this screen in Figure 465).*
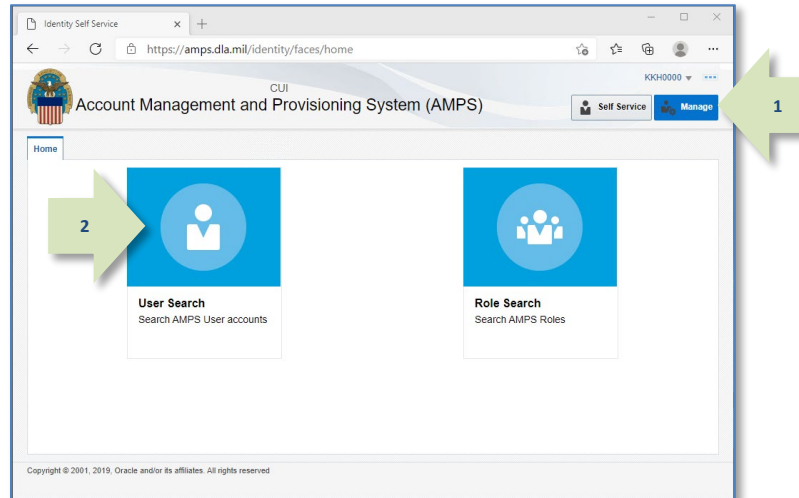
Figure 464: Manage Home Page – User Search Tile

3. In the **User Search** screen enter one or more search criteria, such as all or part of the user's login ID.

4. Click the **Search** button.

    AMPS may display a **Privacy Act Statement** *appropriate for your organization. Click* **Accept** *to proceed. (See* **Appendix A** *in this user guide for more information.)*

    AMPS then displays the results of the search in the **Search Results** *table (see Figure 466).*

Figure 465: User Search Screen - Executing a Search

5. Click the **User Login** link to open the
    user Information screen.

    AMPS displays information for the
    selected user with the **User Information**
    tab displayed by default.

Figure 466: User Search Results

6. Click the Applications & Roles tab.

    AMPS displays the **Applications & Roles**
    tab page for the selected user.

Figure 467: User Information Screen

7. Click the name of the role to be removed.

AMPS highlights the selected role.

Figure 468: Applications & Roles - Select a Role to Remove

8. Click the **Remove Role** button.

   AMPS opens a Request Role Removal dialog (see Figure 470).

Figure 469: Applications & Roles - Remove Role Button

9. In the **Justification** text area (required field), enter an explanation that justifies the removal of the user's role.

10. Click the **OK** button.

   AMPS closes the **Request Role Removal** *dialog and displays an* **Information** *message that confirms the changes and lists the SAAR number for the role removal request (see Figure 471).*

Figure 470: Request Role Removal

11. In the **Information** message dialog, read the messages. You can make a note of the SAAR created for the role removal.

12. Click **OK** to close the message dialog.
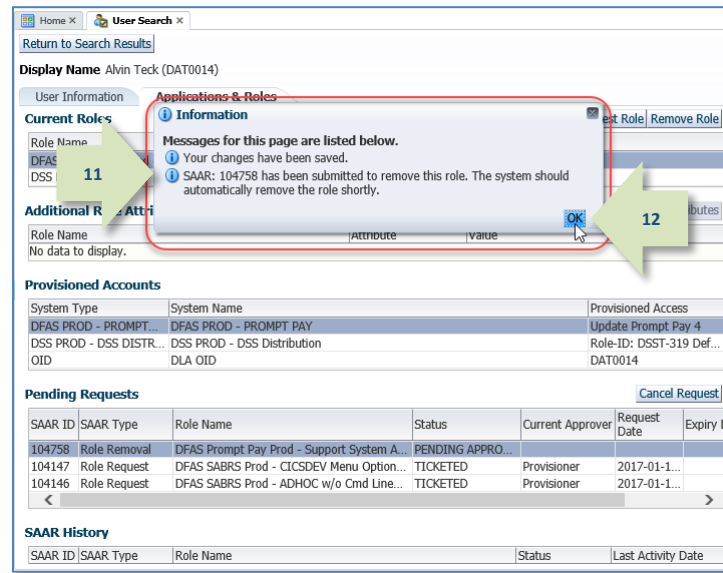
Figure 471: AMPS Information - Confirmation and SAAR Number

13. AMPS displays the role removal request in the user's **Pending Requests** table. (The Security Officer can also see this screen.)

For Total AMPS roles, AMPS sends a role removal request to application provisioners for each account associated with the role. The following list explains the **Status** entry and **Current Approver** entry for the SAAR:

TICKETED: AMPS has sent a provisioning ticket to the application provisioner. Action on the ticket is still pending.

Current Approver: AMPS lists the current approver for the SAAR. The provisioning request remains in the provisioner's queue until the action is complete and the provisioner completes the ticket in AMPS.
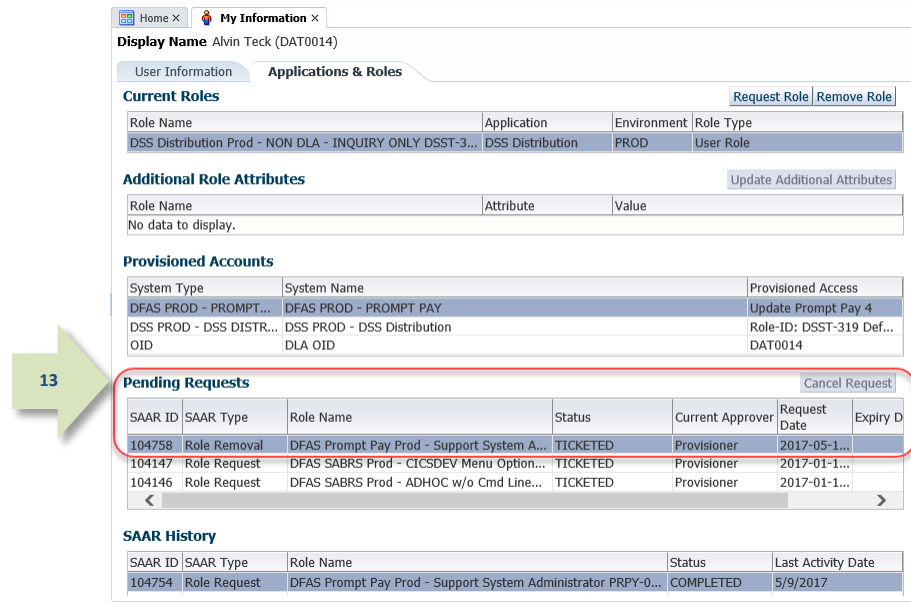
Figure 472: Applications & Role - Pending Requests

14. AMPS sends this email notification to the user whose role is being removed by the Security Officer.
AMPS also sends this email to the user's Supervisor.

There is no action required by the user or the Supervisor.

This notification advises the user that a role removal request has been submitted.

The email identifies the SAAR number, SAAR Type, Removal Type, Role name, and Justification. It also identifies the Security Officer who submitted the role removal SAAR, as well as the date of the request.
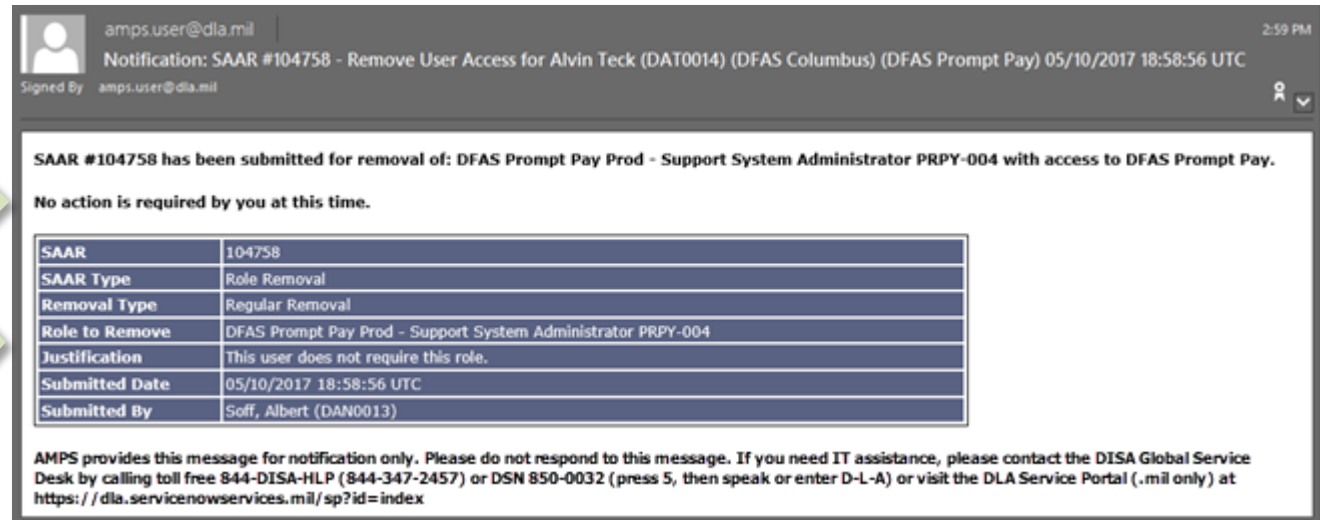
Figure 473: Role Removal - Sample Initial Email

Note:

AMPS sends the email in HTML format, but it can also be viewed in plain text. The sample provided in Figure 473 is an image of the email viewed in HTML format.

15. AMPS sends another email notification to the user whose role is being deprovisioned.

This notification advises the user that the role removal request has been submitted to the application provisioner for action.

Subject: AMPS Application Processing for SAAR #104758

Body: AMPS application processing for SAAR 104758 has started for DFAS Prompt Pay.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

16. AMPS sends this email notification to the provisioner.

16

This notification advises the provisioner that a provisioning ticket awaits action on a SAAR submitted for a role removal. The provisioner uses the SAAR number to locate the SAAR in AMPS and complete the provisioning assignment.

Subject: AMPS Application Processing for SAAR #104758 requires your attention.

Body: AMPS Application Processing request for SAAR 104758 requires your attention.
Please visit AMPS at this URL:
https://amps.dla.mil/

Open your inbox to locate the SAAR. Click the SAAR title to open and complete the task.

Task Details:

Request For:
DLA Login: DAT0014
Name: Teck, Alvin
Phone: 888-555-1212
Email: Alvin.Teck@dla.mil
EDIPI/UPN: nnnnnnnnnn

Access Information:
SAAR #: 104758

Remove Job Role: DFAS Prompt Pay Prod - Support System Administrator PRPY-004

Applications and Access:
        Resource: DFAS PROD - PROMPT PAY
                Remove: Update Prompt Pay 4

Justification: This user does not require this role.

Optional Information: (none)

Role Removal SAAR requested by Albert Soff on 05/10/2017

17. For Total AMPS applications, AMPS lists a provisioning ticket for the application provisioner as an assigned SAAR in the **Inbox** > **My Tasks** list (not shown).

   To complete the role removal process in the application itself, the provisioner completes the work identified in this ticket.

   As with other Total AMP Tickets, the provisioner can claim the ticket by clicking the **Claim** button, and save progress comments without completing the ticket by clicking the **Save Comments** button.

18. To close the Total AMPS provisioning ticket, the provisioner clicks the **Work is Complete** button on the ticket screen.

SAAR #104758 DFAS PROD - PROMPT PAY PROVISIONER Remove Access for Teck, Alvin (DAT0014)   Claim | Sav | 18 | Work is Complete

Application Request

Current Task Owner:
Current Resource Responsibility: DFAS PROD - PROMPT PAY PROVISIONER
Last Updated: May 10, 2017 8:54 AM
* Comments: Deprovisioning work is completed.

Work Details

Request For:
DLA Login: DAT0014
Name: Teck, Alvin
Phone: 888-555-1212
Email: Alvin.Teck@dla.mil
EDIPI/UPN:

Access Information:
SAAR #: 104758

Remove Job Role: DFAS Prompt Pay Prod - Support System Administrator PRPY-004

Applications and Access:
    Resource: DFAS PROD - PROMPT PAY
        Remove: Update Prompt Pay 4

Justification: This user does not require this role.

Optional Information: (none)

Role Removal SAAR requested by Albert Soff on 05/10/2017

User Summary

User ID	DAT0014	Phone	888-555-1212
Name	Teck, Alvin	Email	Alvin.Teck@dla.mil
Organization	DFAS Columbus	Supervisor	
Job Title	Analyst	Annual Revalidation Date	
IT Level	IT3	Cyber Awareness Certification Date	4/1/2017

Current Roles

Current Roles
▷ DSS Distribution Prod - NON DLA - INQUIRY ONLY DSST-319

Figure 474: Security Officer's Role Removal Request - Sample Provisioning Ticket

19. After the deprovisioning process is completed in AMPS, the system sends an email notification to the user who had the role.

    This notification tells the user that the role's access privileges have been removed from his account.

    The email identifies the SAAR number, SAAR Type, Removal Type, Role name, and Justification. It also identifies the Security Officer who submitted the role removal SAAR, as well as the date of the request.

    ## Note:

    AMPS sends the email in HTML format, but it can also be viewed in plain text. The sample provided in Figure 475 is an image of the email viewed in HTML format.

    The Security Officer's role removal request is now finished.
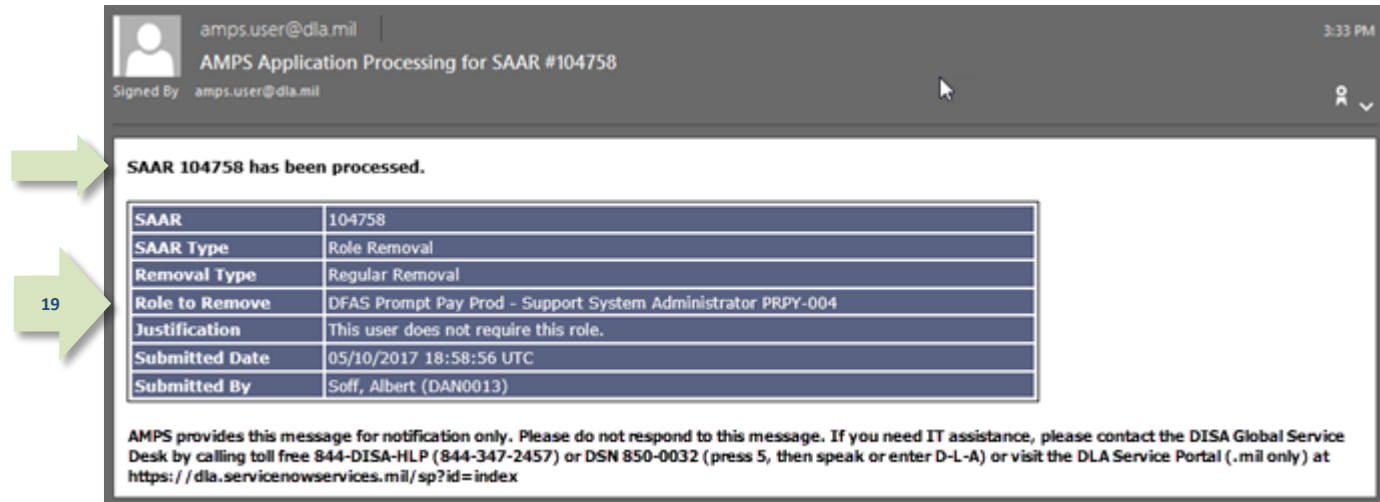
Figure 475: Role Removal - Sample Final Email

User Security Maintenance

Prerequisites	To employ the **User Security Maintenance** utility, a Security Officer must request the ***AMPS Security Officer User Edit Role***. After the request for this role is approved, AMPS automatically provisions the requestor's account with this role and adds the **User Security Maintenance** command on the Administration dropdown menu (see Figure 476). This command provides access to the **User Security Maintenance** screen and functions.
What You Can Do:	The **User Security Maintenance** utility is a time-saving module that enables a Security Officer to enter and submit changes to multiple user records at one time. This utility is an alternative to the **User Search** option, which permits changes to only one user record at a time. The **User Security Maintenance** utility enables a Security Officer to perform the following tasks: • Search for an individual user. • View the user's Security Information as it appears on the user's My Information screen. • Modify a user's Security Information. • Add a record for changes to the user's record. • Repeat this procedure for multiple users. • Update all users with one action. The **User Security Maintenance** utility enables a Security Officer to build a list of several users to update with one confirmation action. Remember that just adding a record to the **Bulk Update** list does not update the user's record until the Security Officer confirms and submits all the updated records with the confirmation action. See Step 5 of the section titled **How to Update Users' Security Information** for more information.
Where to Begin:	After receiving email confirmation that the **AMPS Security Officer User Edit Role** has been assigned, the Security Officer can launch AMPS and check the Administration dropdown menu from the Self Service Home page. If the role has been properly assigned to the account, AMPS displays the **User Security Maintenance** command on the **Administration** dropdown menu (see Figure 476).

Access to the **User Security Maintenance** screen is available from the Self Service Home page:

1. After launching AMPS, click the **Administration** tile on the Self Service Home page to open the Administration dropdown menu.

2. Click the **User Security Maintenance** command from the menu.

   AMPS opens the **User Security Maintenance** *screen (see a sample of this screen in Figure 477).*
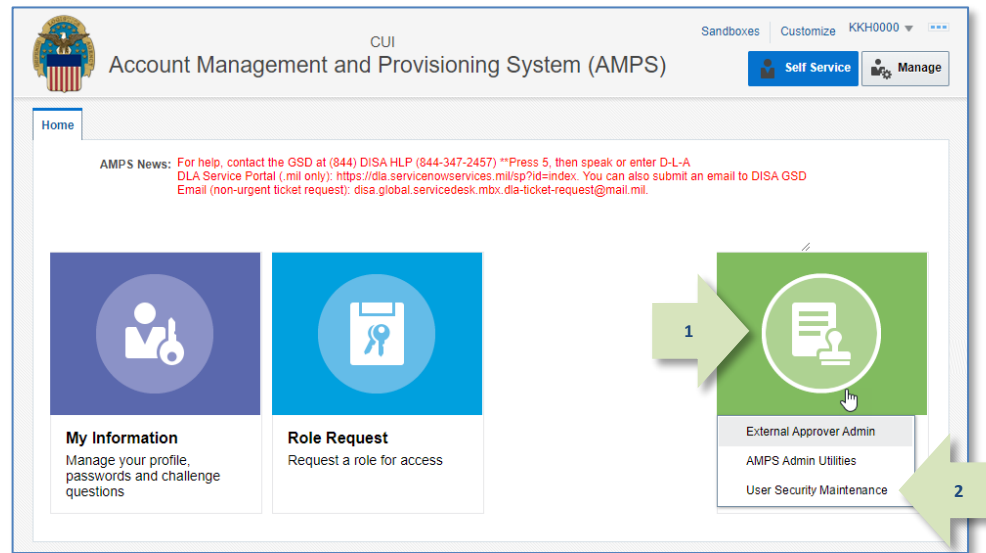
Figure 476: Administration Dropdown Menu - User Security Maintenance Command

The **User Security Maintenance** screen contains three main areas:

A. **Search**: Enables you to search for and select the record of an individual user.

B. **Security Information**: Displays a selection of user-related identifying information, enabling you to verify that the user you searched for and selected is the correct user.

Also, displays the user's **Security Information** fields. These fields are modifiable, enabling you to enter or update entries.

AMPS activates the following buttons after you select a record:

--**Update Single:** click this button to update the displayed record, or

--**Add to Bulk Update:** click this button to populate the **Bulk Update** list.

C. **Bulk Update**: Enables you to assemble a list of security information changes organized by user record. AMPS activates the **Update All in List** button after you add the first record.

When you have completed changes and assembled the list of records to be updated, click **Update All in List** to complete multiple updates with one action.

Figure 477: User Security Maintenance Screen

How to Update Users' Security Information

Valid Search Criteria　　The following list outlines the types of search criteria a Security Officer can enter to display a list of matching selections:

- **Complete AMPS user ID:** AMPS displays the name and ID of the user whose ID matches the user ID search criterion.
- **Partial AMPS user ID:** AMPS displays a drop-down list of users whose AMPS user IDs contain characters that match the search criterion.
- **Complete Last Name:** AMPS displays a selection of users whose last name matches the Last Name search criterion.
- **Partial Last Name:** AMPS displays a selection of users who last name OR user ID matches the characters in the Search Criteria field.

AMPS does not match characters in a user's first name, but search results list the user's last name, first name, and user ID.

1. In the **Search Criteria** field, enter a partial or full AMPS user ID or user last name.

2. Click **Search**.

   *AMPS populates the **Select a User** drop-down list with matching search results.*

3. Open the drop-down list and select the name of the user whose **Security Information** requires an update.

   AMPS displays the user's current security information if it is available in AMPS (see Figure 479). If not, the fields remain blank.

Figure 478: User Security Maintenance - Search

4. Enter or modify data in the following fields:

- **Date of Investigation:** enter the date of the user's most recent security clearance or other investigation.

- **Clearance Level:** select the user's current clearance level, or select **None**.

- **Background Investigation Type:** select the type of background investigation used to verify the user's security eligibility.

- **IT Level:** enter the user's current Information Technology (IT) level.

- **Flag for Security Review:** select **Flagged for Review** if every request submitted by a user should receive a security review.

- **Comments:** Enter comments to clarify changes.

Figure 479: User Security Maintenance - Modify

5. When all security information has been verified and updated where necessary, click **Add to Bulk Update**.

   AMPS adds a record to the **Bulk Update** list.

Note:

At Step 5, the user's security information is not yet updated! See Step 8 for instructions on completing the update action.

Figure 480: User Security Maintenance - Add to Bulk Update

6. Repeat Steps 1 – 3 to search for and select another user.

7. Repeat Steps 4 and 5 to select additional users to update and add to the **Bulk Update** list.

Figure 481: User Security Maintenance - Search and Select Another User

8. When you have completed the list of users you want to update, click the **Update All in List** button in the **Bulk Update** panel.

   AMPS displays a confirmation message listing the names of all users whose records have been updated (see Figure 483).

Figure 482: Bulk Update List

9. Review the messages in the Information box to ensure all user records were updated.

Click **OK** to close the **Information** box.

*AMPS closes the **Information** box and enables you to resume use of the **User Security Maintenance** utility or switch to a different task.*

Figure 483: Bulk Update Confirmation Message Box

Application Access Removal

With the release of AMPS 18.1.0, AMPS now includes a module, called **Application Access Removal**, that enables Data Owners to remove roles from one or more users when a situation calls for such removals. Situations include the following scenarios:

- Application administrators have authorized the direct removal of a user from an application. A direct removal initiated on the application does not automatically update the user's AMPS account, resulting in a need to reconcile the user's application account with the AMPS account. These removals may occur when a user's account times out due to inactivity, or the user loses the requisite authority to certain access privileges, or other business processes that require removal of user access in an application. In any case, a user's AMPS account must be reconciled with the user's application accesses to ensure AMPS reflects the correct role information for the user.
- Application administrators may also want to remove users from a role or roles in bulk, rather than having a Supervisor remove individual roles through the standard Role Removal process (see the section entitled **Role Removal** for more information). A Supervisor can remove only one role at a time, which can be a time-consuming task.
- Applications administrators may want to initiate the removal of multiple users from application roles by starting in AMPS.

In these scenarios, AMPS provides an administrative user interface that provides the Data Owner, or other authorized administrator, with the utilities needed to work through these scenarios within AMPS.

AMPS Account and Access Reconciliation

AMPS has two methods of provisioning user access to an application or system:

- Direct provisioning: in this method, AMPS itself logs in to the target application on behalf of the user and supplies the provisioning information to the application. This method does not require human intervention.

- Manual provisioning through Total AMPS tickets or Remedy tickets: in this method, AMPS produces either a Total AMPS ticket or Remedy ticket for a role request and notifies designated application provisioners that action on a provisioning request is pending.

In both cases AMPS keeps track of the access the user has been granted in an application or system by maintaining a record of current roles held by the user within the user's account.

However, administrators in each application or system, independent of AMPS' tracking, can remove a user's access. Such removals may occur for various reasons, such as a timeout due to inactivity, or a removal for security reasons. When an administrator removes a user's access in a system or application without notifying the AMPS team with a work order, the user's Current Roles information in AMPS is no longer synchronized.

To address the difference in role information, the AMPS team devised and implemented a process to reconcile the difference. Using this process, a Data Owner can update a user's AMPS record to remove any roles that are no longer valid for that user. This update process enables the Data Owner to reflect the correct state of the user's access capabilities.

Application Access Removal also enable a Data Owner to initiate the process of removing a user from a role in AMPS, which submits a notification to remove the user from a selected application. This feature enables the Data Owner to select multiple users to remove from a role, or select multiple roles to remove from a user's account. These procedures do not require the user's participation or approval, a capability that enhances the Data Owner's efficiency.

AMPS has been modified to support the following scenarios:

- Automatic reconciliation for direct-provisioned applications
- Manual reconciliation for Total AMPS, Remedy-supported, or direct-provisioned applications.

The following subsections summarize these modifications.

Automatic Reconciliation for Direct-Provisioned Applications

Applications that stakeholders have configured for direct provisioning can also be configured for automatic removal reconciliation in AMPS. The process previously in place automatically removed a user's provisioned access in AMPS after the user lost his or her access in an application. Rather than remove the user's role, AMPS only revoked specific resources from a user's account. AMPS did not remove a role from a user's account, even if all the associated resources for that role were revoked. This process left a role assignment in the user's AMPS record, with no provisioned resources. The process should remove the role itself and also revoke the resources.

To address this gap in function, the AMPS team developed a custom process that searches for AMPS accounts in which all the resources on a user's role have been revoked. If all resources for a specific role have been revoked, AMPS now removes that role from the user's account record. This function is called "automatic delete reconciliations." For more details, see the section below.

To implement automatic delete reconciliations, application managers must add this function as part of their connector configuration. If they do not plan to implement automatic delete reconciliations, they can use the manual reconciliation process for some directly provisioned applications.

Manual Reconciliations for Total AMPS or Directly Provisioned Applications

Applications that are not directly and automatically provisioned through AMPS rely on manual provisioning and deprovisioning through either Total AMPS or Remedy tickets. When a Provisioner for such an application deprovisions a user's access to a resource, the deprovisioning process does not also remove the user's corresponding role from AMPS. This scenario results in conflicting records of roles and access to resources between AMPS and the remote system.

Because Total AMPS and Remedy-supported applications are provisioned manually, AMPS formerly had no option for administrators to reconcile them automatically through a system-to-system connection. Instead, these administrators needed a manual process that would enable them to log in to AMPS and remove users from roles or remove roles from users.

The administrators who employ this process are specific users, ordinarily Data Owners or Provisioners. These administrators must request and receive a specific role or roles in AMPS that enable them to log in to AMPS and perform the following tasks:

- Select users to remove from roles through the AMPS user interface.
- Select roles to remove from a user's AMPS account.
- Upload a list of user and role combinations that serves as a bulk role removal request.

Each of these of processes generate a removal SAAR that is flagged as a manual reconciliation. In keeping with the business process, AMPS does not require approvals for these SAARs. For audit purposes, AMPS records the user who submits a manual reconciliation SAAR as the Data Owner who fulfills the Data Owner approval step for the SAAR.

During the process of creating a reconciliation request, the user submitting the request must enter a justification for the removal. He or she can then complete and submit the role removal request.

After AMPS generates each SAAR for the requests, the system performs the following actions:

- Removes the roles immediately.
- Marks the SAARs as complete.
- Sends email notifications to users advising them that their roles have been removed. This notification includes the reason for the removal, which is taken from the Justification text entered by the Data Owner.

For directly provisioned applications . . .

For roles directly provisioned to an application, the Application Access Removal process starts an attempt to remove that user's access automatically in the target system. However, the user's access has already been removed. To finish the process, AMPS marks the resource as Revoked in its role record for the user.

Manual Role Removal

Authorized application managers can also start a role removal process by using the manual role removal feature. In this case, users have roles in AMPS and in the related applications, but for administrative reasons, a Data Owner may need to remove a role, or multiple roles, from a user or multiple users.

For Total AMPS roles, removing a role through this utility will not generate tickets for removal, because AMPS assumes by using this process that all access has already been removed from the target system. Email notifications will be sent to the user to notify them that their AMPS access has been removed.

Another scenario exists, where specified users (usually Data Owners or Provisioners) may be given the privilege to initiate Role Removal processes for users of their application from within AMPS. This option will function similarly to the previous option, except that this option will produce Total AMPS tickets to remove the access. The SAARs that are produced using this method will be regular Role Removal SAARs, which are auto-approved due to their being submitted by "privileged" users (i.e.: the Data Owner/Provisioner who has been granted this ability). Because these requests will be treated as "regular" role removals in AMPS, email notifications will be sent in association with each SAAR.

Role Removal File Upload

The Application Access Removal utility provides the user with a method for filling in and uploading a CSV file with multiple user and role combinations. With this feature, the application manager can create a CSV file having user name and role name combinations. After the application manager uploads this file, AMPS removes the specified roles for the specified users in a single pass.

To ensure that the values in the CSV file are valid and acceptable in the process, AMPS produces error messages that help the user spot and correct problems.

Application Access Management: System Roles

Like other functional areas of AMPS, Application Access Management requires application administrators to acquire specific roles that provide access to its process. In AMPS, each application has a corresponding Access Application Management role that provides the role holder with access to that application's role and user assignments.

To set up access to the Application Access Management process, AMPS requires specific administrative users to have one of the following roles:

Application Access Management Manager

The Application Access Management Manager has responsibility for approving the requests for individual Application Access Management roles. Application owners modify their application's Role-based Access Control (RBAC) form to identify the individuals who must have this role. AMPS applies the Application Access Management Manager role to each specified user through a background administrative process.

Application Access Management Roles

Data owners or application provisioners who have responsibility for managing users assigned to roles through the Application Access Management process must request a role that corresponds to an application. For example, a DFAS data owner who approves requests for SABRS Navy application roles must request the **DFAS SABRS Application Access Management** role. Having this role has the following effects on the data owner's or provisioner's AMPS account:

- Adds the following command to the Administration list on the main menu: **Application Access Removal**.
- Provides access to the Application Access Management screens and processes for managing role removals.

The data owner's or provisioner's request for this role is approved in a typical role request path, but the data owner approval is provided by the data owner manager who holds the application's Application Access Management Manager role.

Note:

In Application Access Management, AMPS provides an Application Access Management role for each application, which provides the role holder with access to *all* roles and *all* users in the application. The principle behind this process is that a data owner can remove roles from a user, or remove users from a role, either of which the data owner has previously approved.

- **Application Access Management Manager:** a data owner manager who approves requests for individual Application Access Management roles.
- **Application Access Management:** a data owner or provisioner who handles the removal of users from a specific application's role and the removal of a specific user from one or more application roles assigned to that user.

However, if application owners have segmented an application and created separate data owner roles, AMPS does not accommodate these data owners with corresponding Application Access Management.

For example, even though application owners can create separate data owner roles for separate sites, AMPS does not offer the same separation in Application Access Management roles. Each application has only one corresponding Application Access Management role; data owners or provisioners who hold this role can see all roles and users, regardless of whether or not the data owner approved the original request.

About Removing Roles from Pending SAARs

Because AMPS user accounts may be in flux, with roles undergoing approval and other roles undergoing removal, a condition may exist in which a Data Owner requests removal of a role from an account when the request for that role may not be complete. Also, an internal DLA user may be going through an Annual Account Revalidation request, in which the user has identified roles that need to be removed from his account. In these cases, SAARs exist and are in progress. The Application Access Management module has the capability to handle scenarios in which in-flight SAARs may contain a role that a Data Owner has requested to be removed.

If a user has an open Annual Revalidation, AMPS will remove the roles from that SAAR, but the SAAR otherwise remains open.

Application Access Removal Screens: Quick Tour

The **Application Access Removal** interface is the front-end GUI that enables Data Owners, or other administrative users, to remove users from roles within their application. This section describes each of the screens for this interface, in detail.

Application Access Removal Tile

After you obtain the appropriate Application Access Management role or roles, when you log in to AMPS, click the **Manage** button in the AMPS banner to open the Manage Home page. You will find a tile labeled **Application Access Removal**.

To open the GUI for this process, click the **Application Access Removal** tile.

*AMPS opens the **Application Access Removal** page and displays the Activity Selection screen (see Figure 485).*
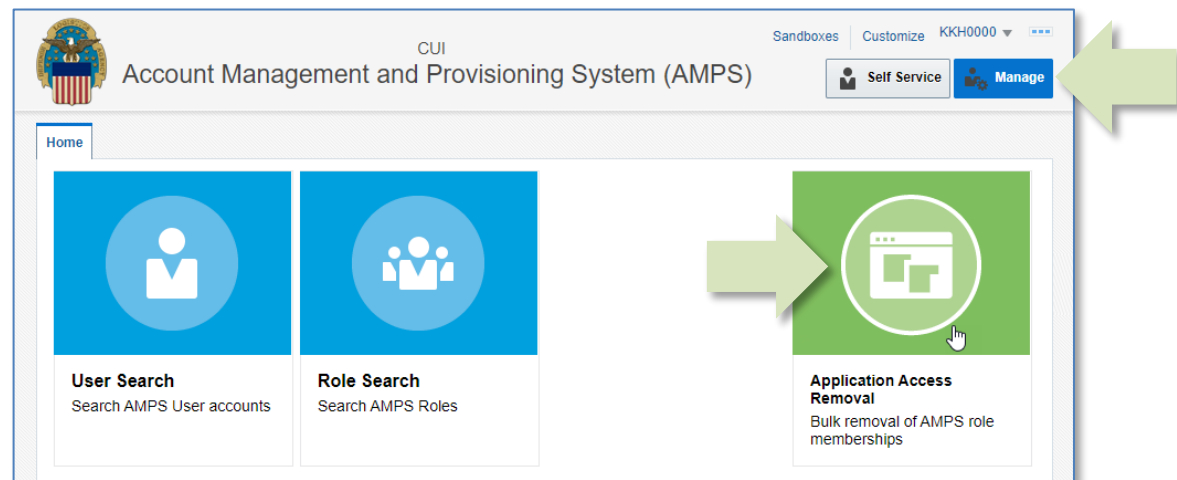
Figure 484: Manage Home Page - Application Access Removal Tile

The following subsections provide a tour of each screen in the **Application Access Removal** process. Each tour provides an overview of the screen's appearance and its features. Use these subsections as reference.

If you are ready to use the **Application Access Removal** features, proceed directly to the section entitled **How to Request an Application Access Removal** (page 472).

Tour of the Activity Selection Screen

The Activity Selection screen is the first screen displayed after you click the **Application Access Removal** tile on the Manage Home page. Use this screen to choose which kind of removal action and result you want to accomplish. You can perform the same actions with either screen, but as the description indicates, the **Regular Removal** activity generates SAARs and, where required, provisioning tickets for role deprovisioning.

The **Reconciliation** activity does not produce deprovisioning instructions, because the user has already been deprovisioned from the account, and you need only to reconcile the user's AMPS account with his or her actual access rights.
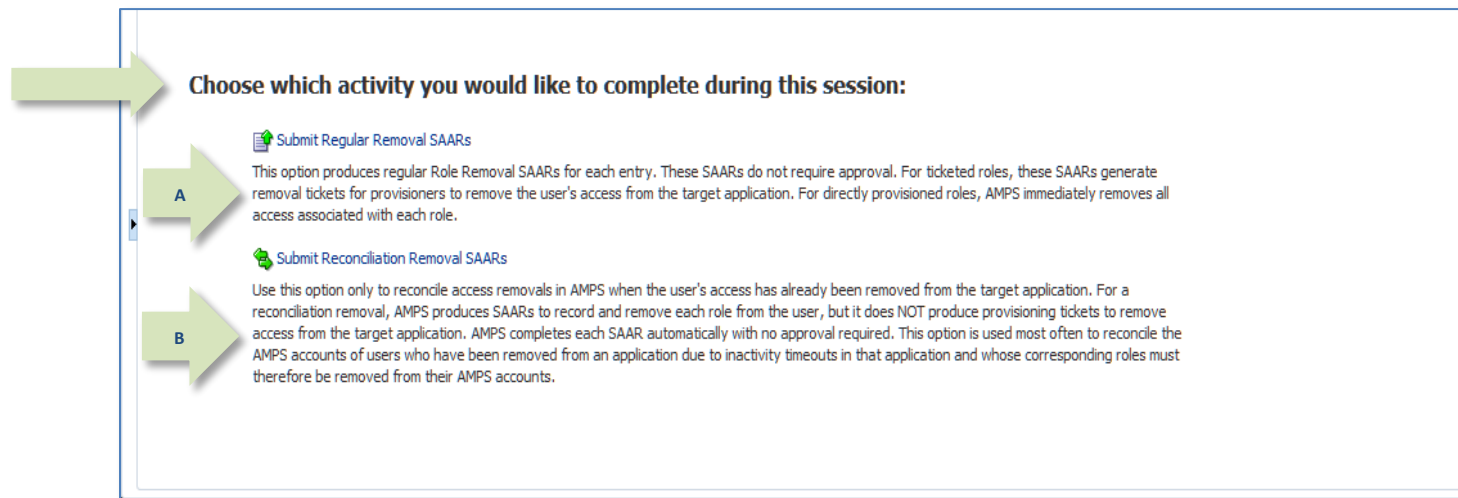
Figure 485: Application Access Removal – Select a Removal Activity

	If you want to perform this task . . .,	And fulfill these objectives . . .	Choose this option:
A	▪ **Remove a role from a user's AMPS account**, and ▪ If needed, send deprovisioning instructions to an application provisioner, *-OR-* ▪ **Remove a user from a role**. ▪ If needed, send deprovisioning instructions to an application provisioner.	Find a faster, more efficient way to . . . ▪ Remove a role from one or more users in a time-saving, bulk-type format. ▪ Remove a user from one or more roles in a time-saving, bulk-type format. ▪ Generate deprovisioning SAARs for role removals.	Submit Regular Removal SAARs
B	▪ **Remove an AMPS role from a user** whose access has already been removed from the target application, *-OR-* ▪ **Remove a user from an AMPS role**, in which the user's access has already been removed in the target application.	Reconcile a user's AMPS account with the account access rights that have been removed on target applications.	Submit Reconciliation Removal SAARs

Tour of Set up a Role Removal Request Screen – Top

The Search by Role/Search by User screen is the next screen displayed after you select one of the two activities. Use this screen to select an application, find a role or find a user, and set up the role removal request you need to submit.

This view of the screen displays the features you would use to select an application and select a specific role. After you select a role, AMPS lists all users assigned to the role in the table under **Users in Selected Role**.

A. **Select Application:** this drop-down box contains a list of one or more applications from which you can choose roles or users.

B. **Files:** buttons to upload or download the bulk upload or template files.

    a. Upload List of Users to Remove

    b. Download Template Remove File

C. Search by Role tab:

    ▪ **View:** choose which columns to view and the order in which they are listed.

    ▪ **Search:** specify and locate a role or range of roles.

    ▪ **Detach:** display the role list in a separate dialog to expand the table view.

D. **Role Display Name:** the role name displayed in AMPS.

E. **JD Code:** Job Description Code, or the short, alphanumeric name of the role.

F. **Primary Role**: Indicator that identifies if the current role is a Primary Role.

G. Classification:

    a. C = role is Classified

    b. U = role is Unclassified

H. Access: Access Type:

    a. **P =** reserved for **Privileged** users

    b. **A =** reserved for **Authorized** users

I. **IT Level:** Position sensitivity level assigned to the role. A user's IT level must not exceed the IT level of the role without the express authorization of a security officer.

Figure 486: Application Access Removal - Search by Role/Search by User

Tour of Set up a Role Removal Request Screen – Bottom

The Search by Role/Search by User screen is the next screen displayed after you select one of the two activities. Use this screen to select an application, find a role or find a user, and set up the role removal request you need to submit.

A. Users in Selected Role:

- **View:** choose which columns to view and the order in which they are listed.

- **Search:** specify and locate a user or range of users.

- **Detach:** display the user list in a separate dialog to expand the list view.

B. User information:

- **User ID:** user's AMPS ID.

- **Last Name:** user who holds the role.

- **First Name:** user who holds the role.

- **EDIPI:** government-authorized identification.

- **Email:** official email address.

- **Account Status:** shows whether an account is active or inactive.

C. Users to Remove from Role:

- **User ID:** user's AMPS ID.

- **Last Name:** user who holds the role.

- **First Name:** user who holds the role.

- **Role Display Name:** the role name displayed in AMPS.

D. Action buttons:

- **Add: a**dd selected user to the list of users to be removed from the selected role.

- **Remove:** take the selected user off the Remove list.

Figure 487: Application Access Removal - Search by Role/Search by User

Tour of Review Screen

The **Review** screen is displayed next. This screen lists all the selections you have made and identifies any that cannot be processed or that will be processed with changes to pending SAARs already awaiting action.

In the example shown in Figure 488, the Data Owner has selected three roles to remove from the AMPS account of user DRT0021:

- The first selection has a **Warning** message attached. The **Status Reason** explains why AMPS attached the **Warning**. In this example, the role is part of a pending SAAR associated with the role and the user. The user may have requested the role, but the role has not been closed through the provisioning process. The Data Owner can process the selection as it is shown or remove it from the list.

- The second selection has an **Error** message attached. The **Status Reason** explains why AMPS cannot process this selection. The Data Owner can remove the selection from the list, but if the item remains in the list, AMPS automatically removes this item after the Data Owner clicks the **Next** button. With either action, AMPS does not process the request.

- The third selection has a **Status** of **Valid**. AMPS can process this selection as is.

Note:

The Remove Selected Items from List button at the bottom of this page allows the Data Owner to remove one or more list items prior to proceeding to the next screen.

1. As the instruction for this screen states, the Data Owner can take advantage of this pause in the process to review the selections to ensure they are valid.

2. A **WARNING** status alerts the Data Owner to a situation in which the assigned role is undergoing more than one action. In the example shown, the role specified by the Data Owner for removal has already been submitted for removal, and the SAAR for that removal is still pending.

3. An **ERROR** status indicates an insurmountable problem with the current request, including one of the four following conditions:

   a. The user does not exist.

   b. The role does not exist.

   c. The user does not have the role.

   d. The role being removed is a Primary Role and the user would still have Additional Only roles associated with their account.

   The Status Reason column explains which condition is causing the error.

4. A VALID status indicates that AMPS has found no issues with the request and will process the request as submitted.
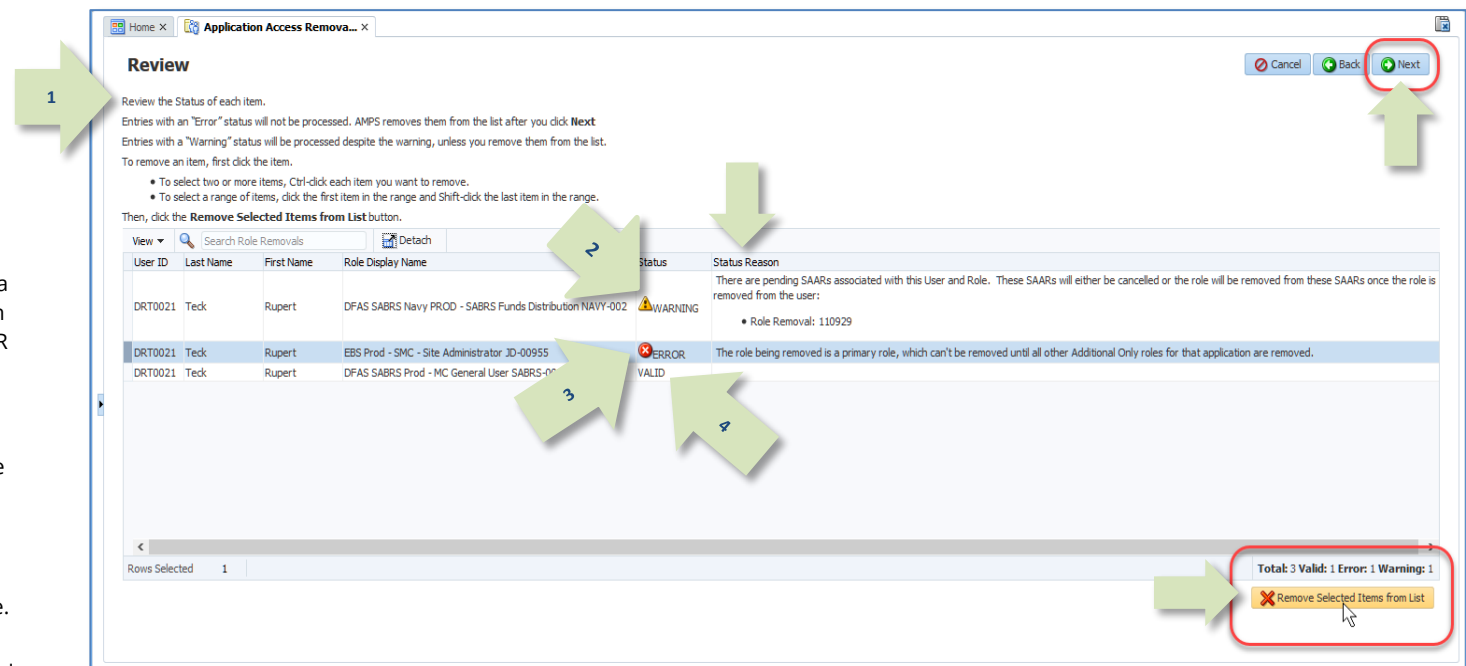
Figure 488: Application Access Removal - Review Screen

Tour of Justification Screen

The **Justification** screen is displayed next. AMPS requires the Data Owner to enter a justification for each request. In the example shown in Figure 489, the sample text entered is minimal. The Data Owner's business process may require much more detailed information.

The text area provided for Justification entries is large enough to accommodate several hundred alphanumeric characters, which the Data Owner can use to record the appropriate reasoning that supports access removal actions.
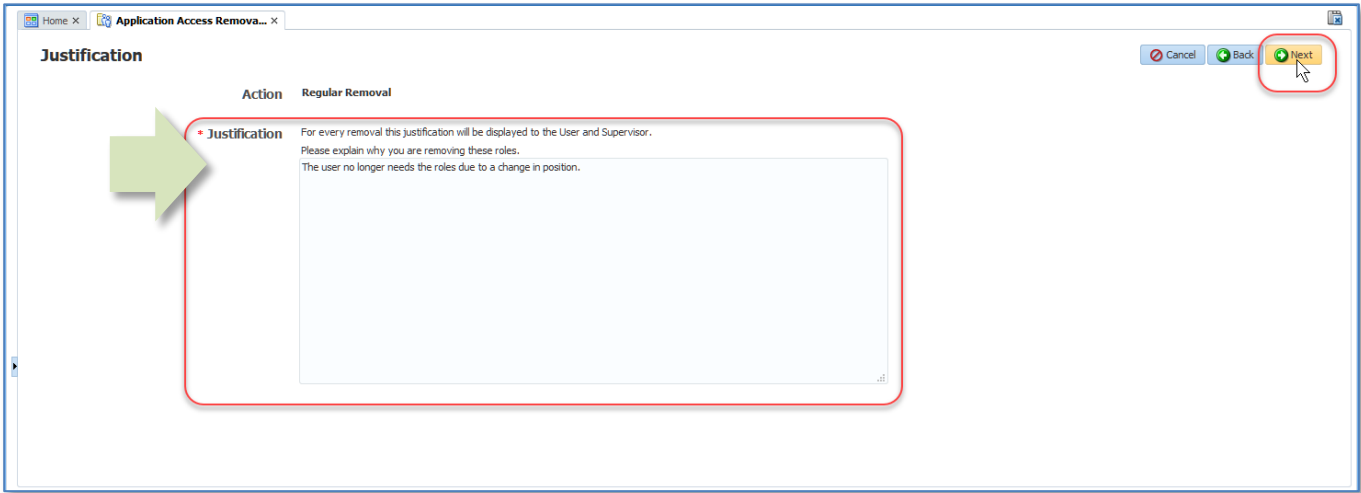
Figure 489: Application Access Review – Justification Screen

Tour of Summary Screen

The Summary screen is displayed next. On this screen, AMPS provides the Data Owner a chance to review their justification statement and combined information for the role(s) and user(s) affected by the removal action. After the Data Owner verifies the information is correct, they submit the request and AMPS processes the removal entries.

Note:

AMPS has removed all items that had an Error status on the Review page.

A. **Justification:** displays the Data Owner's statement to justify the removal(s).

B. **Entries to Process:** Each entry in this table provides user and role information and will generate a SAAR.

   a. **View:** choose which columns to view and the order in which they are listed.

   b. **Search:** specify and locate an entry.

   c. **Detach:** display the entries in a separate dialog to expand the list view.

C. Entry Data:

   a. **User ID:** user's AMPS ID.

   b. **Last Name:** user who holds the role.

   c. **First Name:** user who holds the role.

   d. **Role Display Name:** the role name displayed in AMPS.

   e. **Application:** the application to which the role belongs.
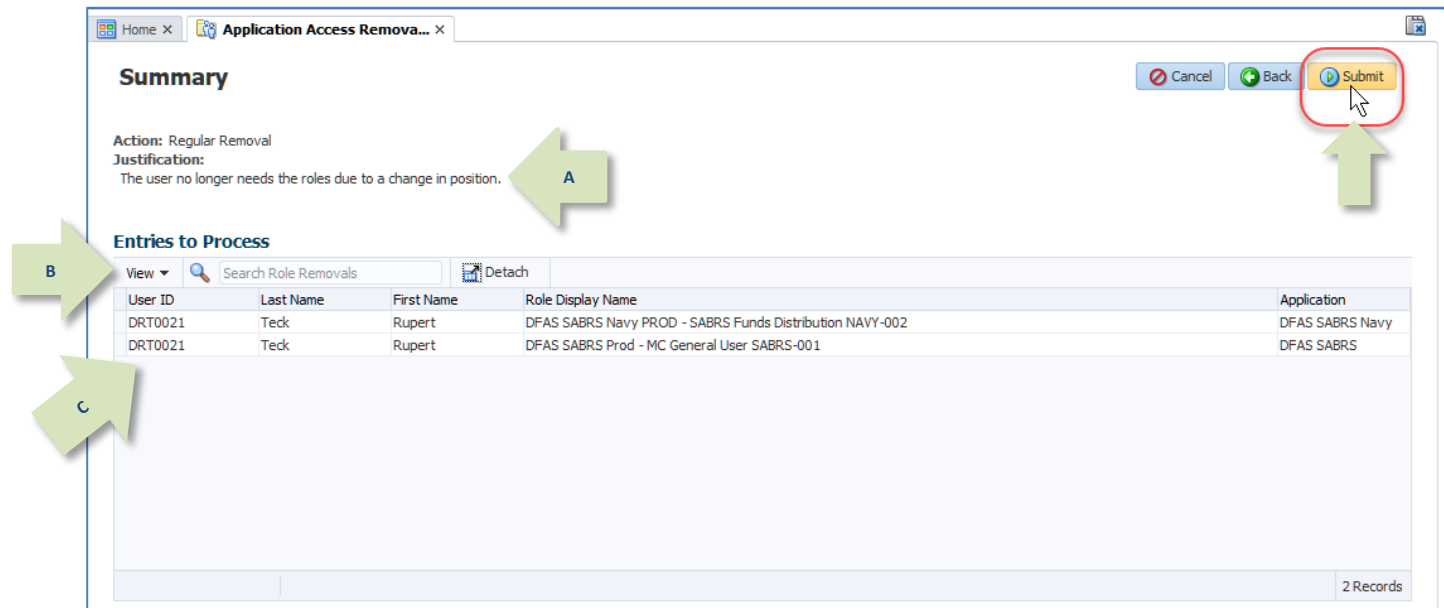
Figure 490: Application Access Removal – Summary Screen

Tour of Confirmation Screen

The Confirmation screen is the last screen displayed in the process. AMPS provides the same information for the entries to process provided on the Summary screen but adds the number for each SAARs generated to process the removal entries. In addition, the Data Owner may download a file containing the final list of removal entries.

A. **SAARs created:** Each entry in this table provides information for each SAAR generated.

   a. **View:** choose which columns to view and the order in which they are listed.

   b. **Search:** specify and locate a SAAR.

   c. **Detach:** display the entries in a separate dialog to expand the list view.

B. **SAAR ID:** the SAAR number.

C. **Download List:** button to download a CSV file of your list.

D. **OK:** button to close the screen and opens the Activity Selection screen.
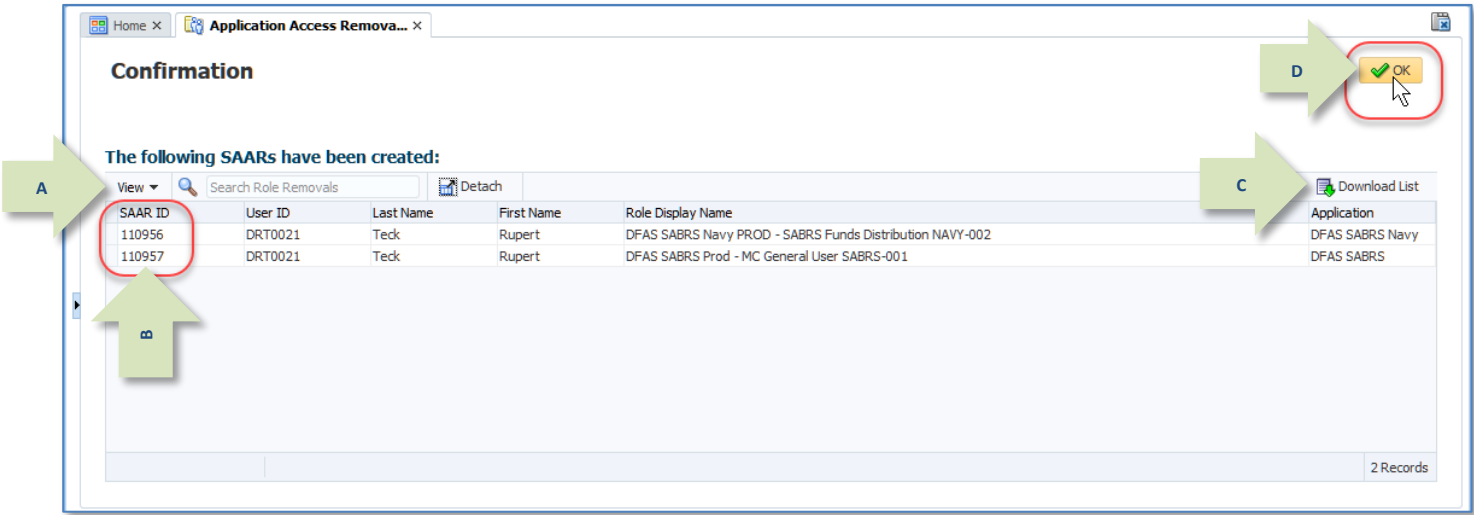
Figure 491: Application Access Removal - Confirmation

How to Request an Application Access Removal

Prerequisites	To get access to the **Application Access Removal** utilities, an application manager—such as a Data Owner or Provisioner—must request a role. This role type was established for application owners to create individual roles for administrators who have the responsibilities of (a) reconciling roles between AMPS accounts and resource accounts and (b) managing the removal of multiple users from roles or multiple roles from users. An application owner can create a role for each application, providing the role holder with access to the application's users and roles. Each Application Manager role grants access to the Application Access Removal screens and procedures.

What You Can Do:	In the Application Access Removal screen, you can perform the following tasks:
	Screen 1: Select the type of removal action needed.
	Screen 2: Download a template.
	      Upload a list of users and roles.
	      Select users and roles.
	    • Choose application.
	    • Search by Role: The object is to find a role and remove selected users or all users from the role.
	    • Search by User: The object is to find a particular user and remove the user from a role or list of roles.
	Screen 3: Review the status of your request entries for warnings and errors.
	      Remove undesirable entries.
	Screen 4: Enter a justification for your request.
	Screen 5: Review a summary of your request.

Where to Begin:	The application administrator starts by collecting the role and/or user information required by the access removal process and logging in to AMPS.

Select an Activity

Access to the **Application Access Removal** screen is available from the AMPS Main Menu:

1. After you launch AMPS, open the **Manage Home** page.

2. Click the Application Access Removal tile.

   *AMPS opens the **Application Access Removal** screen (see Figure 492).*

3. Carefully read the description next to each activity type.

4. Click the link for the activity that best suits your goal.

Note:

Although the backend processes provide different outputs, the request procedure is the same for Regular Removal and Reconciliation activities.
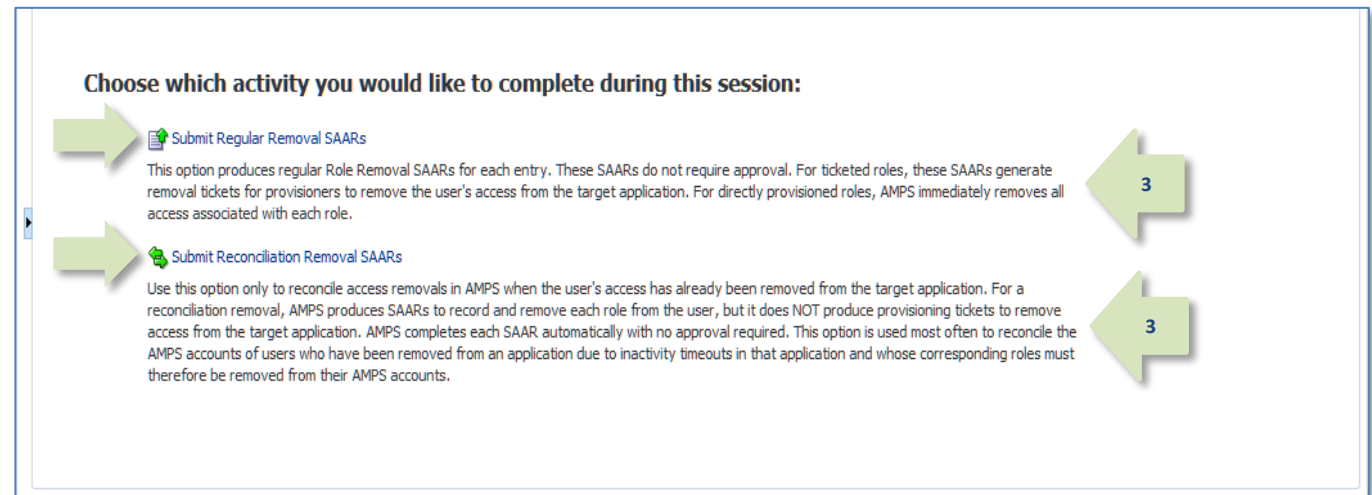
Figure 492: Application Access Removal – Select Activity

List Building by Role

5. Select the **Search by Role** tab.

   (Allow the screen to refresh.)

6. Click the **Select Application** field to open a dropdown menu.

   (If you manage only one application, this field is read only.)

7. Select the application you want to manage from the dropdown menu (not shown).

   *AMPS populates the **Application Roles** table with roles from the application you selected.*

8. Search for and select the role you want to manage.

   (You can narrow your search by using the search field.)

   *AMPS populates the **Users In Selected Role** table.*

9. Search for and select the user(s) you want to remove from the role.

   (You can narrow your search by using the search field.)

10. Click the **Add** button.

    *AMPS creates an entry in the **Users to Remove from Role** table.*

11. Repeat steps 5 to 10 as needed.

12. (optional) To remove an entry from the **Users to Remove from Role** table, select the entry and click the **Remove** button.

13. Click the **Next** button when your list of users and roles is complete.

    *AMPS opens the **Review** screen (see Figure 499).*

14. (optional) Click the **Cancel** button to clear all entries and start over.

Figure 493: Application Access Removal – Search by Role

The purpose of the search screen is to build a list of entries in the **Users to Remove from Role** table. Whether you use the **Search by Role** method (above) or the **Search by User** method (see Figure 494), the end result is the same: a list of users and associated roles to submit to the **Application Access Removal** process. You can use one or a combination of both methods to create your list.

List Building by User

5. Select the **Search by User** tab.

   (Allow the screen to refresh.)

6. Click the **Select Application** field to open a dropdown menu.

   (If you manage only one application, this field is read only.)

7. Select the application you want to manage from the dropdown menu (not shown).

   *AMPS populates the **Users** table with users assigned roles from the application you selected.*

8. Search for and select the user you want to manage.

   (You can narrow your search by using the search field.)

   *AMPS populates the **Selected User's Role in Application** table.*

9. Search for and select the user's role(s) you want to remove.

   (You can narrow your search by using the search field.)

10. Click the **Add** button.

    *AMPS creates an entry in the **Users to Remove from Role** table.*

11. Repeat steps 5 to 10 as needed.

12. (optional) To remove an entry from the **Users to Remove from Role** table, select the entry and click the **Remove** button.

13. Click the **Next** button when your list of users and roles is complete.

    *AMPS opens the **Review** screen (see Figure 499).*

14. (optional) Click the **Cancel** button to clear all entries and start over.

Figure 494: Application Access Removal - Search by User

The purpose of the search screen is to build a list of entries in the **Users to Remove from Role** table. Whether you use the **Search by User** method (directly above) or the **Search by Role** method (see Figure 493), the end result is the same: a list of users and associated roles to submit to the **Application Access Removal** process. You can use one or a combination of both methods to create your list.

Bulk-List File Option

You can submit a removal list through a bulk-removal CSV file. Access to this process is through the "search" screen.

Download Template

1. Click on the Download Template Removal File button.

   Your browser will open a popup with your download options.

2. Select **Save As** and save the template file to your local drive. (Rename the file as needed.)

Prepare Your List

3. Open the template file in Excel.

4. Edit the file to create your list of users to remove from roles:

   a. Remove the sample entry.

   b. Add **User Login** to column **A**.

   c. Add associated **Role Display Name** to column **B**.

   d. Repeat b and c as needed.

5. Save your completed CSV file. (Rename the file as needed.)

   Do not change the file format. It must be in the CSV file format.

Upload List

6. Click the Upload List of Users to Remove button.

   AMPS opens a browse window for you to select your list file.

7. Select your file and click **OK**.

   AMPS checks the file for errors, and provide a message box if a problem is detected.

8. Click **OK** to close the message box.

9. Correct all errors in your file and repeat steps 6 to 8 as needed.

10. AMPS populates the **Users to Remove from Rol**e table with the information in you CSV file. Continue from step 12, page 474.
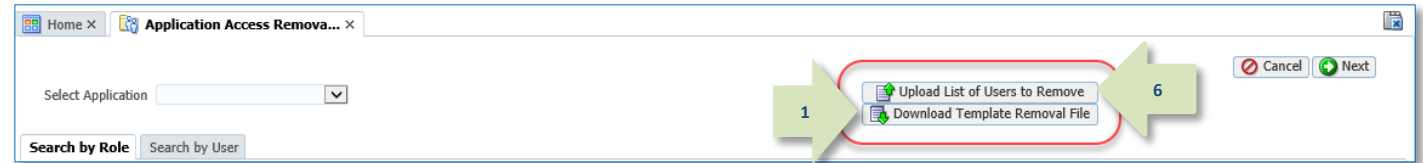
Figure 495: Application Access Removal - Bulk List Options

Figure 496: Application Access Removal – Sample Template File (CSV)
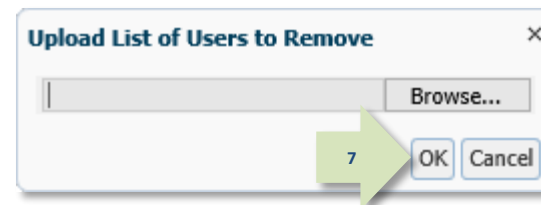
Figure 497: Upload List of Users to Remove – File Browse Window
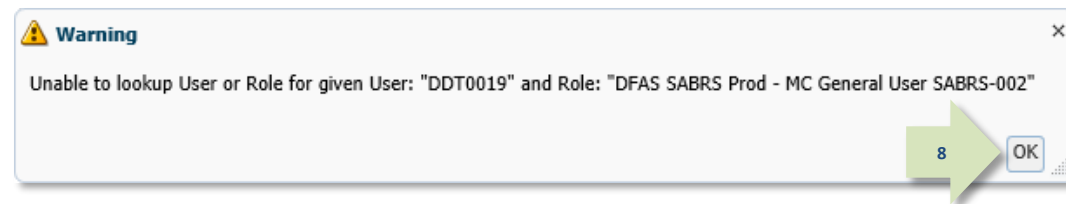
Figure 498: Sample File-Upload Warning

(This warning message was received for an incorrect role name.)

Review Errors and Warnings

This screen displays all the selections you have made and identifies any that cannot be processed or that will be processed with changes to pending SAARs already awaiting action.

Note:

Error and warning information is provided at the top of the page, along with instructions on how to remove items from your list.

15. Review the **Status** of each item.

    a. A **WARNING** status indicates the assigned role is undergoing more than one action.

    b. An **ERROR** status indicates an insurmountable problem.

    c. A **VALID** status indicates no problems were detected.

    *(See **Tour of Review Screen** for more information.)*

16. Review the **Status Reason** on items with a warning of error status.

17. Select any items you want to remove from your list.
    (Removing items with an ERROR status is not required. AMPS automatically removes these when you proceed to the next screen.)

18. Click the Remove Selected Items from List button.

    AMPS removes the selected items from your list.

19. Click the **Next** button.

    AMPS opens the Justification screen (see Figure 500).
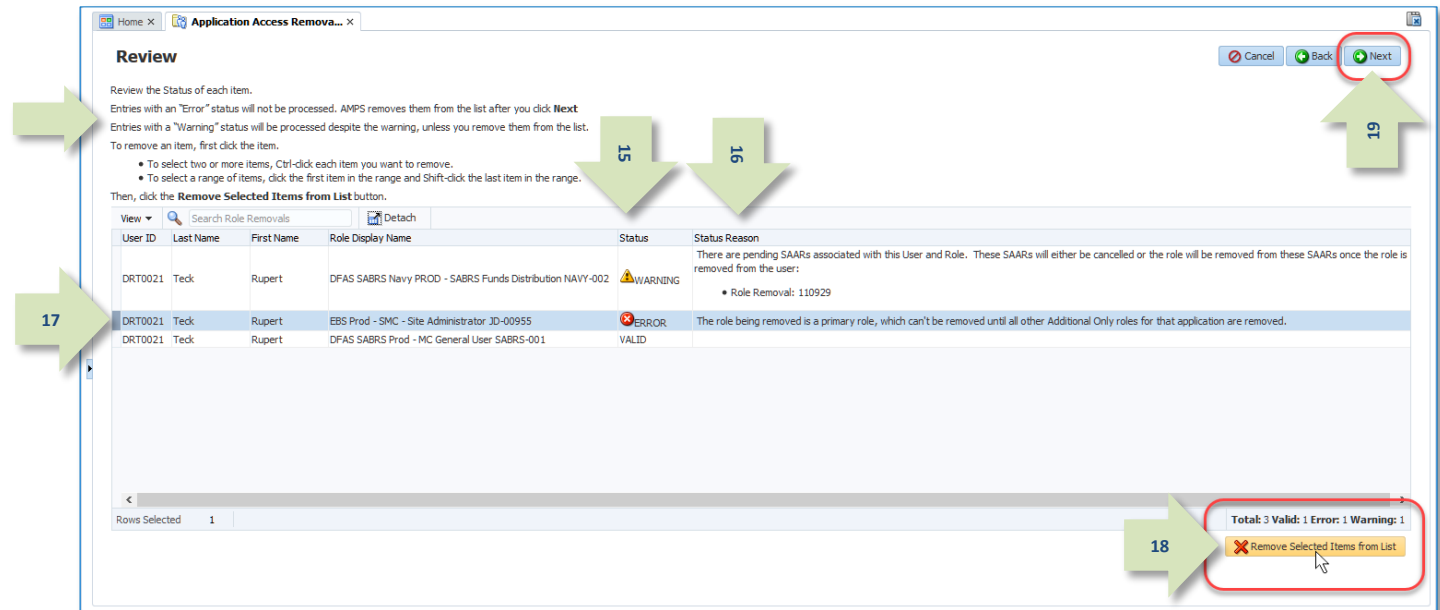
Figure 499: Application Access Removal – Review

Justification and Action

AMPS requires the Data Owner to enter a justification for each request.

In the example shown in Figure 500, the sample text entered is minimal. The Data Owner's business process may require much more detailed information.

20. Verify the **Action** displayed by AMPS is the correct action.

    a. **Regular Removal**: produces Role Removal SAARs that generate provisioning tickets for ticketed-type roles.

    b. **Reconciliation Removal**: produces SAARs to remove each role from the user in AMPS only. This generates no provisioning tickets.

21. If the **Action** displayed is not correct, click the **Cancel** button to return to the activity selection screen (step 4, page 472) and restart the request process.

22. If the **Action** displayed is correct, enter the appropriate reasoning that supports the access removal in the **Justification** text box.

23. Click the **Next** button.

    *AMPS opens the **Summary** screen (see Figure 501).*

Figure 500: Application Access Removal – Justification

Summary and Submission

AMPS provides a summary to give you a chance to review your list, justification, and action, prior to submitting the list for processing.

24. Review your **Justification** statement.

25. Review each item in the **Entries to Process** table.

26. If you want to make any changes, click the **Back** button as needed.

27. Click the **Submit** button.

    *AMPS process your request, creates SAARs and tickets as needed, and opens the **Confirmation** screen (see Figure 502).*
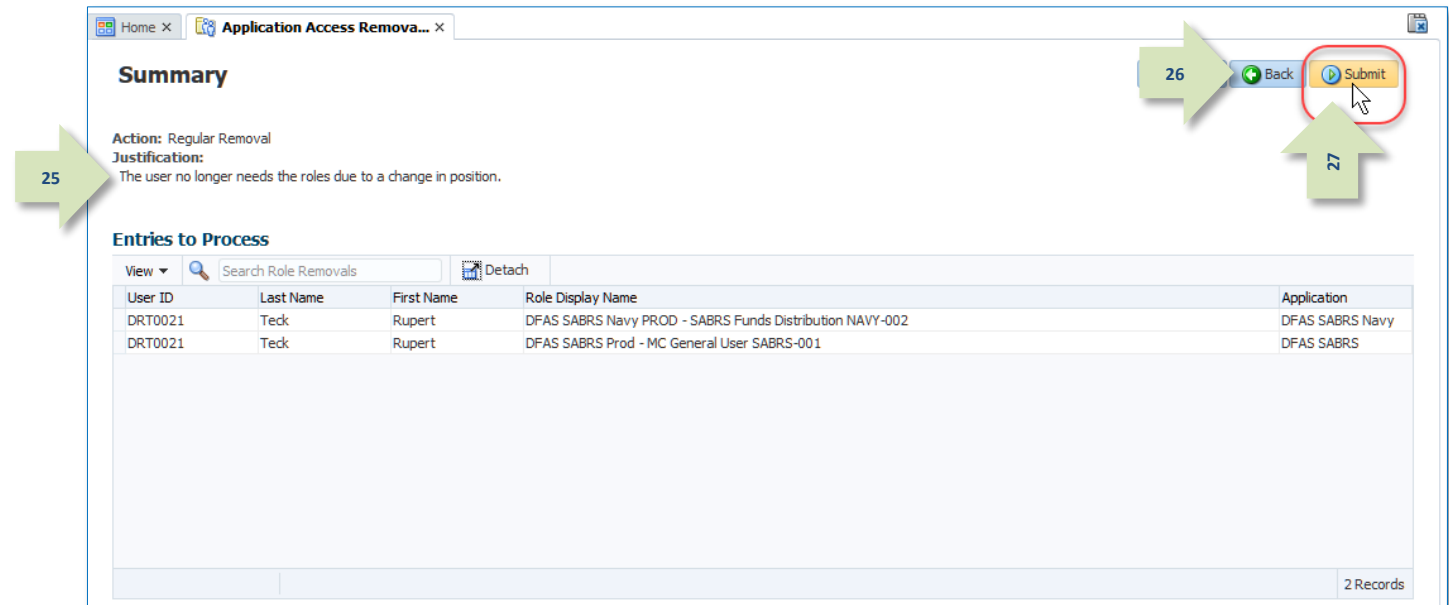
Figure 501: Application Access Removal - Summary

Confirmation

The **Confirmation** screen provides SAAR information and a means to download a file of your list.

28. Review the SAARs in the table. Make note of the SAAR ID(s).

29. (optional) Click the **Download List** button to download a CSV file of your list.

    Your browser will open a popup with your download options.

30. Select **Save As** and save the list file to your local drive. (Rename the file as needed.)

31. Click the **OK** button.

32. AMPS returns the user to the **Activity Selection** screen.
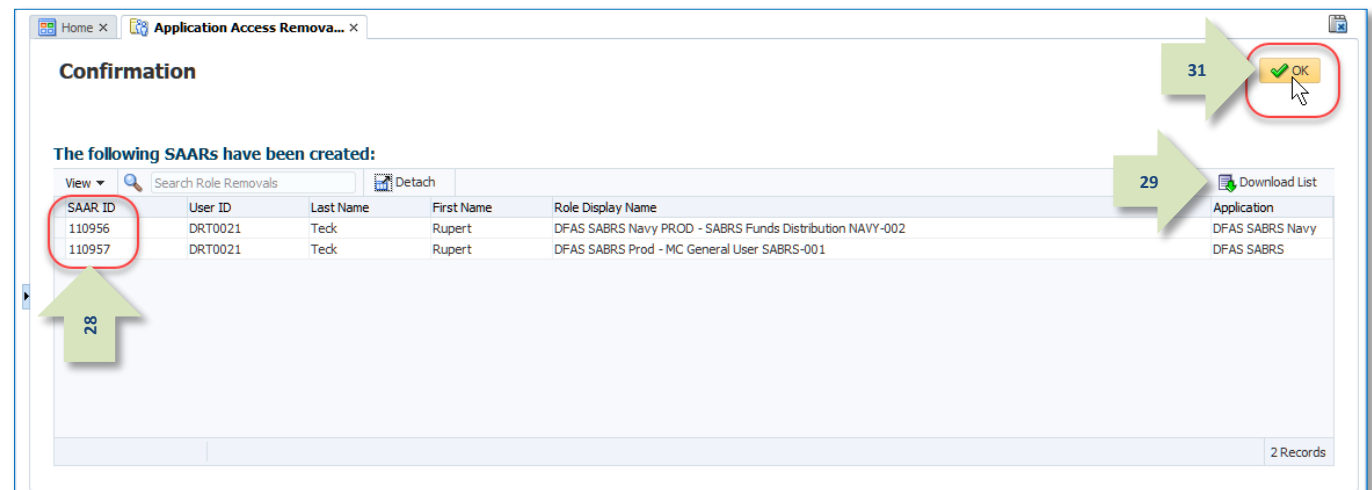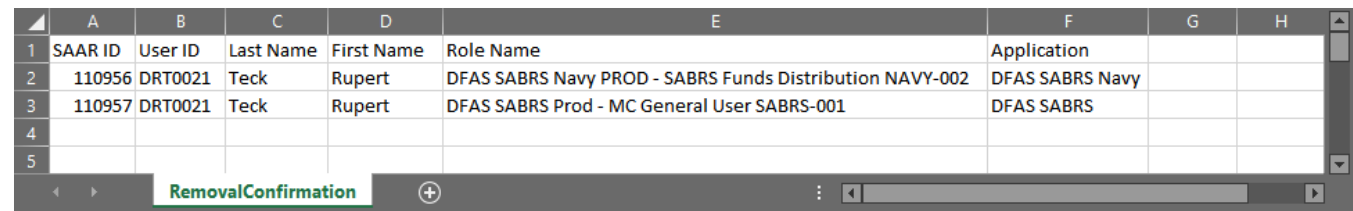
Figure 502: Application Access Removal - Confirmation

Confirmation List File

AMPS does not require you to download the Removal Confirmation list file, but this could prove useful in the future, should you need a record of your transaction(s).

The downloaded CSV file contains the same information that appears in the table on the **Confirmation** screen (see Figure 502).

	A	B	C	D	E	F	G	H
1	SAAR ID	User ID	Last Name	First Name	Role Name	Application		
2	110956	DRT0021	Teck	Rupert	DFAS SABRS Navy PROD - SABRS Funds Distribution NAVY-002	DFAS SABRS Navy		
3	110957	DRT0021	Teck	Rupert	DFAS SABRS Prod - MC General User SABRS-001	DFAS SABRS		
4								
5								

RemovalConfirmation

Figure 503: Application Access Removal – Sample Removal Confirmation List (CSV)

Email Notifications

After you submit an Access Removal request, AMPS sends the user and the user's supervisor an email notification informing them of the status of the role removal request.

There is no action required by the user or the supervisor.

The email contains the SAAR number, SAAR Type, Removal Type, Role name, Justification, name, and User ID of the administrator requesting the removal and when the request was submitted.

Note:

AMPS sends the email in HTML format, but it can also be viewed in plain text. The sample provided in Figure 504 is an image of the email viewed in HTML format.

Sample User and Supervisor Notifications: SAAR Status

amps.user@dla.mil 4/10/2018

Notification: SAAR #110956 - Remove User Access for Rupert Teck (DRT0021) (DFAS Columbus) (DF...

Signed By amps.user@dla.mil

SAAR #110956 has been submitted for removal of: DFAS SABRS Navy PROD - SABRS Funds Distribution NAVY-002 with access to DFAS SABRS Navy.

No action is required by you at this time.

SAAR	110956
SAAR Type	Role Removal
Removal Type	Regular Removal
Role to Remove	DFAS SABRS Navy PROD - SABRS Funds Distribution NAVY-002
Justification	The user no longer needs the roles due to a change in position.
Submitted Date	04/10/2018 16:42:31 UTC
Submitted By	Down, Brenda (DBD0014)

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

Figure 504: Application Access Removal - Sample Initial Email

After AMPS prepares the request for provisioning, AMPS sends the user an email notification informing them that the process of removing the role has started.

Sample User Notification: Role Deprovisioning Process Started

Subject: AMPS Application processing for SAAR #110956

Body: AMPS application processing for SAAR 110956 has started for DFAS SABRS Navy.

AMPS provides this message for notification only. Please do not respond to this message. If you need IT assistance, please contact the DISA Global Service Desk by calling toll free 844-DISA-HLP (844-347-2457) or DSN 850-0032 (press 5, then speak or enter D-L-A) or visit the DLA Service Portal (.mil only) at https://dla.servicenowservices.mil/sp?id=index

AMPS creates the provisioning ticket and sends an email notification to the application provisioner. The email provides instructions and information about the pending deprovisioning task.

The provisioner logs in to AMPS, opens their AMPS **Inbox**, locates the SAAR in the **My Tasks** view and clicks on the SAAR Title.

AMPS opens the provisioning task. See Figure 505 for a sample Total AMPS Ticket for an Application Access Removal.

Sample Provisioner Notification: Action Required

Subject: AMPS Application Processing for SAAR #110956 requires your attention.

Body: AMPS Application Processing request for SAAR 110956 requires your attention.

Please visit AMPS at this URL:
https://amps.dla.mil/

Open your Inbox to locate the SAAR. Click the SAAR title to open and complete the task.

Task Details:

Request For:
DLA Login: DRT0021
Name: Teck, Rupert
Phone: 888-555-1212
Email: Rupert.Teck@dla.mil
EDIPI/UPN: 1286972493

Access Information:
SAAR #: 110956
Remove Job Role: DFAS SABRS Navy PROD - SABRS Funds Distribution NAVY-002
Applications and Access:
        Resource: DFAS PROD - DFAS SABRS Navy
                Remove: NAVY- 002 FUND#AUT; Table 204; 205; 507 and N$USR180

Justification: The user no longer needs the roles due to a change in position.
Optional Information: (none)
Role Removal SAAR requested by Brenda Down on 04/10/2018

Total AMPS Provisioning Ticket

After the provisioner opens the ticket, they have several options: claim the ticket, save comments on their progress only, or complete the deprovisioning work and close the ticket.

1. Check the **Work Details** section for instructions about the provisioning request.

   In the sample screen, the **Work Details** *indicate the provisioner is to remove the specified role currently assigned to the user listed in the* **User Summary**.

2. Enter text in the **Comments** area to clarify the current action taken.

   Comments *text is required, but since a provisioning ticket can be opened, closed, and reopened before it is complete, you can enter progress notes or other appropriate text to clarify the status of the provisioning task.*

   To save comments and reopen the ticket later, click **Save Comments**. *Reopen the ticket from the* **My Tasks** *view in your* **Inbox**.

3. When the deprovisioning tasks are complete, click **Work is Completed.**

   AMPS closes the provisioning ticket screen.

   AMPS then notifies the user that the deprovisioning actions are complete and the user's application access privileges have been removed (see below).

Figure 505: Application Access Removal – Sample Total AMPS Provisioning Ticket

Final Email Notification

AMPS provides email notification to the user when their AMPS access has been removed.

The email contains the SAAR number, SAAR Type, Removal Type, Role name, Justification, name, and User ID of the administrator requesting the removal and when the request was submitted.

The Justification text is the text entered by the Data Owner during the request.

Note:

> AMPS sends the email in HTML format, but it can also be viewed in plain text. The image provided in Figure 336 is a sample image of the email viewed in HTML format.

Sample User Notification: Role Removal Complete
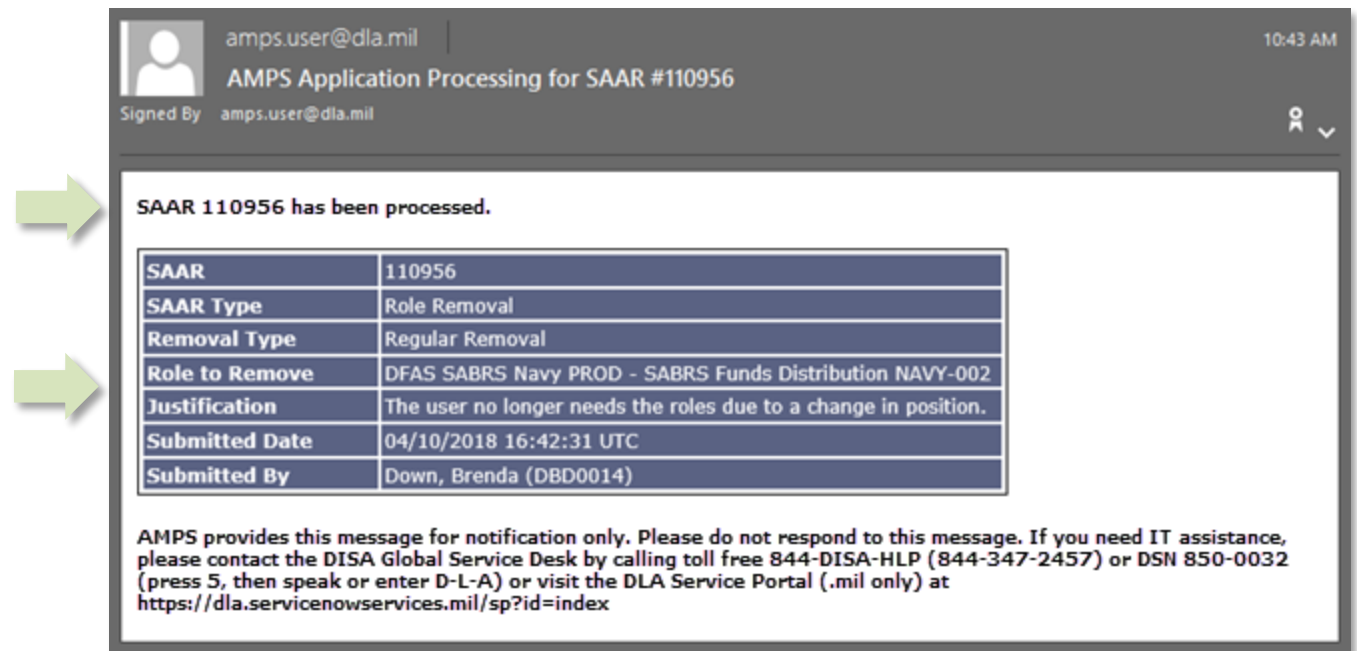
Figure 506: Application Access Removal - Sample Final Email

Appendix A: Online Forms

This appendix lists and describes online forms displayed in AMPS.

What is a Privacy Act Statement?

The following information is taken from "What is a Privacy Act Statement" (Department of Homeland Security: https://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_e3.pdf):

> What is a Privacy Act Statement?
>
> The Privacy Act of 1974, 5 USC 552a, provides protection to individuals by ensuring that personal information collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon individual privacy.
>
> Pursuant to 5 U.S.C. §552a (e) (3) agencies are required to provide what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security Number). Department of Homeland Security (DHS) policy is to provide a Privacy Act Statement regardless of whether the collection is part of a system of records or not. All Privacy Act statements must be reviewed by the Privacy Office or component Privacy Officer.

AMPS includes a **Privacy Act Statement** that is relevant to your organization:

- If you are a DLA application user, you will see the DLA Privacy Act Statement when AMPS is prompted to display it.
- If you are a DFAS application user, you will see the DFAS Privacy Act Statement when AMPS is prompted to display it.

Read these statements carefully to understand the policies that govern the use and storage of any Personally Identifiable Information (PII) that you enter in AMPS.

When is the Privacy Act Statement Displayed in AMPS?

The Privacy Act Statement for your organization is displayed the first time you access one of the functional areas where PII is entered and stored:

- *My Information* screen and tabs: displayed the first time you click the **My Information** tile on the **Self Service Home** page during the current session. Each time you log in to AMPS, you start a new session; if you open the **My Information** screen during a new session, AMPS displays the **Privacy Act Statement**. The Privacy Act statement is displayed in this area only once during a session.
- *Role Request* screen sequence: displayed the first time you click the **Request Role** tile on the **Self Service Home** page during the current session. Each time you log in to AMPS, you start a new session; if you start the **Role Request** sequence during a new session, AMPS displays the **Privacy Act Statement**. The Privacy Act Statement is displayed in this area only once during a session.

Corrected Links:

- **Routine Uses:** http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx
- **DLA System of Record Notices (SORNs):** http://dpcld.defense.gov/Privacy/SORNsIndex/tabid/5915/Category/11156/defense-logistics-agency.aspx
- **DFAS System of Record Notices (SORNs):** http://dpcld.defense.gov/Privacy/SORNsIndex/tabid/5915/Category/11156/defense-logistics-agency.aspx

DLA Privacy Act Statement

The links on these pages have been updated recently. Please see the Corrected Links section on page 483.

Figure 507: DLA Privacy Act Statement

DFAS Privacy Act Statement

Figure 508: DFAS Privacy Act Statement

Consent to Monitoring (CTM)

The following text appears in the **STANDARD MANDATORY DoD NOTICE AND CONSENT AGREEMENT** (Consent to Monitoring or CTM) screen displayed to each user before AMPS displays the user's **Annual Revalidation Request** screen. After reading the information on the screen, the user must click the **I Accept** button to acknowledge the rules and signify a promise to follow the rules.

Defense Logistics Agency (DLA)

STANDARD MANDATORY DoD NOTICE AND CONSENT AGREEMENT

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:

  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.

  - At any time, the U.S. Government may inspect and seize data stored on this information system.

  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests-not for your personal benefit or privacy.

  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privileged or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

I acknowledge receipt of the Standard Mandatory DoD Notice and Consent Agreement.

General Rules of Behavior (GROB)

The following text appears in the **General Rules of Behavior** screen displayed to each user before AMPS displays the user's **Annual Revalidation Request** screen. After reading the information on the screen, the user must click the I Accept button to acknowledge the rules and signify a promise to follow the rules. (Revised August 2017)

Defense Logistics Agency

Information Assurance (IA): Rules of Behavior

General User Agreement

The Information Assurance (IA) rules of behavior included in this agreement delineate the responsibilities and expectations of all individuals with access to DLA information systems. All individuals will review and provide a signature (manual or digital) acknowledging these rules prior to being granted access to any DLA network and/or application.

1. **What is the purpose of the IA Rules of Behavior?**

These IA rules of behavior (including Privileged User and Secret Internet Protocol Router Network (SIPRNET) IA rules, which are contained in separate "user agreements") were established to hold users accountable for their actions and responsible for securing Government data and Information Technology (IT) resources.

2. **What are IA rules of behavior?**

IA rules of behavior summarize laws and requirements from various Department of Defense (DOD) and DLA policies, instructions, manuals, etc., with regard to authorized DLA information system use. IA rules of behavior establish standards of conduct that are vital to a sound and secure enterprise information operations infrastructure. The IA rules of behavior highlight the need for users to understand that taking personal responsibility for securing DLA information and IT resources is an essential part of their mission.

3. **Who is covered by these rules?**

These rules are to be followed by the entire DLA workforce (civilian, military, and contractor) with access to DLA systems, networks, and internal web sites. This DLA workforce should be fully aware of, and abide by, DLA security policies as well as related DOD policies.

4. **What are the penalties for Noncompliance?**

Noncompliance to these rules will be enforced through sanctions commensurate with the level of infraction. Actions may result in removal of system access.

Misuse of Privacy Act data may result in civil and criminal charges and fines.

5.   Users will:

a. Safeguard the information processed, stored, and transmitted on DLA information systems from unauthorized or inadvertent modification, disclosure, destruction, and misuse. DLA information systems are for official use and authorized purposes in accordance with DOD 5500.7-R, Joint Ethics Regulation, section 2-301.

b. Comply with safeguards, policies, and procedures to prevent unauthorized access to DLA information systems.

c. Comply with terms of software licenses and only use DLA licensed and authorized software. Additionally, users will not install single license software on shared hard drives (or servers) without prior approval.

d. Complete periodic IA awareness training when made available.

e. Use DLA Internet access and electronic mail (email) services for non-official purposes only under the following circumstances: I) Usage does not adversely affect the employee's performance or accomplishment of the DLA or DOD mission and usage does not reflect adversely on DLA, DOD, or the Federal Government as a whole; 2) Usage will occur on breaks, lunch periods, and non-duty hours; and 3) Usage precludes any unnecessary costs or appearance of impropriety to the Federal Government.

f. Not transmit sensitive information over the Internet unless it has been encrypted and digitally signed using a Common Access Card (CAC) based DOD public key certificate.

g. Digitally sign email containing attachments and embedded hyperlinks.

6.   Not use DLA Internet access and email services to:

a. Knowingly view, receive, or transmit material with pornographic content.

b. Conduct illegal activities and soliciting for personal gain.

c. Download copyrighted software without express permission.

d. Download without ensuring protection against viruses.

e. Misrepresent personal opinion as official information.

f. Knowingly distribute chain letters, extremist or terrorist material advocating the violent overthrow of the government and/or material or jokes that demean or ridicule others on the basis of race, creed, religion, color, sex, disability, or national origin.

g. Not engage in deliberate activities that overload network resources (e.g., downloading music or video files). Network bandwidth consumption caused by such downloads may inhibit or prohibit network service to other users.

h. Promote partisan political activity.

i. Access, store, process, display, distribute, transmit, or view material that is abusive, harassing, defamatory, vulgar, profane; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, Federal, national, or international law.

j. Access, store, process, or distribute Classified, Proprietary, or Privacy Act protected information in violation of established security and information release policies.

k. Use the DLA network resources for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay). This does not prohibit the use of a local intranet for bulletin boards/want ads.

l. Disseminate religious information unrelated to DLA's established religious program;

m. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers, charitable fund raisers).

n. Gamble, wager, or place any bets.

NOTE: Although DLA uses Web filtering technology to prevent access to inappropriate Web sites, it is not a complete solution and the ability to access a Web site does not mean that it is not prohibited. It is a user's responsibility to recognize the accountability assigned when given authorized access to any DLA information system. Individual user activity is recorded, including Internet and Intranet sites and files accessed.

o. Not knowingly write, code, compile, store, transmit, or transfer unauthorized software code, Trojan horse programs, or malicious software code, to include viruses, logic bombs, worms, and macro viruses into any DLA information system.

p. Not attempt to bypass the Web filtering system (e.g., installing proxy bypass software).

q. Not share account passwords with anyone, including Personal Identification Numbers (PIN) for CAC associated with the Public Key Infrastructure.

r. Not attach any non-DLA issued device (e.g., personally owned Personal Digital Assistants, wireless devices) to any DLA information system without prior approval.

s. Not utilize any removable storage media (e.g., thumb drives, memory sticks, floppy disks, camera flash memory cards, high capacity ZIP floppy drives, secure digital cards other than compact discs (CD) or DVDs without prior approval.

t. Encrypt all data not approved for public release copied to a CD or DVD using approved software. Contact your local Information Assurance Officer (IAO) or help desk for assistance.

u. Immediately report known or suspected incidents to the responsible Information Assurance Manager in accordance with the DLA Computer Incident Response Guide.

v. Log out prior to leaving his/her desk/office/cubicle/work area at the end of his/her work day.

w. Lock his/her workstation when unattended for an extended period of time.

x. Remove his/her CAC from workstation when unattended.

y. Not attempt to modify automated screen-lock functions performed by the information system.

z. Scan files received from untrusted sources prior to opening them. For assistance with this function, please contact your local IAO or help desk.

aa. If applicable, process classified data on classified information systems only.

ab. Not use shared drives to relay Privacy Act data unless the data is password protected and the folder within the shared drive has access set up only for those authorized to access the data.

ac. Be cognizant of all applicable DLA IA policies.

7. Consent to Monitoring Provision

a. In addition to formally acknowledging through signature, the required provisions documented above, all users with access to a DOD information system are required to read and acknowledge the following consent to monitoring provision.

b. By signing this document, you acknowledge and consent that when you access DOD information systems:

c. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

d. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Note: Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(5) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(6) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged

communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(7) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(8) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

(9) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(10) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(11) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (law enforcement for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise authorized use or disclosure of such information.

(12) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the provisions that are set forth in this user agreement, regardless of whether the banner describes these provisions in full detail or provides a summary of such conditions. In addition, this applies regardless of whether the banner expressly references this user agreement.

I acknowledge receipt of this General User Agreement, understand my responsibilities, and will comply with these provisions when accessing a DLA information system.

Privileged Rules of Behavior (PROB)

The following text appears in the **Privileged Rules of Behavior** screen displayed to each user who requires elevated privileges. After reading the information on the screen, the user must click the **I Accept** button to acknowledge the rules and signify a promise to follow the rules. AMPS captures this acknowledgement as a digital signature and stores it with the approved SAAR. (Revised August 2017)

Defense Logistics Agency (DLA)

Information Assurance (IA): Rules of Behavior

Privileged (Access) User Agreement

Privileged users are authorized users who have the ability to modify secure configurations (e.g., access controls, etc.) or bypass IA controls enforced by DLA information systems (e.g., account setup, account termination, account resetting, auditing).

1. What is the purpose of the IA rules of behavior?

These IA rules of behavior (including general user and Secret Internet Protocol Router Network (SIPRNet) IA rules, which are contained in separate "user agreements") were established to hold users accountable for their actions and responsible for securing Government data and Information Technology (IT) resources.

2. What are IA rules of behavior?

IA rules of behavior summarize laws and requirements from various Department of Defense (DOD) and DLA policies, instructions, manuals, etc., with regard to authorized DLA information system use. IA rules of behavior establish standards of conduct that are vital to a sound and secure enterprise information operations infrastructure. The IA rules of behavior highlight the need for users to understand that taking personal responsibility for securing DLA information and IT resources is an essential part of their mission.

3. Who is covered by these IA rules of behavior?

These IA rules of behavior apply to the DLA workforce (i.e., civilian, military, and contractor), to include authorized personnel not considered members of the DLA workforce with access to DLA information systems. In particular, Privileged Users include, but are not limited to, System and Network Administrators, Web and Database Administrators, Firewall and Application Administrators, Software Developers, and Security Administrators (e.g., IA Managers (IAM), IA Officers (IAO)).

4. What are the penalties for noncompliance?

Noncompliance with these rules will result in sanctions being imposed on an individual(s) commensurate to the level of the infraction(s). Depending on the severity of the violation, sanctions may include a verbal or written/reprimand, removal of information system access for a specified period of time, reassignment to other duties or termination. Misuse of Privacy Act, sensitive (to include classified) data may result in civil and criminal charges and/or fines. Military Service members may be subject to administrative or disciplinary action as authorized by applicable regulations and the Uniform Code of Military Justice.

NOTE: The rules of behavior delineated in the DLA "General User" agreement are applicable to all DLA information system users and used in conjunction with the privileged user rules of behavior documented herein.

5. Privileged Users will:

a. At a minimum, have undergone an appropriate personnel security investigation commensurate with the IT level (e.g., IT- I [privileged], IT- II [limited privileged]) required to perform the duties assigned.

b. Hold a U.S. Government security clearance, when privileged access is required for an information system storing, processing, and/or transmitting classified (i.e., Secret) information.

c. Configure and operate information systems and IA controls in accordance with applicable Security Technical Implementation Guides (STIG) and DLA policies and procedures.

d. Notify the responsible IAO of any configuration changes that might adversely impact the information system.

e. If applicable, create user accounts only after receipt of an approved system access authorization request (automated or manual).

f. Establish and manage authorized user and system (e.g., service accounts) accounts for DLA information systems, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed.

g. Not add/remove any users' names to the Root Level, Domain Administrators, Local Administrator, or Power Users group without the prior approval of the system manager and/or IAM.

h. Access only that data, control information, software, hardware, and firmware for which you are authorized access to and have a need-to-know.

i. Not access sensitive application data for other than official purposes based on roles and responsibilities associated with mission requirements.

j. Maintain separate accounts for administrative transactions (privileged account) and for day-to-day user transactions (general user account). This includes the use of privileged accounts only for privileged functions and the use of your general user account for all non-privileged functions (e.g., email, Web browsing, etc.).

k. Comply with the privileged account password construct requirement, if applicable.

l. Not share access to privileged accounts (e.g., will not share alternate tokens/personal identification numbers (PIN) or privileged account password(s) with unauthorized personnel).

m. Assume only those roles and privileges for which you are authorized.

n. Not install, modify, or remove any hardware or software (i.e., freeware/shareware and IA-related tools) without written permission/approval from the system manager and/or IAM.

o. Not obtain, install, copy, transfer, or use software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

p. Not knowingly write code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.

q. Limit the use of vulnerability scanning tools for their intended purposes and only after proper coordination with and approval by the responsible system manager and/or IAM.

r. Not attempt to run "sniffer" or hacker-related tools on any information system unless authorized by the Designated Approving Authority and system manager/IAM. This includes the introduction of any foreign devices (non-approved equipment) to any DLA information system without specific authorization.

s. Immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate system manager and/or IAM.

6. Consent to Monitoring Provision

a. In addition to formally acknowledging through signature, the required provisions documented above, all users with access to a DOD information system are required to read and acknowledge the following consent to monitoring provision.

b. By signing this document, you acknowledge and consent that when you access DOD information systems:

c. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

d. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Note: Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(5) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(6) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(7) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(8) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

(9) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(10) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(11) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (law enforcement for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise authorized use or disclosure of such information.

(12) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the provisions that are set forth in this user agreement, regardless of whether the banner describes these provisions in full detail or provides a summary of such conditions. In addition, this applies regardless of whether the banner expressly references this user agreement.

I acknowledge receipt of this Privileged User Agreement, understand my responsibilities, and will comply with these provisions when accessing a DLA information system.

Appendix B: Windows Procedures for AMPS Users

How to Disable Compatibility View Feature in IE

When you launch AMPS in Internet Explorer (IE), you may see a **Compatibility View** message. Compatibility View is meant for users who run applications developed for IE 7 and prior versions.

The **Compatibility View** in IE 8 or later can affect the display of certain screen elements, such as action buttons, in some AMPS screens. Follow these instructions to turn off **Compatibility View** and prevent IE from displaying this message again.

1. In the **Message from webpage** box, click **OK** to close the message.

   AMPS displays the Home screen in Internet Explorer.
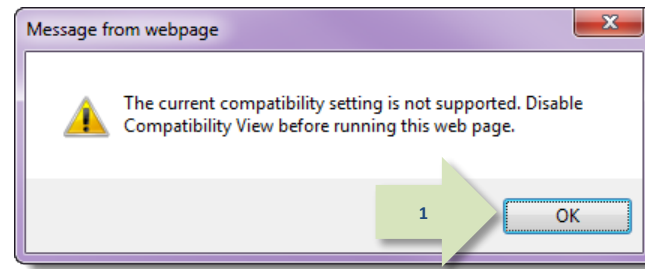
Figure 509: Compatibility View Message

2. In the IE Command Bar, click **Tools**.

   IE opens the Tools dropdown menu.

3. Click **Compatibility View Settings**.

   *IE opens the **Compatibility View Settings** dialog (see Figure 511).*
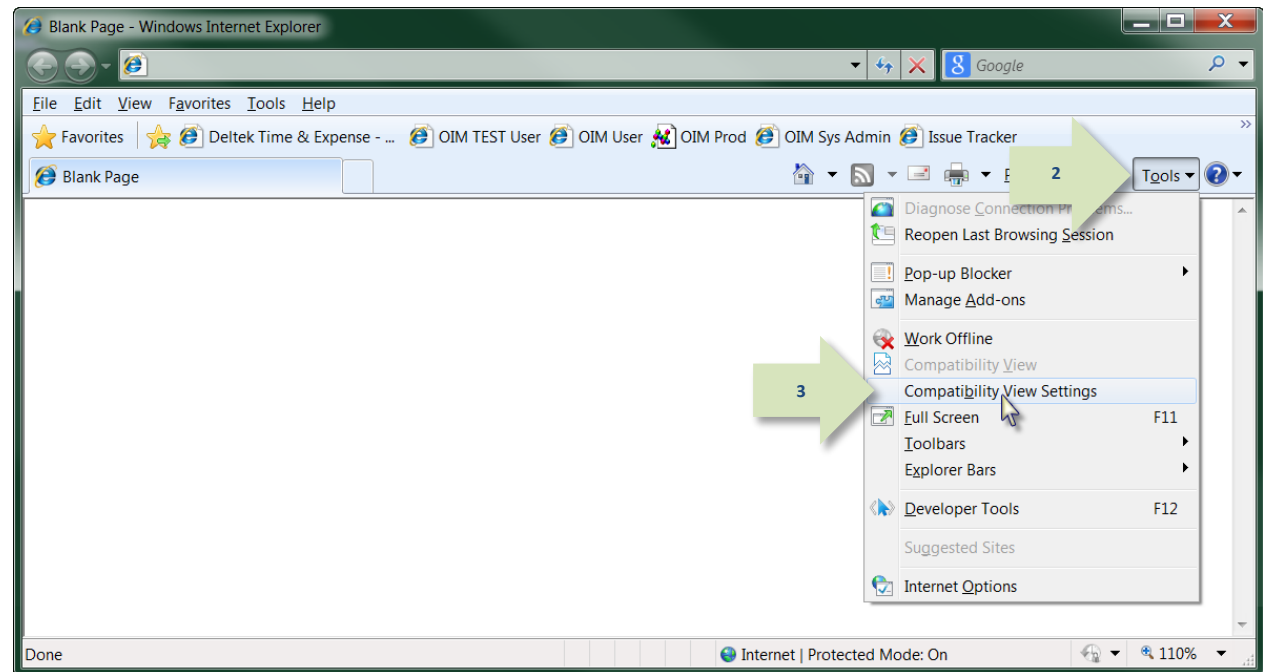
Figure 510: Internet Explorer - Tools Menu

4. Review any entries in the text area labeled **Websites you've added to Compatibility View**.

5. If your **Compatibility View Settings** dialog contains any entries for ***dla.mil***, ***dfas.mil***, or other Web sites, select each entry and click the **Remove** button.

    *IE removes the specific **Compatibility View** setting from all sites in **dla.mil** or **dfas.mil**.*
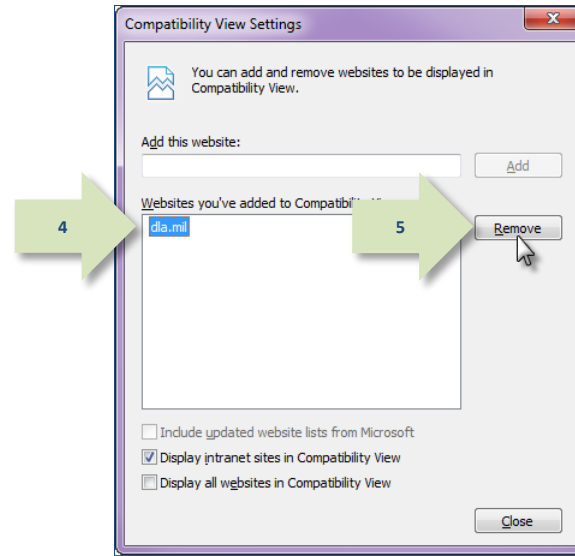
Figure 511: Compatibility View Settings: Remove All Web Sites

6. Locate the checkbox for option to Display intranet sites in Compatibility View.
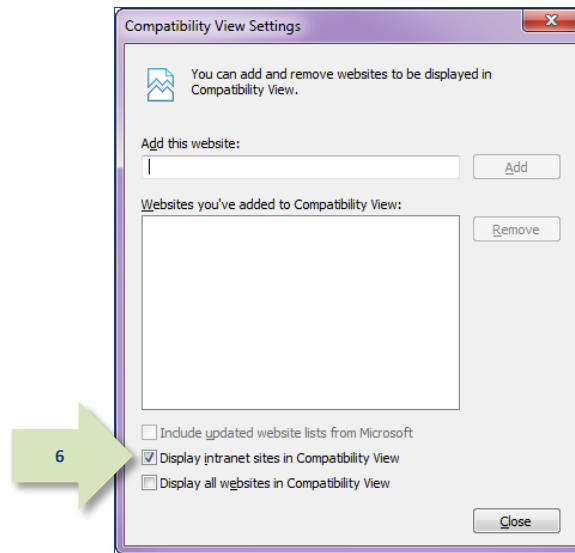
Figure 512: Compatibility View Settings – Deselect the Compatibility View Option

7.   Click the checkbox to deselect the option.

8.   Click **Close**.

*IE closes the **Compatibility View Settings** dialog and returns to the AMPS home screen.*

*After you make this change, opening AMPS in IE will not force the display of the application into **Compatibility View** for AMPS or any other application in **dla.mil** or **dfas.mil**.*
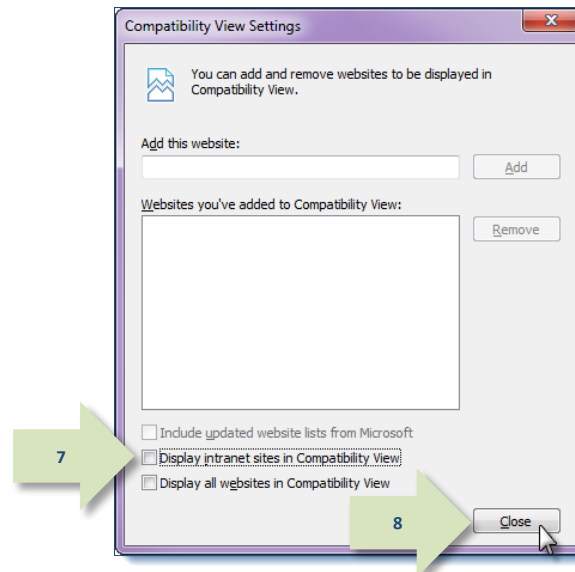
Figure 513: Internet Explorer - Deselect the Option to Display in Compatibility View

How to Activate Emulation Mode in Internet Explorer 11

Some of the features in AMPS, such as button functions, work properly in Internet Explorer 8 (IE8). AMPS was developed in an IE8 environment and thoroughly tested for functional accuracy and reliability. However, changes introduced in Internet Explorer 11 (IE11) can cause problems with certain features.

The solution for IE11 users is to operate IE11 in "emulation mode," which is a group of settings that cause IE11 to behave like IE8.

To use AMPS in IE11, you can activate the emulation mode through a series of steps in which you choose the appropriate settings. You can easily save the settings to make a return to emulation mode faster, and you can disable emulation mode quickly for operating other Web-based applications. Follow the instructions in this section to enable and disable Emulation mode in IE11.

Enable IE11 Emulation Mode

1. Start IE 11 and launch AMPS with the following URL: **https://amps.dla.mil/**.

   IE11 displays a message indicating the browser you are using is not supported for the current version of AMPS.

2. Click **OK** to close the message.

   The system launches the AMPS Gateway screen.

CAUTION!

Do NOT click the link to open AMPS yet.

Proceed to Step 3.
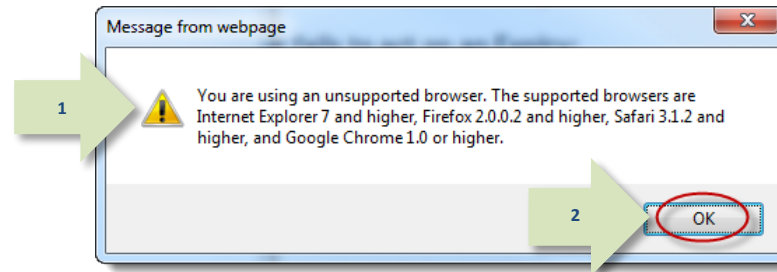
Figure 514: Internet Explorer 11 Message - Unsupported Browser
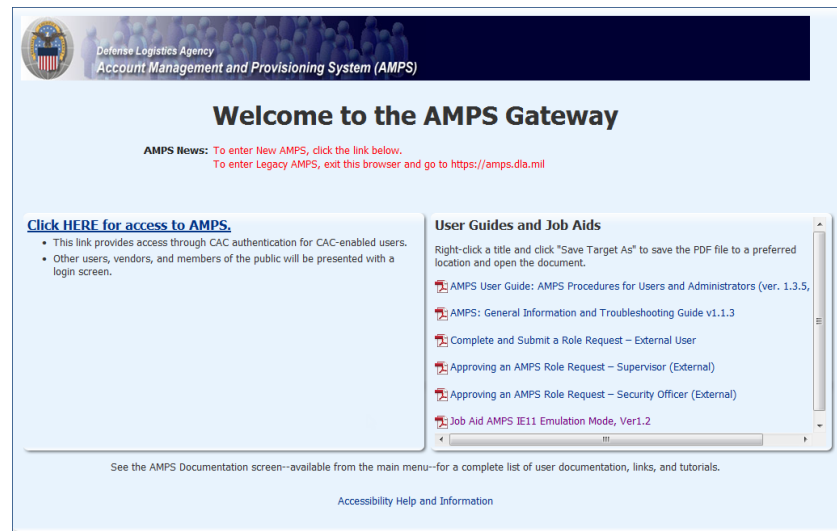
Figure 515: AMPS Gateway

3. On the keyboard, press **F12** (not shown).

   IE displays the Debug panel (see Figure 516).

4. Locate the Debug menu bar and click the **Emulation** command.

   *IE opens the **Emulation** panel.*
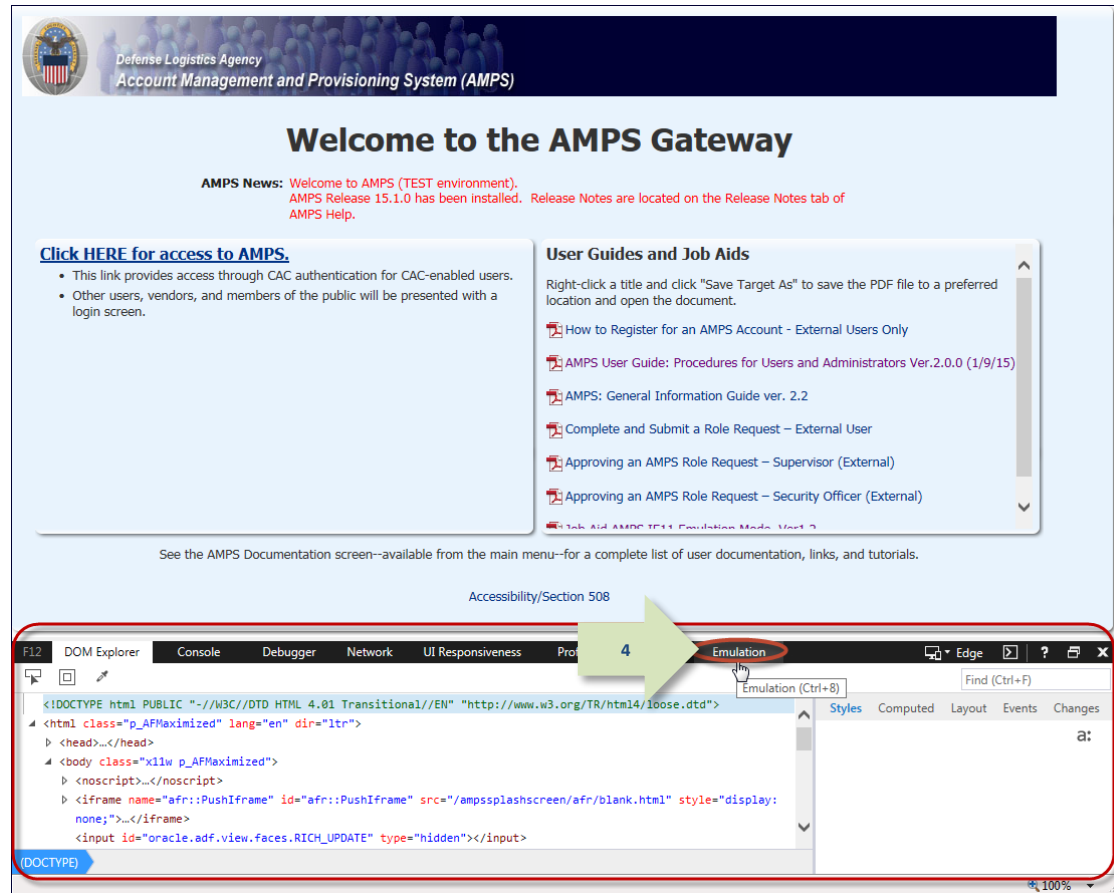
Figure 516: AMPS Home - IE11 Debug Panel

5. In the Emulation panel, locate the **User agent string** drop-down list box.
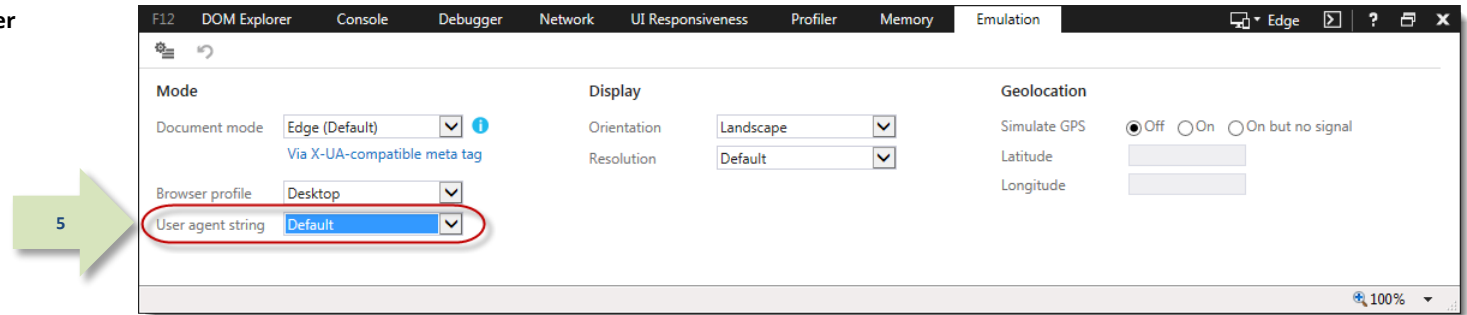
Figure 517: IE11 - Emulation Panel

6. Click the down arrow in the **User agent string** drop-down list box to open the selection list.

   IE displays a list of browsers, including **Internet Explorer 8***.*

7. In the User agent string dropdown list, click Internet Explorer 8.

   IE11 refreshes the dropdown box selection and immediately starts emulating IE8.
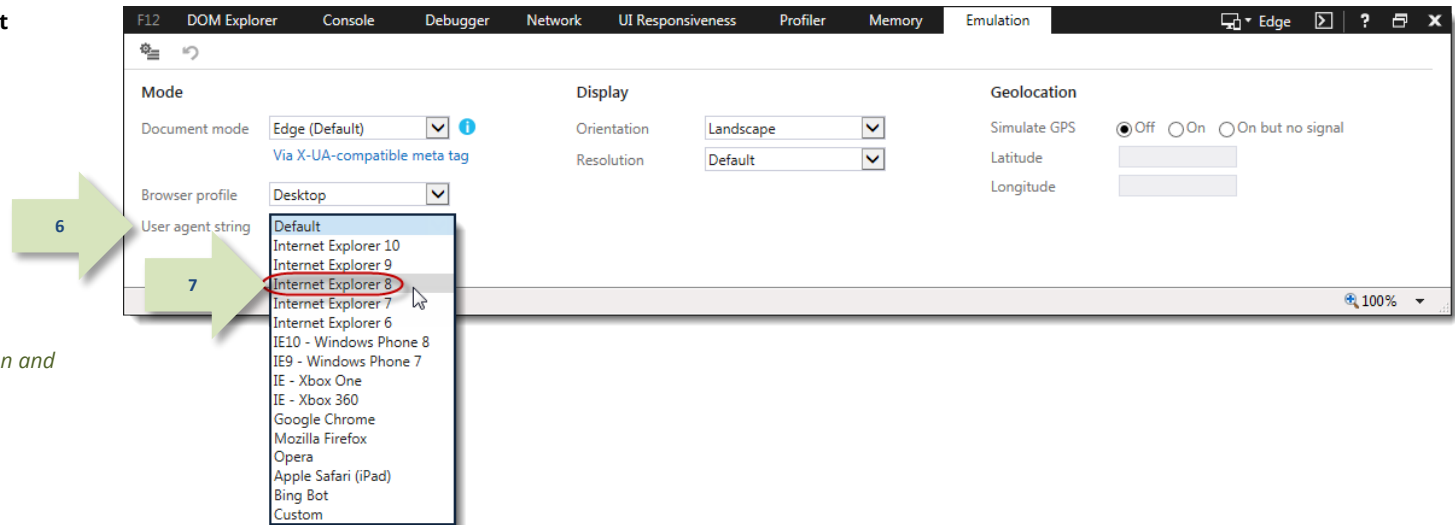
Figure 518: User Agent String - Browser List

8.   If the system displays a **Webpage Error** message that asks if you want to debug the Web page, click **No**.
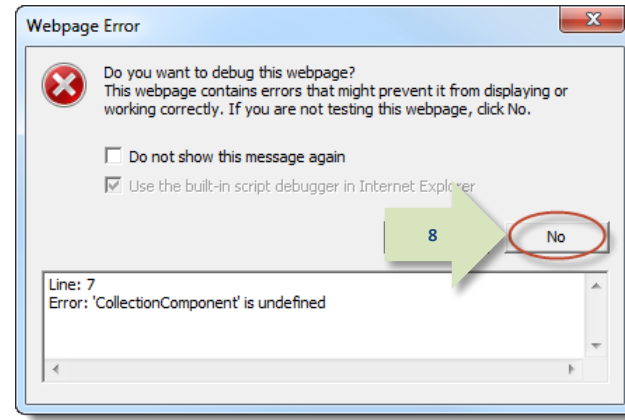
Figure 519: Webpage Error Message

Note:

Let the Debug panel remain active to continue working in Emulation mode.

If you close the browser or the Debug panel, the emulation stops. Repeat steps 1 to 8 to restart IE8 Emulation.

Save IE11 Emulation Mode Settings

To save current IE11 Emulation Mode settings, click the **Persist Emulation** icon.

This action saves the current settings. When you press the F12 button (see step 3), IE11 performs the following actions:

- *Restarts the **Debug** panel*
- *Enables **Emulation** mode using the previously selected settings.*
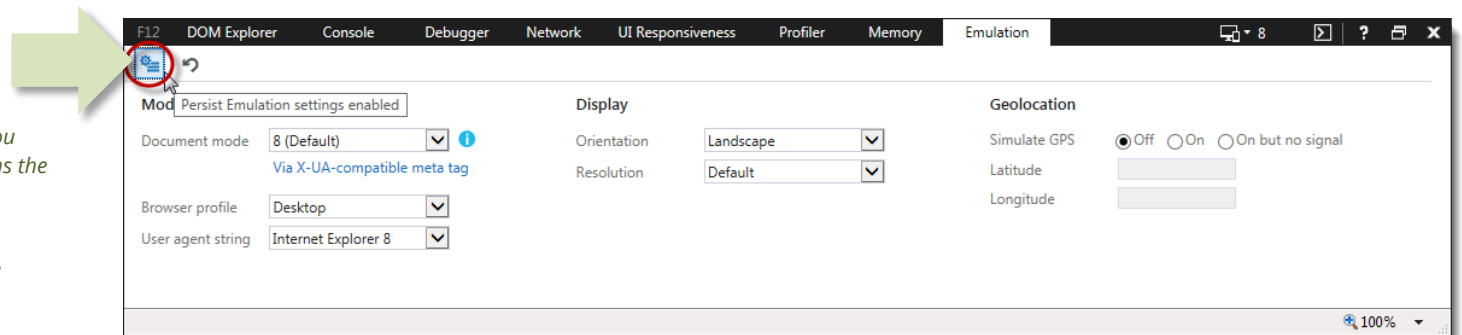
Figure 520: Emulation Panel - *Persist Emulation* Icon

Disable IE11 Emulation Mode

To disable IE11 Emulation Mode, click the **X** icon in the upper right corner of the **Emulation** panel.

*This action closes the **Emulation** panel and returns IE11 to normal function.*

*When you press the **F12** key on your keyboard with IE11 open, IE11 performs the following actions:*

- *Restarts the **Debug** panel*

- *Enables **Emulation** mode in the default **Document mode**.*
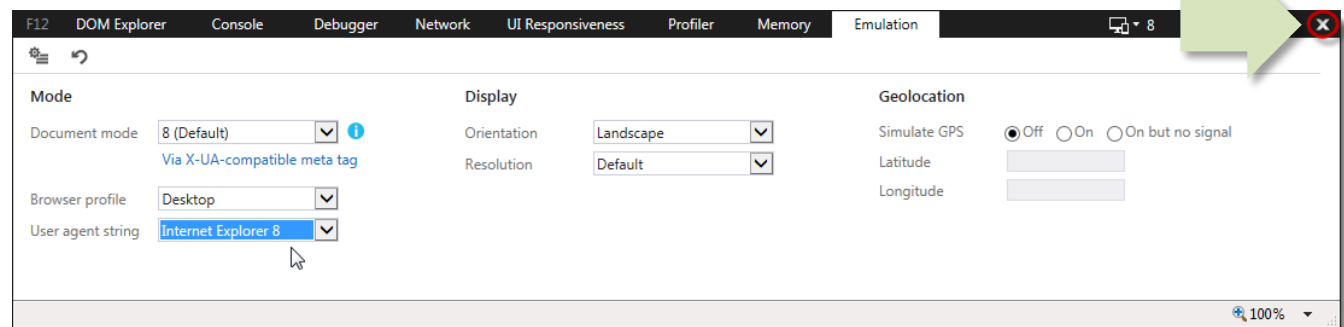
Figure 521: Emulation Panel - Disable Emulation Mode

How to Clear Browser History in Internet Explorer

When Internet Explorer starts providing unexpected or unwanted results while an application such as AMPS is running, you can try clearing the browser's history and restarting the browser. Depending on the issue, this procedure can help reduce or eliminate problems in viewing the screens you need.

If you start having trouble with AMPS screen displays, follow these steps to clear the browser's history.

This procedure is also called "clearing the cache."

How to Delete Browser History in Internet Explorer

1. With Internet Explorer (IE) started, click the **Tools** command on the browser's main menu bar.

    IE displays the **Tools** *menu.*

2. Click the Delete browsing history option.

    IE displays the **Delete Browsing History** *dialog.*
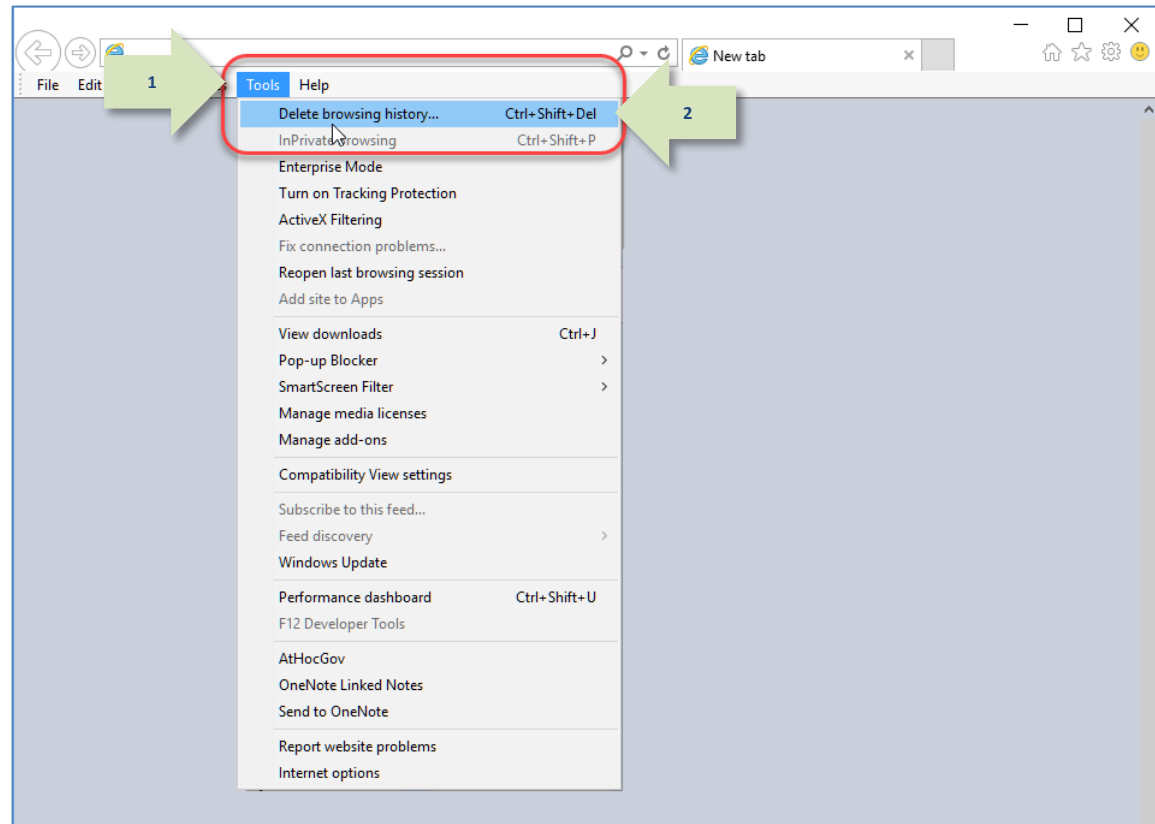
Figure 522: Tools - Delete browsing history

3. In the **Delete Browsing History** dialog, ensure that the following two options are checked:

    - Temporary Internet files and website files

    - Cookies and website data

4. Click the **Delete** button.

    AMPS displays a confirmation banner at the bottom of the browser window confirming the deletion of browsing history.
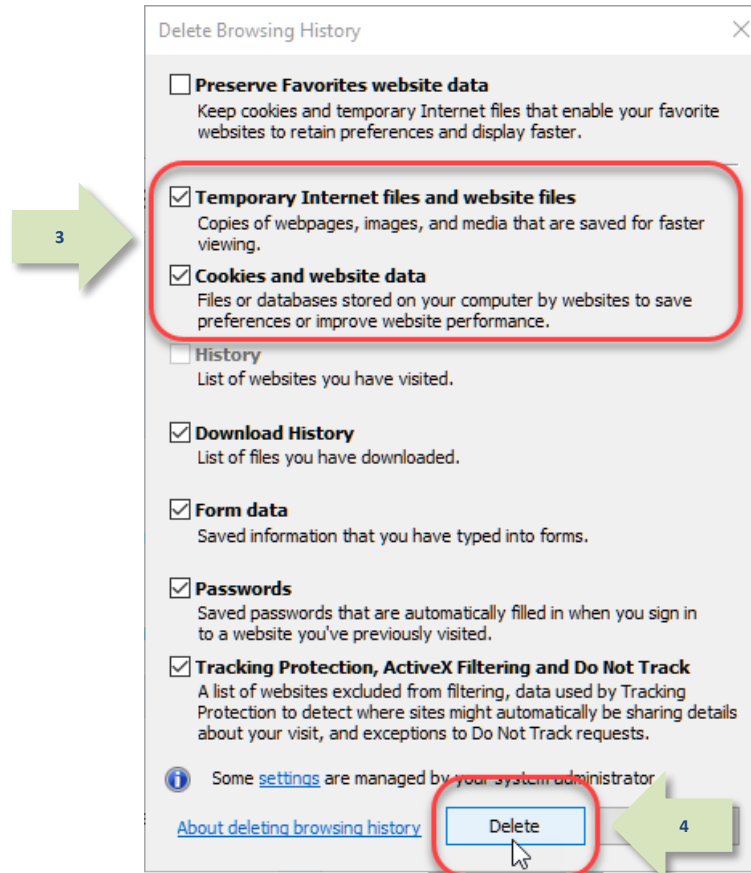
Figure 523: Delete Browser History Dialog

5. Click the *close* icon in the banner to dismiss the message.

    Close the browser and reopen it to continue work.
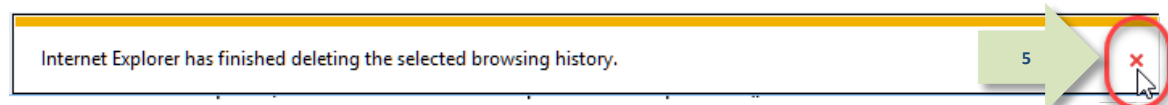
Figure 524: Confirmation Banner - Browser History Deleted

How to Refresh Stored Pages in Internet Explorer

1. With Internet Explorer started, click the **Tools** command on the browser's main menu bar (see Figure 522).

   IE displays the **Tools** *menu.*

2. Click Internet options.

   IE displays the **Internet Options** *dialog.*
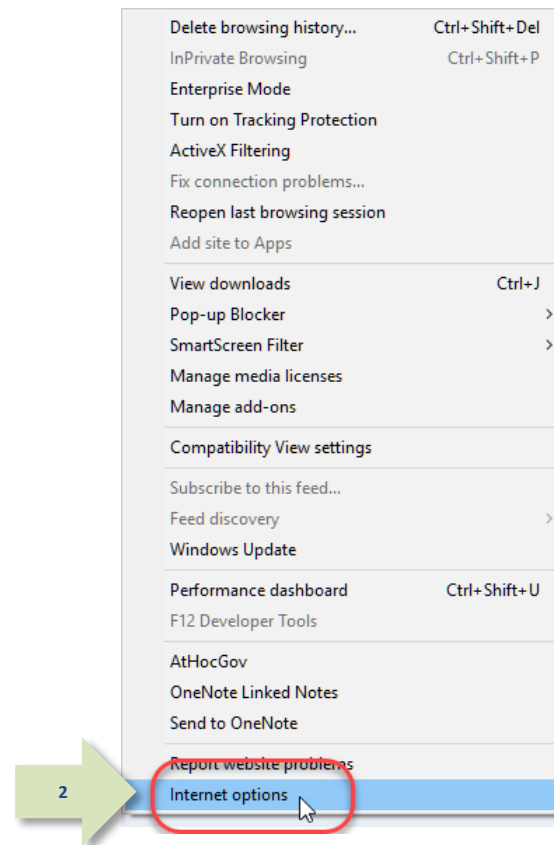
Figure 525: Tools – Internet Options

3. In the **Browsing history** section, on the **General** tab, click the **Settings** button.

   *IE displays the **Website Data Settings** dialog.*
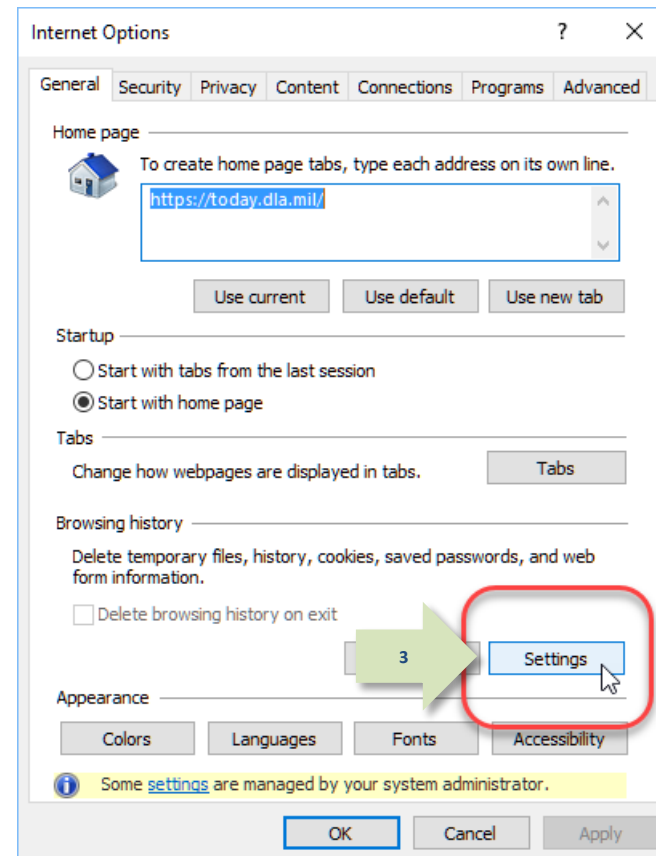
Figure 526: Internet Options Dialog

4.   In the **Website Data Settings** dialog, click the radio button for this option: **Every time I visit the webpage**.

5.   Click the **OK** button.

IE closes the **Website Data Settings** *dialog.*
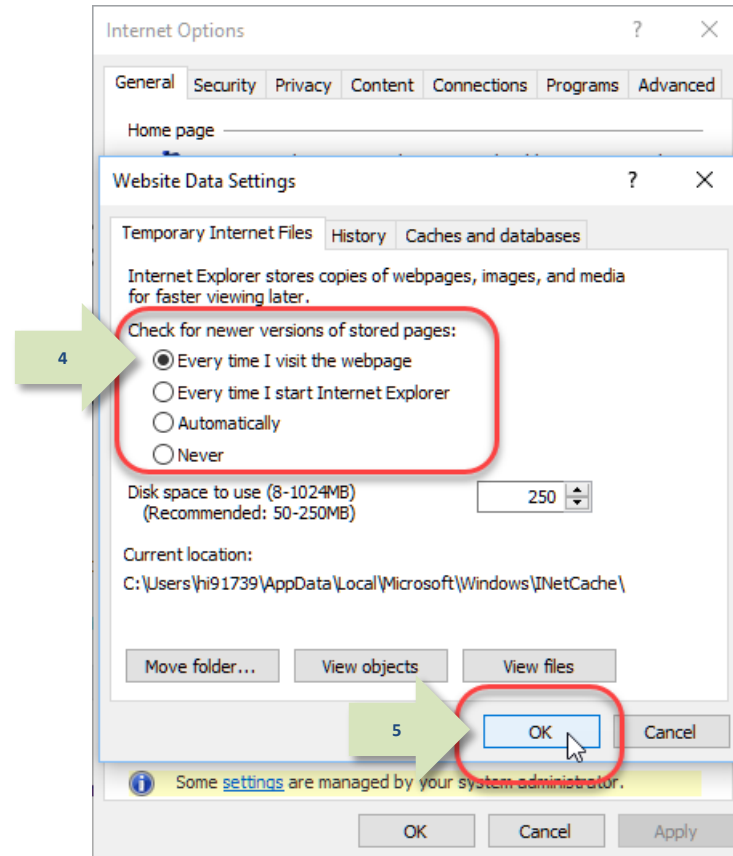
Figure 527: Website Data Settings

6. In the **Internet Options** dialog, click **OK** to close the dialog.

    IE closes the **Internet Options** *dialog and returns to normal function.*

7. Close the browser and reopen it to continue work.
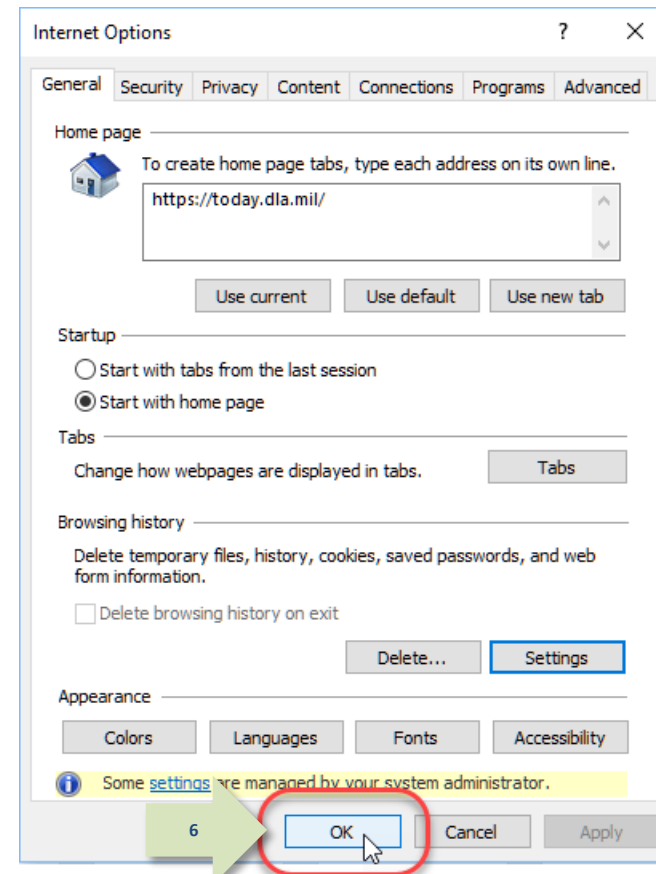
Figure 528: Internet Options

Appendix C: Password Rules

AMPS password policies enable you to set up a strong password using multiple character types Note that the password you choose must fulfill ALL of the character type policies to be valid. These policies include the following rules:

Valid values include the following characters:

a-z A-Z 0-9 + ! # ^ : . ~ - _

Use these characters according to the following guidelines.

✓ 15 to 32 characters in **length**

✓ 4 or more *alpha* characters:

  o   2 or more lower case characters

  o   2 or more UPPER case characters

✓ 2 or more *numeric* characters

✓ 2 or more *special* characters, **EXCEPT** the following characters:

  ✓ Accent mark **`**

  ✓ Ampersand **&**

  ✓ "At" sign **@**

  ✓ Brackets, parentheses, or braces **[ ] ( ) { }**

  ✓ Dollar sign **$**

  ✓ Double, single, or straight quotes **" " ' ' " '**

  ✓ Greater than/ Less than symbols **< >**

  ✓ Percent sign **%**

  ✓ Question mark **?**

  ✓ Slashes **/ **

✓ **A password must not contain any non-US English keyboard special characters.**

Tip!

AMPS password rules are set up to ensure a strong, secure password.

When you change your AMPS password, this change is propagated to each application for which you have a role. Occasionally, an application may not accept a character that AMPS does accept, and a password valid in AMPS is invalid in the application.

If you have difficulty resetting a password, contact the Service Desk (see page 9) for assistance and recommendations.

Additional rules include the following:

✓ Password must begin with at least one alpha character.

✓ Password cannot begin with a numeric or special character.

✓ **INCLUDE** any of the following valid characters: a-z A-Z 0-9 + ! # ^ : . ~ - _

✓ **EXCLUDE** any combination of characters that spells a recognizable word.

✓ **EXCLUDE** the value of these attributes: your account ID, your email address, your first name, full name, or last name.

✓ Do not repeat any of your previous 10 passwords when resetting a password.

How to Change Your AMPS Password
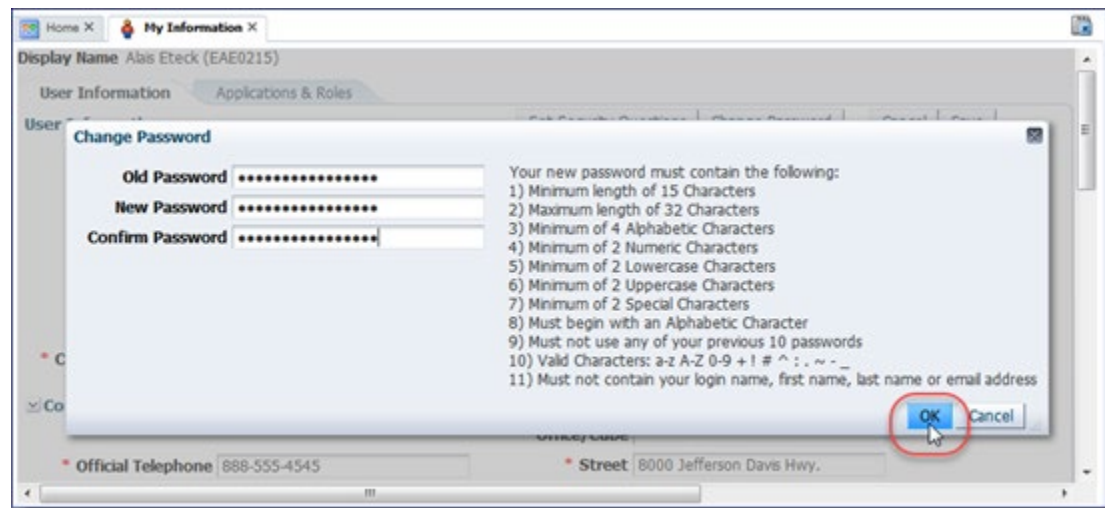
Figure 529: Change Password - Dialog

1. Open the **My Information** screen.

2. Click Change Password in the User Information tab.

3. Fill in the old, or current, password.

4. Fill in a new password that fulfills the policies and rules.

5. Reenter the new password to confirm it.

6. Click **OK**.

7. Close the browser.

Appendix D: AMPS Security Questions

If you forget your password, you can request a password reset through the AMPS login screen. However, AMPS requires you to respond with the answers you provided for three of the following questions during the account registration process:

- What is your mother's maiden name?
- What is your favorite color?
- What is the city of your birth?
- What is the name of your pet?

The following procedure enables you to manage the set of questions and answers that AMPS presents if you request a password reset from the AMPS login screen.

How to Manage Security Questions and Answers

On the **My Information** screen, you can select a new array of questions and enter new answers. The minimum number of characters for any answer is three characters.

Note:

AMPS requires you to select three different questions.

1. Open the **My Information** screen.
2. Click Set Security Questions in the User Information tab.
3. Select a different question from each drop-down list.
4. Fill in an answer to each question (minimum: 3 characters).
5. Click **OK**.

Figure 530: Manage Security Questions - Dialog

Appendix E: Introduction to Primary Roles

Introduction to Hierarchical Role Structure

Certain applications, such as EBS and EAGLE, have interdependent roles that function in a two-level hierarchy: primary and additional:

- At the *primary* level, an application requires users to request and receive an assignment for one **Primary Role** containing a basic permission set.
- At the *additional* level, a user can request and receive one or more additional roles to supplement permissions and resources in the **Primary Role**. These additional roles may include the following role categories as they are labeled in AMPS:
  - o **Additional and Primary** (sometimes called **Primary/Additional**)
  - o **Additional Only**
  - o **Not Applicable** (neither Primary nor Additional)

Together, a **Primary Only** role and one or more **Additional** roles represent a set of permissions that provides users with the access needed to perform their application tasks. The only exception to this hierarchy is the **Additional and Primary** role. As the name suggests, **Additional and Primary** roles can serve as either an **Additional** or a **Primary** role. Unlike **Primary Only** roles, AMPS does not limit the number of **Additional and Primary** roles a user can have for one application.

Application owners are responsible for defining the attributes of each role to ensure that AMPS manages the role requests and provisioning according to the application owners' business rules and processes.

The following sections outline general guidelines in AMPS for requesting and removing **Primary** and **Additional and Primary** roles based on application requirements.

AMPS Guidelines for Primary Only Roles

A **Primary Only** role is an exclusive role that provides baseline access privileges for one application and serves as the foundation privilege set for an application. Here are some guidelines for understanding and requesting a **Primary Only** role:

- AMPS allows a user to select only one Primary Only role per application at a time during the Request Role process. The user must submit a role request for and receive this **Primary Only** role before he or she can obtain additional roles for that application.
- AMPS allows a user to have only one **Primary Only** role per application.
- A user who needs to change from one **Primary Only** role to another submits a request that goes through the following steps:
  1. The user starts a request for the new **Primary Only** role through the **AMPS Role Request** process.

2. During the request process, AMPS responds to the user's selection of a **Primary Only** role with a message asking the user whether or not he wants to change **Primary** roles.

3. If the user confirms the choice of a new **Primary Only** role, he or she submits the completed request, and AMPS generates a SAAR for the following actions:
   a. Remove the existing **Primary Only** role.
   b. Add the newly requested **Primary** role.

4. After the SAAR is approved, the provisioner receives notification of a ticket. The ticket may be Total AMPS or Remedy, depending on the application. The provisioner for each resource receives one ticket.

5. The provisioner opens the ticket, finds the instructions to remove one **Primary Only** role and add a different **Primary Only** role, and completes the provisioning tasks.

When a user removes a Primary Only role . . .

A user who wants to remove a **Primary Only** role can submit a request to remove the role through the **Applications & Roles** screen (see the *User Guide* section entitled **Role Removal** for procedures on removing a role) after removing all associated Additional roles. The role removal request must go through a short approval process, after which the application provisioner removes the role from the user's account. The user can then submit a request for a new **Primary Only** role.

A user who has both a **Primary Only** and an **Additional and Primary** role for an application can request the removal of just the **Primary Only** role. After the role is removed, AMPS treats the remaining **Additional and Primary** role as the user's **Primary** role for the application.

Removing a **Primary Only** role *does not* remove the related or supporting **Additional and Primary** and **Additional Only** roles. The user must submit separate requests to have these roles removed, as needed.

AMPS Guidelines for Primary/Additional Roles

A role with the designation "**Additional and Primary**" is, unlike a **Primary Only** role, a non-exclusive role. That is, it can function as either a **Primary Role** or an **Additional Role** according to the following guidelines:

- It acts as a **Primary Role** if the user does not already have any other roles requested or provisioned in the application.
- It acts as a supplemental role if the user already has a **Primary Role** in the application.

A user can have multiple **Additional and Primary** roles for a single application, if necessary.

When a user removes an Additional and Primary role . . .

A user who wants to remove an **Additional and Primary** role can submit a request to remove the role through the **Applications & Roles** screen (see the *User Guide* section entitled *Role Maintenance* for procedures on removing a role).

The role removal request must go through a short approval process, after which the application provisioner removes the role from the user's account.

Roles Marked "Not Applicable": Non-hierarchical Roles

These roles are not part of a predefined hierarchy. A user, authorized to request multiple roles in an application, can be assigned a combination of roles labeled "Not Applicable" without encountering an error condition in AMPS.

Multiple Role Selections

AMPS enables you to select multiple roles during a single request sequence. However, due to the business rules imposed on the system by application owners who define **Primary Only** roles, AMPS limits the selection of **Primary Only** roles according to the following guidelines:

- You can select ONLY one **Primary Only** role at a time for an associated application.
- If you already have a **Primary Only** role in place, you must remove all associated **Additional** roles, wait for the **Additional** role removals to be approved and the roles deprovisioned. You can then submit a request to remove the **Primary Only** role.

With regard to **Primary Only** and **Additional** roles, the following combinations are permissible:

- Multiple **Additional and Primary** roles, if you already have a **Primary Only** role.
- Multiple **Additional Only** roles, if you already have a **Primary Only** role.
- Combinations of **Additional and Primary** roles and **Additional Only** roles, if you already have a **Primary Only** role.
- Combinations of all role types, except **Primary Only** roles. Within an application, you can have only one **Primary Only** role.

AMPS Guidelines for *Primary Only* Roles

Role Type	Definitions	Selection Guidelines	Removal Guidelines
Primary Only role	• Provides baseline access privileges for one application and • Serves as the foundation privilege set for an application. • Available for selection and assignment to a user account only one at a time. AMPS does not permit the request of two or more **Primary Only** roles in a single request.	• Use the **Role Request** procedure in AMPS. • AMPS allows a user to select only one **Primary Only** role per application at a time during the **Request Role** process. • A user must submit a role request for and receive this **Primary Only** role before she can obtain additional roles for that application.	• First, remove all **Additional** roles associated with the **Primary** role in the application. After the role removals have been processed and the roles deprovisioned, submit a role removal request to remove the **Primary** role.
Additional and Primary role	• Serves as a **Primary** role if you do not already have a **Primary** role for the application. • Serves as an **Additional** role if you already have a **Primary** role.	• Use the **Role Request** procedure in AMPS. • AMPS allows a user to select multiple **Additional and Primary** roles. • A user can submit a request for multiple **Additional and Primary** roles at one time.	• Use the Role Removal procedure in AMPS (see Role Maintenance) to remove the *Additional and Primary* role.
Additional Only role	• Serves as a supporting role to an application **Primary** role. • Provides extra privileges or permissions to expand application access requirements for a particular user's job.	• Select a corresponding **Primary Role** before attempting to select an **Additional Only** role. • Use the **Role Request** procedure in AMPS.	• Use the Role Removal procedure in AMPS (see Role Maintenance) to remove the *Additional Only* role.

Guidelines for *Primary Only, Additional and Primary*, and *Additional Only* Roles in AMPS

This guideline is for...	In this Situation...	Use this Procedure in AMPS...	and Remember...

Requesting Primary and Additional roles	Your job requires a *Primary Only* role and one or more additional roles.	1. Request the ***Primary Only*** role first and confirm from the email notification that the ***Primary Only*** role has been approved and provisioned.
		
		2. Then, request one or more additional roles of the following types, as needed:
		
		  a. Additional and Primary
		
		  b. Additional Only
		
		  c. ***Not Applicable*** (if available for your application)
			Certain applications require you to have a ***Primary Only*** role before you can request roles with supporting permissions and capabilities.

Managing your Primary roles in AMPS	You already have a ***Primary Only*** role, but you need a different ***Primary Only*** role.	1. In AMPS, request the new ***Primary Only*** role through the role request process. 2. When AMPS displays an information message cautioning you that your account already has a provisioned ***Primary Only*** role, close the message and continue with the new request. 3. AMPS creates one SAAR that requests addition of the new role and removal of the existing role.	AMPS alerts you when you already have a ***Primary Only*** role before enabling you to request a different role. The message reads as follows: [Role Name] is a primary role. You already have a primary role for this [Job Type] ([Role Name]). Adding this role will result in a primary role change, replacing your current primary role.
Removing a Primary role	You have a ***Primary Only*** role and supporting additional roles for an application. You request a removal of the ***Primary Only*** role.	1. Open the **Applications & Roles** tab of the **My Information** screen for your account. 2. In the **Current Roles** list, click the role you want to remove. 3. Click the **Remove Role** button. 4. Enter a **Justification** in the Role Removal dialog. 5. Click the **OK** button.	AMPS displays an error message. You must first remove all the **Additional** roles, and an application administrator must deprovision those roles before you can remove the **Primary** role. Check with your AMPS Supervisor to determine which Primary role and supporting Additional roles you need for a specific application.
Requesting an Additional and Primary role	You need a **Primary** role, and the only available role that fulfills this criterion is labeled *Additional and Primary*.	Request the role as you would a ***Primary Only*** role.	Roles designated as ***Primary and Additional*** work in either capacity: • If you need a Primary role, a ***Primary and Additional*** role will serve that purpose. • If you have a ***Primary Only*** role and need to request a ***Primary and Additional*** role, the role will function as an ***Additional Only*** role.

Primary Role Selection: AMPS Messages

During the **Role Request** process in AMPS, the user searches or browses for a role and selects the role. Some applications restrict role selection based on Primary role assignment. As a precaution, AMPS displays information messages when a user attempts to select **Primary** and **Additional** roles incorrectly. The following illustrations explain how to correct a given problem.

If you see this message, . . .

"[Application Name] requires a role designated as 'Primary Only' on your account before you may request [Role Name]. You can use the Primary Roles filter in the Roles Search box to select a Primary role."

Here's how to address the cause . . .

If you attempt to select an **Additional Only** role during the role request process without first having a current **Primary Only** or **Additional and Primary** role assigned, you cannot complete the request.

You can, however, search for and select the appropriate **Primary Only** role or **Additional and Primary** role.

If you do not have the name of the required **Primary Only** or **Additional and Primary** role, check with your AMPS Supervisor for more information.

Follow these steps to select a **Primary Only** or **Additional and Primary** role:

1. Click **OK** to close the Information message box.

2. In the Search Roles area of the Select Roles tab, select either Primary Only or Additional and Primary in the Primary Role dropdown list.

3. Enter other search criteria, as needed, to reduce the number of search results.

4. Click **Search**.

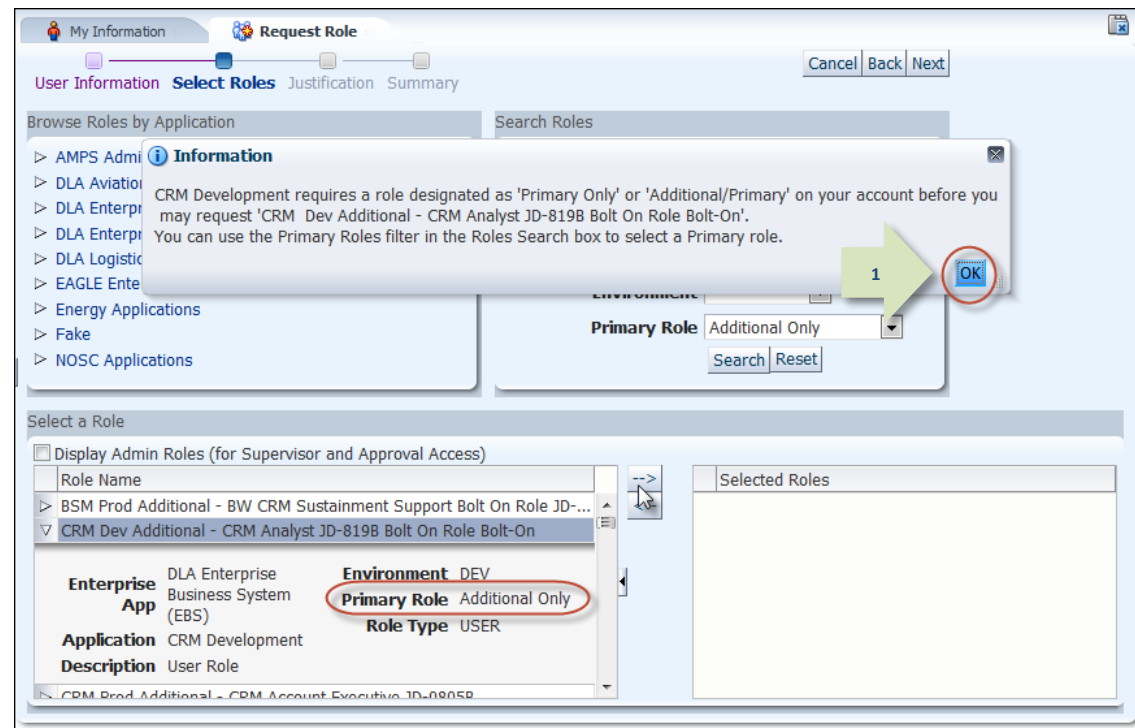5. In the **Select a Role** search results list, select the role you need.

Figure 531: Select Additional Only Role - Information Message
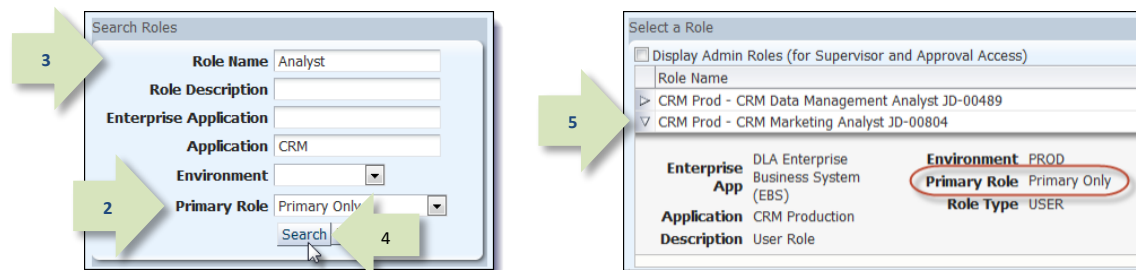
Figure 532: Search for and Select a Primary Only Role

If you see this message, . . .

"You have already selected a Primary Role for [Application Name]. You may select only one Primary Role per application at a time."

Here's how to address the cause . . .

1. Click **OK** to close the Information message box.

2. Verify you have one correct **Primary Only** role in the **Selected Roles** list.

3. If necessary, remove the incorrect role, and search for and select the correct **Primary Only** role.

4. Click the Add button to move the selected role name to the **Selected Roles** list, ensuring you select only one **Primary Role** for an application.

5. Click **Next** to continue the role request process.

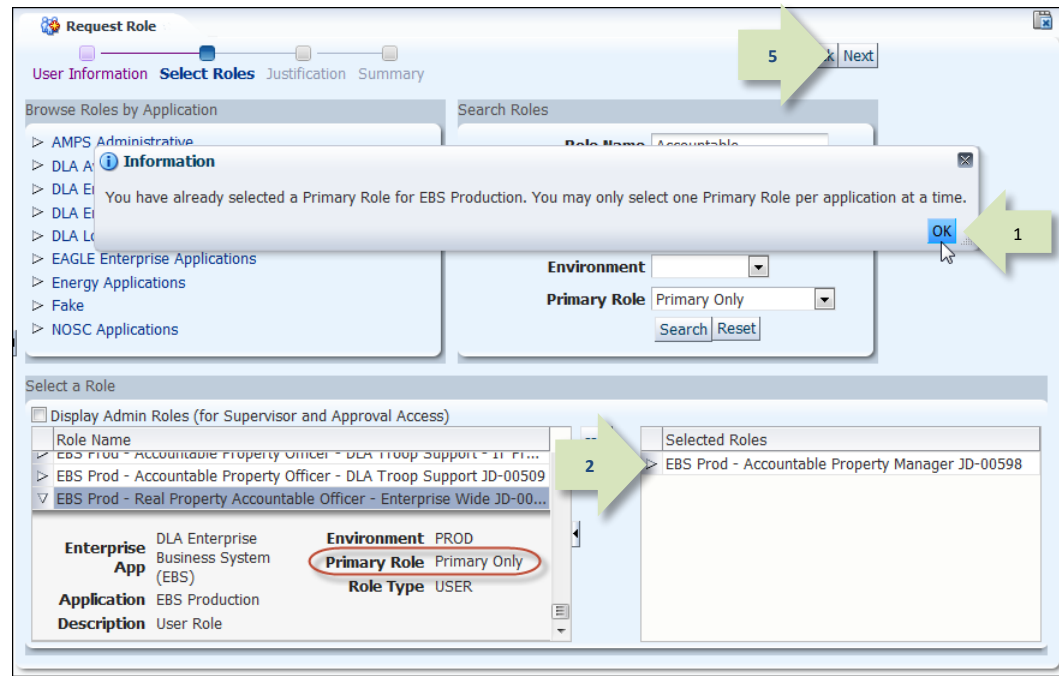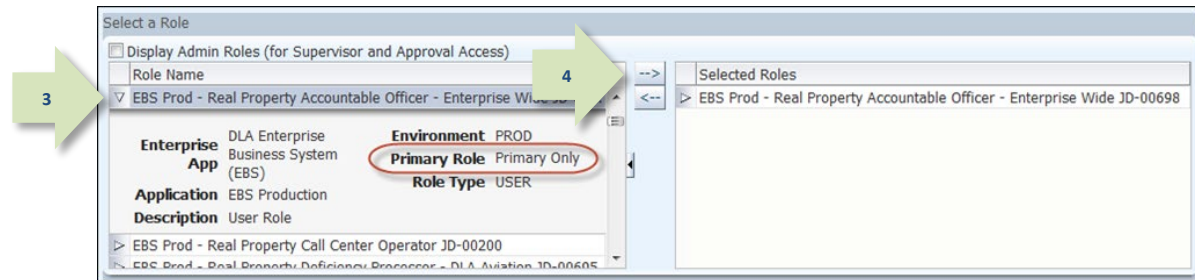**Figure 533: Select Multiple Primary Roles - Information Message**

Figure 534: Select One Primary Role Per Application

If you see this message, . . .

"You may select only one Primary Role per application at a time."

Here's how to address the cause . . .

In this situation, you have selected two **Primary Only** roles at once.

Although AMPS enables you to select and request multiple roles in one sitting, the system prevents you from selecting more than one **Primary Only** role at a time for a specific application.

Follow these steps to correct the selection:

1. Click **OK** to close the **Information** message box.

2. Verify you have selected ONLY one **Primary Only** role in the **Role Name** list.

3. If you have selected two or more roles, **click the application role name you intend to request** during the current process.

4. Click the right arrow (→) button (also known as the Add button) to move the selected role name to the **Selected Roles** list.

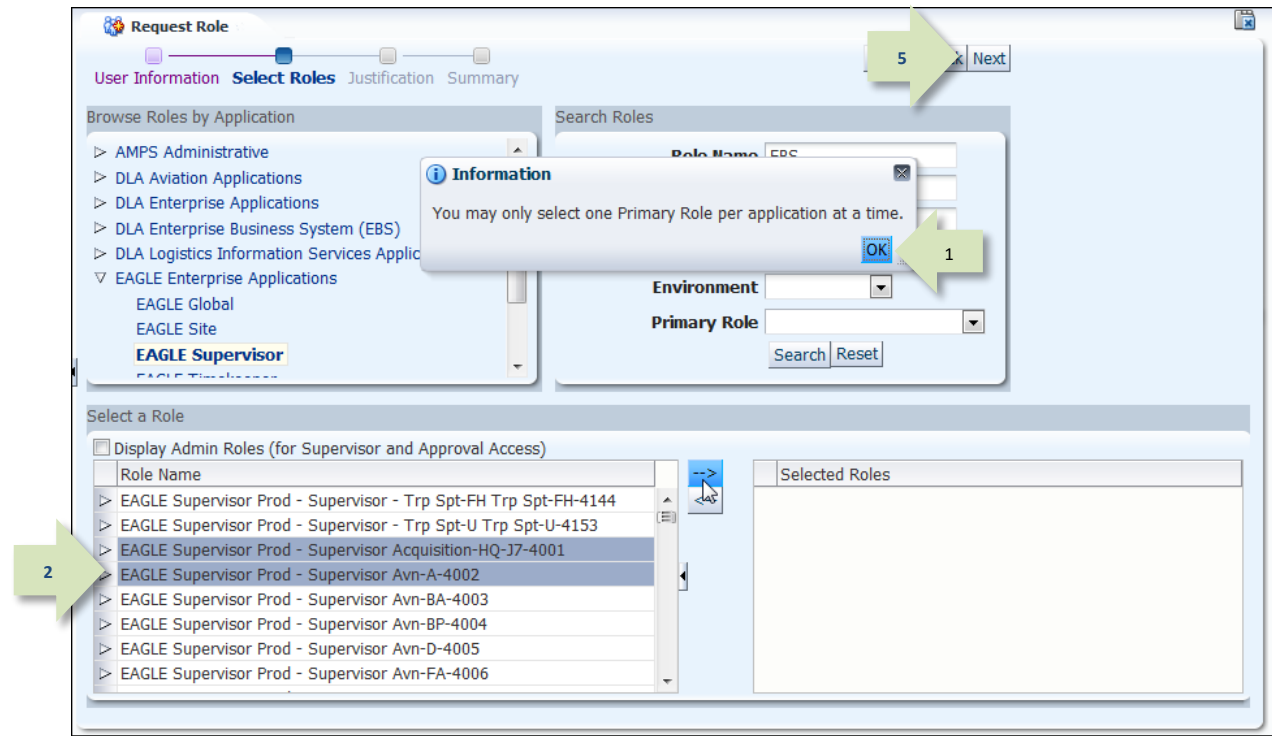5. Click **Next** to continue the role request process.

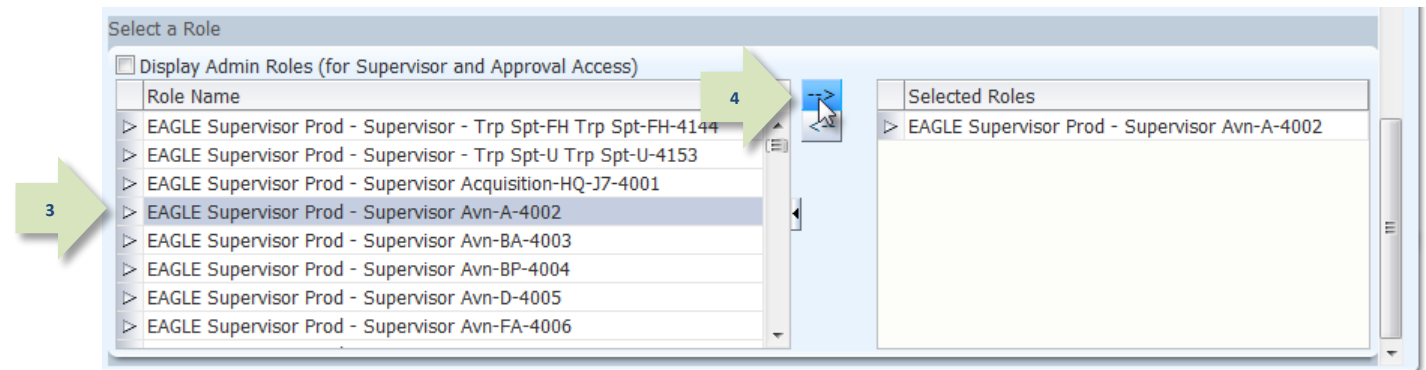**Figure 535: Select Multiple Primary Roles - Information Message**

Figure 536: Select a Primary Only Role

If you see this message, . . .

"You have a pending request for [Role Name], which is a Primary Role for [Application Name]. You may select only one Primary Role per application at a time. The pending request must be completed before you can request a different Primary Role for this application."

Here's how to address the cause . . .

In this situation, you have already requested a **Primary Only** role for a specific application, but you have not yet been granted the role.

While a **Primary Only** role request is pending approval or pending provisioning, you cannot request a different **Primary Only** role for the same application.

Follow these steps:

1. Click **OK** to close the Information message box.

2. Click **Cancel** to close the request screen and cancel the current request.

3. Check your Pending Requests table. (See How to Check Your Role Status on page 97.)

4. Choose one of these options.

   a. If a current Primary Role request's status is PENDING APPROVAL, follow the procedure in the *AMPS User Guide* section How to Cancel a Request: End User.

   b. If a current Primary Role request's status is **TICKETED**, inform your AMPS Supervisor and contact the Service Desk for assistance (see page 9).

5. **DO NOT cancel a TICKETED role request.** Wait for the role to be provisioned and then submit a request to remove the **Primary Role**.
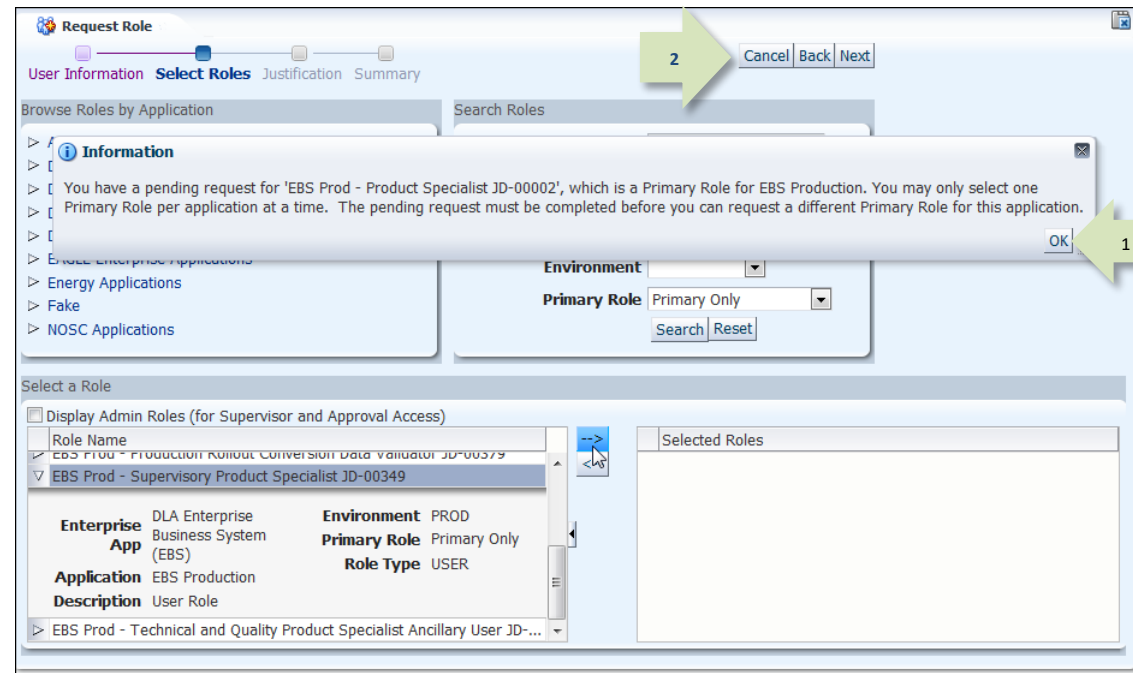

Figure 537: Pending Request for Primary Only Role

Figure 538: Pending Requests List

If you see this message, . . .

"[Role Name] is a primary role. You already have a primary role for this [Application] [(Role Name)]. Adding this role will result in a primary role change, replacing your current primary role."

Here's how to address the cause . . .

If you intend to replace the existing role with the newly selected role, you can proceed with the request:

1. Click **OK** to close the Information message box.
2. Verify your role choice, knowing that the selected **Primary Role**, if approved, will replace the current **Primary Role** now on your account.
3. Click **Next** to proceed with the request.

AMPS creates a SAAR to remove the current Primary Role and add the new Primary Role to your account.
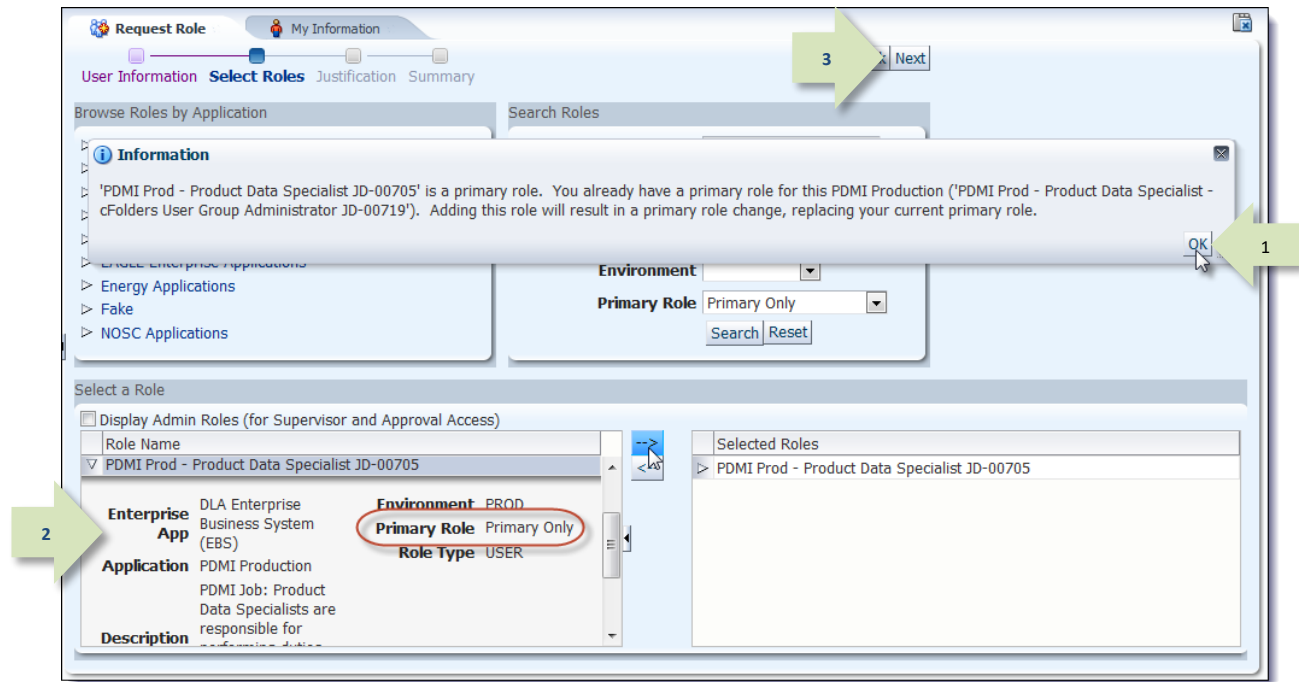
Figure 539: Primary Role Change - Information Message

If you see this message, . . .

"Cannot remove primary role before removing additional roles associated with the application: [application name]."

Here's how to address the cause . . .

For applications that require a **Primary Only** role, AMPS requires a user to request the Primary Only role first, before adding supporting roles (*Additional* or *Additional and Primary* roles).

AMPS also requires a user who wants to remove a Primary Only role to remove the Additional roles first, before removing the Primary Only role. If the user attempts to remove the Primary Only role first, AMPS displays an error message.

The following steps explain how the error is displayed and how to dismiss the error and address the cause:

1. After you select a Primary role for removal and click the **Remove Role** button, AMPS displays the **Request Role Removal** dialog.
2. To proceed with a role removal AMPS requires you to fill in a **Justification** for the removal and click **OK**.
3. If you have selected a Primary role without first removing the Additional roles, AMPS displays the error message box (see Figure 542).
4. Click OK to close the error message.

Return to the Current Roles section and request removals of all Additional roles in the application.

After those removals are approved and the roles are deprovisioned, you can submit a role removal request to remove the Primary Only role.
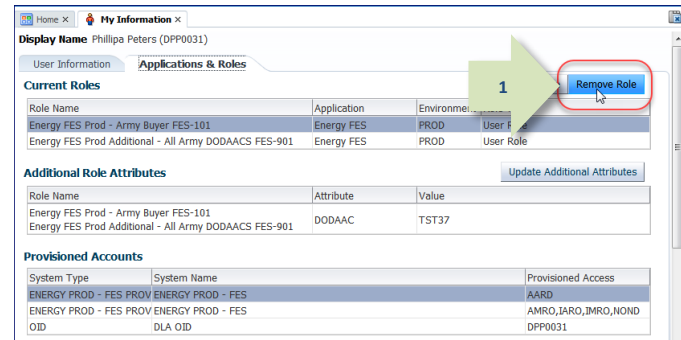

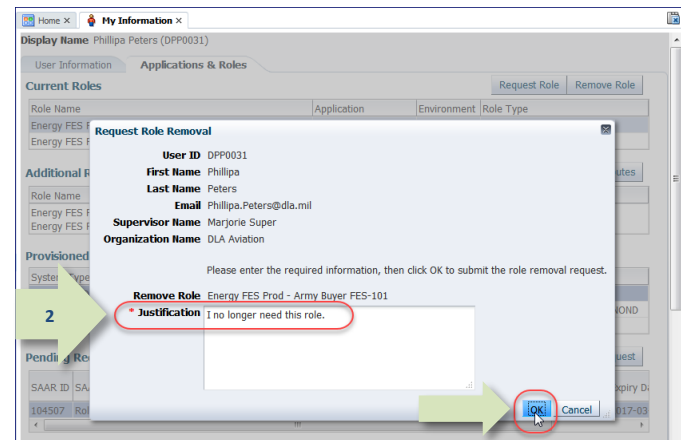**Figure 540: Applications & Roles - Remove Role button**

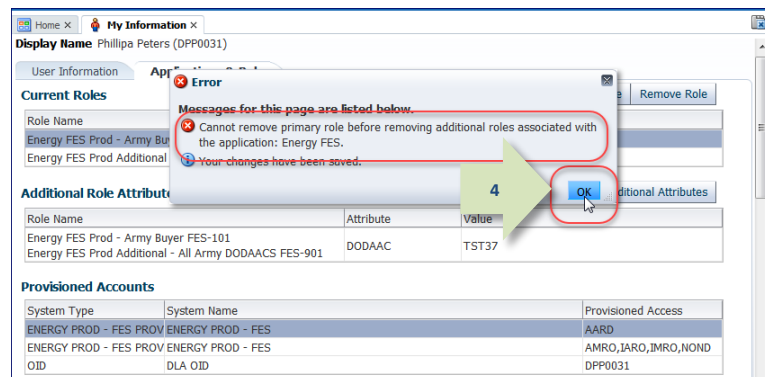**Figure 541: Request Role Removal dialog**

Figure 542: Error Message

Appendix F: SOD/GRC Reports in the Role Request Approval Process

The Governance, Risk and Compliance (GRC) system was developed to enable role request approvers to review and compare each user's access privileges in current and pending application roles across multiple systems. At present, the GRC system applies only to Enterprise Business System (EBS) roles, since EBS systems are now integrated into the GRC system.

GRC helps EBS approvers—specifically Supervisors and Data Owners—identify Segregation of Duties (SOD) violations between application roles. Violations may exist between resources combined in one role, or between two or more roles for disparate systems. The GRC system is programmed to handle the detection of the violations that have been defined and programmed into the system.

GRC gives role approvers the capability to view a report in which SOD violation conditions have been detected should a violation occur. Violation results are displayed in a report that corresponds to a specific SAAR. Violation results may be posted for display in the following conditions:

- Permissions in the current role request conflict with permissions in a user's currently held role.
- Permissions in the current role request conflict with permissions in a user's pending role request.
- Permissions within the currently requested role conflict between role resources. In other words, the role itself represents a Segregation of Duties conflict.

AMPS and GRC

Although GRC is a system external to AMPS, the GRC and AMPS teams have established a connection between the two systems. This connection enables AMPS to import GRC report results directly into the Supervisor's and Data Owner's approval screens. This connection means each AMPS approver does not have to exit AMPS and open the GRC system to view an SOD violation report. The report results are readily available on screen within AMPS.

The AMPS—SOD/GRC Report

AMPS accommodates users who employ the SOD/GRC report for spotting Segregation of Duties violations by displaying this report within a specific section of an approval screen during the request approval process:

- Supervisor Application Decision Screen
- Data Owner Application Decision Screen

The following sections provide screen samples that show how GRC report results are displayed on the Supervisors' and Data Owners' approval decision screens.

SOD/GRC Report in AMPS

The SOD/GRC report is displayed only on the Supervisor's approval screen and the Data Owner's approval screen with regard to a specific role request. The following illustration and key explain the location and parts of the report.

A. SAAR information provides the name of the requested role that is subject to review for SOD violations.

B. The SOD/GRC report is located on the **Role Request Details** tab.

C. If one or more violations occur as a result of the current request, the SAAR report lists those violations in the report table, as shown in the example.

D. If the approver needs to copy the report results to an external resource, such as Excel, clicking the **Download Report** button automatically opens Excel and displays the results in a worksheet.

Figure 543: SOD/GRC Report - Sample Screen
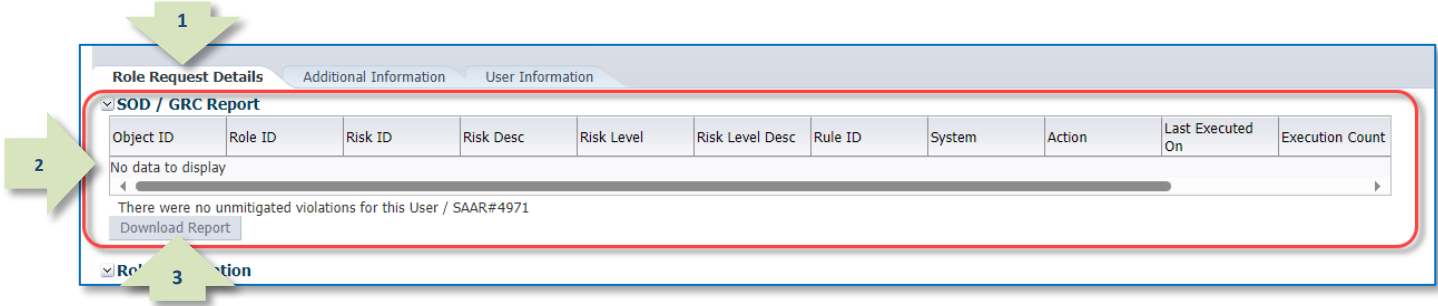
Approval Screen: No Violations

The sample from a Supervisor approver's screen in Figure 544 shows an SOD/GRC report that displays no unmitigated violations. The same report appears on the Data Owner approver's screen.

1.　Locate the **SOD/GRC Report** section in the approver's screen, on the **Role Request Details** tab.

2.　View the report results: The **Risk Description** in the sample report indicates there are no unmitigated violations for the requesting user.

3.　As an option, click the **Download Report** button to view the report in Excel.

Figure 544: Sample Supervisor Approver Screen -
This sample screen shows the SOD/GRC Report section for a user with no violations.

Approval Screen: Violations Reported

The sample approver's screen shows an SOD/GRC report that displays fewer than 50 unmitigated violations. The same report appears on the Data Owner approver's screen.

1. Locate the **SOD/GRC Report** section on the approver's screen, on the **Role Request Details** tab.

2. View the report results: The **Risk Description** indicates the type of violation that has occurred.

3. Note the presence of a role in the **Current Roles** section, found on the **User Information** tab. The requested role is compared with the current role by the GRC system, and results are reported in the **SOD/GRC Report** section.

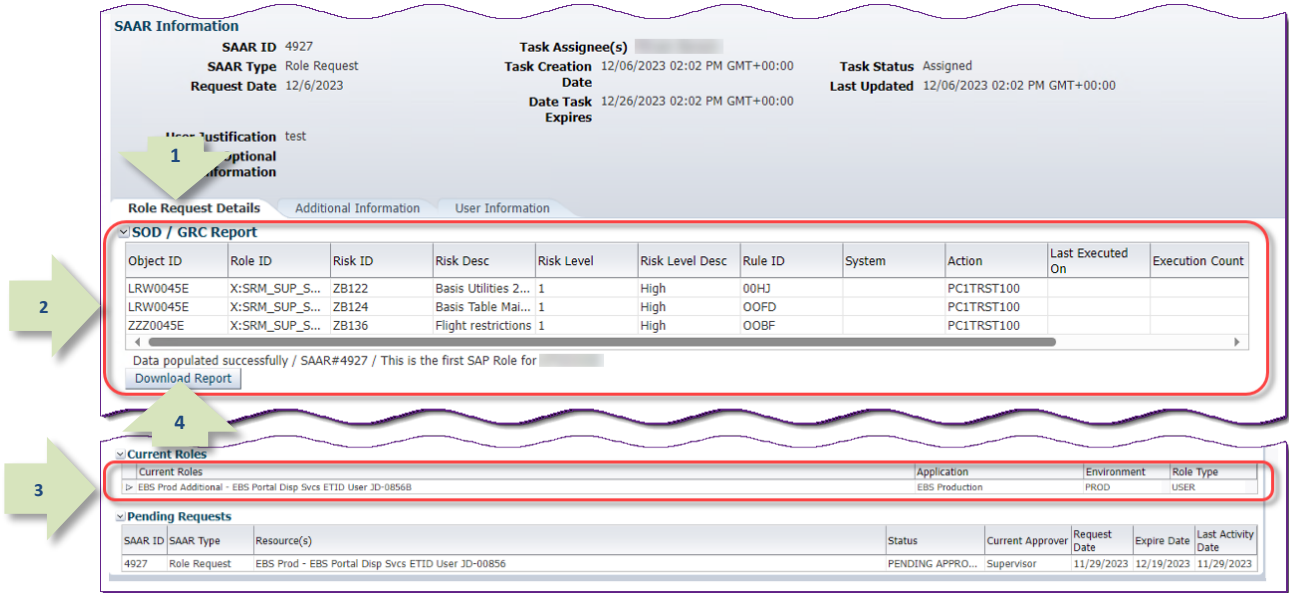4. As an option, click the **Download Report** button to view the report in Excel.

Figure 545: Sample Supervisor Approval Screen -

This sample screen shows the SOD/GRC Report section for a user with three violations.

5. As an option, review GRC report results in Excel. Reformat the display of data, as needed.

Figure 546: GRC Report in Excel Format -

When you download a GRC report, the system automatically opens Excel and displays the report results.

Approval Screen: Excessive Violations Reported

The sample approver's screen shows an SOD/GRC report that displays 50 or more unmitigated violations. The same report appears on the Data Owner approver's screen.

1. Locate the **SOD/GRC Report** section in the approver's screen, on the **Role Request Details** tab.

2. View the report results: The **Risk Description** indicates the type of violation that has occurred.

3. Note the message under the table indicates the output has exceeded the 50-risk limit.

4. As an option, click the **Download Report** button to view the report in Excel.

Figure 547: Sample Supervisor Approval Screen -

This sample screen shows the SOD/GRC Report section displaying 50 or more violations.

Download the report to view the results separately (see Figure 548).

5. As an option, review GRC report results in Excel. Reformat the display of data, as needed.

5

	Object ID	Role ID	Risk ID	Risk Desc	Risk Level	Risk Level Desc	Rule ID	System	Action	Last Executed On	Execution Count	Control	Monitor
2	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	002Y	SR1TRST100	LSMW				
3	TEC_USER_402	Y:BWX_SUP_SUT2_BW_DEVELOPER	ZB001	Basis Development & System Administration	0	Medium	00J0	SB1TRST100	SM51				
4	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JH	SR1TRST100	S_ALR_87101026				
5	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FM	SR1TRST100	SM13				
6	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0038	SR1TRST100	SE93				
7	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0032	SR1TRST100	LSMW				
8	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JG	SR1TRST100	S_ALR_87101026				
9	TEC_USER_402	Y:ECC_SUP_SUT2_ALL_FUNCTIONAL	ZB001	Basis Development & System Administration	0	Medium	00FY	SR1TRST100	ZDLAMIR6				
10	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JC	SR1TRST100	SE11				
11	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0032	SR1TRST100	SE37				
12	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0038	SR1TRST100	LSMW				
13	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FL	SR1TRST100	SE37				
14	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00EU	SR1TRST100	CMOD				
15	TEC_USER_402	Y:ECC_SUP_SUT2_ALL_FUNCTIONAL	ZB001	Basis Development & System Administration	0	Medium	003F	SR1TRST100	ZDLAMIR6				
16	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FH	SR1TRST100	SE11				
17	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JF	SR1TRST100	S_ALR_87101026				
18	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01IP	SR1TRST100	S_ALR_87101026				
19	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FR	SR1TRST100	SE93				
20	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0033	SR1TRST100	LSMW				
21	TEC_USER_402	Y:BWX_SUP_SUT2_BW_DEVELOPER	ZB001	Basis Development & System Administration	0	Medium	00HV	SB1TRST100	SE37				
22	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JC	SR1TRST100	S_ALR_87101026				
23	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	002Y	SR1TRST100	SE11				
24	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0033	SR1TRST100	SE38				
25	TEC_USER_402	Y:ECC_SUP_SUT2_ALL_FUNCTIONAL	ZB001	Basis Development & System Administration	0	Medium	003E	SR1TRST100	ZCONF				
26	TEC_USER_402	Y:ECC_SUP_SUT2_ALL_FUNCTIONAL	ZB001	Basis Development & System Administration	0	Medium	00FX	SR1TRST100	ZCONF				
27	TEC_USER_402	Y:MSTR_CPT_FINANCE_DEV	ZB001	Basis Development & System Administration	0	Medium	0031	SR1TRST100	SE15				
28	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FX	SR1TRST100	SM13				
29	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00EU	SR1TRST100	SM13				
30	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	002B	SR1TRST100	CMOD				
31	TEC_USER_402	Y:BWX_SUP_SUT2_BW_DEVELOPER	ZB001	Basis Development & System Administration	0	Medium	00J0	SB1TRST100	SE37				
32	TEC_USER_402	Y:MSTR_CPT_FINANCE_DEV	ZB001	Basis Development & System Administration	0	Medium	00FK	SR1TRST100	SE15				
33	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FK	SR1TRST100	SM13				
34	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FL	SR1TRST100	SM13				
35	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FH	SR1TRST100	SM13				
36	TEC_USER_402	Y:MSTR_CPT_FINANCE_DEV	ZB003	Basis Development & Client Administration	0	Medium	01JF	SR1TRST100	SE15				
37	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	003F	SR1TRST100	LSMW				
38	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FY	SR1TRST100	SM13				
39	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01IP	SR1TRST100	CMOD				
40	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JG	SR1TRST100	SE37				
41	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	0031	SR1TRST100	LSMW				
42	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	003E	SR1TRST100	LSMW				
43	TEC_USER_402	Y:ECC_SUP_SUT2_ALL_FUNCTIONAL	ZB003	Basis Development & Client Administration	0	Medium	01JS	SR1TRST100	ZCONF				
44	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	002B	SR1TRST100	LSMW				
45	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JS	SR1TRST100	S_ALR_87101026				
46	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JM	SR1TRST100	SE93				
47	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FM	SR1TRST100	SE38				
48	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JH	SR1TRST100	SE38				
49	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB001	Basis Development & System Administration	0	Medium	00FR	SR1TRST100	SM13				
50	TEC_USER_402	Y:BWX_SUP_SUT2_BW_DEVELOPER	ZB001	Basis Development & System Administration	0	Medium	00HV	SB1TRST100	SM50				
51	TEC_USER_402	Y:ECC_FID_SUTF_FINANCE	ZB003	Basis Development & Client Administration	0	Medium	01JM	SR1TRST100	S_ALR_87101026				

Figure 548: GRC Report in Excel Format -

When you download a GRC report, the system automatically opens Excel and displays the report results.

Appendix G: External Approver Authentication

The features that support the external role request and approval processes in AMPS have been available since the inception of AMPS with few changes requested in the interim. When customers learned from the user community that certain business processes related to the approval of role requests were not fully supported in the application under the previously specified requirements, these customers submitted anecdotal evidence of a support gap. Customers also reexamined the business processes that support external user role requests and worked with the AMPS team to submit additional business requirements. These additional requirements help ensure that the AMPS technical solution addresses the needed support.

The result is an external approver module that features minimal change requiring virtually no retraining, and that better handles the authentication of external approvers. The External Approver Process has undergone three major changes in past releases:

- An attestation screen, called **Verify Approver**, which asks an approver to verify he or she is the identified and appropriate approver for the specified user.

- A requirement to use a CAC or other smart card if an approver initially authenticates entry to the External Approval Portal using a CAC or smart card. Approvers who do not authenticate with a CAC will not be required to present this form of authentication, but their email address must match the address of record, and they must confirm their identity as the correct approver through the **Verify Approver** screen.

- A section on the **Approval Information Update** screen that enables the first-time external approver to enter their name and telephone number into the approver's record. The email address is managed by the requesting external user in their **My Profile**>**My Information** screen.

These features offer much better authentication support with minimal interruption to the approvers' familiar procedures.

The AMPS External Service

AMPS added several features and functions that exact more control over how external approvals are handled. These new features and functions are not reflected in most of the user interface. AMPS has incorporated changes in some screens, while others remain the same:

- External users now identify their External Supervisors, External Security Officers, and External Authorizing Officials by providing only email addresses for these approvers during account registration.

- External approvers must be separate and distinct individuals having different addresses.

- External users still maintain up-to-date information on their approvers through the **My Information** section of their individual profiles.

- External users can still make changes to approver information through the role request process by updating the entries provided in the **User Information** screen of the role request sequence.

- AMPS notifies external approvers of approval requests through email notifications.

- External approvers still open approval forms through the AMPS External Service. They can apply changes to the approval forms as before, and either approve or reject the role request.

External Supervisors, External Security Officers, and External Authorizing Officials who provide approvals for these role requests have seen changes in how the approval forms are delivered

by the AMPS External Service. AMPS now applies several backend and frontend changes to the delivery method that improves approver authentication support:

- After the external approver uses a CAC or other smart card to log in to the AMPS External Service, the Service requires the approver to use this authentication method on all successive approval requests submitted by the associated user.

- Since the DoD's CAC modernization directive was implemented, CAC-enabled external approvers should use the Authentication certificate on their CAC to authenticate.

- AMPS stores each approver's email address. If a CAC is used for authentication, AMPS may compare the email addresses from the approver's AMPS record and the CAC. If the comparison detects an email-address mismatch, AMPS cannot display the approval forms to the approver.

- An external approver must verify, through the **Verify Approver** screen, that he or she is the designated approver for the external user. This verification is requested only the first time the approver starts the approval process for that particular user. The verification answered during the first approval for the user is stored in the database for reference.

The procedures included in this guide present new features and functions in the external approval context, and identify the business rules introduced for this release.

External Approval Service

The External Approval Portal (EAP) provides the entry point for an external approver to the external approver's processes. An approver gains access to the portal by copying and pasting the unique, encrypted URL provided in the **Action Required** email notification that AMPS sends for each SAAR requiring an approval.

This portal is a module, separate from AMPS, that provides a bridge for communicating and displaying information from the external approver to AMPS. This bridge enables external

users to take maximum advantage of a limited number of AMPS features without requiring the same account access needed by internal approvers. Using the portal, approvers can take action on email notifications sent to them for role request approvals.

Access to the EAP requires the approver to enter the appropriate credentials for authentication purposes before he or she can proceed to a user's role request SAAR.

External Approval Processes

This section provides you with a narrative description of the three major phases of an external user's role request and approval. The information helps you understand the process through the following steps:

- What happens during an external user's role request submission?
- What happens during an external approver's login to the EAP?
- What happens during an external approver's review of a SAAR?

User's Role Request Submission

When an external user submits a role request, AMPS creates a SAAR that is automatically forwarded to the External Supervisor identified in the User Information screen of the role request sequence. AMPS sends the user's external approver information along with the request. This information includes only the approver's name and email address, but the approver can adjust the name, and fill in a telephone number in the approval form presented later, during their initial approval.

AMPS responds to the external user's SAAR submission in the following steps:

- Creates the SAAR,
- Checks the approver's email,

- Sends an email notification to the approver containing a link to the EAP.

The following rules govern the actions of external users who have submitted role requests:

- Users can no longer approve their own role requests by identifying themselves as their own Supervisor or Security Officer.
- Users will continue to identify their External Supervisors and External Security Officers during account registration. AMPS creates approver records for previously unrecorded approvers when their information is entered by the user during registration or profile update.

External Approvers' Login to the EAP

External Approvers in this description include the following business roles:

- **External Supervisor (ESU):** this approver is required for every role request submitted by an external user.
- **External Security Officer (ESO):** this approver is required for every role request submitted by an external user.

- **External Authorizing Official (EAO):** this approver is required only for certain roles with role definitions that require this approval stage. The user supplies the EAO's email address as part of a role request. The EAO provides his or her name and phone number on the Approval Work Queue during the EAO approval process.

CAC- and Smart Card-Enabled Approvers

An external user who receives an **Action Required** email notification works through these basic steps with AMPS:

1. The external approver, following the directions provided in the **Action Required** notification, copies the approval URL from the email to a browser.
2. Activating the URL prompts AMPS to check for a credential: did the approver use a CAC or other smart card?

3. If the approver did not log in with a CAC or other smart card, see the sequence of actions in the **Non-CAC-Enabled Approvers** section.
4. If the approver used a CAC or other smart card but did not choose the PIV or Authentication certificate, AMPS may display an error message.
5. For approvers who choose the email certificate while logging in with a CAC or other smart card, AMPS detects the email address from the certificate and compares it with the encrypted email address in the **Action Required** notification.

a. If the email addresses match, AMPS checks the database for a preexisting external approver record.

    i. If there is no preexisting record, AMPS creates a record for the external approver and stores the user's EDIPI with the record.

    ii. If there is a preexisting record without an EDIPI, AMPS stores the EDIPI in the record.

b. If the email addresses do not match, AMPS displays an error message. The approver will not be allowed to view the work queue listing the pending approval while they use this certificate.

6. For CAC and smart card users, AMPS performs an additional check next: the system verifies whether or not an approver with a preexisting record has EDIPI information associated with the record.

a. If the preexisting record does not have EDIPI information, AMPS adds the EDIPI to the preexisting record.

b. If the record does have EDIPI information already, AMPS then compares the CAC's EDIPI with the approver record's EDIPI.

    i. If the two EDIPIs match, AMPS searches for approvals and matches the correct ones by comparing the email address and the EDIPI. Only those that match are provided to the approver.

    ii. If the two EDIPIs do not match, AMPS displays an error message indicating the approver is not allowed to view the approvals.

7. After the appropriate matches to authentication information are complete, AMPS assembles a list of pending approval SAARs, opens the EAP, and displays the pending SAARs in a Work Queue tailored for the logged-in approver.

Non-CAC-Enabled Approvers

1. The external approver, following the directions provided in the **Action Required** notification, copies the approval URL from the email to a browser.

2. Activating the URL prompts AMPS to check for a credential: did the approver use a CAC or other smart card?

a. If the approver did not use a CAC, AMPS checks to see if an external approver's record exists for the email address encrypted in the URL.

    i. If the external approver record does not exist, AMPS creates an external approver record for the approver and stores it without an EDIPI. For approvers who do not use a CAC or other smart card, AMPS will match the approver's email of record with the email address in the approval notification.

    ii. If the external approver record does exist, AMPS checks for existing EDIPI information in the record.

        1) If the approver's preexisting record already has EDIPI information stored with it, AMPS displays an error message: a CAC- or smart card-enabled approver who has already used this credential to authenticate as an approver and approve one or more SAARs must continue to use the CAC or smart card. The approver can use only the existing CAC or smart card used before to gain access to the Approval Work Queue list of pending approvals.

        2) If the approver's preexisting record does not have EDIPI information stored with it, then AMPS must match the user's email address in the Action Required URL to the approver's email address associated with the SAAR. The pending approvals with matching email addresses will be displayed to the approver.

b. If the approver used a CAC or smart card, see Step 2 in the **CAC- and Smart Card-Enabled Approvers** section.

3. After the external user's credentials have been verified, AMPS searches for approvals, assembles them in a list, and displays the list in the External Approver's **Work Queue**.

External Approvers' Work Queue List

After AMPS opens the EAP and displays the approver's **Work Queue** list of SAARs, the approver can select a SAAR to open and approve. AMPS associates the approver's encrypted email address (from the URL) with the approval task and passes that email address to the EAP.

The following list provides the sequence of steps that AMPS follows to further ensure an approval task is displayed for the correct approver.

1. AMPS first verifies the approver's email address is present and that it matches an existing approver record email address.

a. If the email addresses do not match, AMPS displays an error message: the approver has made an invalid request.

b. If the email addresses match, AMPS goes to Step 2.

2. AMPS verifies that the email address matches the specified external approver's email address.

a. If the email addresses are not a match, AMPS displays an error message: the selected SAAR has been assigned to someone else.

b. If the email addresses are a match, AMPS goes to Step 3.

3. AMPS compares the requestor's email address to the approver's email address.

a. If the addresses match, AMPS displays an error indicating that a requestor does not have permission to approve his or her own SAAR.

b. If the addresses do not match, AMPS goes to Step 4.

4. AMPS compares the approver's email address to email addresses of all previous approvers for this SAAR:

    a. If the current approver's email address matches any previous approver's email address, AMPS displays an error: the system does not permit an approver to approve a SAAR more than one time. Each approver must be a different person.

    b. If the current approver's email address does not match any previous approver's email address, AMPS goes to Step 5.

5. AMPS checks the approver's record to determine whether or not the approver has previously verified that he or she is an ESU, ESO, or EAO for the user identified in the SAAR:

    a. If the approver has not already established this verification, AMPS displays the Verify Approver dialog.

    i. If the approver agrees that he or she is the correct approver for the specified user, AMPS updates the approver's record with a confirmation that the approver is the user's approver.

    ii. If the approver does not agree to this verification, AMPS automatically rejects the SAAR.

    b. If the approver has already established this verification, AMPS goes to Step 6.

6. After the approver clicks the pending approval action from the Work Queue and, if necessary, verifies he or she is the correct approver for the specified user, AMPS displays the decision screen appropriate for the approver's role.

After Step 6 is completed, AMPS captures the approver's decision and proceeds with the workflow as determined by the decision.

Contact Information for an Approver

The business rules applicable to External Supervisors, External Security Officers, and External Authorizing Officials apply only to external users who work for a federal agency outside DLA or DFAS and who are either members of the military, members of the civilian workforce, or government contractors. Vendors and members of the public who have external user accounts are not required to obtain Supervisor or Security Officer approval for their roles.

Note:

Only a user, working with an External Approver, can maintain the approver's email address of record. If the approver's email address changes, he or she must notify all direct reports to advise them of the change.

Appendix H: References

Some information in this user guide has been supplied from one or more of the following sources:

Document Type	Author	Title	Source Location
DoD Policy	Craig Alderman	Department of Defense Policy Number 5200.2-R, January 1987 Subject: Personnel Security Program	http://www.cac.mil/policies/
NIST Resource List	N/A	National Institute of Standards and Technology (NIST): Role-based Access Control (RBAC) and Role-based Security	http://csrc.nist.gov/groups/SNS/rbac/
ECA root certificate download instructions	N/A	DoD Class 3 PKI Download Root CA Certificate: Instructions for downloading the certificate for the Root Certificate Authority (CA).	http://dodpki.c3pki.chamb.disa.mil/rootca.html
Web Site	N/A	PKI and PKE tools	https://www.idmanagement.gov/IDM/s/ https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XRrC

Index: AMPS Task Topics

I

J

L

M

N