Mass General Brigham

PERSONNEL AUTHORIZATION SYSTEM: RFA REFERENCE GUIDE

This guide is designed to provide an overview of managing Research File Areas (RFAs) using the Personnel Authorization System (PAS), the application used to manage access to network resources.

1 GETTING STARTED

1.1 Keygiving - PAS Support

Training is required to gain access to PAS and become a Keygiver. For more information, view article KB0013211 or contact the Digital Service Desk.

1.2 Obtaining your Keygiver Rights

- Training is required to become a Keygiver. You will need Keygiver rights to grant RFA access to others.
- After training is completed, your manager can request your Keygiver rights to any existing RFAs through the Digital Service Desk.

1.3 Accessing PAS

To access PAS, log in using your Mass General Brigham user name and password.

From a Workstation

1. Go to Applications.
2. Select Personnel Authorization System.

From a Non-standard Workstation, VPN or a MAC

1. Go to http://myapps.partners.org.
2. Click Personnel Authorization System.

Tip! You may need to click **+** on the left to add PAS to your My Apps home page.

2 FIND AND VIEW ACCOUNT INFORMATION

When you first log in to PAS, the Find Account window will display. When searching for an account (user) always:

- Search by **User Name** (*e.g. ABC15*), which may also be referred to as **Network ID** (**NID**) or **Alias** (*as it appears in the Outlook Global Address List*).
- Search by name (*last name, first name*) only when necessary.
- Verify their name and user name before proceeding.
- If an account is **Disabled**, it will be noted in the systems list.

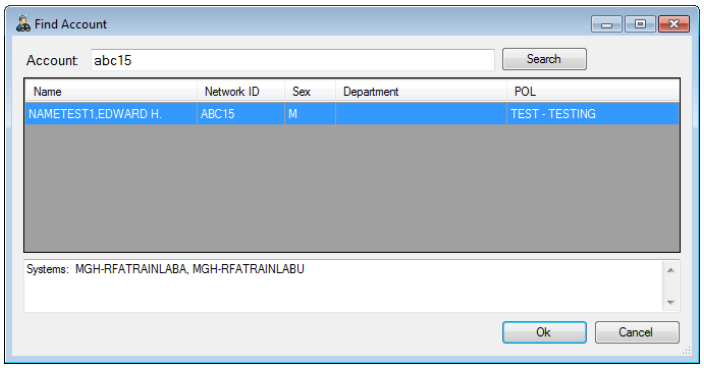
Search Tips

- If you are unable to find a user, ensure you have the correct user name or contact your Help Desk.
- If a user's account is disabled, it must be reactivated first before you can grant any RFA access.

2.1 Search for a User

1. Enter their **User Name**.
2. Click **Search** or press **Enter**.
3. Double-click the correct user (*or select the user, and then click OK*) to proceed to the PAS home screen.

To search for a new user from the home screen, click **Account**, and then select **Find Account**.



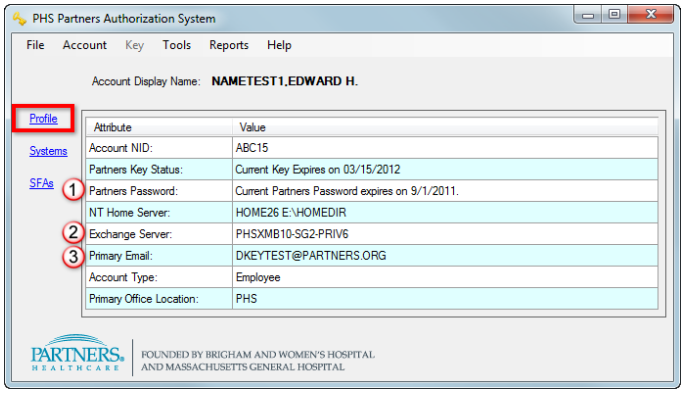
2.2 View Account Profile, Systems, & SFAs

When a user's account is selected, the PAS home screen will display their Profile, Systems, and SFAs.

The **Profile** displays information about the user, such as:

1. Password status
2. Outlook Exchange Server
3. Primary email address

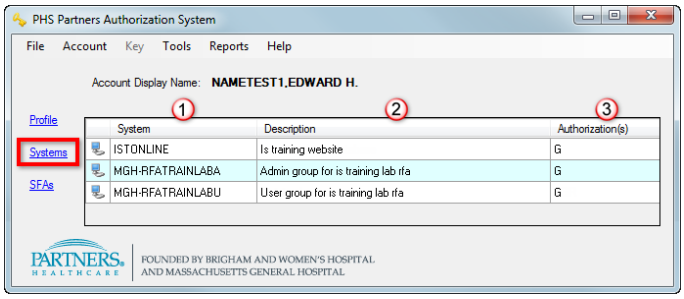
The Profile is displayed by default when you first reach the home screen.



Account Profile

Click **Systems** to display the user's current RFA and system access:

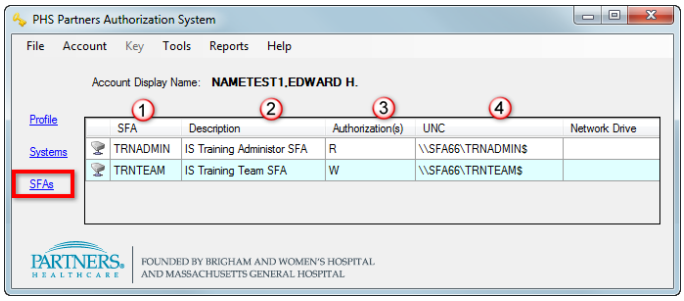
1. RFA or System name
2. Description
3. Current authorization(s)



Current Authorized Systems & RFAs

Click **SFAs** to display the user's current SFA access:

1. SFA name
2. Description
3. Current authorization(s)
4. Path for drive mapping



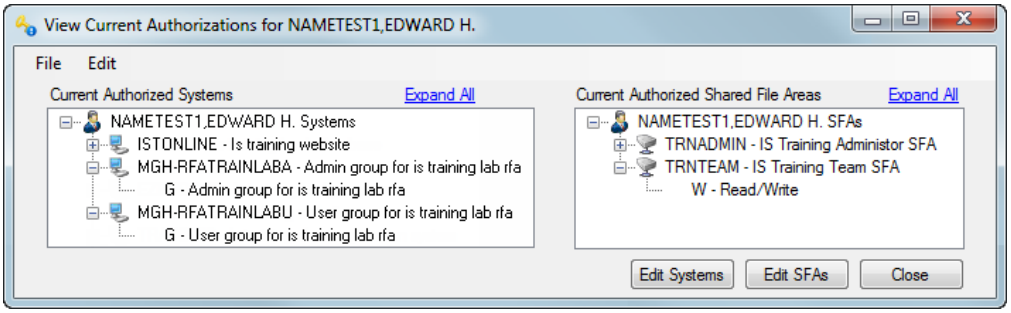
Current Authorized SFAs

For either view, click a **Column Heading** to sort.

2.3 View Current Authorizations

View Current Authorizations allows you to see a user's system and SFA access in the same screen.

1. Click **Account**, and then select **View Current Authorizations**.
2. Their RFAs and Systems will be listed on the left and SFAs on the right.
3. Click **+** or **Expand All** to expand a system or SFA and view assigned authorizations.
4. If you need to make changes to their access, click **Edit Systems** or **Edit SFAs**.



3 MANAGING RFA ACCESS

RFAs are found in a user's Systems list. Each RFA is divided into two groups:

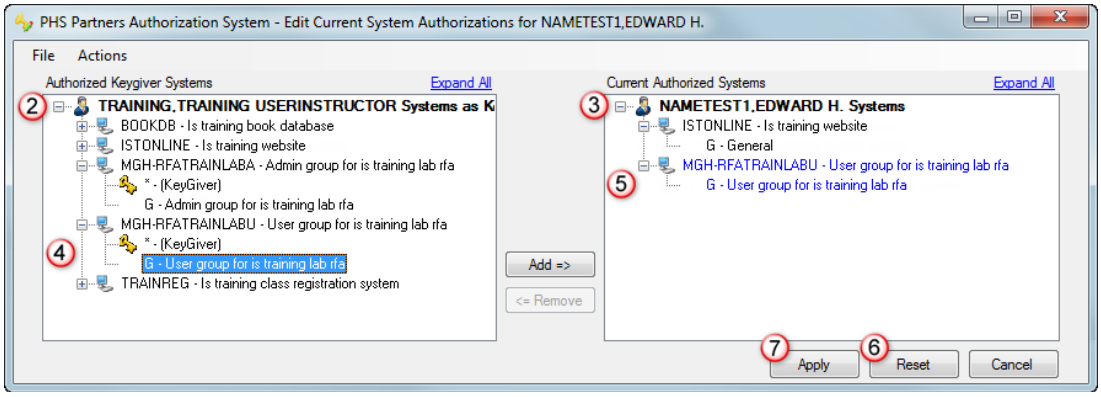
Group	Definition	Example
"**U**" or User	Allows user ability to create, edit, and delete files and folders.	[Institution]-RFA[LabName]U *e.g., MGH-RFATrainLabU*
"**A**" or Admin	Allows user the same as "U", but also the ability to manage individual folder permissions in the RFA*.	[Institution]-RFA[LabName]A *e.g., MGH-RFATrainLabA*

Within each group you will see the authorization letter "G", which is used to grant access to the user.

**Visit the Keygiver Support Site for instructions related to managing individual folder permissions.*

3.1 Assigning Access to an RFA

1. Click **Account**, and then select **Edit System Authorizations**.
2. The RFAs and Systems for which **you** are a Keygiver are on the left.
3. The RFAs and Systems to which the user has access are on the right.
4. Under your authorized Systems, click **+** to expand the desired **RFA Group**.
5. Select **G**, and then click **Add**. The RFA group will display in the user's access list on the right in blue.
6. Click **Reset** to clear changes and start over, if needed.
7. Click **Apply**. A confirmation window will display.
8. Review the changes, and then click **Apply**. Enter your **Password**, and then click **OK**.
9. A confirmation window will display. Click **OK**.



3.2 TIPS FOR MANAGING ACCESS

When managing access, keep the following tips in mind:

- After making changes to a user's account, they will need to log off and log back in to their workstation for the changes to take effect.
- On a non-standard workstation, the RFAs will need to be "mapped" before it appears in the user's Network Drive list. Visit the Keygiver Support Site for directions.
- Users are not notified when access is granted, changed, or removed.

3.3 REMOVING ACCESS TO AN RFA

If someone no longer needs access to an RFA you manage, be sure to remove their access.

1. Click **Account**, and then select **Edit System Authorizations**.
2. In the **Account's** authorizations list, systems and RFAs for which you are a Keygiver will display in black.
3. Click **+** to expand the desired **RFA Group**.
4. Select **G**, and then click **Remove**. You may also double-click the letter.
5. Click **Reset** to clear changes and start over, if needed.
6. Click **Apply**. A confirmation window will display.
7. Review the changes, and then click **Apply**. Enter your **Password**, and then click **OK**.
8. A confirmation window will display. Click **OK**.