Introduction

During the Version 1.1 software upgrade, the Microsoft® operating system was upgraded to Windows® 10. This document describes how to change a user account password on the Affirm® prone biopsy system. This should be performed by on-site personnel who manage user access to the system, such as a Technologist Manager.

To increase product security, changes were made to your Affirm prone biopsy system during the Version 1.1 software upgrade, which require your attention.

All existing customer accounts on the system have reset passwords that are temporary defaults and are set to expire. Default built-in accounts (for example, Rad Tech) also have temporary passwords. Review and update user passwords before using the system.

It is important that all user accounts are reviewed and the following actions are taken:

- Remove users who no longer require account access.
- Users who are required to retain access must change their temporary default passwords as soon as possible.
- Hologic® recommends changing the built-in product user passwords for increased security. If the Hologic service user password is changed, inform the Hologic service representatives, so they can continue to service the system.
- Review user account security settings.

For instructions specific to updating temporary passwords assigned during the upgrade, refer to the following “How Do I Update User Account Passwords?” section. For any questions or concerns, talk to your Hologic service representative.

What Changes Have Been Made?

As Hologic transitions our products to Windows 10, we use the Windows operating system for user management in the product application. This allows for a shared user management experience in the system.

We no longer have to separately manage the secure storage of user credentials in the product database. As Microsoft continues to maintain and update its user management security, the Hologic product software benefits from the updates.

Hologic products integrate with Microsoft user management technologies used by our customers, such as Active Directory®. This allows us to achieve better least privilege design by running our product application as a standard user, where appropriate. Hologic has better accountability through unique operating system accounts for each user.

Default passwords have been updated from previous passwords for built-in product accounts. This was done to meet updated password length and complexity requirements. Although Hologic has taken steps to increase security of our default accounts, we recommend changing passwords and maintaining them according to your security policy.

There are other user account security settings available, along with Hologic configured defaults that are described in this document, such as minimum password length and account lockout. Most Windows user account settings are available for customization to meet your security needs.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

What Are the New Default Passwords for Built-In User Accounts?

Table 1: List of Default Passwords Based on Role After Software Upgrade

Username	Password	Role
PacsAdmin	PacsAffirm2	PACS Administrator
HologicApps	AppsAffirm2	Applications
BioMed	BioAffirm2	Biomedical Engineer
TechMgr	MgrAffirm2	Manager
MedPhys	PhysAffirm2	Medical Physicist
TechRad	RadAffirm2	Radiological Technologist

Note
Some of the default built-in user accounts may have been removed from the system during installation or setup.

Note
When changing or creating passwords, the new password provided should meet the security policies configured for the system, that is, complexity and minimum password length.

How Do I Update User Account Passwords?

There are several ways to change user account passwords. Refer to the following methods and instructions. Refer to the “Are There Additional User Account Security Settings Worth Considering?” section for defaults and instructions for customization.

If the system is configured for Active Directory, users are typically restricted to updating only their own password. Contact your IT department if you must change the Active Directory password for another user.

Procedure to Change User Account Passwords

The software upgrade to Windows 10 reset all customer user passwords to temporary defaults. Users log into Windows with their user name to update their password. They must use the temporary default password assigned to them. Default passwords are assigned based on roles. For example, if the user is configured as a Radiological Technologist, the new temporary password is RadAffirm2. If the user is configured as a Manager, the new temporary password is MgrAffirm2. Refer to previous Table 1 for default passwords configured for each default role.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

During the login process, a password-expired page is provided, which enables a new password to be entered. Refer to the following four methods for detailed instructions. A Manager user may update a password on behalf of another user.

Method #1–Change Expired Password at Windows Login

1. Log into Windows as the user.
2. If the current password is expired, a message appears stating the password must be changed.
3. Select **OK** to change password.
4. Enter new password in the "New Password" and "Confirm Password" boxes.
5. Press the **ENTER** key.
6. A message stating the password has been changed appears. Select **OK**.
7. Windows continues to log into that user account with the new password.

Method #2–Change Password Using the Hologic Product Application

1. Log into the product application as the user.
2. At the Select Patient page, select **Admin**.
3. On the Admin page, select **My Settings**.
4. Select **Change Password**.
5. Enter new password in both password boxes.
6. Select **Save**.
7. The Update Successful message box appears. Select **OK**.

Perform the Following Steps When a Manager Changes the Password of Another User:

1. Log into both Windows and the Hologic product application as an administrator user, that is, a Manager.
2. At the Select Patient page, select **Admin**.
3. On the Admin page, select **Manage Operators**.
4. On the Manage Operators page, select the user and select **Edit**.
5. Select **Change Password**.
6. Enter new password in both password boxes.
7. Select **Save**.
8. The Update Successful message box appears. Select **OK**.

Method #3–Change Current Password for Another User with Windows

1. Log into Windows as the user.
2. Press the **CTRL+ALT+DEL** keys on the keyboard.
3. A window appears; select **Change a password**.
4. Enter current password of the user in "Old Password" box.
5. Enter new password in the "New Password" and "Confirm Password" boxes.
6. With new password entered, press **ENTER**.
7. A message stating the password has been changed appears. Select **OK**.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Method #4–Force Change of Existing Password Using Windows Computer Management

1. Log into both Windows and the Hologic product application as an administrator user (for example, a Manager).
2. In the product application, on the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Users and Groups**.
5. Under Local Users and Groups, select **Users** folder.
6. Right-click selected user account in the list and select **Set Password.**
7. At the warning message, select **Proceed**.
8. Enter password and select **OK**.
9. If successful, a message stating the password has been set appears. Select **OK.**

How Do I Remove User Accounts that Are No Longer Required?

Manage user accounts configured for the product application through the product application. The product application tracks known Windows user accounts and links them to the product application user settings. If a user is deleted using Windows, orphaned database entries appear in the product application. The product application login screen shows the user as available although the user has been deleted. To remove users from the product application, refer to the following Method #1 instructions. If a user account is unknown to the product application, that is, created purely for Windows management, remove the account by following “Method #2– Remove a User Through Computer Management.”

Method #1–Remove a User Through the Hologic Product Application (Preferred Method)

1. Log into both Windows and the Hologic product application as an administrator user (for example, a Manager).
2. In the Hologic product application, on the Select Patient page, select **Admin**.
3. On the Admin page, select **Manage Operators**.
4. On the Manage Operators page, select the user, and then select **Delete.**
5. In the confirmation dialog, select **Yes**.
6. User is removed from the list of Operators.

Method #2–Remove a User Through Computer Management

Follow these steps only when users are not available for removal in the product application.

1. Log into both Windows and the Hologic product application as an administrator user, for example, a Manager.
2. In the Hologic product application, on the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Users and Groups**.
5. Under Local Users and Groups, select **Users** folder.
6. Right-click the user account from the list and select **Delete**.
7. At the prompt, select **Yes** to continue. The user account has been removed from the list.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Method #3–Remove an Active Directory User

Your IT department manages user accounts in the Active Directory. If a user account is removed or the user should no longer have access to the product application, refer to the following steps.

- Work with your IT department to remove the user account from Active Directory or from the Hologic Active Directory groups.
- Perform previous steps in the "Method #1–Remove a User Through the Hologic Product Application (Preferred Method)" section to delete a user setting from the product application.

How Do I Add New User Accounts?

Depending on the intended use, the three primary methods for adding a user account to the system are as follows.

Method #1–Adding a User Account for Intended Product Application

1. Log into both Windows and the Hologic product application as an administrator user, for example, a Manager.
2. In the Hologic product application, on Select Patient page, select **Admin**.
3. On the Admin page, select **Manage Operators**.
4. On the Manage Operators page, select **New**.
5. Provide the appropriate user details, role, and password.
6. Select **Add**.
7. The Update Successful message box appears. Select **OK**.

Method #2–Adding a User Account Intended for Windows Administration Only

Perform the following steps to add a user account intended for Windows administration only. This means that the user will have no access to run the product application.

1. Log into both the Windows and the Hologic product application as an administrator user, for example, a Manager.
2. In the Hologic product application, on the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Users and Groups**.
5. Under Local Users and Groups, select **Users** folder.
6. In the menu, select **Action** and then select **New User** from the dropdown menu.
7. Enter the user details, password, and password options.
8. Select **Create**.
9. Select **Close**.
10. Confirm that the new user account is in the list of users.
11. Add the user to the Windows groups.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Method #3–Adding an Active Directory User for Product Application

If the system has been configured for Active Directory, refer to the following steps to configure a new user for product application use.

1. IT department creates the user account in Active Directory.
2. IT department adds the new user account to the appropriate Hologic user group in Active Directory.
3. New user logs into Windows in the system.
4. If the user account was properly configured, the product application launches and allows the user to log in with the newly-created Active Directory account.
5. At this point, the new user can customize any of the product application user settings.

Does the System Support Active Directory for User Management?

If your organization supports Active Directory, this product can be configured for application login and user management. Work with your IT department to configure the Active Directory functionality. The following information and instructions help with the configuration process.

Add a System to an Existing Active Directory Domain

1. Log into Windows as an administrator user, for example, HologicService.
2. Navigate to Windows Start → Windows System → Control Panel.
3. At the Control Panel, select **System**.
4. Under Computer name, domain, and workgroup settings, select **Change settings**.
5. The System Properties window opens. Under the Computer Name tab, select **Network ID**.
6. Select "**This computer is part of a business network…**" and then select **Next**.
7. Select "**My company uses a network with a domain,**" and then select **Next**.
8. Select **Next** again.
9. Fill in the information using an Active Directory user name, password, and the domain name.
10. If a dialog appears stating that an account for this computer has been found, select **Yes** to use the account.
11. Enter the computer name and domain again (if it is not already entered) and select **Next**.
12. You may need to enter the Active Directory user credentials again to establish a domain connection.
13. Follow the prompts and restart the system. Log in as an Active Directory user with local administrator privileges.

Configure Active Directory Groups in the Domain

For the Hologic product application to use Active Directory, request that your IT department creates Active Directory groups that correspond to the respective roles of the product application. The groups can have any name, but each name should be recognizable as corresponding to a specific role. Refer to the following Table 2 for example names.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Table 2: Examples of Active Directory Group Names for Each Role

Role	Suggested Active Directory Group Name	Local Windows Administrator
PACS Administrator	Hologic.PACSAdmin	Yes
Applications	Hologic.Applications	Yes
Biomedical Engineer	Hologic.BioMedEngineer	Yes
Connectivity Specialist	Hologic.Connectivity	Yes
Manager	Hologic.Manager	Yes
Medical Physicist	Hologic.MedPhysicist	No
Radiological Technologist	Hologic.RadiologicalTechnologist	No

Configure the System to Support Active Directory Groups in the Domain

When the Active Directory groups (refer to previous Table 2) are created in the domain, configure the system to use them. To achieve this, add each Active Directory group as a member of its corresponding local group:

1. Log into Windows as an administrator user (for example, HologicService).
2. Right-click Windows Start and select **Computer Management**.
3. Under System Tools, expand Local Users and Groups.
4. Select **Groups** folder.
5. For each Hologic group listed, perform the following steps:
   a. Right-click the group and select **Add to Group**.
   b. Select **Add**.
   c. Ensure that Active Directory is selected under the "From this location" field.
   d. Enter the name of the corresponding Active Directory group under the "Enter the object name to select" field. For example, add the created Hologic.Service Active Directory group as a member of the local Hologic.Service group.
   e. Select **OK**.
   f. Repeat the steps for the remaining Hologic groups.

For each Active Directory group marked as a local Windows administrator in previous Table 2, perform the following:

1. Right-click the **Administrators** group and select **Add to Group**.
2. Select **Add.**
3. Ensure that Active Directory is selected under the "From this location" field.
4. Enter the name of the Active Directory group under the "Enter the object name to select" field.
5. Select **OK.**
6. Repeat the steps for the remaining appropriate Hologic groups.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Important Considerations for Active Directory Configuration

- Configure the system in a separate Active Directory organizational unit (OU). The IT department should limit configuration changes and/or software changes pushed to Hologic systems. Pushing unsupported software or configuration changes can result in the product application not functioning correctly.
- Each Active Directory user must belong to only one Hologic Active Directory group. For example, a Radiological Technologist user should be part of the Hologic.RadiologicalTechnologist Active Directory group. The user must not be assigned multiple Hologic roles. If the configuration is incorrect, problems with the product application will occur.

Migrating Product Application Settings for Existing Local Users to Active Directory Users

If the system contains existing customer users with existing product settings, it is possible to remap these users to the newly configured Active Directory users. After configuration, an existing user is able to log into Windows and the product application as their Active Directory user, while maintaining pre-existing product settings. Contact your Hologic field service representative to make this configuration change. Supply the Hologic field service representative with the local accounts that need to be migrated along with the new respective Active Directory user names.

Are There More User Account Security Settings Worth Considering?

Following are some additional security settings to consider. Instructions for customization are included. Work with your IT department to configure the settings. Hologic recommends configuring the settings according to your security policy. The following information assumes that the system is not configured for Active Directory (local policy). If configured for Active Directory, work with your IT department to make and push changes to the systems.

Minimum Password Length

The minimum password length security setting controls the minimum number of characters required when creating a user account password.

Hologic Default: Eight characters

To customize this value, perform the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Account Policies and select **Password Policy**.
6. Customize user account password settings to meet your security policy. The specific setting referenced here is the minimum password length.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Password Complexity

Password complexity and security settings ensure that user account passwords meet Microsoft password complexity rules. To review how Microsoft defines these rules, follow this link:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

Hologic Default: Require complex passwords (Enabled)

To customize this value, perform the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Account Policies and select **Password Policy**.
6. Customize user account password settings to meet your security policy. The specific setting referenced here is that the password must meet complexity requirements.

Password Expiration

Password expiration and security settings control if and when user account passwords automatically expire, which forces the user to change the password.

Hologic Default: Do not automatically expire user account passwords

This value may be customized by performing the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Account Policies and select **Password Policy**.
6. Customize user account password settings to meet your security policy. Decide how many days after the user password is created that it automatically expires. The particular setting referenced here is the maximum password age.

Password Expiration Warning

The password expiration warning security setting configures how many days in advanced the user is warned that the will password expire and it requires an update.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Hologic Default: Five days before password expiration

This value may be customized by performing the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Local Policies and select **Security Options.**
6. Locate and customize the interactive login. Set the number of days in advance to notify the user that they must update their password before it expires to ensure your security policy is met.

Minimum Password Age

After its creation, the minimum password age security setting configures the number of days before a user account password may be changed.

Hologic Default: One day to be able to change the password

This value may be customized by performing the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Account Policies and select **Password Policy**.
6. Customize user account password settings to meet your security policy. The specific setting referenced here is minimum password age.

Enforce Password History

The enforce password history security setting configures how many user-account passwords are remembered which were previously used. Previous passwords that are remembered cannot be reused during password creation.

Hologic Default: No passwords are remembered

This value may be customized by performing the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Account Policies and select **Password Policy**.
6. Customize user account password settings to meet your security policy. The specific setting referenced here is to enforce password history.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.

Account Lockout

The account lockout security settings configure how many invalid login attempts are allowed before a user account is locked and for how long it is locked.

Hologic Default: User account locks after three invalid login attempts and is locked for 15 minutes

These settings may be customized by performing the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Security Policy**.
5. Under Security Settings, expand Account Policies and select **Account Lockout Policy**.
6. Customize user account lockout settings to meet your security policy. The specific settings referenced here are account lockout threshold and account lockout duration.

If a user account is locked, unlock it by performing the following steps:

1. Log into both Windows and the product application as an administrator user, for example, a Manager.
2. At the Select Patient page, select **Admin**.
3. Under System, select **Windows OS Tools**.
4. Select **Local Users and Groups**.
5. Under Local Users and Groups, select **Users** folder.
6. Find the locked user in the list, select the **user**, and select **Properties.**
7. In the Properties window, uncheck the “Account is locked out” option.
8. Select **OK**.

© 2023 Hologic, Inc. The information contained in this document is proprietary. Unauthorized distribution is prohibited.