Customer Technical Bulletin

CTB-00571 Rev 003

Date: *November 4, 2019*

Author: Service Engineering, Software Engineering

Product: Selenia Dimensions/3Dimensions

Subsystem: Acquisition Workstation (AWS)

Subject: Procedure to Change User Account Passwords after Selenia Dimensions Version 1.10 or 3Dimensions Version 2.1 Software Upgrade

---

Revision History

Rev 003 – Updated Tables 1 and 2.

Rev 002 – Updated Tables 1 and 2.

Purpose

To provide information on how to change user account passwords on Selenia Dimensions and 3Dimensions systems that have been upgraded to Versions 1.10 and 2.1 due to the change of Microsoft Operating System to Windows 10 during the software upgrade.

Scope

In an effort to further increase product security, changes are made to your Selenia Dimensions/3Dimensions system during the Version 1.10/2.1 software upgrade that require your attention.

All existing customer accounts on the system have had their passwords reset to a temporary default and have been set to expired. Default built-in accounts (e.g. Rad Tech) have also had their passwords changed. You will need to review and update user passwords **before** using the system.

It's important that all user accounts be reviewed and the following actions taken:

- Users that are no longer required should be removed.
- Users that are required, should have their passwords changed from the temporary default as soon as possible.
- Hologic also recommends changing the built-in product user passwords for increased security. If Hologic Service user password is changed, please inform your Hologic service representative, so that they may continue to service the system.
- Review user account security settings.

For instructions specific to updating temporary passwords assigned during the upgrade, see “Changing expired temporary passwords for customer user accounts” under the "How do I update user account passwords" section. Your service representative will be assist you with any questions or concerns.

What changes have been made?

As Hologic transitions our products to Windows 10, we will be leveraging the Operating System for user management in the product application. This allows for a shared user management experience on the system.

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

Another benefit is that Hologic products will more easily integrate with Microsoft user management technologies leveraged by our customers, such as Active Directory. Importantly, it also allows us to achieve better least privilege design through support of running our product application as a standard user where appropriate, as well as having better accountability through unique Operating System accounts for each user.

Built-in product accounts, such as Rad Tech, have had their default passwords updated from previous defaults. This was done to meet updated password length and complexity requirements. It's a good practice to update these periodically. Although Hologic has made steps here to increase security of our default accounts, we strongly recommend changing passwords of the default accounts and maintaining them according to your security policy.

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

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	PacsDimensions2	PACS Administrator
BioMed	BioDimensions2	Biomedical Engineer
Connectivity	ConnectDimensions2	Connectivity Specialist
TechMgr	MgrDimensions2	Manager
MedPhys	PhysDimensions2	Medical Physicist
TechRad	RadDimensions2	Radiological Technologist

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

How do I update user account passwords?

There are a few methods for changing user account passwords. The methods and instructions are provided below. Note that when changing or creating passwords, the new password provided should meet the security policies configured for the machine, i.e. complexity and minimum password length. See the "additional user account security settings" section of this document for defaults and instructions for customizing.

If the product system is configured for Active Directory, users are typically restricted to updating their own password only. If you need to change a different users Active Directory password, contact your IT department for assistance.

Changing expired temporary passwords for customer user accounts (for system upgrades to Windows 10):

Upgrades of existing product systems to Windows 10 will reset all customer user passwords to a temporary one as they are transitioned to Windows user accounts. Those users should login to Windows with their username to update their password at their earliest convenience. When doing so, they should use the new temporary default password assigned to them. Default passwords are assigned based on roles. Reference Table 1 in this document for default passwords configured for each default role.

(For example, if the user is configured as a Radiological Technologist, their new temporary password will be RadDimensions2. If the user is configured as a Manager, their new temporary password will be MgrDimensions2.)

During the login process, they will be presented with a password expired page that allows entering a new password. See the "Changing expired password at Windows logon" section below for detailed instructions. Alternatively, Manager users may update a users password on their behalf using methods provided on the next two pages.

Method #1 - Changing expired password at Windows logon:

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

Method # 2 - Changing passwords via the Hologic Product Application:

1. For current user changing their password, perform the following steps:
    1. Log into the product application as the desired user.
    2. In the Hologic application, at the Select Patient page, click the Admin button.
    3. On the Admin page, click My Settings.
    4. Click Change Password.
    5. Enter the desired new password in both password boxes.
    6. Click Save.
    7. The Update Successful message box appears. Click OK.

2. For manager user changing a different users password, perform the following steps:
    1. Log into both Windows and the Hologic product application as an administrator user (e.g. Manager).
    2. At the Select Patient page, click the Admin button.
    3. On the Admin page, click Manage Operators.
    4. On the Manage Operators page, select the desired user and then click the Edit button.
    5. Click Change Password.
    6. Enter the desired new password in both password boxes.
    7. Click Save.
    8. The Update Successful message box appears. Click OK.

Method #3 - Changing current users existing password via Windows:

1. Log in to Windows as the desired user.
2. Press CTRL+ALT+DEL keys on the keyboard.
3. At the window that appears, click Change a password.
4. Enter the current password for the user in "Old Password" box.
5. Enter the desired new password in the "New Password" and "Confirm Password" boxes.
6. With password entered, press the ENTER key.
7. A message appears stating that the password has been changed. Click OK.

Method #4 - Force changing existing passwords via Windows Computer Management:

1. Log into both Windows and the Hologic product application as an administrator user (e.g. Manager).
2. In the Hologic application, at the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Users and Groups button.
5. Under Local Users and Groups, click the Users folder.
6. Right click the desired user account in the list and select Set Password...
7. At the warning, click Proceed.
8. Enter desired password and click OK.
9. If successful, a dialog will be presented stating that the password has been set. Click OK.

How do I remove user accounts that are no longer required?

All user accounts configured for use by the product application should be managed through the application. This is because the application keeps track of known Windows user accounts and links them to the product application user settings. Removing a user directly via Windows instead will leave orphaned database entries in the application for their settings. This will show them in the application login screen as available when they're not. Use the instructions provided below for removing users in the product application. If a user account is unknown to the product application, i.e. created purely for Windows management, they can be removed using the "Remove a user via Computer Management" section below.

Method #1 - Remove a user via the Hologic Product Application (preferred):

1. Log into both Windows and the Hologic product application as an administrator user (e.g. Manager).
2. In the Hologic application, at the Select Patient page, click the Admin button.
3. On the Admin page, click Manage Operators.
4. On the Manage Operators page, select the desired user and then click the Delete button.
5. At the confirmation dialog, click Yes.
6. User is removed from the list of Operators.

Method #2 - Remove a user via Computer Management:

Steps here should only be followed for users not available for removal in the product application.

1. Log into both Windows and the Hologic product application as an administrator user, e.g. Manager.
2. In the Hologic application, at the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Users and Groups button.
5. Under Local Users and Groups, click the Users folder.
6. Right click the desired user account in the list and select Delete.
7. At the prompt, click Yes to continue.
8. User account should be removed from the list.

Method #3 - Remove an Active Directory user:

Your IT department will manage user accounts in Active Directory. If a user account is removed or should no longer have access to the product application, see guidance below.

1. Work with your IT department to either remove the user account in Active Directory and/or from the Hologic Active Directory groups.
2. Perform steps in the "Remove a user via the product application" section above to delete user settings from the application.

How do I add new user accounts?

The primary methods for adding a user account to the product system, depending on their intended use, are provided here.

Method #1 - Adding a user account for the product application:

Perform the following steps to add a user account intended for product application use.

1. Log into both Windows and the Hologic product application as an administrator user, e.g. Manager.
2. In the Hologic application, at the Select Patient page, click the Admin button.
3. On the Admin page, click Manage Operators.
4. On the Manage Operators page, click New.
5. Provide the appropriate user details, role, and password.
6. Click the Add button.
7. The Update Successful message box appears. Click OK.

Method #2 - Adding a user account for Windows administration only:

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

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

Method #3 - Adding an Active Directory user for the product application:

If the product system has been configured for Active Directory, reference the steps below for configuring new users for product application use.

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

Does the system support Active Directory for user management?

If your organization supports Active Directory, this product can optionally be configured to utilize it for application login and user management. Work with your IT department to configure Active Directory, if this functionality is desired. Information and instructions in this section can help with this process.

Adding a product system to an existing Active Directory domain:

1. Log into Windows as an administrator user, e.g. HologicService.
2. Navigate to Windows Start → Windows System → Control Panel.
3. In the Control Panel, click System.
4. Under Computer name, domain, and workgroup settings, click Change settings.
5. The System Properties window will open. Under the Computer Name tab, click Network ID.
6. Select "This computer is part of a business network…" and then click Next.
7. Select "My company uses a network with a domain" and then click Next.
8. Click Next.
9. Fill out the information with an Active Directory username, password, and the name of the Domain.
10. If a dialog appears stating that an account for this computer has been found, click Yes to use the account.
11. Enter Computer Name and Domain again, if it is not already entered, and then click Next.
12. You may need to reenter the Active Directory user credentials again in order to establish a domain connection.
13. Continue to follow the prompts and restart the machine, logging in with an AD user with local administrator privileges on restart.

Configuring Active Directory groups on the domain:

In order for the Hologic product application to use Active Directory, your IT department should create Active Directory groups corresponding to the Roles of the application. The groups can have any name, but should be recognizable as corresponding to a specific role. Table 2 below shows an example of AD group names for each role:

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
Biomedical Engineer	Hologic.BioMedEngineer	Yes
Connectivity Specialist	Hologic.Connectivity	Yes
Manager	Hologic.Manager	Yes
Medical Physicist	Hologic.MedPhysicist	No
Radiological Technologist	Hologic.RadiologicalTechnologist	No

Configuring the product system to support Active Directory groups on the domain:

Once the Active Directory groups (Reference Table 2) are created on the domain, the product system should be configured to use them. To do this, add each Active Directory group as a member of its corresponding local group:

1. Log into Windows as an administrator user, e.g. HologicService.
2. Right click Windows Start and select Computer Management.
3. Under System Tools, expand Local Users and Groups.
4. Click the Groups folder.
5. For each of the Hologic.* groups listed, perform the following steps:
    1. Right click the group and click Add to Group...
    2. Click Add...
    3. Ensure that Active Directory is selected under the "From this location" field.
    4. Enter the name of the corresponding Active Directory group under the "Enter the object name to select" field. For example, you will add the created Hologic.Service Active Directory group as a member of the local Hologic.Service group.
    5. Click OK.
    6. Repeat steps for the remaining Hologic groups.
6. For each Active Directory group marked as a local Windows administrator in the table above, perform the following:
    1. Right click the Administrators group and click Add to Group...
    2. Click 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. Click OK.
    6. Repeat steps for the remaining appropriate Hologic groups.

Important considerations for Active Directory configuration:

- The product system should be configured 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 functioning improperly.

- 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. It should not be assigned multiple Hologic roles. Configuring this improperly will result in issues with the product application.

Migrating product application settings for existing local users to Active Directory users:

If the product system contains existing customer users with existing application settings, it is possible to remap these users to the newly configured Active Directory users. Once configured, an existing user would then be able to login to Windows and the product application as their Active Directory user, maintaining pre-existing application settings. You will need to contact and work with your Hologic field service representative to make this configuration change. The Hologic field service representative will need to know which local accounts need to be migrated and what the new Active Directory user name for each is.

Are there additional user account security settings worth considering?

Yes! Here are some additional security settings to consider including instructions for customization. You may want or need to work with your IT department to configure these settings. Hologic recommends configuring these according to your security policy. Information below assumes the system is not configured for Active Directory (local policy). If configured for Active Directory, feel free to work with IT to make and push desired changes to the product 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: 8 characters.

This value may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Account Policies and click on Password Policy.
6. Customize user account password settings to meet your security policy. Particular setting of note here is **Minimum password length**.

Password Complexity

The password complexity security setting controls whether or not created user account passwords must meet Microsoft password complexity rules. These rules are defined by Microsoft and can be found at the link below.

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

Hologic Default: Require complex passwords (Enabled).

This value may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Account Policies and click on Password Policy.
6. Customize user account password settings to meet your security policy. Particular setting of note here is **Password must meet complexity requirements**.

Password Expiration

The password expiration security settings control if and when user account passwords will automatically expire, forcing the user to change them.

Hologic Default: Do not automatically expire user account passwords.

This value may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Account Policies and click on Password Policy.
6. Customize user account password settings to meet your security policy. Particular setting of note here is **Maximum password age**. How many days after user password creation until it automatically expires.

Password Expiration Warning

The password expiration warning security setting configures number of days before password expiration to begin showing user a warning that their password requires update.

Hologic Default: 5 days before password expiration.

This value may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Local Policies and click on Security Options.
6. Locate and customize the **Interactive logon: Prompt user to change password before expiration** setting to meet your security policy.

Minimum Password Age

The minimum password age security setting configures number of days before a user account password can be changed after its creation.

Hologic Default: 1 day.

This value may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Account Policies and click on Password Policy.
6. Customize user account password settings to meet your security policy. Particular setting of note here is **Minimum password age**.

Enforce Password History

The enforce password history security setting configures how many user account passwords previously used will be remembered. Configured number of previous passwords remembered can not be reused during password creation.

Hologic Default: 0 passwords remembered.

This value may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Account Policies and click on Password Policy.
6. Customize user account password settings to meet your security policy. Particular setting of note here is **Enforce password history**.

Account Lockout

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

Hologic Default: User account locked after 3 invalid logon attempts and locked for 15 minutes.

These values may be customized by performing the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Security Policy button.
5. Under Security Settings, expand Account Policies and click on Account Lockout Policy.
6. Customize user account lockout settings to meet your security policy. Particular settings of note here are **Account lockout threshold** and **Account lockout duration**.

If a user account becomes locked, you may unlock the account using the following steps:

1. Log into Windows and the product application as an administrator user, e.g. Manager.
2. At the Select Patient page, click the Admin button.
3. Under System, click the Windows OS Tools button.
4. Click the Local Users and Groups button.
5. Under Local Users and Groups, click the Users folder.
6. Find the locked user in the list, right click the user, and select Properties.
7. In the Properties window, uncheck the "Account is locked out" option.
8. Click OK.