Security in Bluehill® Software

This document outlines the security options in Bluehill Universal, Bluehill Elements, Bluehill Central. When enabled, security requires users to log in with a username and password prior to operating the testing frame, modifying a method template, or performing any other action in the application. Lab managers can configure permissions, granting access to trained personnel and limiting access where needed.

Three different security options offer various levels of integration with your organization's existing security network. It is recommended to use your Instron frame with security enabled to reduce the risk of unintended changes and to increase the integrity of your testing data.

Security Types

A comparison of security types is summarized in the table below. Additional information for each security type and a list of all user permissions can be found in subsequent sections.

	No security	Bluehill	Active Directory	Windows®
Host location	N/A	Application based	Network based	Computer based
User management	N/A	Login credentials are managed in the software.	Login credentials use the individual's network credentials.	Login credentials are based on local Windows user accounts.
Permission assignment	N/A	Users are assigned to one of three user types with defined permissions: Administrator, Manager, Operator. Additional permissions are assigned to each user.	Permissions are assigned to an Active Directory security group. The groups are created on the network domain. Users that members of that group have those rights.	Permissions are assigned to a group. The groups are based on Windows user groups. Users that are included in the assigned group have those rights.
Administration	N/A	User profiles are managed by any user that is an Administrator user type.	The Permissions section of security is managed by any user included in the Active Directory security group assigned to Configure security.	The Permissions section of security is managed by any user included in the Windows group assigned to Configure security.
User group administration	N/A	N/A	Security groups are managed by the network domain administrator.	Groups are managed by any user included in the Windows Administrators group.
Multiple systems	N/A	Security is managed separately on each system. Each user requires a user profile on each system. *Bluehill Central enables centralized Bluehill security user management.*	Security is managed separately on each system. Network security groups are shared among all systems. *Bluehill Central enables centralized Active Directory user group configuration.*	Security is managed separately on each system. Windows user groups are managed separately on each system.
Availability in Bluehill Universal	Available	Available	Available	Available
Availability in Bluehill Elements	Available	Available	Not available	Not available
Availability in Bluehill Central	Not available	Available	Available	Not available

No security

No security is the default setting for the Bluehill Universal and Bluehill Elements (Bluehill Central requires security to be enabled). This setting provides all users with full access to all sections of the software. Anyone can edit:

- the system configuration
- all method files
- all report template files
- all sample files

With this option, the system does not monitor the person that ran a test or last saved the method/sample. Therefore the User, Method author and Sample author parameters are not available in the method template.

Bluehill

Bluehill security is internal to the software and is based on creating a user profile for each person that requires access to the system. Permissions are organized into three user types that provide different levels of access to the software. There must be at least one user designated as an administrator to manage the security feature and user profiles.

An administrator creates a user profile for each person and assigns a user classification of Administrator, Manager or Operator. The type of classification that is assigned determines the level of access within the software. Each user profile, regardless of the user type, can be further customized with the listed permissions. Disabling these permissions prevent a user from performing that task.

Active Directory

Active Directory security uses the network domain that is managed by your network administrator. The security permissions are assigned to an Active Directory security group and any user that is included in that group has those rights. The user groups are created and managed by the network administrator.

This type of security establishes team permissions rather than individual user permissions, as compared to the Bluehill security format. The Active Directory groups are managed by your IT department. After a group is assigned to each permission, any changes to the users included in a group is done by the network administrator. You will need to work with your IT department to request changes to these groups, as described in the following sections.

For the Lab Manager – Active Directory

The lab manager will be responsible for identifying what groups need to be created and which users should be assigned to those groups. As seen below, the lab manager will need to select an Active Directory group for each permission. When the user logs in to the software with their Active Directory credentials, the software determines if the user is part of the group assigned to each permission. If the user is part of that group, they will be given the corresponding permission.

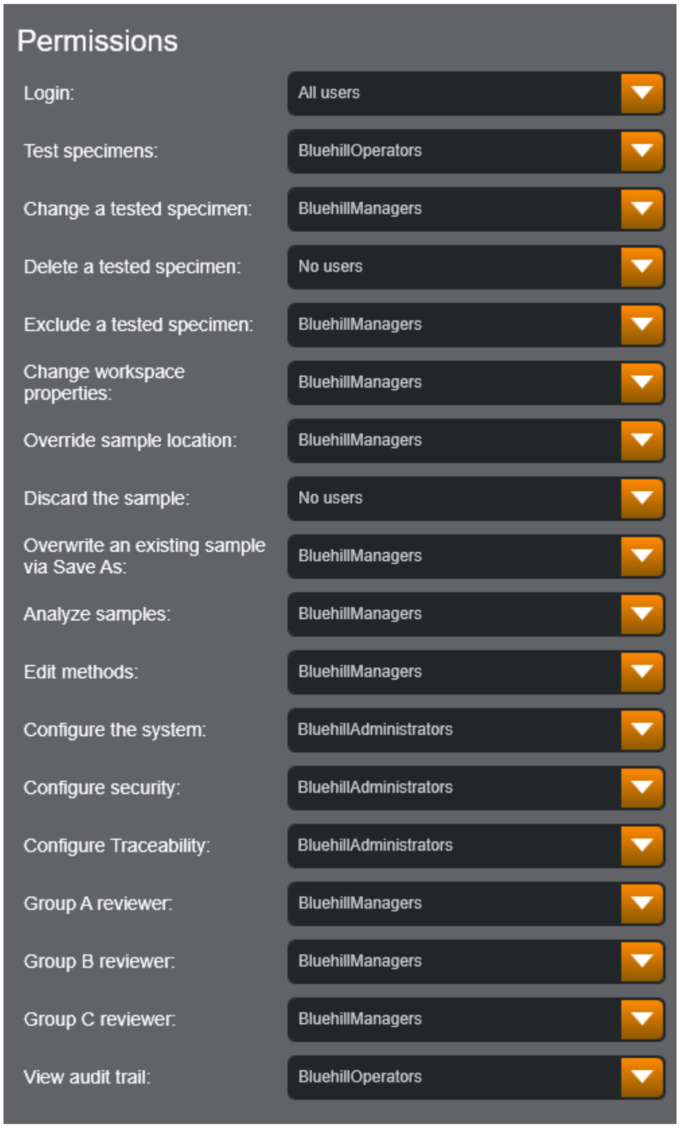
To identify what Active Directory groups need to be created, lab managers should determine what roles and permissions Bluehill Universal or Bluehill Central users should have. For example, do you need just one for administrators and one for operators? If so, you can make a request to your IT department to create two security groups: a *BluehillAdministrators* and a *BluehillOperators* group. You can then select the appropriate group for each permission. Assigning user groups to permissions must occur on each system running Bluehill Universal, unless the system is connected to Bluehill Central, in which case security settings are automatically received from the Bluehill Central's Team settings.

It should be noted that you can only choose one group per permission. This means that if you want John Smith to be an Administrator and have all permissions, he will need to be added to both the *BluehillAdministrators* and *BluehillOperators* groups in Active Directory. If you want complete customization on a user-by-user basis, you could create an Active Directory group per permission.

In addition to selecting specific Active Directory groups, there are two common groups: *All users* and *No users*. If the *All users* group is selected for a permission, this will allow all users to have this permission. If the *No users* group is selected for a permission, this permission is not allowed for any user.

Great care should be made when identifying what users should be part of each Active Directory group. You do not want to configure your security system where no one can log in or change the security settings. For example, by selecting a security group that your team is not a member of will prevent them from logging into the software.

As the lab manager, you will need to specify to your IT department what groups are needed, and which users should be part of that group. Over time, as new members join your lab and have proper training on the Instron system, you can simply ask your IT department to add those new members to your pre-determined groups.



Permissions

Login:	All users
Test specimens:	BluehillOperators
Change a tested specimen:	BluehillManagers
Delete a tested specimen:	No users
Exclude a tested specimen:	BluehillManagers
Change workspace properties:	BluehillManagers
Override sample location:	BluehillManagers
Discard the sample:	No users
Overwrite an existing sample via Save As:	BluehillManagers
Analyze samples:	BluehillManagers
Edit methods:	BluehillManagers
Configure the system:	BluehillAdministrators
Configure security:	BluehillAdministrators
Configure Traceability:	BluehillAdministrators
Group A reviewer:	BluehillManagers
Group B reviewer:	BluehillManagers
Group C reviewer:	BluehillManagers
View audit trail:	BluehillOperators

Active Directory security group configuration in Bluehill Universal (example)

For the IT Administrator - Active Directory

The lab manager will have provided you with a series of groups and users that should be added to each group. You will need to create a security group for each of the specified groups and add the specified users to each group. Bluehill will only check for security groups and not distribution groups, so it is important to create a security group.

When Bluehill Universal or Bluehill Central is started, it will connect to the domain that the computer is configured for, and first validate the user's credentials against the domain. If the user is attempting to connect to a domain that is different than the domain that the computer is configured for, the user can include the domain in the username, for example, *acme\jsmith*. If the login is successful, Bluehill will then run a query against the domain to evaluate each of the permissions by checking to see if the user is a member of each Active Directory group.

As a precaution, if the lab manager incorrectly configures the security settings within Bluehill Universal or Bluehill Central, an IT domain administrator can always log in and configure the security settings within the software, even if they are not part of the groups specified. The IT domain administrator will not have any other permissions unless he or she are members of the Active Directory groups for each permission.

Windows®

Windows security uses the local user accounts and groups provided by the Windows operating system. In the software, the security permissions are assigned to a group and any user that is included in that group has those rights. The user groups are created and managed via the Windows user accounts.

This type of security requires very little maintenance from within the software. After groups are assigned to the various permissions, any changes to the users included in a group is done via the Windows control panel, by any user included in the Administrators group. The software includes several common groups:

- *All users* - By default includes all users. There is no specific group to maintain
- *No users* - By default excludes all users. There is no specific group to maintain
- *Administrators* - Includes any user that is included in the Windows Administrators group
- *Users* - Includes any user that is included in the Windows Users group

The security feature can be enabled using just the common groups listed above. Additional groups can be created to further customize the security feature, if necessary. For example, a group can be created for each permission and then add only the users that should perform each task. It is recommended that you work with your IT department to create the user accounts and the groups that will be assigned in the software.

Permissions

The following permissions are available as specified for Bluehill Universal, Bluehill Elements, and Bluehill Central:

Permission	Description	Software Application		
		Bluehill Universal	Bluehill Elements	Bluehill Central
Log in	Allows access to the software by logging in with proper login credentials. *Bluehill security provides login permissions to all users.*	✔	✔	✔
Configure the system	An authorized user can: • change the configuration of the frame, including Operator Protection settings • edit transducer configurations • configure the TrendTracker database, if purchased • configure email and Instron® Connect • customize the default units the system uses for new methods. • connect and disconnect the testing system from Bluehill Central. *In Bluehill security, only an Administrator can access these sections of the Admin tab.*	✔	✔	×
Configure the team	Allows access to the Bluehill Central application as follows: • Settings module to edit: ○ the team name and the modules for the team ○ the security settings, including member permissions ○ TrendTracker connections ○ email notifications for the team This individual is responsible for creating user profiles and adding/removing team members as necessary. • System administration to add additional teams, remove teams from the server, edit the identification information in a user profile and remove a user profile from the server.	×	×	✔

Permission	Description	Software Application		
		Bluehill Universal	Bluehill Elements	Bluehill Central
Configure security	Allows access to the Security section of the Admin tab. An authorized user can enable or disable security, add or remove users, and change permissions. *In Bluehill security, only an Administrator can access the Security section.*	✔	✔	×
Configure Traceability*	Allows access to the Traceability > Setup screen to configure the Traceability feature and signature requirements. *In Bluehill security, only an Administrator has this permission.*	✔	×	✔
View audit trail*		✔	×	✔
Group A reviewer* Group B reviewer* Group C reviewer*	Assigns an individual to a review group, or multiple review groups, for Traceability reviews. When one of these groups is assigned to review a file, anyone included in the assigned group may complete the review.	✔	×	✔
Manage files and folders	Allows a team member to manage files on the team database in the following ways: • upload files to the team database in Bluehill Central • download files to a local device • edit the attributes for a file • move a file within the team database If a team member does not have this permission, the associated icons for the above actions do not display in the Lab Management module.	×	×	✔
Remove files and folders	Allows a team member to remove files and folders from the team database.	×	×	✔
Test specimens	Allows access to the Test tab to set up and test specimens. *In Bluehill security, all users have access to the Test tab.*	✔	✔	×
Edit methods	Allows access to the Method tab to edit parameters in a method file. *In Bluehill security, only an Administrator or Manager can access the Method tab.*	✔	✔	×
Delete a tested specimen	Allows a user to delete specimens from a sample. When a specimen is deleted, its data is erased from the test data file and it cannot be recovered. Specimens in the sample are renumbered. This may not be desirable if you need to comply with certain standards.	✔	✔	×

Permission	Description	Software Application		
		Bluehill Universal	Bluehill Elements	Bluehill Central
Change a tested specimen	Allows a user to change values for tested specimens. For example, when enabled, the user can change the dimensions shown in the Operator Inputs area after a specimen is tested and recalculate the results.	✔	✔	×
Exclude a tested specimen	Allows a user to exclude a specimen from the statistics for the sample. Excluding a specimen only removes the specimen from the statistics. The specimen can be included again if necessary.	✔	✔	×
Change workspace properties	Enables the properties icon on the Test tab components to edit the settings for the test workspace. Note that this button provides limited access to the method tab settings (e.g. graph, result columns, and web camera settings).	✔	✔	×
Override sample location	Allows a user to browse to a different folder when using “save as” to save the sample in a different folder. A user not authorized for this task can save the sample under a different name using “save as” but the user cannot browse to a different folder. If users will be prevented from changing the sample location, it is important that the method specifies a default folder. Go to Exports > File Settings on the Method tab to specify a default folder. This ensures that all samples using this method are saved to the same folder. If no default folder is specified, the sample will be saved to the folder used for the previous sample. If it is not the correct folder for the current sample, an unauthorized user cannot change the folder.	✔	✔	×
Discard the sample	Allows a user to close the Test tab without saving a sample that was not previously finished or saved. The user can either close the software or return to the home screen without saving the sample. Discarding a sample permanently deletes all changes made since the sample was last saved. These changes cannot be recovered. A user not authorized for this task must save the sample to close the Test tab.	✔	✔	×
Overwrite an existing sample via Save As	Allows a user to save the currently open sample with the Save As option and enter a previously used sample name. This option overwrites the previously saved sample. The contents from previous sample cannot be recovered. A user that does not have this permission must use the Save option to save an existing sample with the original file name. When this user selects the Save As option, the user must create a unique file name that has not been previously used, thus protecting all previously saved samples.	✔	✔	×
Analyze samples*	Allows access to the Analysis tab in the software. This tab lets a user replay an existing sample with limited parameters from a different method. When a user has access to the Analysis tab, carefully consider authorizing permission to overwrite an existing sample. If both permissions are authorized, the user can save a replayed sample and thus overwrite the original sample. If Overwrite an existing sample via Save As is not allowed, the software prompts the user for a new sample name.	✔	×	×

* *Only available if associated add-on is purchased*