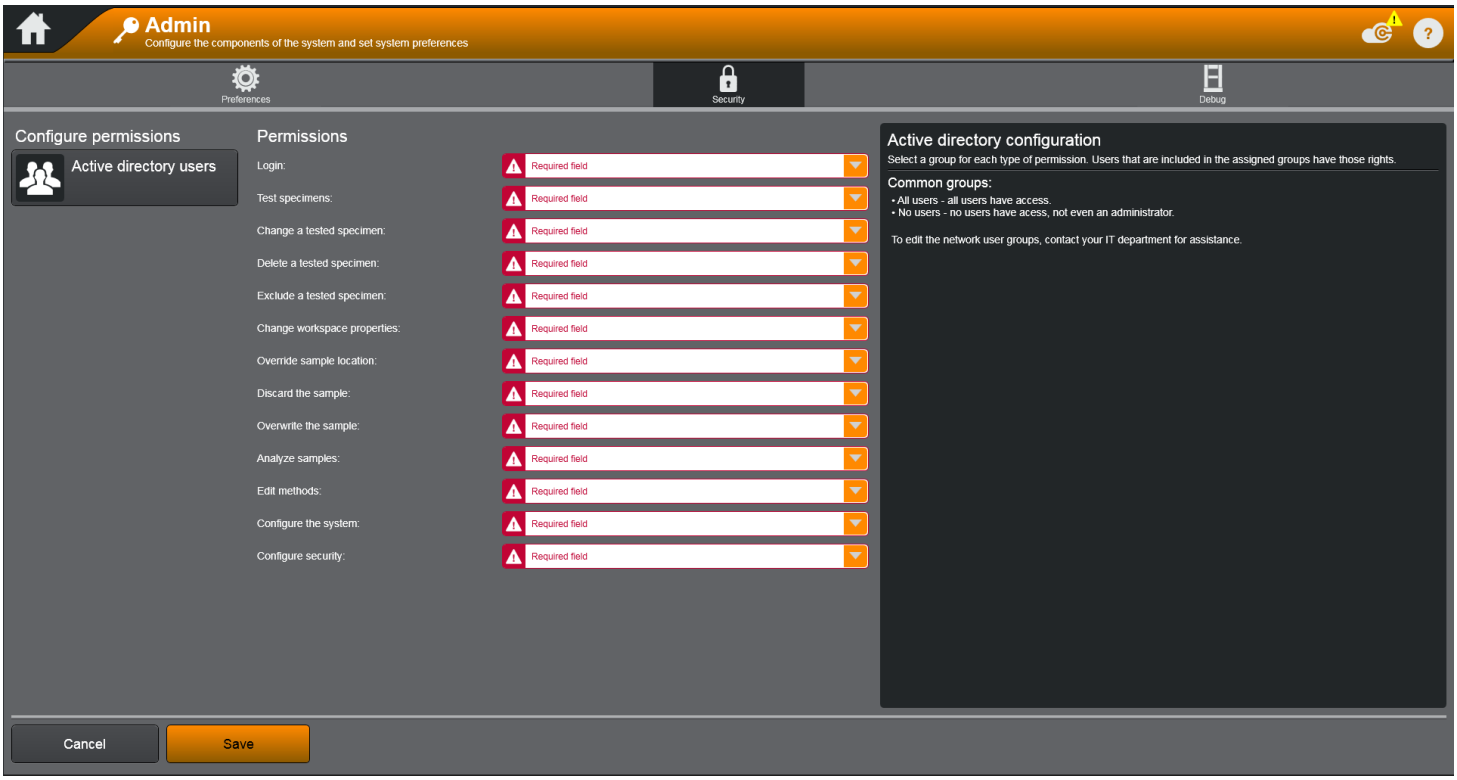
Bluehill® Universal Active Directory Security

Bluehill Universal now supports validating a user's credentials and permissions from Active Directory. This setup will require a Lab Manager to identify what user levels are required, and coordinate with their IT department to create the appropriate Active Directory groups and assign the appropriate users to each of those groups.

For the Lab Manager

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.



Permissions

With Active Directory security, Lab Managers have complete control over a variety of permissions available within Bluehill® Universal. In addition to existing permissions, several new permission fields have been added in Bluehill Universal v4.08. Permissions with an asterisk (*) were not available in versions prior to Bluehill Universal v4.08.

Login*: The ability to log in to the software.

Test specimens*: The ability to run a test.

Change a tested specimen: The ability to change values of specimen that have already been tested.

Delete a tested specimen: The ability to delete a specimen that has been tested.

Exclude a tested specimen*: The ability to exclude and include specimen that have been tested.

Change workspace properties*: The ability to change workspace component properties, for example, the graph settings.

Override sample location*: The ability to save a sample in a location other than what is specified in the method, or the last saved location.

Discard the sample*: The ability to close a sample, either by exiting the software or going to the home screen, without saving it.

Overwrite the sample*: The ability to overwrite a sample that already exists.

Analyze samples*: The ability to review or analyze a sample using the Analysis Module. This module may or may not be visible on your system as it requires a separate purchase.

Edit methods: The ability to create or edit an existing method.

Configure the system: The ability to change system settings, such as frame settings.

Configure security: The ability to change security settings.

Active Directory Groups

To identify what Active Directory groups need to be created, Lab Managers should determine what roles and permissions Bluehill® Universal operators should have. For example, do you need just one administrator and multiple users? If so, you can make a request to your IT department to create two groups: a BluehillAdministrators and a BluehillOperators group. You can then map each permission to the appropriate group, as seen below.

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 inhibits all users from having this permission.

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 'no users' for the login permission, it will result in no users being able to log in to the software and prevent everyone from using the testing machine.

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, you can simply ask your IT department to add those new members to your pre-determined groups after those new members have had proper training on the Instron® system.

For the IT Administrator

At this point, 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® Universal will only check for security groups and not distribution groups, so it is important to create a security group.

When Bluehill Universal is started and security is enabled, 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 Universal 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, 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.