

RESTRICTING CONTENT

Explanation of Security

Due to the potential of sensitive data being shared on HeelStream, there are a few things in place to minimize the chances of content being used inappropriately.

- Content is uploaded securely to our system.
- Content is encrypted when streaming.
- Users are trained prior to using this system to understand the acceptable usage policy and to be able to understand their obligations to helping keep content secure.
- Content can be restricted by ONYEN using security groups that can be setup by OIS.

This document will review the steps to applying restrictions to content and playlists using security groups. If you would like to go over this with our team in person or via an online meeting, you may contact Instructional Media Services at ims@med.unc.edu.

Requesting a Security Group

A Security Group is a list of Onyens. Security groups may be requested using our online form linked to [HERE](#). You may also visit our HeelStream website at <http://go.unc.edu/HeelStream> and scroll to the bottom of the page and click "Security Group Request" under Request Services/Support.

You may request as many security groups as necessary to allocate the appropriate security. You may use the form to request to add users to existing groups setup through the form. To have users removed from these groups, you may e-mail ims@med.unc.edu.

If you are already aware of a security group that exists in the university Active Directory system that contains and excludes the appropriate persons, you may choose to use that group, but you may need to contact IMS so that we can allow your department's groups to function on the system.

Applying Security to Content

1. Go to your **Media Library**.
2. Click **Publish** for the content you want to restrict.



3. Click the **Security** header, and you will have a few options which are detailed later in this document.



Applying Security to a Playlist

1. Click the **Playlists** button.



2. Click the **Access Control** button for the playlist you want to restrict.



3. Click Add.



You will see the same options described in the previous section.

Restrict with a Login Form (Security Group/Onyen)

This option will require people to login with an Onyen and Password. This is currently the **ONLY** security option that we allow you to use for sensitive data.

1. Select this option, and you will get a dropdown to select an **Identity Provider**. Select **AD** and click **Save**.

2. At this point, your content/playlist is restricted to require Onyen login. For further security, you can apply a security group. Click **Edit** for the AD entry in the security list.

Restriction	Type	OR	Status		
AD	Restrict with a Login Form	<input type="checkbox"/>	✔ Enabled		

3. Click the **Enter Group** option and enter the name of the security group, and click Save. You can also use the Select Group option to find a group, however this lists ALL groups in the system.

RESTRICTING CONTENT

Restrict to a Domain/IP Address

This option allows you to restrict access to your media to a certain IP Address or range of addresses. The best use case for this would be only allowing people in a certain location to view your content, or allowing it to be viewed from a specific computer.

When you click the option, you will be able to enter an IP Address or range of IP addresses. You may need to contact IT Support for the location that needs to view the content to use this. A list of UNC IP Subnet ranges is available at <https://help.unc.edu/help/what-subnets-are-used-on-campus/>.

* Domain Name or IP Address: 123.45.67.89

For Example:
demo.ensembleVideo.com or ensembleVideo.com
IP Address: 192.168.0.1 or 192.168.0.1/24

Save Cancel

Restrict to a Web Address

This option allows you to restrict access to your media such that it can only be played when embedded in a certain webpage. This only restricts at the domain level-- this means that if you are restricting access through Sakai, you would have to use "sakai.unc.edu" as opposed to the whole URL. This also means that the media would be accessible on any page within Sakai that it is embedded on.

When you click the option, you will be able to enter the domain for the website that you're restricting access to.

* Web Address: sakai.unc.edu

For Example:
www.ensembleVideo.com or lms.institution.edu

Save Cancel

Restrict to Specific User(s)

This is not currently supported as we do not manage user accounts for end-users outside of security groups.

Restrict with a Password

This option allows you to set a password that will need to be entered to view your media. While this is a very simple security option for keeping videos restricted to certain audiences that you share the password with, it is **not** allowed to be used for sensitive data.

Notes

- When anyone tries to access a playlist or content with security they will receive a login screen. If they are not a part of the security group entered, change they will not be allowed to view it.
- Note that content that is part of a secure playlist can not be shared directly or embedded any longer.