



**BrightSign®**

WEB UI

# PERMISSIONS

BrightSign Network Version 2.5

# TABLE OF CONTENTS

<b>Introduction</b>	1	Overview	11
Permissions Overview	2	Editing Object Permissions	11
<b>Beginner</b>	4	Using Object Permissions	12
Overview	4		
Assigning Roles	4		
Using Default Roles	5		
<b>Intermediate</b>	8		
Overview	8		
Creating Custom Roles	8		
Using Custom Roles	9		
<b>Expert</b>	11		



# INTRODUCTION

The BrightSign Network offers a robust set of security and permissions features that allow you to protect your content and maintain the efficiency of your digital-signage system—no matter how large it gets. These security features are scalable: you can choose exactly how complex you want your permissions system to be, depending on the needs of your organization.

This document will walk you through the BrightSign Network permissions system using the scenario of a hypothetical chain of donut shops. As the company expands and more locations are added, you will be gradually introduced to the more complex, more powerful permissions features offered by BrightSign.

Here is a quick overview of what will be covered in each chapter:

## **Beginner**

You will learn how to use *default roles* to maintain an up-to-date digital menu board and announcement system for a chain of five donut shops using BrightSign networked players.

## **Intermediate**

You will learn how to create and edit *custom roles* for a digital-signage system of 25 shops spread out over a large geographical area.

## **Advanced**

You will learn how to create and edit *object permissions* in conjunction with *custom roles* for a national chain of 100 shops with diverse content and pricing needs.

## Permissions Overview

You can view the permissions of a user or group at any time while logged into the BrightSign network.

1. Click the **Account** button at the top right of the page.
2. Navigate to the **Users and Roles** subgroup on the right of the page.
3. Click on the **properties** underneath either the desired role or desired user.

## Users and Roles

The screenshot shows the 'Users and Roles' interface. On the left, under the heading 'Roles', there is a list of system roles: Administrators, Creators, General Managers, Network Managers, Publishers, and Viewers. Each role has a 'properties' link below it. On the right, under the heading 'Assigned Users', there is a list of users. The first user is 'Administrator', and its 'properties' link is highlighted in yellow.

The screenshot shows the 'Role "Administrators" Properties' dialog box. The 'Permissions' tab is selected. The title of the dialog is 'Role "Administrators" Properties'. The main content area is titled 'Permissions for role 'Administrators''. It contains a list of permissions, each with a checkmark and a 'Full Control' label: User (Full Control), Role (Full Control), Content (Full Control), Dynamic Playlist (Full Control), Presentation (Full Control), Schedule (Full Control), Group (Full Control), Device (Full Control), Subscription (Full Control), and LiveText Feed (Full Control). At the bottom left, there is a checkbox labeled 'Show Denied Permissions' which is currently unchecked. At the bottom right, there is a 'Close' button.

The **Permissions** tab displays whether the user or group is permitted to carry out a certain action. Every possible user action in the BrightSign network is listed here, divided by category.

**Note:** A checkmark by a category indicates that the user or group has *complete* access to all options in that category. An “X” by a category does not necessarily mean that all actions in the category are restricted. Click on the + symbol to expand a category and view the permissions for every possible action within it.

The permissions categories can be understood in terms of the different functions of the BrightSign Network:

- **Content:** Content, Presentation, Live Text Feed  
These categories correspond to the process of creating and updating BrightSign presentations.
- **Scheduling:** Dynamic Playlist, Presentation, Schedule  
These categories allow a user to schedule presentations for certain times and dates, as well as coordinate the content of different presentations using Dynamic Playlists (view the [BrightAuthor User Guide](#) for more information on the uses of Dynamic Playlists).
- **Infrastructure:** Group, Device  
These categories contain the capabilities to monitor, maintain, and coordinate all BrightSign players that are connected to the BrightSign Network.
- **Administration:** User, Role, Subscription  
These categories correspond to customizing and maintaining your BrightSign Network account, including the ability to assign permissions and create new user accounts.

# BEGINNER

This chapter will introduce you to common applications of various default roles. Default roles are great for BrightSign Network accounts with a small amount of users who have clearly defined roles and responsibilities within the organization.

**Note:** The default roles for the BrightSign Network correspond to the user permissions system in BrightAuthor.

## Overview

You are the systems administrator for a small chain of five donut shops located around the city. The chain has just replaced all of their chalkboards used for menus, special offers, and announcements with digital displays powered by BrightSign players, which are linked to the company's BrightSign Network account. There are many employees who need to use the network in order to keep the store menus and special offers up-to-date. You are faced with several personnel and security challenges when configuring the network, all of which can be solved using the default roles provided with every BrightSign Network account.

## Assigning Roles

**Note:** You can assign a user to only one role at a time.

1. Click the **Account** button at the top right of the page.
2. Navigate to the **Users and Roles** subgroup on the right-hand side of the page.
3. Click the role to which you wish to add the user.
4. Drag and drop the user's name/email from the **User List** into the gray field under **Assigned Users**.

## Users and Roles

### Using Default Roles

#### Administrators

In order to keep everything running smoothly, you want to make sure that, as the systems administrator for the account, you are the only one who can add or delete users. If other users have full permissions, they might accidentally delete a user, add a user who is not a member of the company, or change permissions for an individual or group.

Being assigned to the **Administrators** role gives you access to all the features offered on the BrightSign Network. This is the only role that allows you to edit the account status of other users: as a member of **Administrators**, you can add new users, delete existing users, and assign users to different roles; furthermore, you can create and edit custom roles, a feature that will be explained in the [Intermediate](#) section of this document.

**Note:** The user who creates the BrightSign Network account will automatically be assigned to the **Administrators** role. If you did not create the account, you will need to have the user who did assign you to the **Administrators** role.

### Creators

The company employs a graphic designer to create the digital menus for the company. She is also frequently updating the content and layout of the menus, so she will be logging into the company's BrightSign Network account often. She doesn't know which menu will be displayed where, nor is she in charge of deciding how the devices and groups should be organized. You don't want her to accidentally delete a group or reassign a device while she is uploading content.

The **Creators** role will give the graphic designer complete control of content, including presentations, dynamic playlists, and Live Text feeds. She will not have the ability to view or change schedules, groups, or devices. This role is best suited for those tasked solely with creating content for BrightSign players.

### General Managers

The co-owners of the company want to log in to the network whenever they wish to check that pricing and product information is correct. They also want the ability to change, reassign, or reschedule presentations at any location.

Assigning the co-owners to the **General Managers** role gives them full control of content creation and distribution. The only permissions they won't have are the user and account features that are unique to **Administrators**.



## Network Managers

Another systems administrator is assigned to maintaining all of the BrightSign players, as well as purchasing and setting up additional players when a new store location is opened. He is also tasked with periodically clearing the network of old presentations and drafts.

The **Network Managers** role gives him control of the company's digital-signage infrastructure: a user assigned to this role can add, remove, maintain, and group together networked BrightSign players. In addition, he can view and delete (but not add or edit) certain kinds of content such as Dynamic Playlists, Live Text feeds, and presentations.

## Publishers

Members of the marketing department determine when promotions and deals will be announced, as well as what day of the week certain specials will be offered.

Being assigned to the **Publishers** role, the marketing department can schedule when and where BrightSign presentations will be played. They also have the ability to upload content in case a new presentation needs to be scheduled quickly. Otherwise, they do not have access to content that is uploaded to the company's BrightSign Network account.

## Viewers

There are other members of the company who are not directly involved with the digital signage system, but who may need to view presentations, schedules, playlists, or logs as part of their job.

Users who are assigned to the **Viewers** role can view almost all aspects of a digital-signage system: content, groups, hardware status, and schedules. However, they cannot affect anything on the company's BrightSign network account.

# INTERMEDIATE

This chapter will explain how to create and edit custom roles. The roles introduced here are used as examples to help explain how to conceptualize and create a custom role. The needs of your organization may be different from the examples included in this section.

**Note:** In order to create a custom role, you will first need to check the **Show Advanced Security Settings** and **Enable Custom Roles Management** checkboxes located in the **Advanced** section of the **Account** page.

## Overview

Your company now has 25 donut shops in multiple states, and the central office has many more employees. Though the BrightSign Network’s default roles have worked well up until this point, they are no longer able to serve a large group of users with many diverse roles and responsibilities.

## Creating Custom Roles

Since there are nearly 70 individual permissions, it may be easiest to base a custom role on one of the preexisting default roles.

**Note:** Default roles cannot be modified.

1. Click the **Account** button at the top right of the page.
2. Navigate to the **Permissions** subgroup on the right-hand side of the page.
3. Click the **Create New Roles** button beside the **Roles List**.
4. Enter a name and (optional) description for the custom role.
5. Check the **Copy Permissions From** checkbox to base the custom role’s permissions on a preexisting role. As long as you have the advanced

**Create Role** [X]

Name:

Description:

Copy Permissions From:

- Administrators
- Creators
- General Managers**
- Network Managers
- Publishers
- Viewers
- Role1

**Create** **Close**

settings enabled on the **Account** page, you will be able to change all copied permissions.

**Note:** If you do not copy permissions, you will need to set up permissions manually by dragging and dropping the role name into each **Operations** category. When you do this, the permissions will be automatically set to “Allow.” If you don’t add the role to an **Operations** category, the permissions for that category remain set to “Deny” by default.

## Using Custom Roles

### Accountants

The accountant in charge of accounts payable needs to keep track of the invoices that are automatically generated by the BrightSign network. He is not involved in the digital signage network in any other way.

In this case, it would be best to create a custom role without copying permissions from a default role. As stated above, all permissions are set to “Deny” by default if you choose not to copy permissions from another role. Therefore, all you need to do is create a new role and leave the **Copy Permissions From** box unchecked. You can then drag the new custom role into the **Subscription** category.

### Presentation Creators/Live Text Creators

The responsibility for creating and editing menu boards is now split between two employees. The graphic designer is still in charge of uploading new editions of the menu boards, but the Live Text feeds used for special deals are maintained by an employee from the marketing department. The graphic designer integrates Live Text zones into the menus, but does not update the Live Text herself. The **Creators** default role no longer reflects how their responsibilities are divided.

The easiest way to deal with slight variations in default roles is to use the **Copy Permissions From** feature when creating custom roles. In this case, you can create both a **Presentation Creators** and a **Live Text Creators** role based on the default **Creators** role. To create **Presentation Creators**, copy permissions from the default role and deny full control to Live Text Feeds. To create **Live Text Creators**, copy permissions from the default role and deny full control to **Content**, **Dynamic Playlist**, and **Presentation**.

## Senior Network Managers

You need to expand the role of the **Network Manager** so that he can add and edit schedules in addition to maintaining the network of BrightSign players. He is not involved with the daily activity of menu revisions and updates, so you don't want him to have control of adding or removing the presentations on a schedule.

You will need to modify the default permissions of the **Network Manager** in a more minute way than allowing or denying "full control" of a category. On the permissions page, click the arrow symbols next to the Schedule and Group operations categories to expand the list of permissions. These expanded menus enable you to allow or deny specific actions within an operations category. Enable "Add Presentation" and "Remove Presentation" in the Schedule category, and enable "Change Schedule" in the Group category. You have now expanded the permissions of your **Network Manager** without having to enable full control of an operations category.

# EXPERT

This chapter will explain how to use object permissions in conjunction with custom roles to meet the organizational needs of a large digital signage network. Currently, object permissions can only be set for Dynamic Playlists and Live Text feeds. Object permissions for presentations, groups, devices, and other features will become available on the BrightSign Network at a later date.

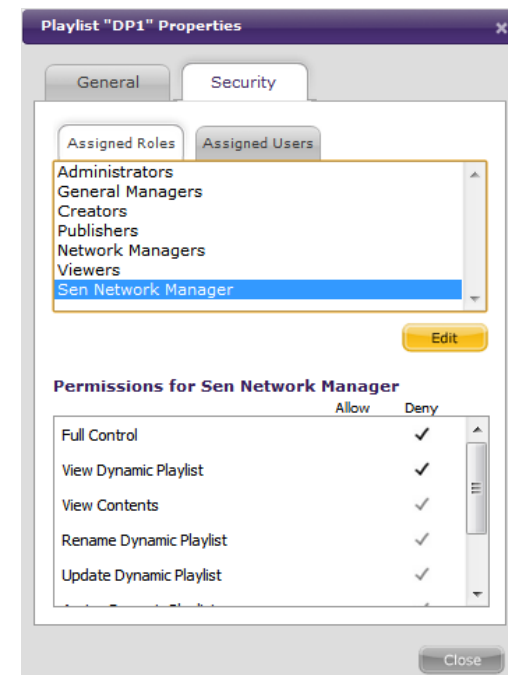
## Overview

Your company has now expanded to over 100 donut shops across the country. Menu pricing and offerings vary widely depending on region and availability: new donut recipes are introduced to certain test markets; different regions have different pricing depending on material costs; and certain stores offer regional favorites that are not offered elsewhere. Custom roles are no longer enough to keep the network functional for the employees who use it. You need to limit or allow access according to the objects (presentations, dynamic playlists, etc.) themselves.

## Editing Object Permissions

The permissions for any object are accessed through the **properties** button, which is usually located below the name of the object.

1. Click on the **Security** tab in the **Properties** window.
2. Assign permissions for the object by role or by individual user.
  - a. In the **Assigned Roles** subgroup, click the **Add** button and select the desired role. Remember that you can only edit permissions for custom roles.
  - b. In the **Assigned Users** subgroup, click the **Add** button and select the desired user.



3. You can now choose whether to “Allow” or “Deny” certain actions for a specific Dynamic Playlist, Live Text feed, etc.

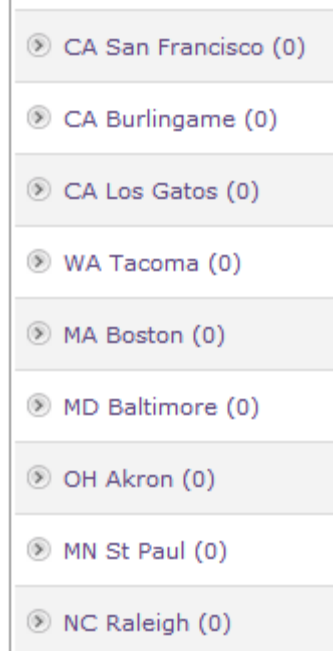
**Note:** Permissions settings for objects overrule permissions settings for roles. For example, if the **Presentation Creators** are restricted from creating Live Text feeds, but full control for the role is enabled for a certain Live Text feed, then the allowance for that specific object takes precedence over the general restriction for the **Presentation Creators** role.

## Using Object Permissions

### Store Managers

The company wants to give individual store managers some leeway in deciding which deals they want to promote—after all, they have the best idea what donuts are most popular in their neighborhood. Store managers need the ability to view various presentations and schedule them for the BrightSign players located in their store. However, assigning them a custom role based on **Publishers** does not completely solve this problem: they have access to the presentation schedules of every store in the nation, not just their own, and they might accidentally delete or modify them.

1. Create a custom role based on **Publishers**
2. Assign all of the store managers to this role.
3. Change the role so that the actions “View Groups” and “Change Schedule” in the Group category are denied.
4. Make sure that each group of players reflects a different store location.  
**Note:** You can also assign object permissions based on individual BrightSign players. This is helpful if you already organize groups in some other way (by region, by store type, etc.).
5. Change the object permissions of each group on the network so that each user assigned to the custom **Publishers** role can only view and schedule the group that corresponds to the store that he or she manages.



You have now created a system of object permissions that allows store managers to schedule menus and special offers only at their own store locations. You can customize this system even more: for example, if you want certain store managers to have access to certain menus or promotions depending on region or store type, you can use the object permissions for presentations to deny or allow access as you see fit.

## Prototypes

The marketing department wants to upload an announcement for a new flavor of donut in order to test how it will look on a digital display. However, the board of directors is worried that the competition will get wind of this new flavor before it is rolled out across the nation. To minimize the risk of a leak, you want to make sure that, for the moment, only the employees directly involved with testing the announcement have the ability to view, edit, or schedule the presentation.

**Note:** In order for this scenario to work, most or all users need to be assigned to *custom roles*. Just like operations permissions, the object permissions for default roles cannot be edited.

You can limit access to this presentation either by role or by individual user. You can also allow access to a user who is working on this project but who doesn't normally have access to presentations.

Keep in mind that there are other factors beside object permissions that can limit access to a presentation or other object. For example, you can give a user full permissions for a Dynamic Playlist object, but that user will not be able to drag and drop content into the playlist if the role restricts the "Assign Content" action in the Content permissions category.

