IVS – Users and access roles

Table of Contents

1. Introduction, important information

This guide summarizes the details of IVS users and their permission settings. For a complete overview of the system architecture and configuration, please refer to the ***IVS Installation Manual*** documentation.

2. Users / Roles

The system uses a global authentication system that allows users to have permissions not only within local Sites but across the entire Domain.

Each user has a unique username and password. Every user is assigned a role, which defines their detailed permissions. A user can only have one role at a time, but multiple users can share the same role (for example, each operator has a separate username but all have the operator role).

These settings can be accessed in the **System Configuration / Security** menu.

By default, IVS includes 2 roles and 2 users (administrator, operator). The number of available roles and users depends on the IVS version (Soho: 2-2, Corporate: 6-6, Enterprise: unlimited).

Additionally, the permissions of RTSP users can also be configured here, with detailed usage described in the ***RTSP Gateway module*** documentation.

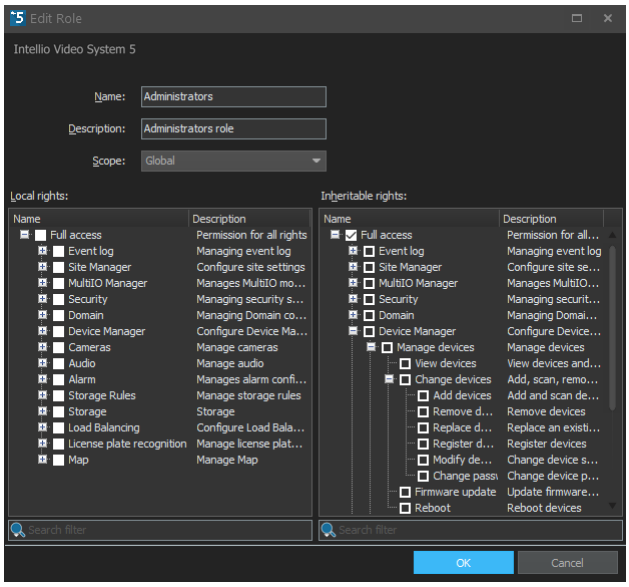
2.1. Roles

Roles define user permissions within the system. Roles act as permission groups, granting the same rights to all users assigned to the same role. This allows for a flexible system setup where changes can be made easily when needed.

2.1.1. Create roles

The system allows the creation of both Global and Local roles as needed. **Local roles** exist only on the specific Site where they are created and grant permissions only within that Site. **Global roles** appear on the Site where they are created and are also inherited downward within the Domain hierarchy, granting permissions to users with the role across multiple Sites

Roles can have both local and inheritable permissions. A **local permission** (regardless of role type) only applies to the Site where the role is being modified. **Inheritable permissions** grant access to the given Site and to all Sites located below it in the Domain hierarchy.



This system allows easy configuration—for example, a user can have administrator rights on their own Site, while having only operator rights on other Sites within the same Domain.

The inheritable permissions of a Global role can only be modified on the Site where the role was originally created.

On Sites where a Global role appears as an inherited role, the inherited permissions cannot be restricted but can be extended with additional local permissions.

To create a role/user that is accessible across all Sites within a Domain, it must be created at the top-level Domain.

Local permissions must always be configured separately for each Site.

2.1.2. Delete roles

When deleting a role, make sure that all users assigned to that role are reassigned to a different role. The system will not allow the role to be deleted until this condition is met.

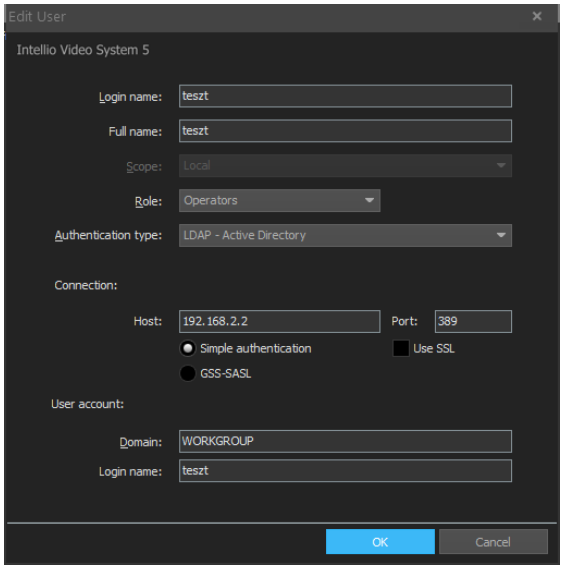
2.2. Users

Each user has a unique **Login Name**, **User Name**, and **Password**. The login name and password are required for logging in, while the user name is the displayed name of the user. The user name and login name can be the same.

The user's access is determined by the assigned role. Make sure there is always at least one user who can modify roles and users; otherwise, some functions may become unavailable. By default, this user is the **Administrator**.

2.2.1. Create Users

When creating a new user, you must enter the **login name** and **user name**, set whether the user is **Local** or **Global**, choose a **role**, and set the **password**.



Since each user must be assigned a role, make sure the appropriate role is already available.

A **local** user exists only on the specific Site and cannot be accessed or used to log in from other Sites in the Domain. A **global** user allows access to multiple Sites within the Domain without the need to create separate profiles for each Site. A global user profile will be available on the Site where it was created and on Sites located deeper in the Domain hierarchy. Only a global role can be assigned to a global user.

2.2.2. Authentication type

The default authentication method is **IVS – Intellio Video System**, where user authentication is handled by the IVS system itself.

When **LDAP authentication** is selected, the authentication is performed by the computer's domain controller, checking against the appropriate Windows user account. It is important that during authentication, only the password is verified, the user permissions are stored in the IVS. LDAP authentication works only with local user profiles.

Note: *LDAP authentication is available only in the IVS-Enterprise version.*

2.2.3. Edit User details

All user data can be modified except for the login name. If you want to change the login name, you must create a new user.

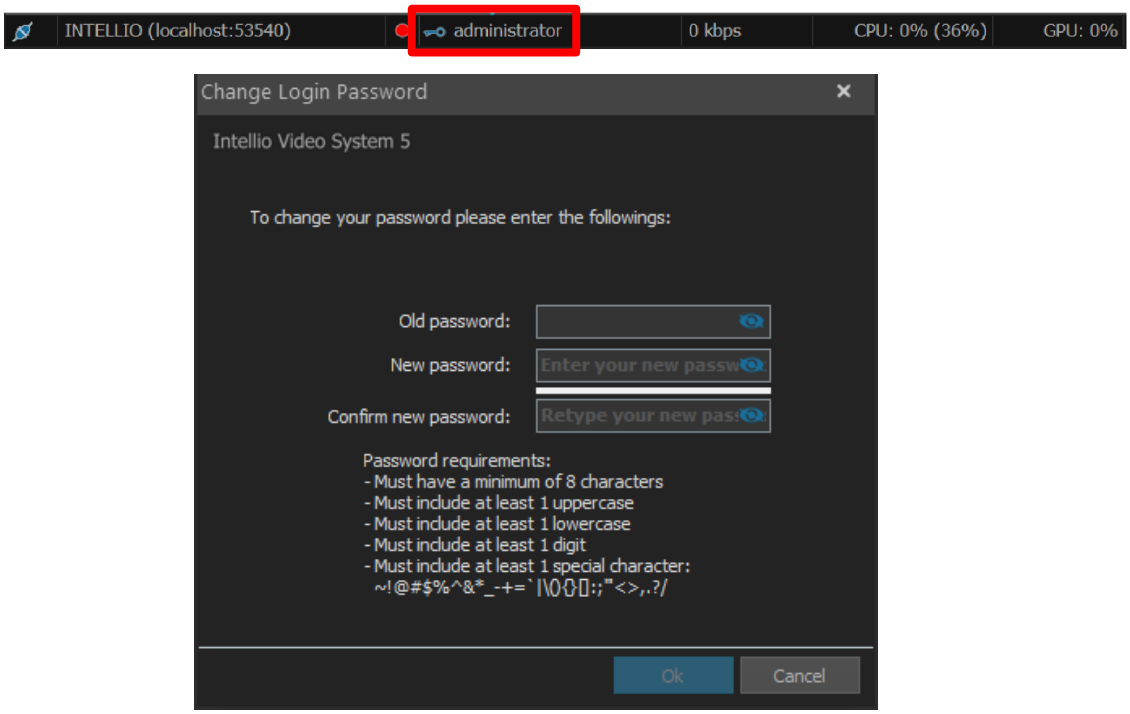
Important: *Don't forget to change the default passwords!*

2.2.4. Change your password

In the bottom status bar of the Client program, there is a key icon next to the logged-in user's name. By clicking the key, the user has the option to change their own password.

The new password must be at least 8 characters long and must contain at least 1 lowercase letter, 1 uppercase letter, 1 number, and 1 special character. The yellow color between the password input fields indicates that the basic requirements have been met, meaning the entered password is already accepted as sufficiently complex. The color turns green if the password meets more extensive requirements than the basic ones.

For newly entered passwords, the typed password can be displayed in the password input fields by clicking the icon that appears at the end of the input field.



3. Further steps

For an overview of additional system settings, please refer to the ***IVS Installation Manual*** documentation.