MICAS SM

# AGENT

## SECURITY CONFIGURATION

## V.4.0.1

# Security Configuration

Create roles and users to control access to features of the MICAS Agent based on a local or Windows Active Directory environment

# Overview -Version 4.0.1 Authentication and Authorization (Users and Roles).

- Up to version 3.5.9

  no authentication

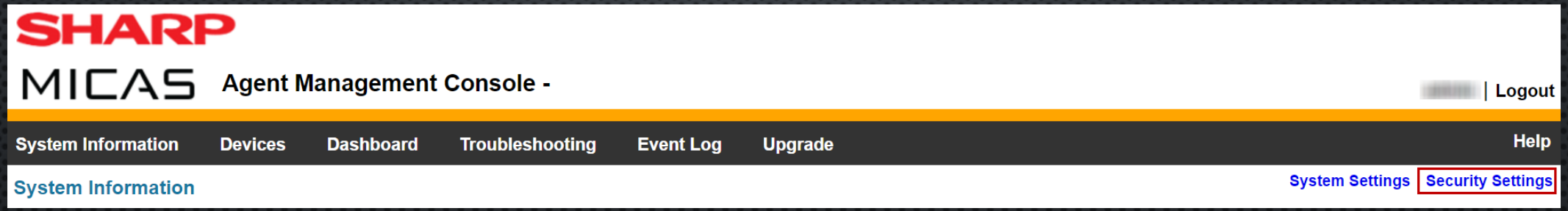
  any user could access any page within the Agent

- Access to pages (and edit function within pages) can be controlled per-role, and users can be assigned to a role to control their access rights.

- The Authorization function can be enabled (or disabled) in the "Security Settings" page, which can be accessed by clicking the "Security Settings" link in the system information page

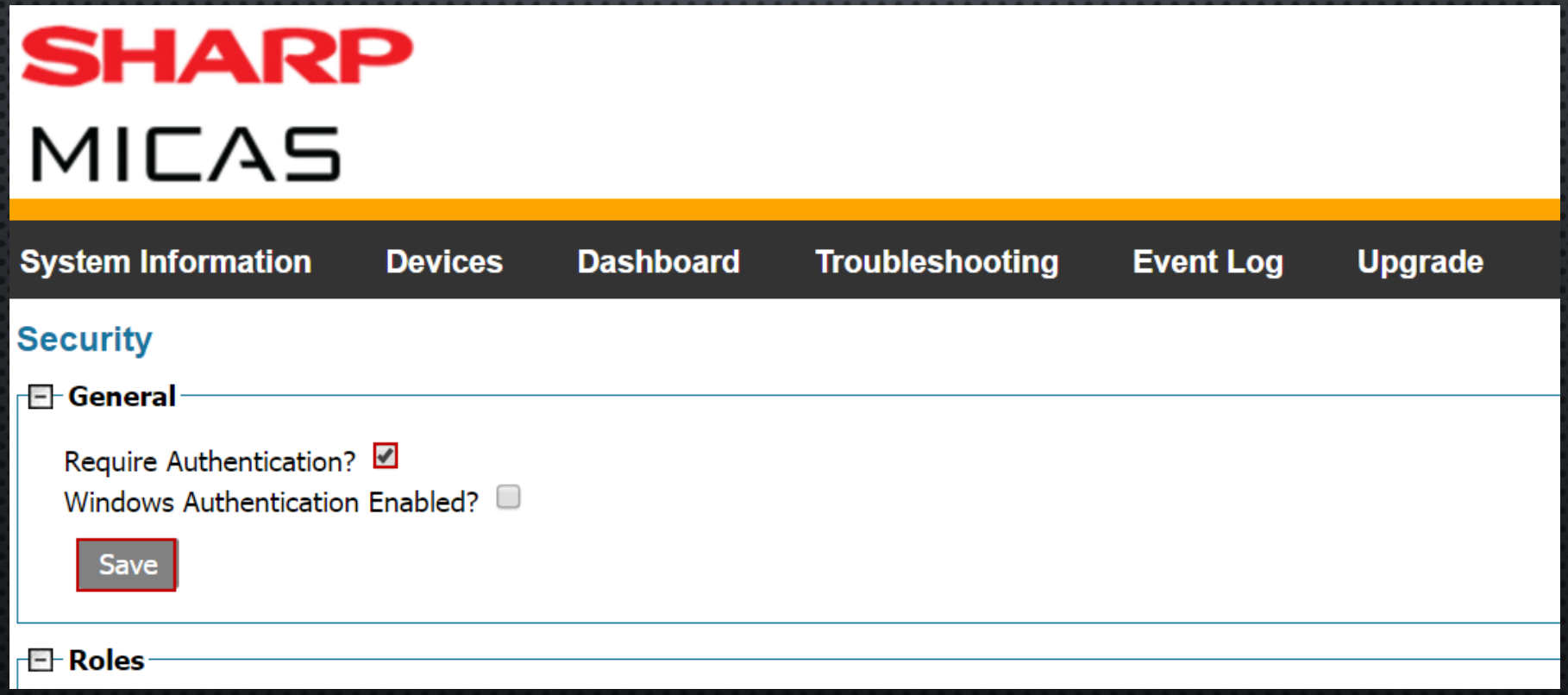
# SETUP AND CONFIGURATION

1. To enable authentication, use the Security Settings link in the top-right of the System Information page to navigate to the Security Settings page.



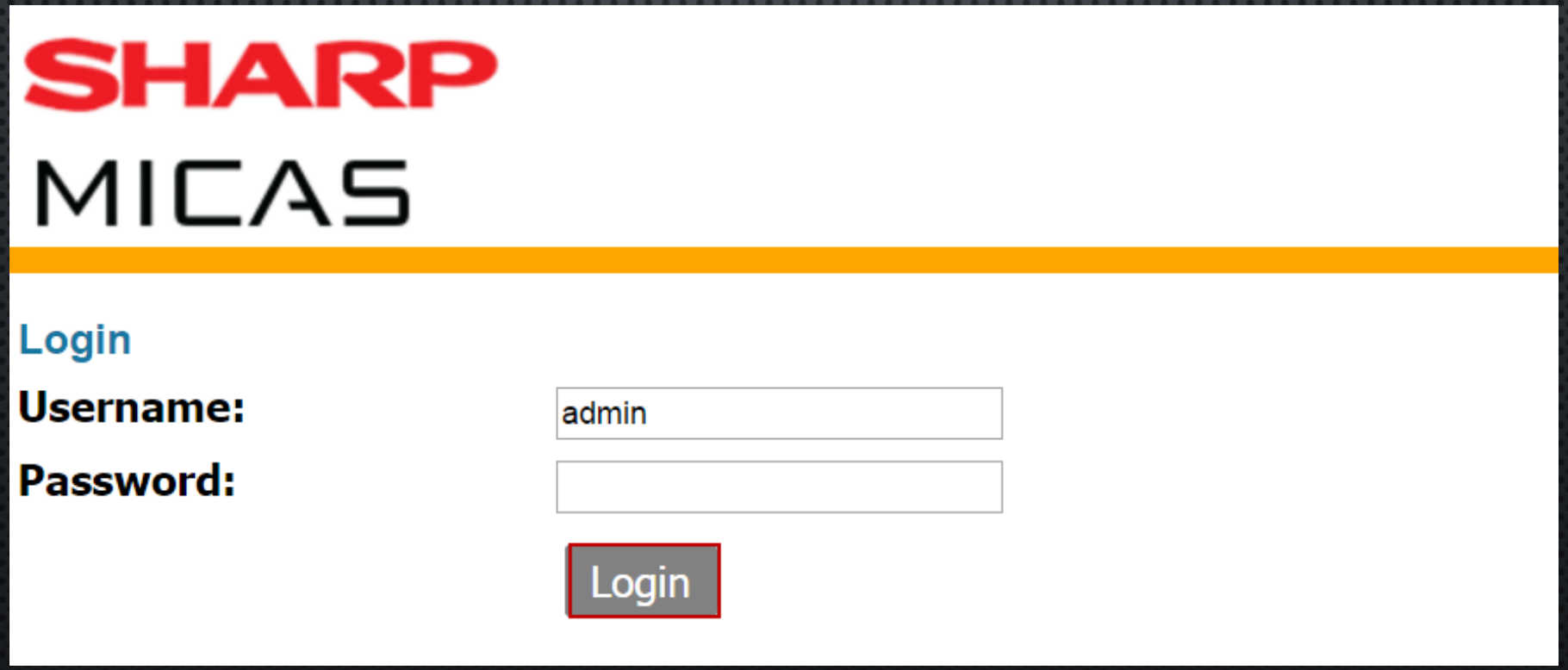
# SETUP AND CONFIGURATION

2. SELECT REQUIRE AUTHENTICATION? AND CLICK SAVE TO ENABLE AUTHENTICATION.



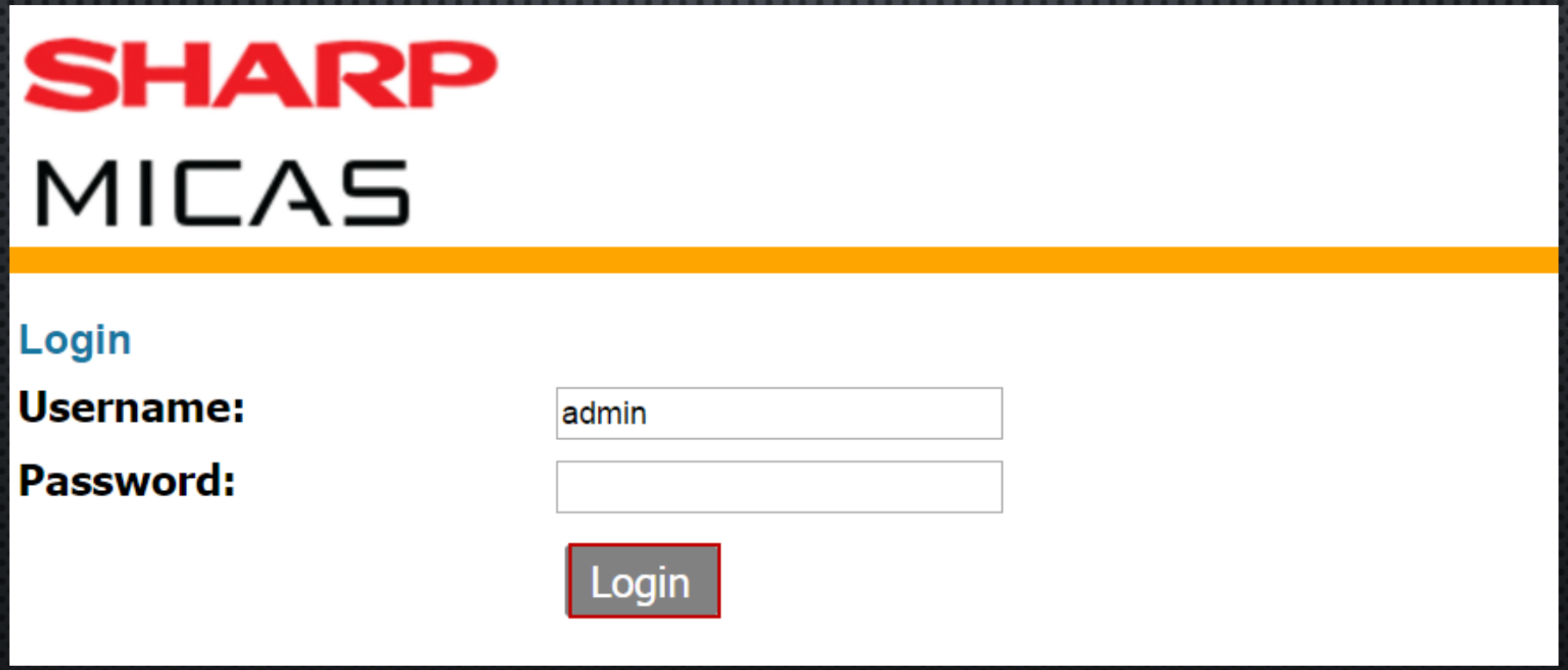
# SETUP AND CONFIGURATION

3. On the post-authentication log in page, enter administrator username “admin" and leave password blank. Click Login.



# SETUP AND CONFIGURATION

4. On the post-authentication log in page, enter administrator username "admin" and leave password blank. Click Login.



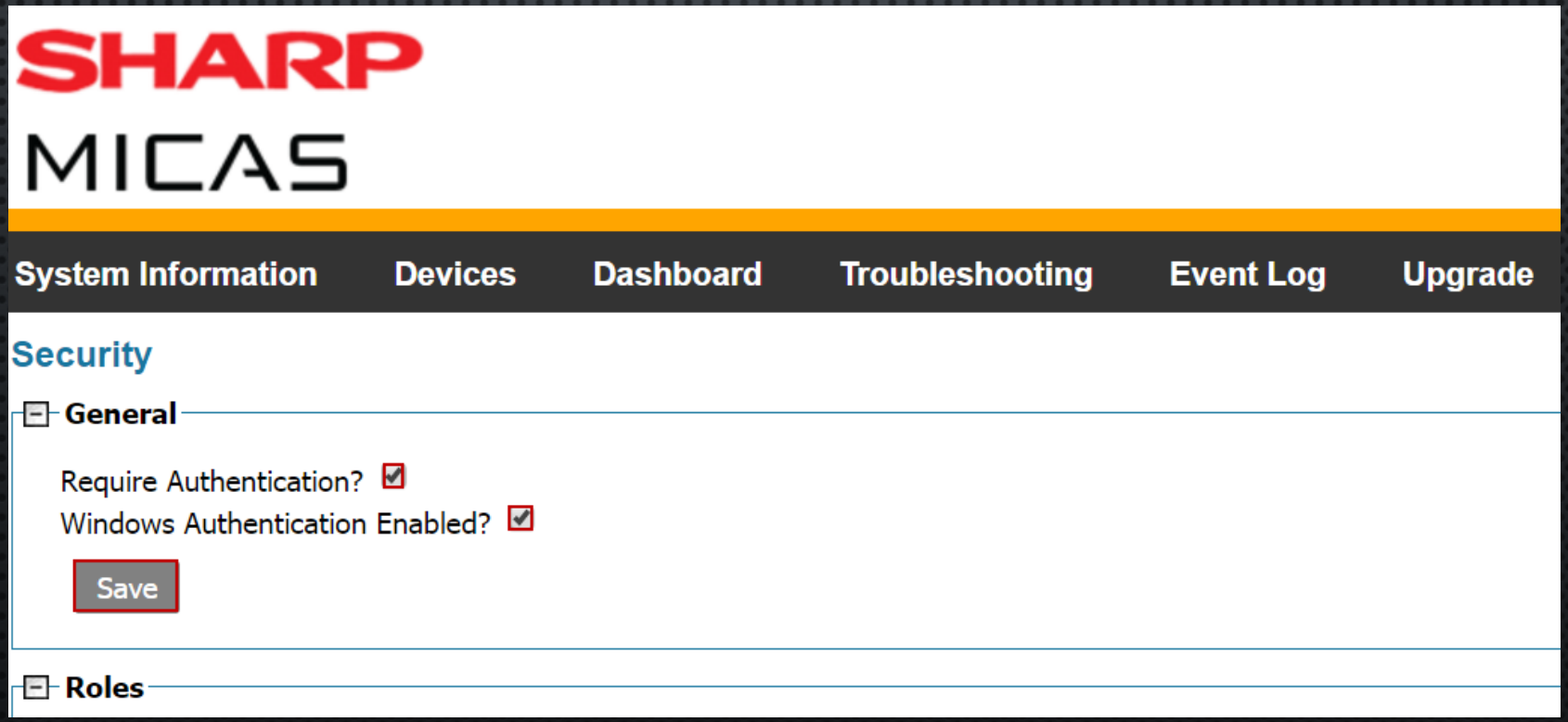
# Windows Authentication

**Important:** Prior to enabling Windows Authentication in the Security Settings page, an Active Directory Group (**AD group**) called "**MICAS Agent Administrators**" must be created on the location's network Active Directory.

Any user within this AD group that logs into the MICAS Agent for the first time using the Windows Login will automatically be assigned the MICAS Agent Administrators role

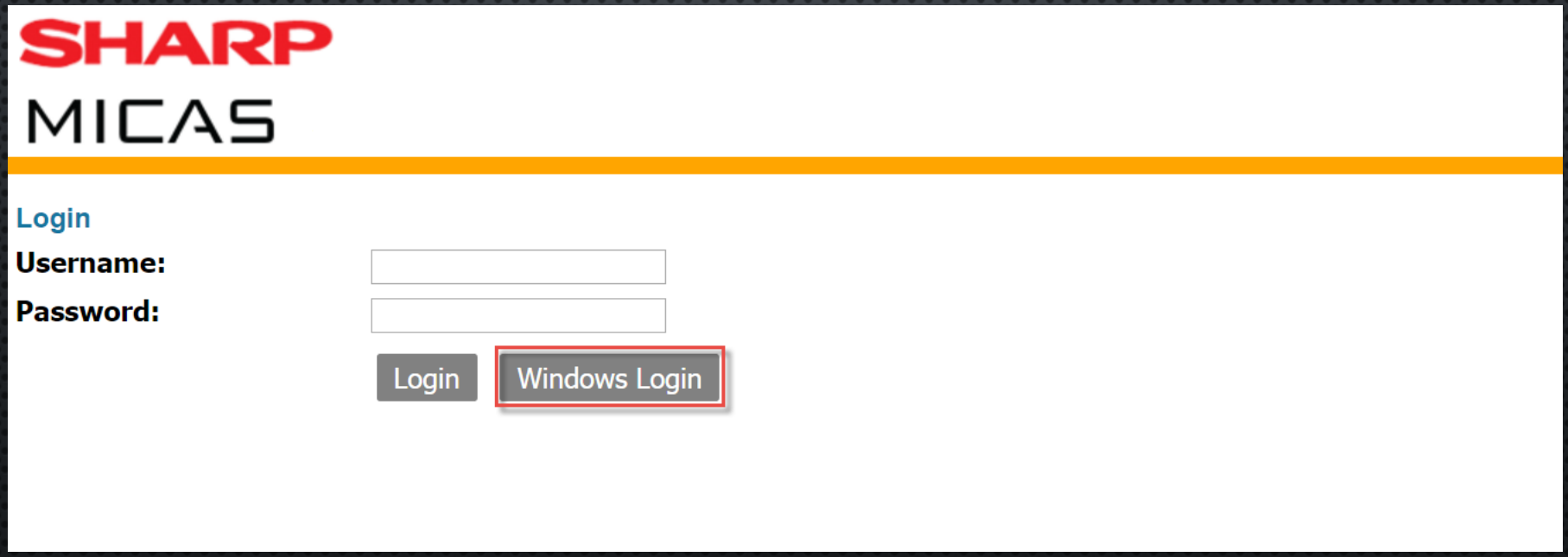
# WINDOWS AUTHENTICATION

1. To enable Windows Authentication, use the Windows Authentication Enabled? in the General panel on the Security Settings page. Click Save to enable a Windows Login button on the login page.



# WINDOWS AUTHENTICATION

2. ENTER YOUR WINDOWS AUTHENTICATION (MICAS ADMINSTRATORS GROUP) CREDENTIALS AND CLICK WINDOWS LOGIN.



# Windows Authentication

3. When you log in using Windows Authentication:

- A user account will be automatically created in the MICAS Agent Database.
- If you are a member of the "MICAS Agent Administrators" role in Active Directory, the user account will be automatically assigned to the MICAS Agent "Administrators" role, with access to all functions.
- If you are not a member of the "MICAS Agent Administrators" role the automatically-created account is not assigned to any role, and your account is not able to access any protected functionality.

# Default Roles and Users

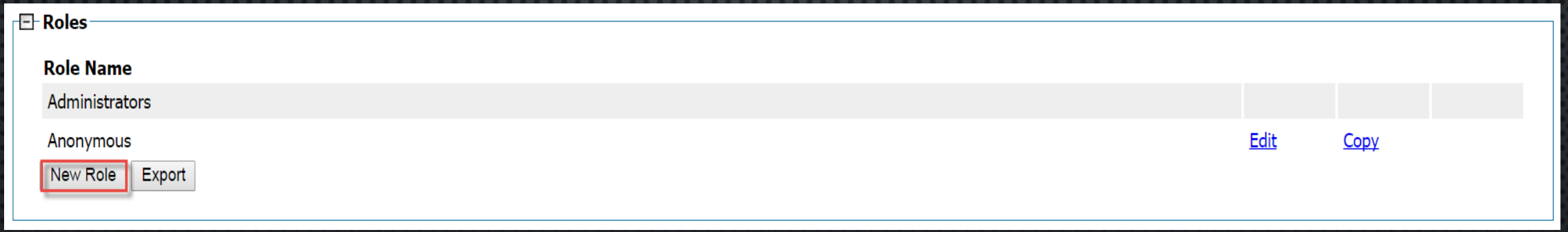
By default, the Agent database contains two roles and two users:

- Administrators - Members of the Administrators role have access to all functions
- Anonymous - The Anonymous role is used to control access rights (Authorization) for users who are not logged in.

The admin user has a blank password. The anonymous user represents users who are not logged in (and is not editable).

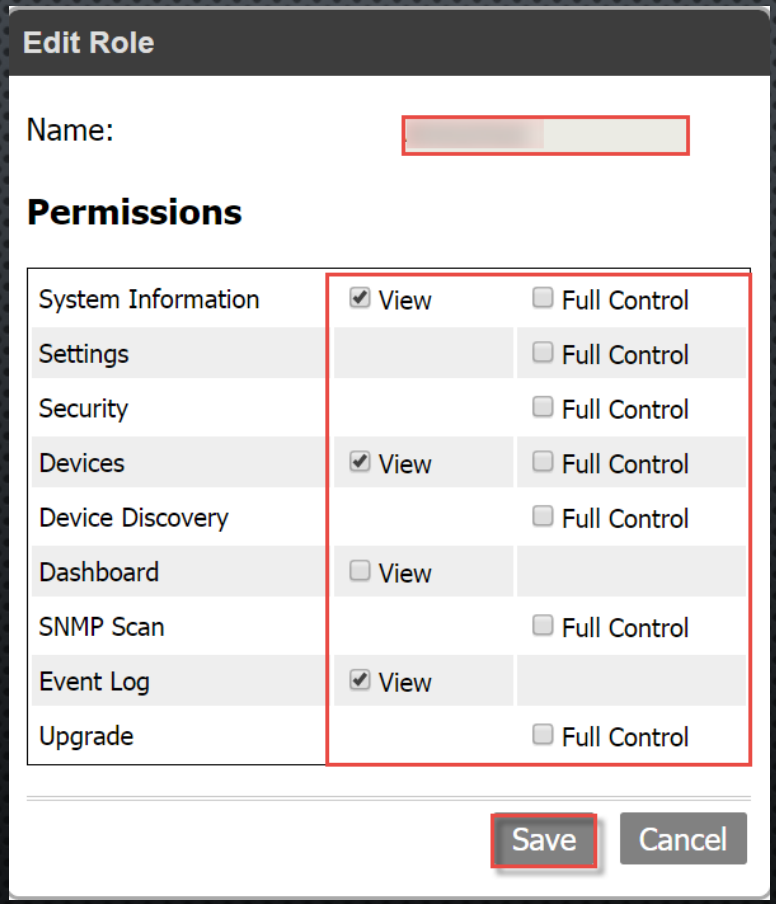
# CONFIGURING ROLES

1. ENTER A ROLE NAME AND SELECT APPROPRIATE PERMISSIONS. CLICK SAVE.



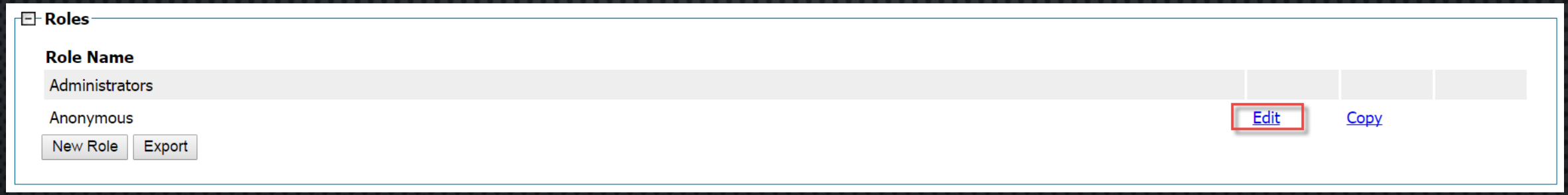
# CONFIGURING ROLES

2. ENTER A ROLE NAME AND SELECT APPROPRIATE PERMISSIONS. CLICK SAVE.



# CONFIGURING ROLES

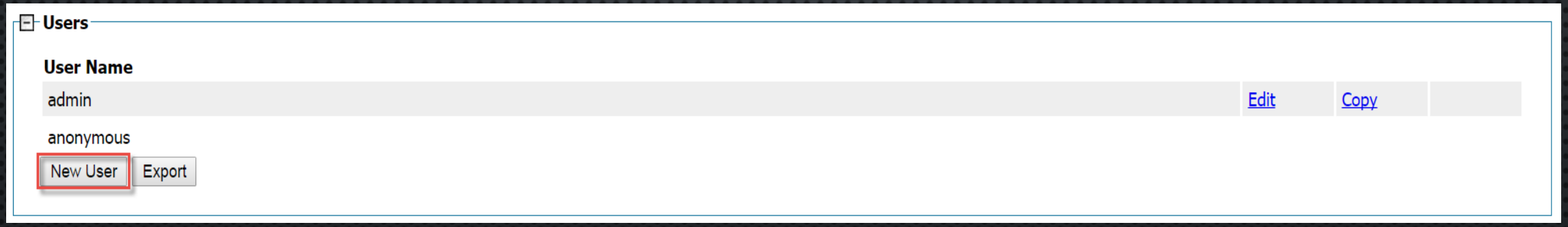
3. YOU CAN EDIT AN EXISTING ROLE BY CLICKING THE EDIT LINK. TO MANAGE PERMISSIONS FOR USERS WHO ARE NOT LOGGED IN, EDIT THE PERMISSIONS FOR THE ANONYMOUS ROLE.



# CONFIGURING USERS

1. FROM THE USERS PANEL, CREATE ADDITIONAL USERS BY CLICKING NEW USER.

NOTE: THE ANONYMOUS USERS CANNOT BE EDITED.



# CONFIGURING USERS

2. THE TABLE DESCRIBES THE STANDARD AND WINDOWS INTEGRATED (AD GROUP) CONFIGURATION.

| | |
|---|---|
| **Name** | **Standard: User's name is the same name used in login screen.**<br>**Windows Authentication: Include the DOMAIN\ prefix before user name. (See Example)** |
| Type | Standard: Uses user name and password from the Agent database.<br>Windows Integrated: Used for active directory users and do not have a password.<br>Once saved, the user type cannot be changed. |
| Password | User's password used in the login screen or assigned in AD |
| Role | Assigned role |

# EDIT USER EXAMPLE