



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

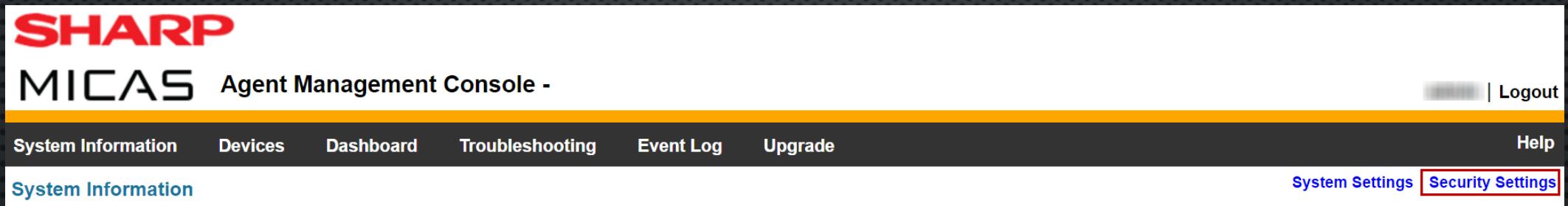
NO AUTHENTICATION

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.

The image shows a screenshot of the Sharp MICAS web interface under the 'Security' section. At the top, there is a navigation bar with links: System Information, Devices, Dashboard, Troubleshooting, Event Log, and Upgrade. Below the navigation bar, the title 'Security' is displayed in blue. Under the 'Security' title, there are two expandable sections: 'General' and 'Roles'. The 'General' section is currently expanded, showing two configuration options: 'Require Authentication?' with a checked checkbox and 'Windows Authentication Enabled?' with an unchecked checkbox. A red 'Save' button is located below these options. The 'Roles' section is collapsed, indicated by a minus sign icon.

SHARP
MICAS

System Information Devices Dashboard Troubleshooting Event Log Upgrade

Security

General

Require Authentication?

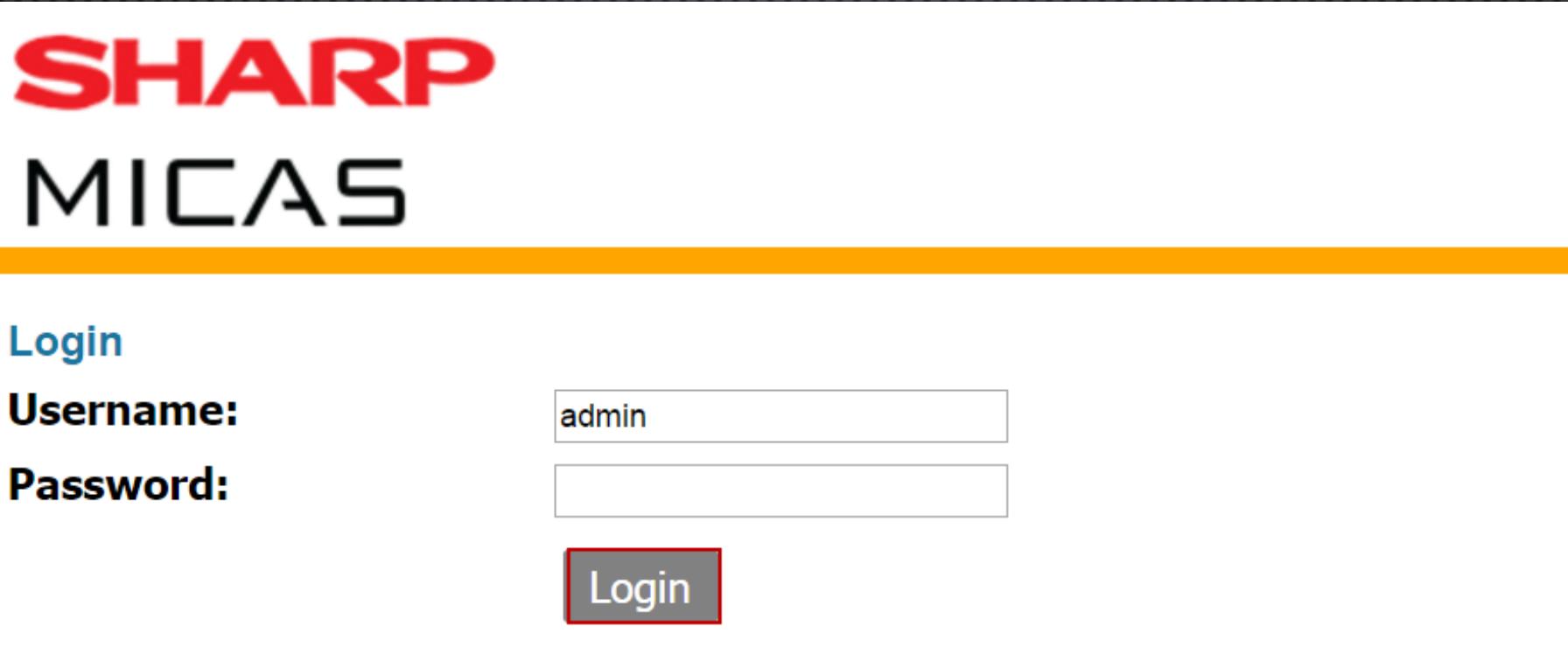
Windows Authentication Enabled?

Save

Roles

SETUP AND CONFIGURATION

3. ON THE POST-AUTHENTICATION LOG IN PAGE, ENTER ADMINISTRATOR USERNAME "ADMIN" AND LEAVE PASSWORD BLANK. CLICK LOGIN.



The screenshot shows the Sharp MICAS login interface. At the top, the Sharp MICAS logo is displayed, with 'SHARP' in red and 'MICAS' in black. Below the logo is a yellow horizontal bar. To its left is the word 'Login' in blue. The form fields are labeled 'Username:' and 'Password:' in bold black text. The 'Username:' field contains the value 'admin'. The 'Password:' field is empty. A large red-bordered 'Login' button is located at the bottom of the form.

SHARP
MICAS

[Login](#)

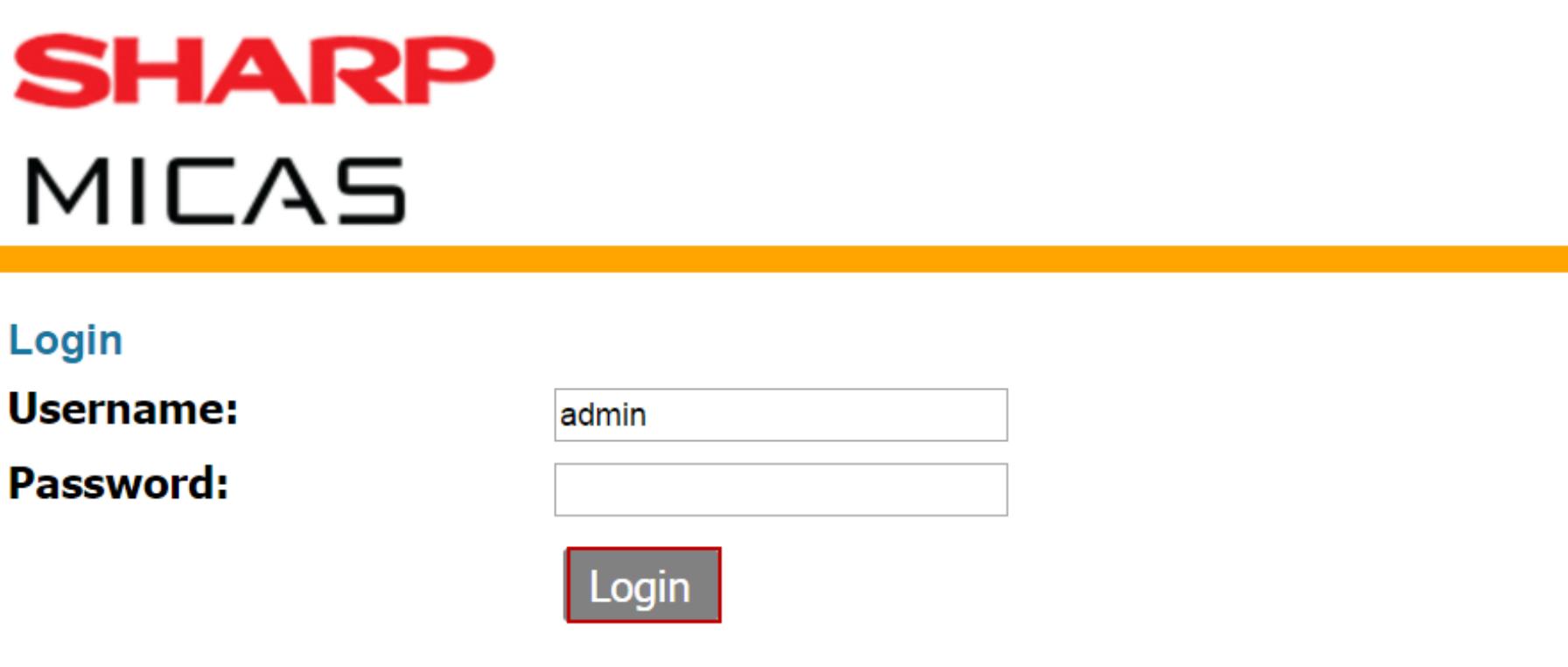
Username: admin

Password:

Login

SETUP AND CONFIGURATION

4. ON THE POST-AUTHENTICATION LOG IN PAGE, ENTER ADMINISTRATOR USERNAME "ADMIN" AND LEAVE PASSWORD BLANK. CLICK LOGIN.



The image shows a login page for Sharp MICAS. At the top, there is a red logo with the word "SHARP" and a black logo with the word "MICAS". Below the logos is a yellow horizontal bar. To the left of the input fields, there is a "Login" link. The "Username:" label is followed by a text input field containing "admin". The "Password:" label is followed by a blank text input field. At the bottom center is a red "Login" button.

[Login](#)

Username: admin

Password:

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

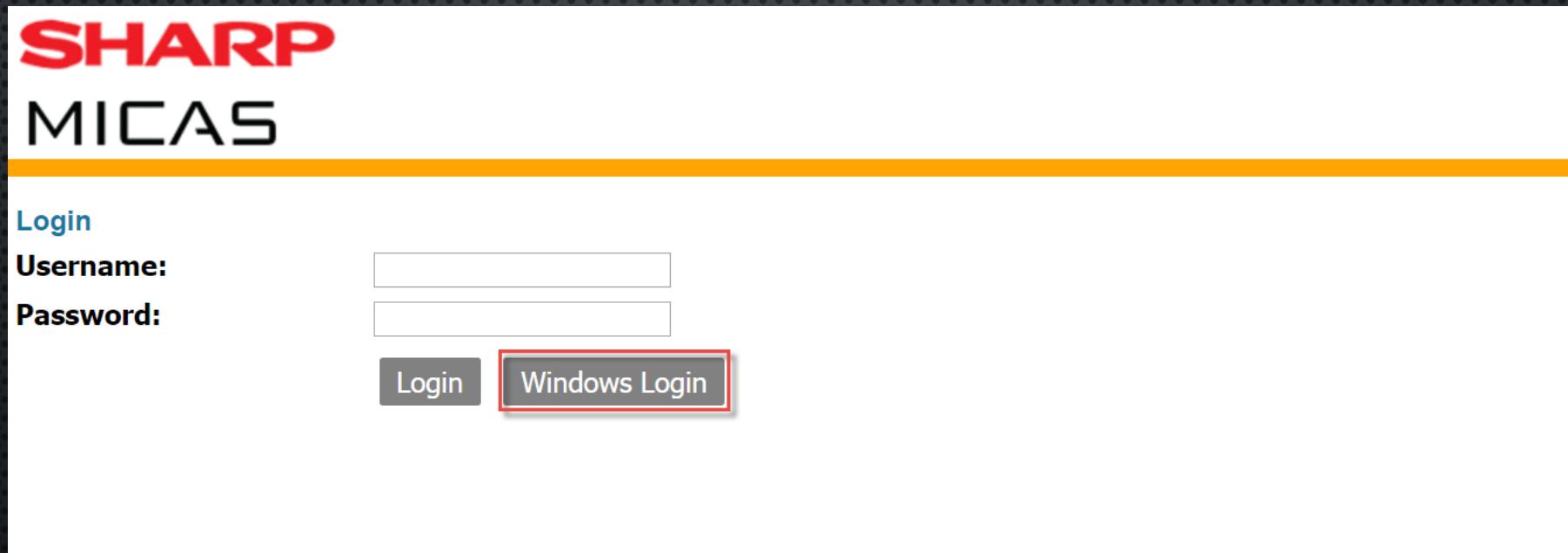
WINDOWS AUTHENTICATION

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.

The image shows a screenshot of the Sharp MICAS web interface. At the top, there is a logo with the words "SHARP" in red and "MICAS" in black. Below the logo is a navigation bar with links: "System Information", "Devices", "Dashboard", "Troubleshooting", "Event Log", and "Upgrade". The "Upgrade" link is underlined, indicating it is the active page. Under the "Upgrade" link, there is a section titled "Security" with a blue background. This section contains two expandable categories: "General" and "Roles". The "General" category is expanded, showing two checkboxes: "Require Authentication?" (which is checked) and "Windows Authentication Enabled?" (which is also checked). Below these checkboxes is a red "Save" button. The "Roles" category is collapsed, indicated by a minus sign icon.

WINDOWS AUTHENTICATION

2. ENTER YOUR WINDOWS AUTHENTICATION (MICAS ADMINISTRATORS 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.

Roles

Role Name				
Administrators				
Anonymous				

[Edit](#) [Copy](#)

[New Role](#) [Export](#)

CONFIGURING ROLES

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

Edit Role

Name:

Permissions

Module	View	Full Control
System Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Settings	<input type="checkbox"/>	<input type="checkbox"/>
Security	<input type="checkbox"/>	<input type="checkbox"/>
Devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Discovery	<input type="checkbox"/>	<input type="checkbox"/>
Dashboard	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Scan	<input type="checkbox"/>	<input type="checkbox"/>
Event Log	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Upgrade	<input type="checkbox"/>	<input type="checkbox"/>

Save **Cancel**

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.

The screenshot shows a user interface for managing roles. On the left, there's a sidebar with a 'Roles' section. The main area displays a table with two rows: 'Administrators' and 'Anonymous'. To the right of the table are two buttons: 'Edit' and 'Copy', with 'Edit' being highlighted by a red box. At the bottom left are 'New Role' and 'Export' buttons.

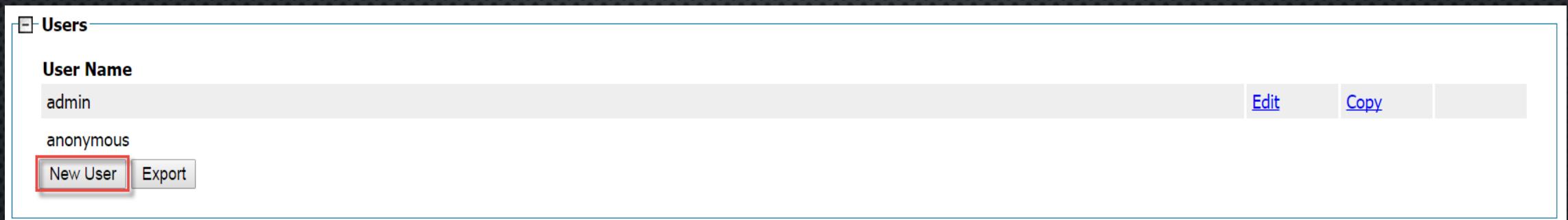
Role Name					
Administrators					
Anonymous					

New Role Export

CONFIGURING USERS

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

NOTE: THE ANONYMOUS USERS CANNOT BE EDITED.



The screenshot shows a user interface titled "Users". Under the "User Name" column, there are two entries: "admin" and "anonymous". To the right of each entry are "Edit" and "Copy" buttons. At the bottom left, there are "New User" and "Export" buttons. The "New User" button is highlighted with a red rectangular box.

User Name	Edit	Copy
admin	Edit	Copy
anonymous		

New User Export

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. Windows Authentication: Include the DOMAIN\ prefix before user name. (See Example)
Type	Standard: Uses user name and password from the Agent database. Windows Integrated: Used for active directory users and do not have a password. 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

Edit User EXAMPLE

Name:	MSGTEST\.....
Type:	Windows Integrated ▾
Password:
Role:	(no role selected) ▾

Save **Cancel**

