

User Management.

SanerNow provides role-based access in which access decisions are based on the roles that an individual user is assigned. SanerNow supports three different user roles Organization Admin, Account Admin, and Normal User. You can assign any of these roles to users during user creation or modify the role by updating the role of an existing user. In addition to the three roles, we have an admin role created during the organization creation.

Roles and Access permission:

Admin: Has full access to create organizations and accounts; allowed to perform all administrative tasks. This role is restrictive and gets assigned to the user during the initial onboarding of the organization. The admin role cannot be assigned to other users while creating new or modifying existing users from the SanerNow Management console.

Organization Admin: Has full access to the organization; allowed to perform all administrative tasks. Can create new users and assign Account Admin or Normal user roles. Can customize user access to tools (VM, CM, PM, AM, EM, and EDR) by selecting the Full Access, Read-Only, or Custom option.

Account Admin: Has full access to the account; allowed to perform all administrative tasks within the account. Can create new users and assign Normal user roles. Can customize Normal user access to tools (VM, CM, PM, AM, EM, and EDR) by selecting the Full Access, Read-Only, or Custom option.

Normal User (Full Access): Has full access to Create, Modify, and Delete tasks for the provisioned tools access. Does not have access to the control panel page to perform tasks related to **User Management, Deployment, and Settings**.

Normal User (Read-only): Has access to perform read-only operations. Does not have access to Create, Delete, or Edit tasks for the assigned provisioned tools. Does not have access to the control panel page to perform tasks related to **User Management, Deployment, and Settings**.

The normal User Custom option provides further flexibility to assign Full Access or Read-only for each provisioned tool.

New User

Login Id (*)

Name (*)

Organization (*)

Password (*) Confirm Password (*)

Role

Managing Organizations (*)

MFA Policy (*)

Manage Full Access Read Only Custom

Accounts	Tools																	
	VM		CM		PM		AE		EM		EQR		Device Management		Reports & Alerts			
	Full access	Read only	Full access	Read only	Full access	Read only	Full access	Read only	Full access	Read only	Full access	Read only	Full access	Read only	Full access	Read only		
<input type="checkbox"/> Select All																		
<input type="checkbox"/> trs-test																		
<input type="checkbox"/> 5.0.6-agents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 5.1.0.1-agents	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Bangalore	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> .computers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> test1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The following table outlines the access control and allowed actions for a tool based on the user's role.

Modules	Actions	Admin	Organization Admin	Account Admin	Normal User (Full Access)	Normal User (Read-Only)
Control Panel	Users	✓	✓	✓	✗	✗
	Deployment	✓	✓	✓	✗	✗
	Settings	✓	✓	✓	✗	✗
VM	Export CSV	✓	✓	✓	✓	✓
	Create New Benchmark	✓	✓	✓	✓	✗

CM	Apply Selected Configurations	✓	✓	✓	✓	x
	Fix Misconfiguration	✓	✓	✓	✓	x
	Revert Selected Patches	✓	✓	✓	✓	x
	Create Automation Rules	✓	✓	✓	✓	x
	Status View	✓	✓	✓	✓	✓
	Export CSV	✓	✓	✓	✓	✓
PM	Apply Selected Patches	✓	✓	✓	✓	x
	Reverted Selected Patches	✓	✓	✓	✓	x
	Create Automation Rule	✓	✓	✓	✓	x
	Rollback Patches	✓	✓	✓	✓	x
	Remove device	✓	✓	✓	✓	x
	Reboot device	✓	✓	✓	✓	x
	Status	✓	✓	✓	✓	x
	View	✓	✓	✓	✓	✓
	Export CSV	✓	✓	✓	✓	✓
AE	Edit	✓	✓	✓	✓	x
	Currency Filter	✓	✓	✓	✓	x
	Load/Filter	✓	✓	✓	✓	x
	Add new row	✓	✓	✓	✓	x
	Upload from CSV	✓	✓	✓	✓	x
	Export CSV	✓	✓	✓	✓	✓

EM	Checks	✓	✓	✓	✓	✓
	Actions	✓	✓	✓	✓	x
	Status view	✓	✓	✓	✓	✓
	Delete	✓	✓	✓	✓	x
	Export CSV	✓	✓	✓	✓	✓
EQR	Create New Detection	✓	✓	✓	✓	✓
	Create New Response	✓	✓	✓	✓	x
	Export CSV	✓	✓	✓	✓	✓
	Run	✓	✓	✓	✓	✓
	View info	✓	✓	✓	✓	✓
Device Management	Scan Now	✓	✓	✓	✓	✓
	Create Group	✓	✓	✓	✓	x
	Delete Device	✓	✓	✓	✓	x
	Disable Device	✓	✓	✓	✓	x
	Enable Device	✓	✓	✓	✓	x
	Uninstall Agent	✓	✓	✓	✓	x
	Move Device	✓	✓	✓	✓	x
	Export CSV	✓	✓	✓	✓	✓
Reports	Create New Reports	✓	✓	✓	✓	x
	Download Report	✓	✓	✓	✓	✓
	Email Report	✓	✓	✓	✓	✓
	Report Settings	✓	✓	✓	✓	x

	Export CSV	✓	✓	✓	✓	✓
Alerts	Update	✓	✓	✓	✓	✘
	Export CSV	✓	✓	✓	✓	✓

To add a new user, complete the following steps:

1. Log in to SanerNow Management Console
2. Click on the **Control Panel** icon on the top right corner of the organization level dashboard and select the **Users** option.
3. Click **New Users** on the **Users** page. Specify the **Login Id, Name, Organization, and Password**. Select the **Role** of the user from the drop-down menu

New User

Login Id (*)

Name (*)

Organization (*)

Password (*) Confirm Password (*)

Role

Managing Organizations (*)

MFA Policy (*)

Manage Full Access Read Only Custom

4. If the role is Normal User, access can be set to **Full Access** or **Read Only** for all the provisioned tools. This can be further customized by selecting the Custom option.
5. Select **Managing Organization** from the drop-down. You can select one or more organizations.
6. Select **MFA Policy** from the drop-down. By default, none is selected. Refer Multi-Factor Authentication section for more details.
7. Click **Create**.

Modify User:

- From the Users table, click the **Edit** icon in the Action column for the user to be modified.
- Update the necessary changes and click **Update**.

Delete User:

- From the Users table, click the **Delete** icon in the Action column of the user to be deleted.
- To delete multiple users, select one or more users and click on the delete icon from Action, which appears on the top right of the user's table.

Enforce, Change, Withdraw Multi-Factor Authentication:

- Lock icon in the Action column is used to Enforce, change, or withdraw Multi-Factor Authentication. If the Lock icon is green, Multi-Factor Authentication is Enforced, and if the Lock icon is grey, Multi-Factor Authentication is not enforced.
- To Enable Multi-Factor Authentication, click on the lock button in the Action column of the user. Select the MFA Policy and click Confirm to Apply.
- To Change the Multi-Factor Authentication Policy, click on the lock button in the Action column of the user. Select a different MFA Policy from the drop-down and click on Change.
- To Withdraw Multi-Factor Authentication, click on the lock button in the Action column of the user. Click on the Withdraw.
- To Enforce, Change or Withdraw Multi-Factor Authentication for multiple users. Select one or more users and click on the green lock icon to enforce or click on the grey lock icon to change or withdraw.

Control Panel

TestOrg

Users

Deployment

Settings

Users

Manage your users and their preferences.

New User

Show 25 entries

Role Organization Managing Organiza... Managing Accounts Search:

<input type="checkbox"/>	Login Id	Name	Role	Organization	Managing Organizations	Managing Accounts	Action
<input type="checkbox"/>	testdomain@...	testuser1	Normal User	TestOrg	TestOrg	TestAccount	
<input type="checkbox"/>	testuser@...	testuser	Admin	Testorganization	TestOrg	TestAccount	
<input type="checkbox"/>	trial@...	trial	Normal User	secpod	TestOrg	TestAccount	
<input type="checkbox"/>	xyzuser@domain.com	xyzuser	Normal User	testorganization	TestOrg	TestAccount	

Showing 1 to 4 of 4 entries

Previous 1 Next