SanerNow Active Directory Integration

Technical Guide

Document Version: 5.1

Published Date: 9th April 2022

Contents

Overview of Active Directory integration in SanerNow

SanerNow provides an accurate depiction of the security posture of organizations - large and small. With Active Directory (AD) integration, SanerNow can represent the organization hierarchy in AD and synchronize the organizations, groups, and devices every day. New devices are commissioned/moved/decommissioned; it shall automatically synchronize the updated hierarchy info with SanerNow. Additionally, AD integration enables seamless deployment of SanerNow agents and reduces IT teams' effort to ensure maximum security for their organization.

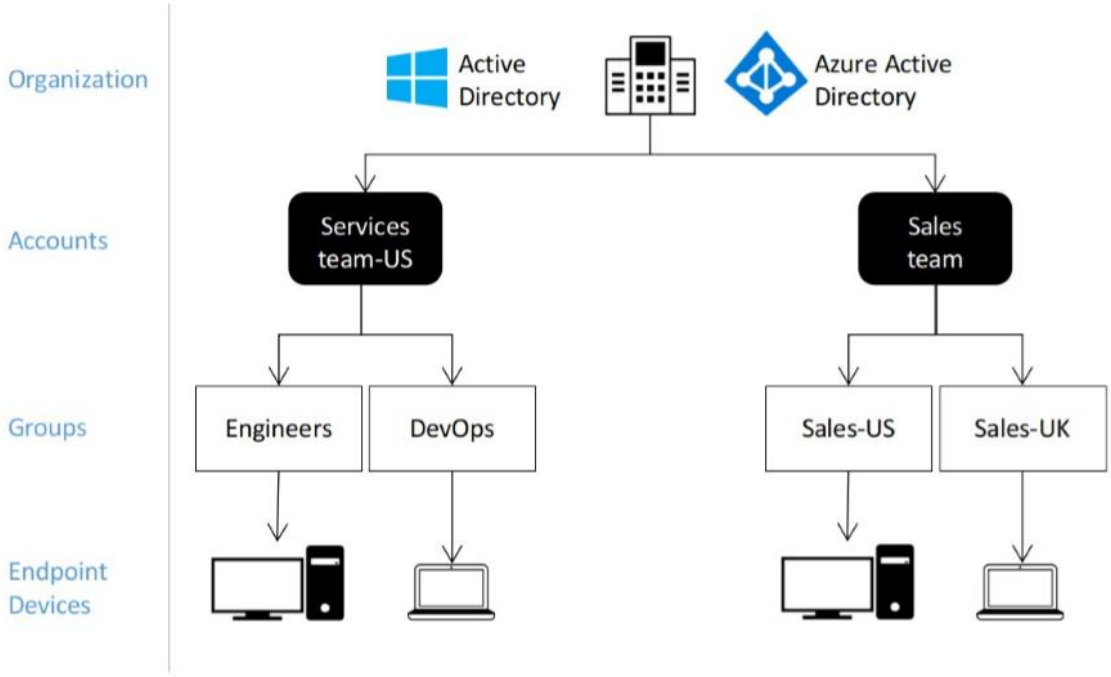


Figure 1: Microsoft Active Directory (AD) and Azure Active Directory (AD) integration

Hierarchy of user roles in SanerNow

Following is the list of user roles in the SanerNow

Level-1) SUPERUSER : This role is available only for in-house deployments. SUPERUSER can able to create users for the role:

- ADMIN

Level-2) ADMIN : Creates organizations, accounts, and users of roles. ADMIN has the rights to edit, delete and modify any changes to the following user roles:

- ORGADMIN
- ACCOUNTADMIN
- NORMAL

Level-3) ORGADMIN : This user role was introduced at the SanerNow 4.7 release to manage organizations and accounts. Creates accounts and users of roles (for the organization they are managing):

- ACCOUNTADMIN
- NORMAL

Level-4) ACCOUNTADMIN : Manages an account and creates users of the role:

- NORMAL

Level-5) NORMAL : This role has restricted access to an account.

What does Active Directory Integration in SanerNow mean for our customers?

Active Directory makes it easier for IT support teams to manage thousands or even hundreds of thousands of endpoint devices and organizational information across geographically scattered offices. Seeing this to be an opportunity we could leverage and help IT support teams spend less time deploying SanerNow, we defined what should Active Directory integration in SanerNow provide its users:

- From Active Directory, import a hierarchy of organizational units, groups, and devices into SanerNow.
- Deploy SanerNow agents into endpoint devices without repeating the installation procedure in each device.
- SanerNow web console shall display an organization's security posture in the same hierarchical relationship seen in Active Directory.
- An admin user in SanerNow can have more than one organization. Each of those organizations can be integrated with a different Active Directory. Some of those organizations may not have Active Directory at all. This feature and its adaptability will cater to our customers' needs who manage IT systems of more than one organization.
- Active Directory integration shall maintain itself without manual human intervention. If the hierarchy in Active Directory has an update with the highest integration level, it shall reflect in the SanerNow web console and reports without any manual intervention.
- Changes to hierarchy in SanerNow should remain only in SanerNow. Active Directory integration is a one-way flow of information wherein changes in AD are visible in SanerNow, but not the other way around.

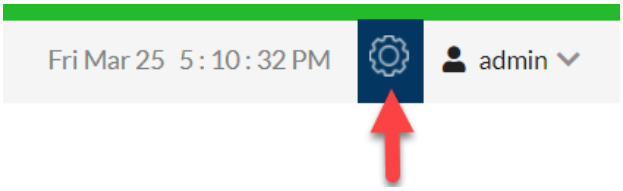
As one might have noticed from the above, at SecPod, we always think about making it happen in the easiest way possible but still leave that option for our customers to exercise some flexibility at their discretion.

All of the above design considerations are met with Active Directory integration in SanerNow 4.7 and onward.

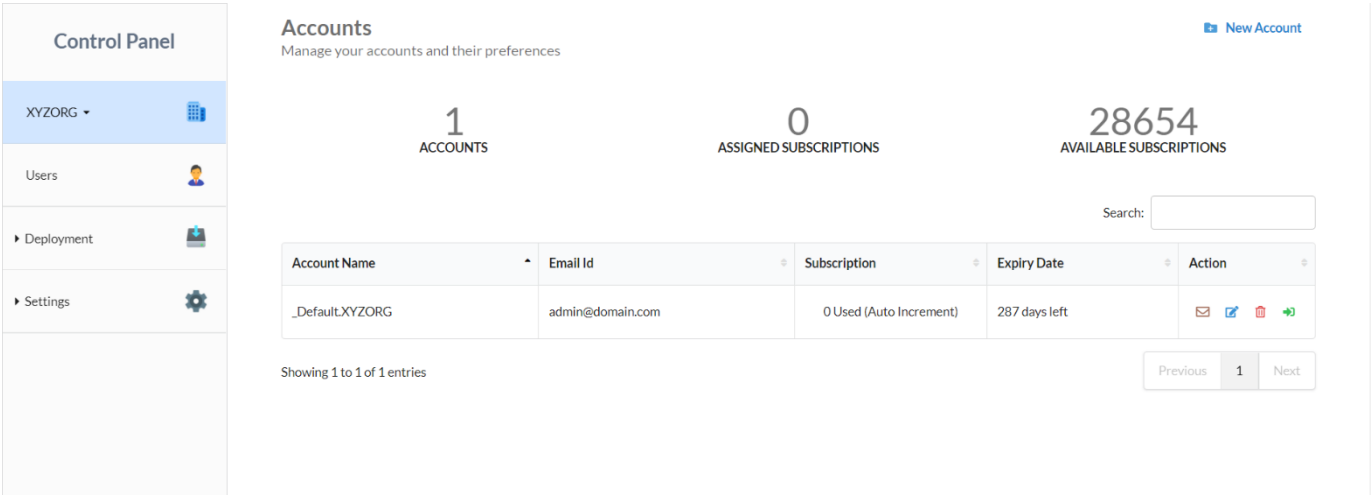
Configuring Active Directory integration for an organization

Integrating SanerNow with Active Directory allows importing organization hierarchy and deployment of Saner Agents to all devices in your organization through the following simple steps:

1. Log in to SanerNow and click **Control Panel** at the top-right to access the **Control Panel** page.

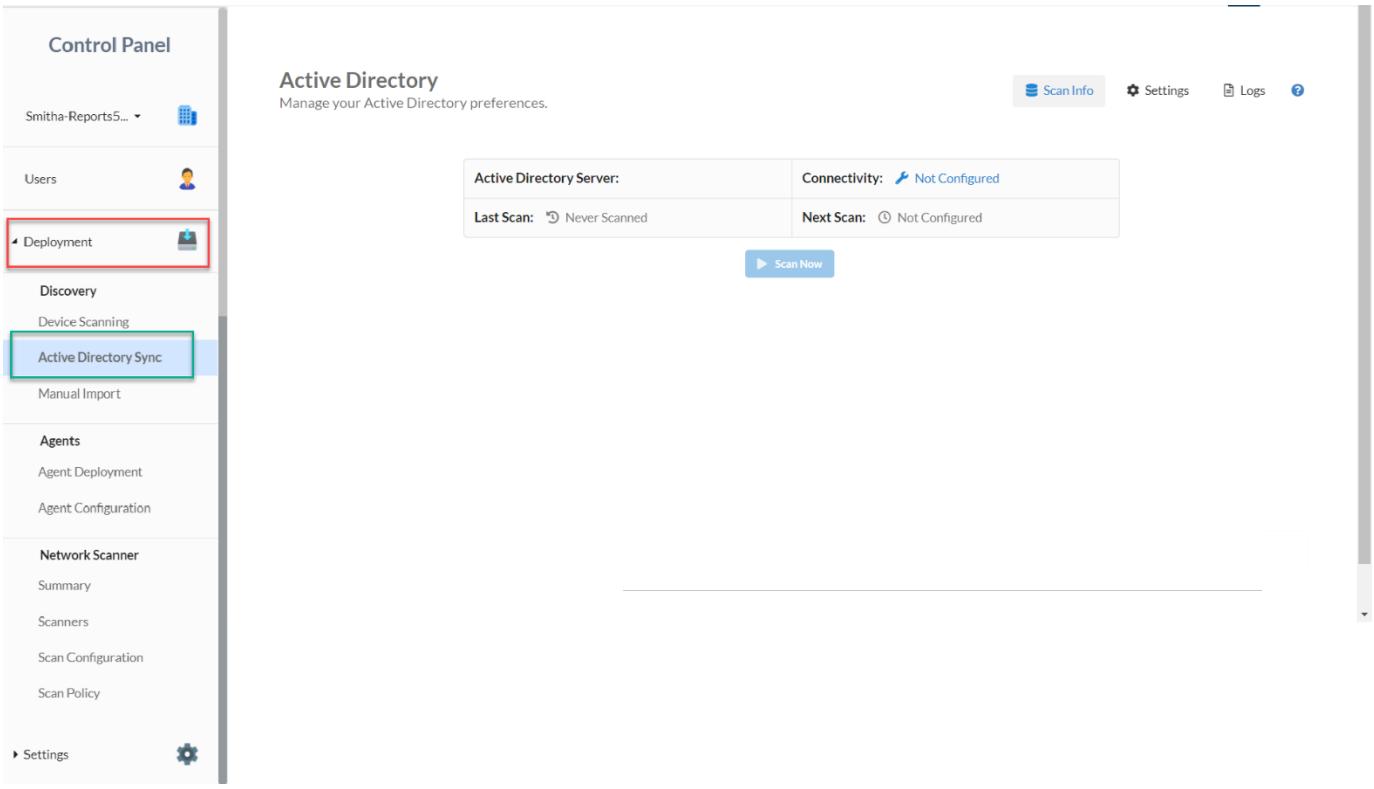


2. Select an organization from the dropdown menu on the left under Control Panel

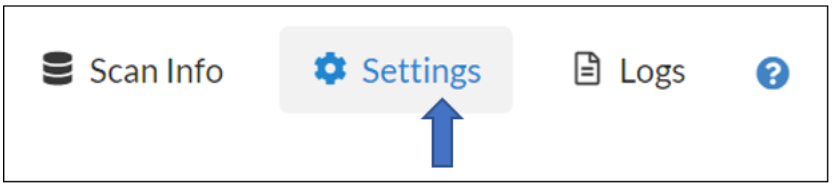


3. After selecting an organization, choose the Deployment section on the control panel page.

4. Select **Active Directory Sync** option for synchronization with Active Directory.

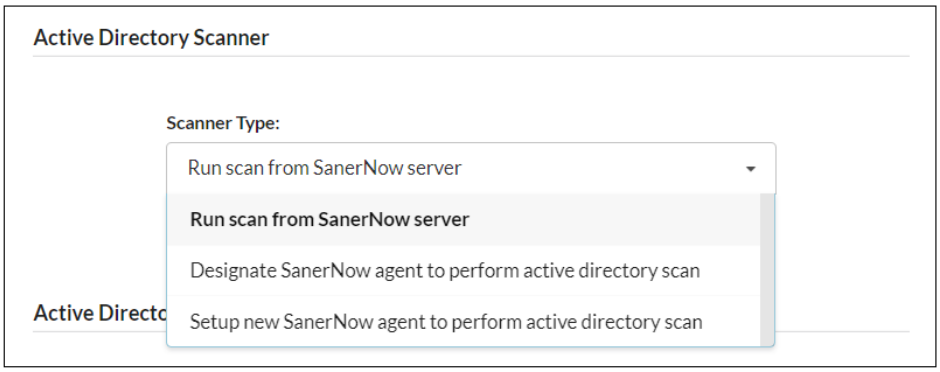


5. The **Scan Info** tab will be empty since the Active Directory is not configured yet. Proceed to click the Settings tab.



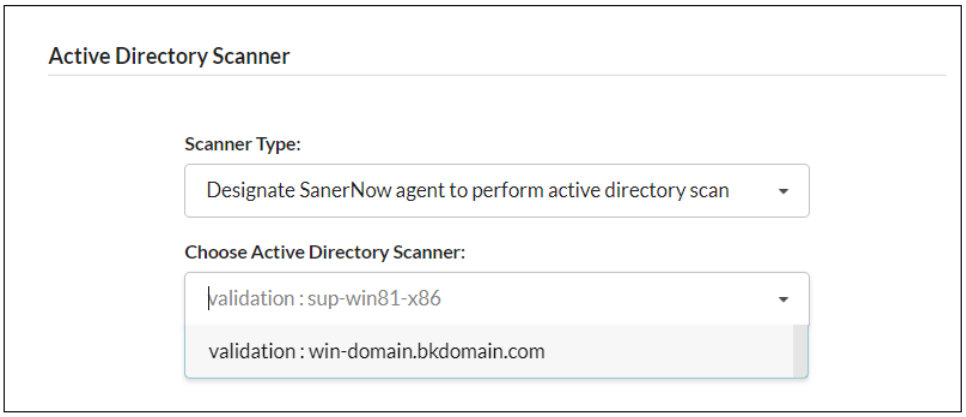
6. Select the AD Scanner Type: Select the preferred scanning method from the drop-down menu. The scanning method can be one of the following:

a) Run scan from SanerNow server



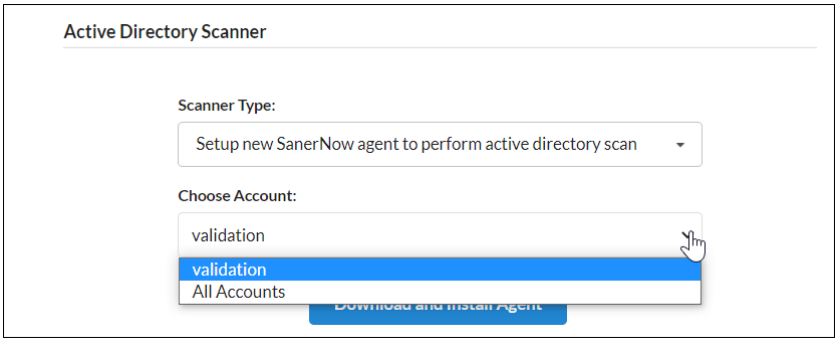
Use this method to allow SanerNow Server to perform the AD discovery scan. Please note that SanerNow Server will securely store the AD credentials supplied in later steps. This will enable the SanerNow server to scan the AD and fetch hierarchy information.

b) Designate SanerNow agent to perform active directory scan

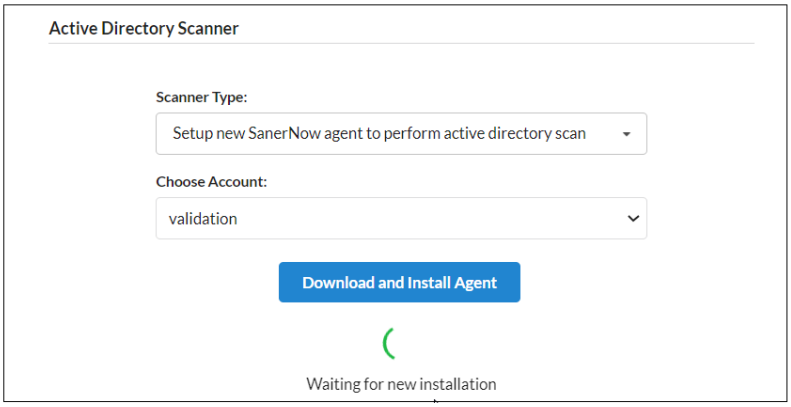


Select an endpoint device that has the SanerNow agent installed. The agent will automatically upgrade itself to the role of AD scanner. The selected endpoint device will securely store the AD credentials. After filing in AD credentials in later steps, the selected device will scan the AD and fetch hierarchy information.

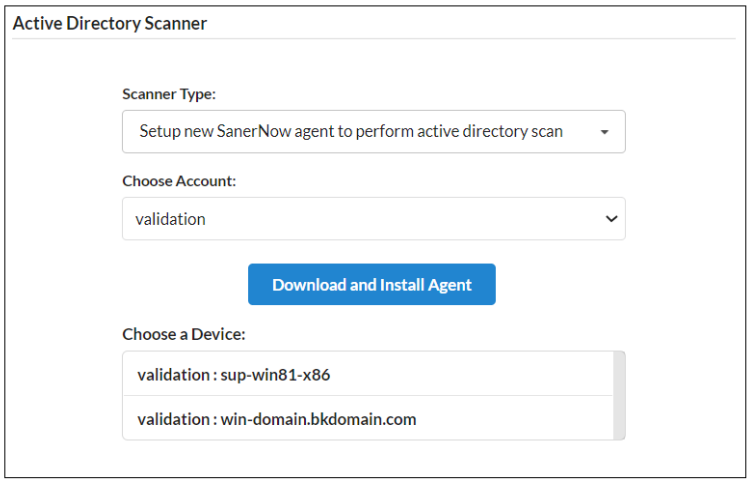
c) Setup a new SanerNow agent to perform an active directory scan



Suppose none of the endpoint devices has a SanerNow agent installed. You may download the agent for any account or All Accounts from the dropdown list (in this latter case, the user can download a zip file containing the agent installer for each account). The user has to install a minimum of one SanerNow agent.

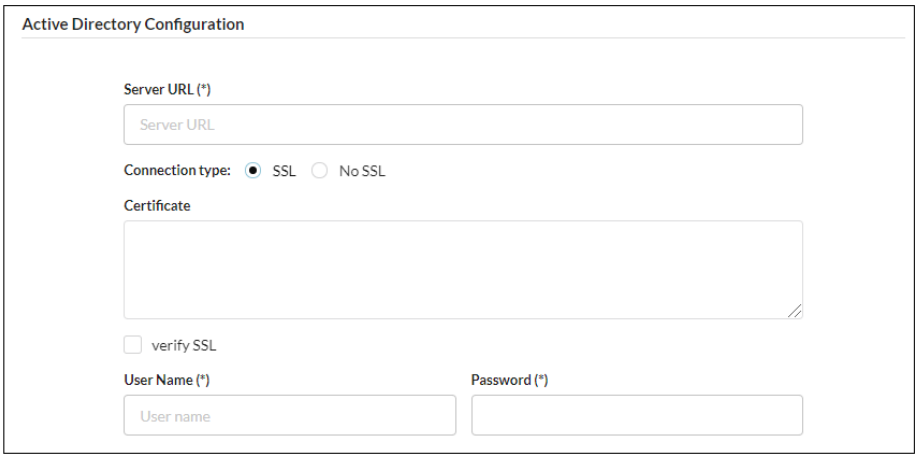


Once agent installation completes and communication with the SanerNow server is established, the page will list all the device/s with the SanerNow agent installed. Select one that should execute the AD scan, as shown below.



After filing in AD credentials (explained in later sections), the agent in the device selected will scan the AD and fetch hierarchy information.

7. Input AD server credentials:



a) **Server URL** - AD server LDAP URL that SanerNow should contact.

b) **Connection type** - If SSL is set, the user must provide the SSL Certificate. If No SSL is set, the user does not have to provide the SSL Certificate.

c) **Certificate** - SSL certificate when SanerNow attempts to connect to the AD server. This will be the AD server SSL certificate that should be verified and trusted.

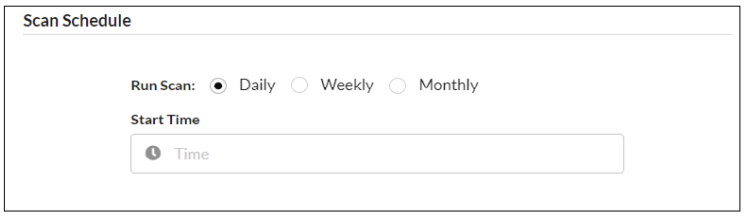
d) **verify SSL** - When selected, the SanerNow Server will verify whether the SSL Certificate is valid before connecting to the AD server.

e) **Username** - Username of AD server login account. This user should have enough privileges to perform an AD scan and collect the entire organization's hierarchy for synchronizing with SanerNow.

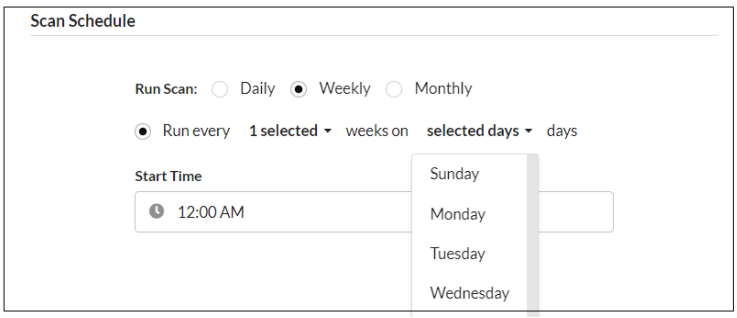
f) **Password** - Password of AD server login account, which the SanerNow Server will store securely.

8. Set AD Scan schedule: SanerNow can do a scheduled AD scan and use the results to present changes in the Domain Server to the SanerNow administrator. Suppose the Auto Sync is enabled; it automatically imports Domain Server changes about organization hierarchy.

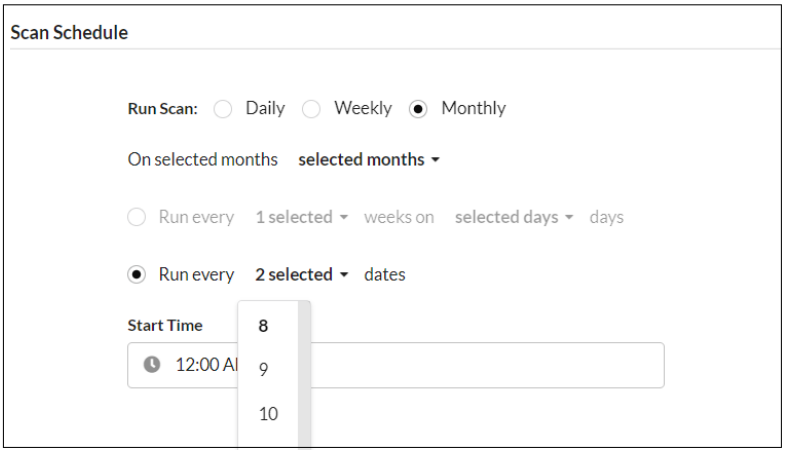
a) Daily - Every day at a specific HH: MM time, an AD scan will be initiated.



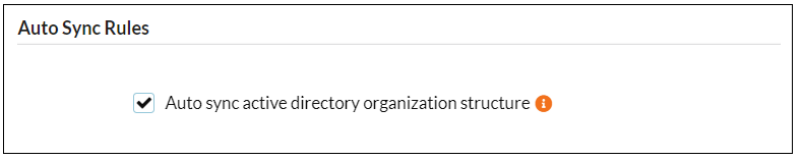
b) Weekly - On specific day/s every week, at HH: MM time, an AD scan will be initiated.



c) Monthly - On specific day/s of every month, at HH: MM time, an AD scan will be initiated.



9. Choose to enable or disable the **Auto Sync Rules**, as shown below.



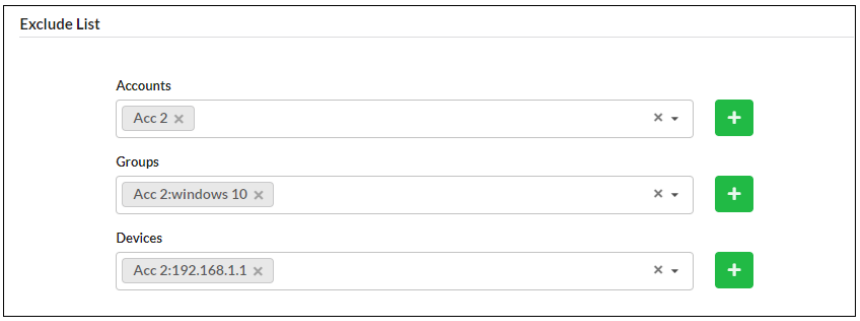
If Auto sync is enabled, the following steps happen automatically after every AD scan operation:

a) All the edits in the AD hierarchy of items will be fetched and used to update accounts/groups/devices relations.

b) Items in Exclude List will not be considered for changes in the AD hierarchy and will not be imported.

c) Changes in accounts/groups/devices relations in SanerNow will not get reflected in the AD hierarchy

10. Exclude Lists: You may do this after the AD scan completes and the SanerNow Server has imported the organization hierarchy. The drop-down menu will show the accounts/groups/devices that can be added to the Exclude List. You may also remove the items in the Exclude List as needed.

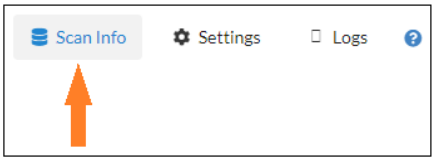


11. Click the **Save** button at the bottom of the page for changes to take effect.

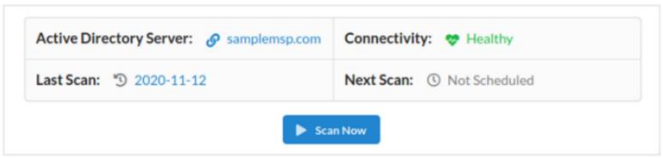
Note-1: *You may click the Validate button first to ensure that the AD credentials are proper. Suppose it is appropriate, success! It would be shown at the right top as a pop-up message.*

Note-2: *If this is not the first time you are configuring Settings on the Active Directory Sync page, click the Update button.*

12. Once the Settings are successfully updated, go back to the **Scan Info** tab to run the AD scan.



13. Run AD scan: If an AD scan has not started, click on the **Scan Now** button.



Above that button, the following info is shown:

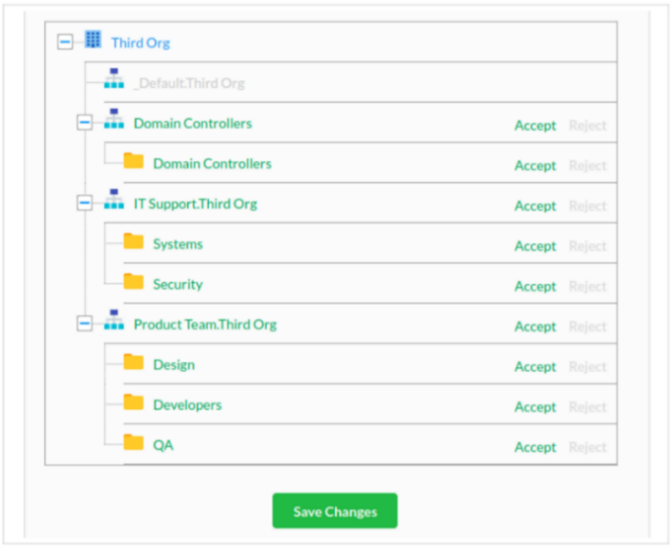
a) Active Directory Server - URL address of AD server.

b) Connectivity - Shows connection health to the AD server.

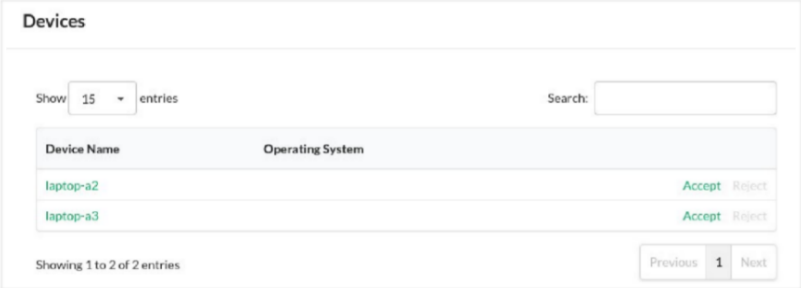
c) Last Scan - Date of previous AD scan.

d) Next Scan - Date of following AD scan scheduled. Wait until the AD scan finishes.

14. Import AD hierarchy: The hierarchy of accounts/groups/devices in AD is shown in the SanerNow web interface (Viser). For items that should not be imported into SanerNow, set Reject.

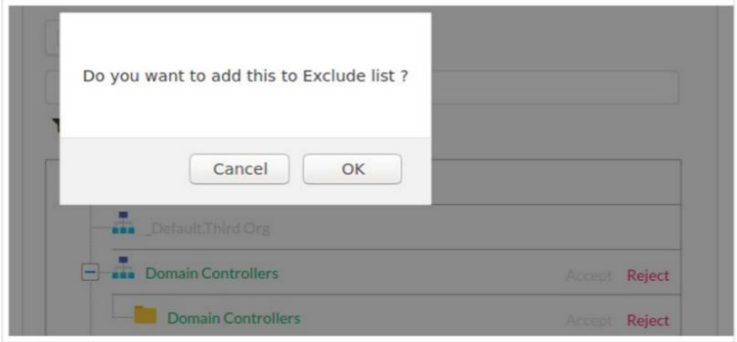


15. Devices list from AD scan: To see the list of devices in a group, click on the Group name. Pop-up shows a list from which a device can be set to Accept / Reject.

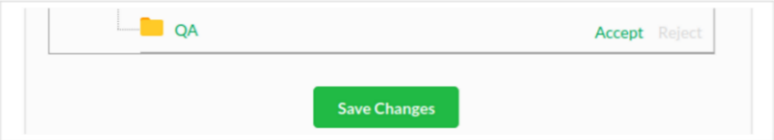


Add it to the Exclude List if an item should not be imported into SanerNow and should not be listed in any subsequent AD scan operations. This will be prompted when setting any item to Reject status.

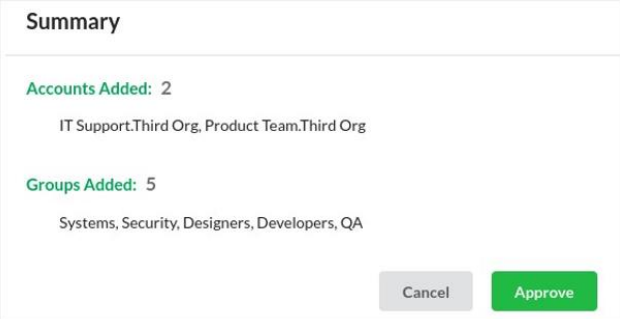
16. Adding an item from the AD scan list to Exclude List: You may choose to put **Domain Controller** into Exclude List. Clicking on **Reject** will show a pop-up prompt. Click **OK** on it.



17. Save the AD hierarchy that must be imported: Click on the **Save Changes** button at the bottom to import every item that has an **Accept** state into SanerNow.



18. Approving the import of AD hierarchy to SanerNow: Click Approve to confirm your choice of AD hierarchy import.

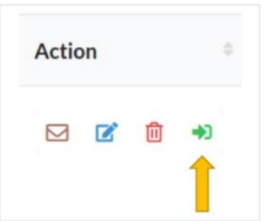


19. Accounts imported through AD integration: Select the organization in the left sidebar to open the Accounts page.

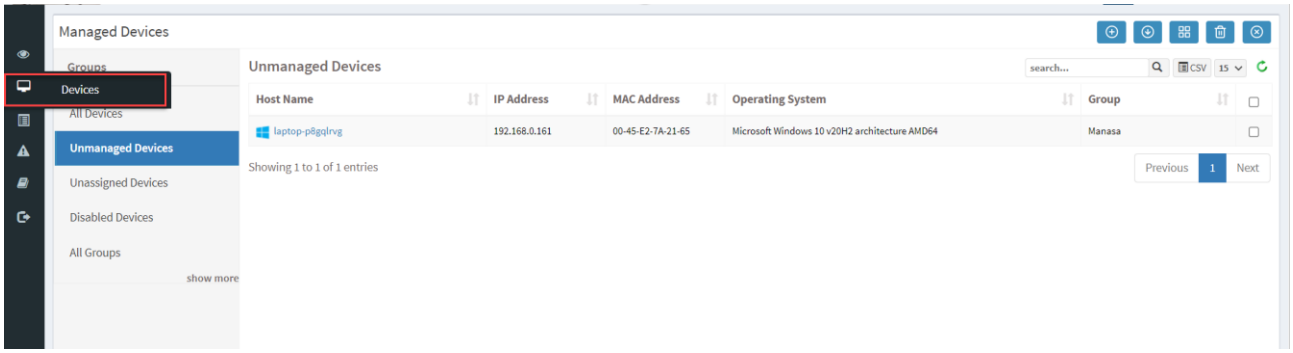
The SanerNow Server will import the accounts, and the spinner will indicate the build creation status of SanerNow agents for each account.

_Default. Third Org is the default account created during the creation of this organization, and you may rename it as needed. After the build creation is complete, you can download SanerNow agents for this default account (after the build creation is complete) and install them into devices. If you import accounts from AD, this default account may not be helpful, and you may delete it by clicking on the delete icon in the corresponding row, the last column. Devices imported will also be available on the SanerNow page for managing devices (shown in later steps).

20. Once build creation for an account completes, navigate to the Account dashboard page. After that, we can download the SanerNow agent for that account.

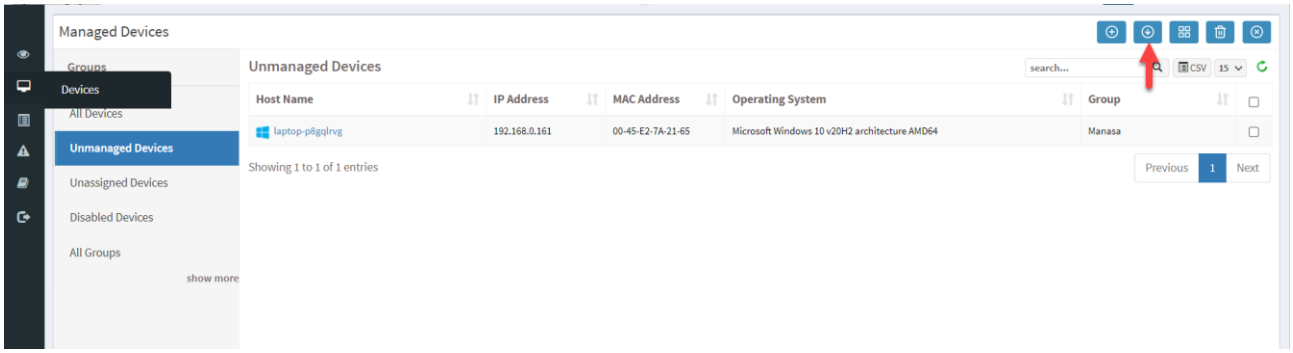


21. Select Devices from the left sidebar from the account dashboard page.

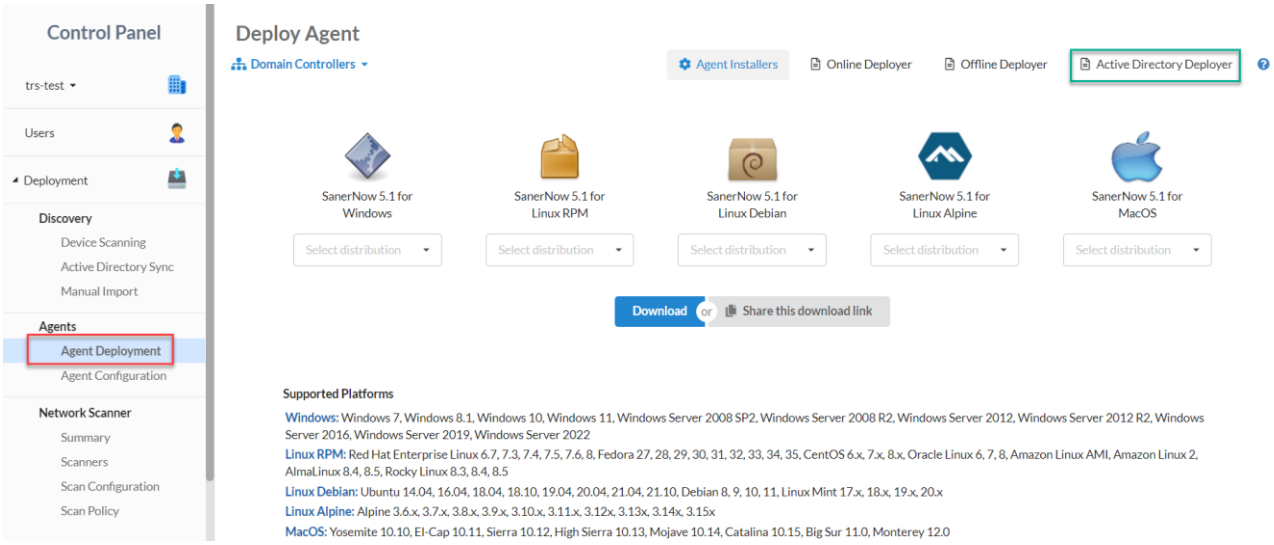


22. Devices imported through AD integration: The Unmanaged Devices page displays the list of devices and groups in the account that the SanerNow server imports through an AD scan.

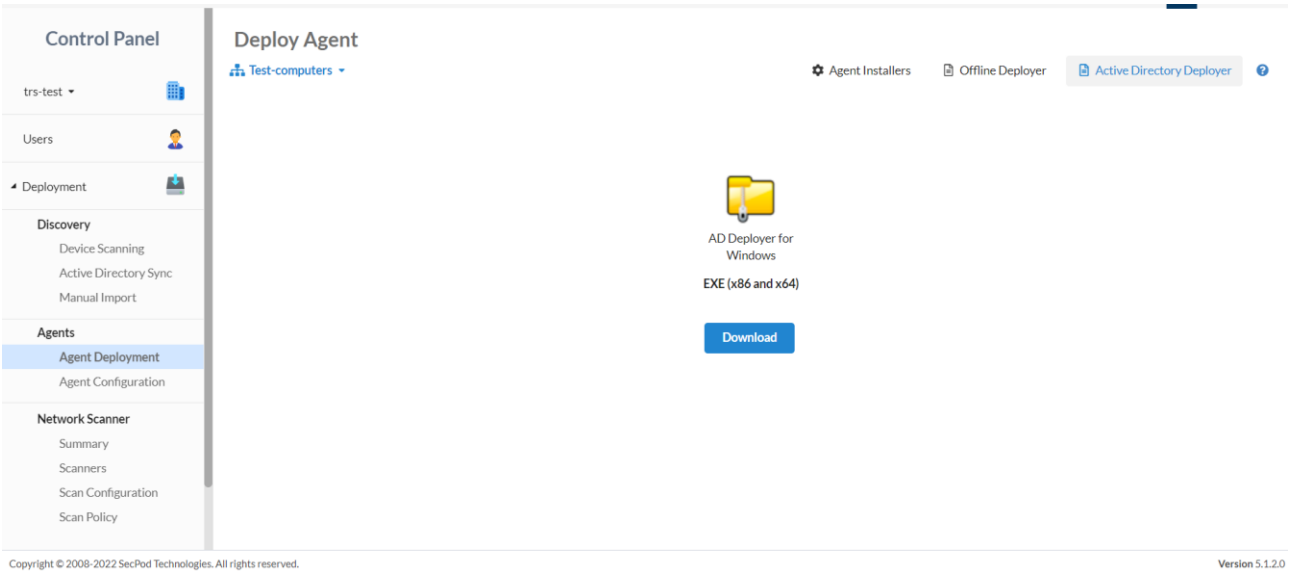
23. Downloading SanerNow Agent will be attempted by clicking the **Deployment** icon on the top-right of the Unmanaged Devices page.



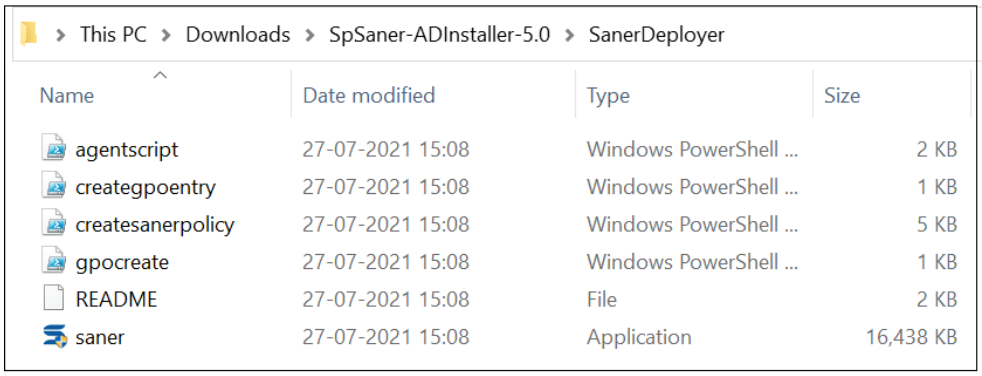
24. It navigates to the **Agent Deployment** section on the control panel page. Click **Active Directory Deployer**



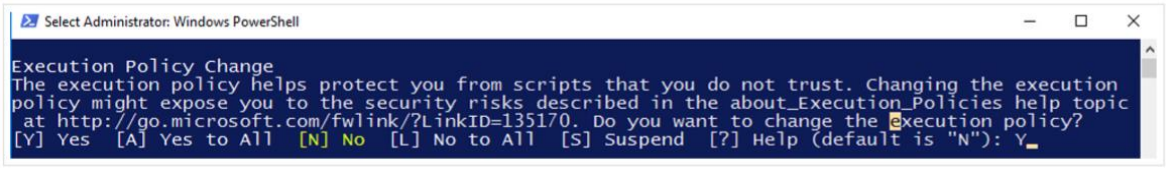
25. To download AD deployer for windows, click download to get a zip file containing all necessary files for the GPO policy update for that account. Extract the zip file into the AD server.



26 (a). Install devices with SanerNow agent through GPO policy update: This must be done separately for each account. The GPO policy update is to install the SanerNow agent into endpoint devices.



Execute gpocreate—ps1 PowerShell script.

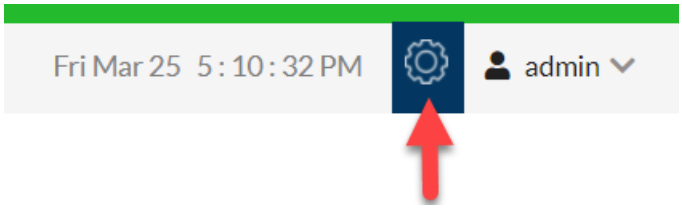


Enter Y for Yes to execute the policy update. Once the script has been successfully executed, the policy will take effect, and agents will be installed on the endpoints once they are rebooted.

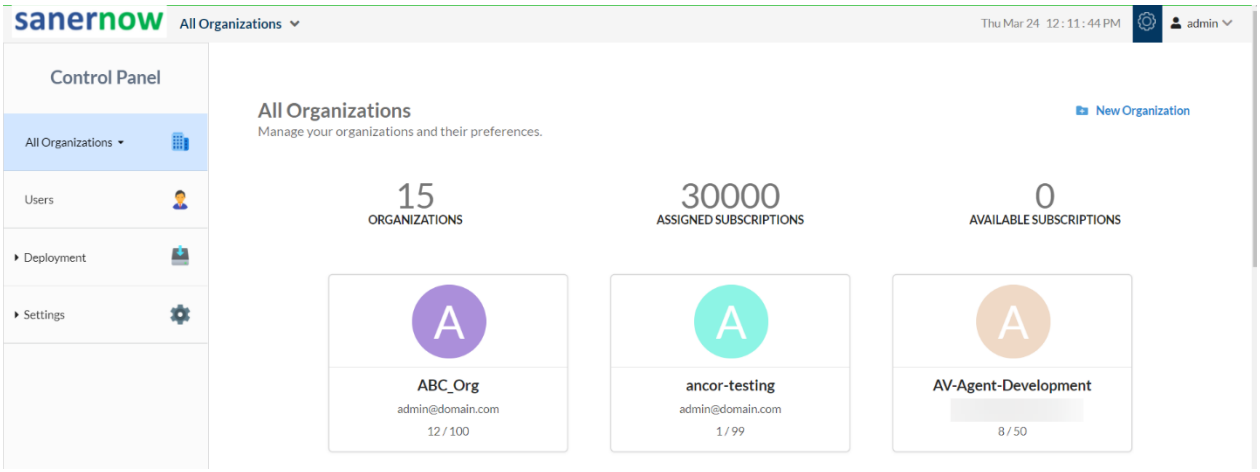
26 (b). Install devices with the SanerNow agent individually: This has to be done separately for each device in an account.

SanerNow platform supports most operating systems like Windows, Linux, and Mac OS. Users can deploy the agent from the deployment section on the control panel.

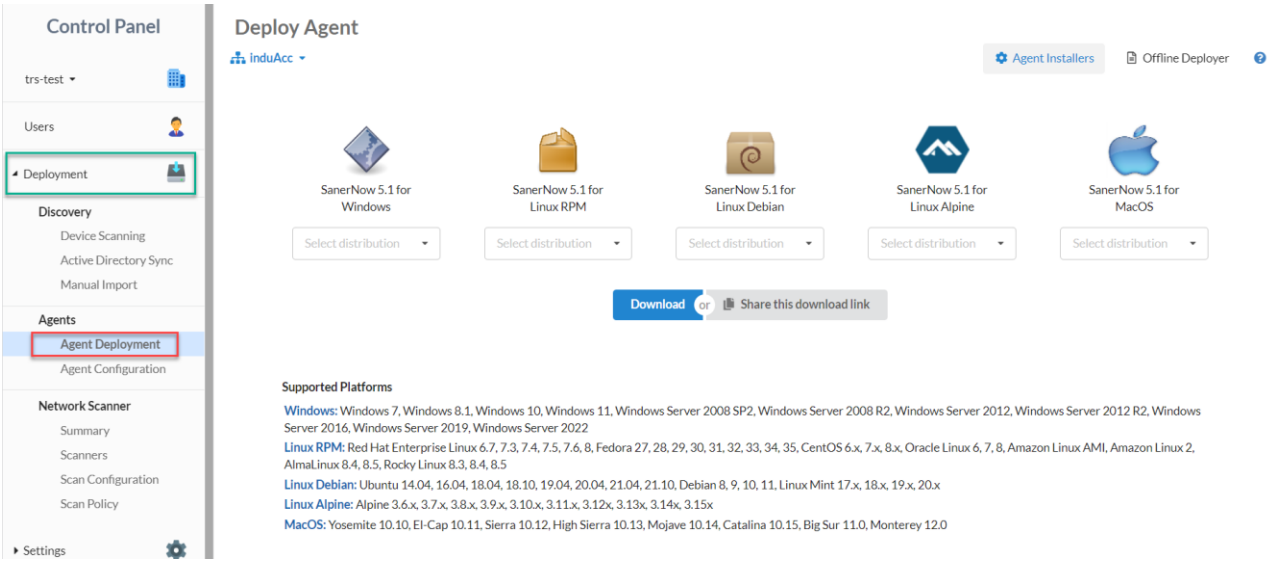
Step 1: Log in to SanerNow and click **Control Panel** at the top-right to access the **Control Panel** page.



Step 2: Select an organization from the dropdown menu on the left under Control Panel



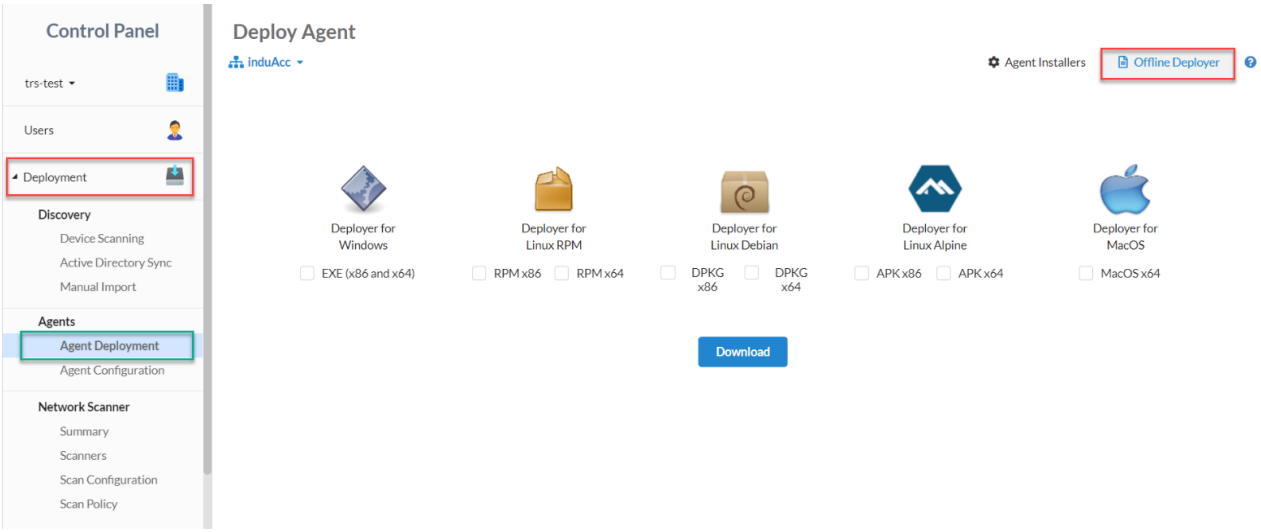
Step 3: After selecting the organization, select **Agent Deployment** that is in the **Deployment** section of the control panel page



Step 4: Select the appropriate distribution for the endpoint operating system from the drop-down and click the **Download** button.

Step 5: You can also share the download link by clicking on the share this download link option, and the download link will be copied. The help icon will provide the instructions to install and uninstall the saner agen.t

Step 6: Besides **Agent Installers, Offline Deployer** is displayed. Click Offline Deployer to deploy the agent. Select the Deployer for the OS corresponding to the endpoints or network devices you want to install the

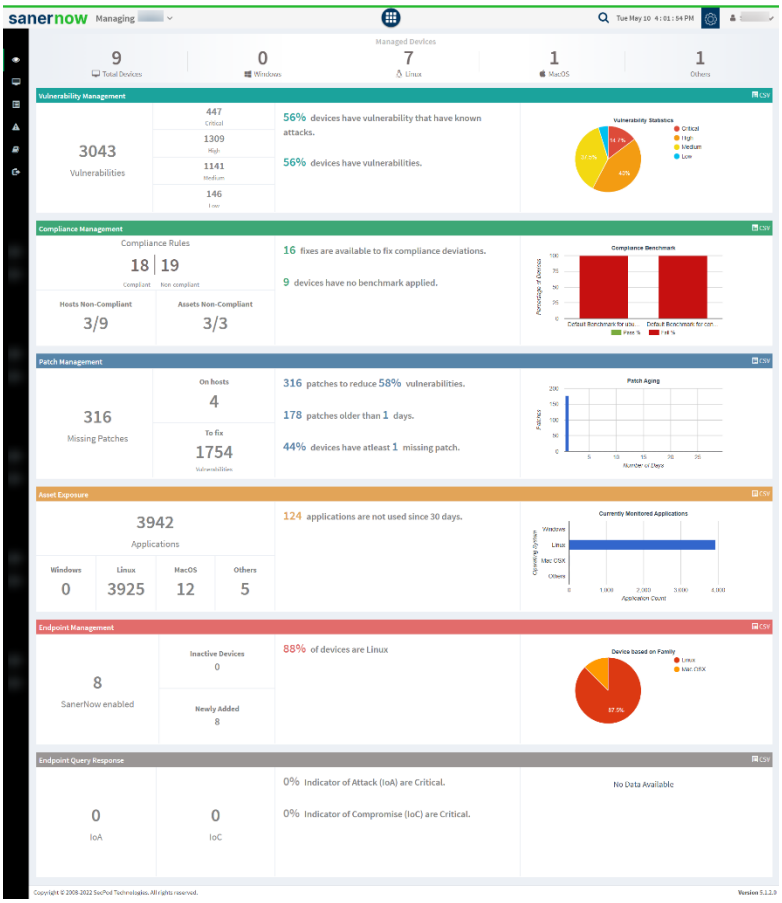


agent. Then, click **Download**. The offline deployer can also be used to discover devices on the network.

Step 7: The deployer tool is downloaded in .zip format; unzip the file and run the offline deployer.

Once the Saner agent is installed on the device successfully, those devices will be listed under the unmanaged devices page. The help icon will provide the instructions to install and uninstall the saner agent through an offline deployer.

27. SanerNow agent completes a scan in devices: Once the SanerNow agents complete the scan in the device and upload the report, the account dashboard will show its security posture.



Congratulations! You have configured Active Directory integration in SanerNow.