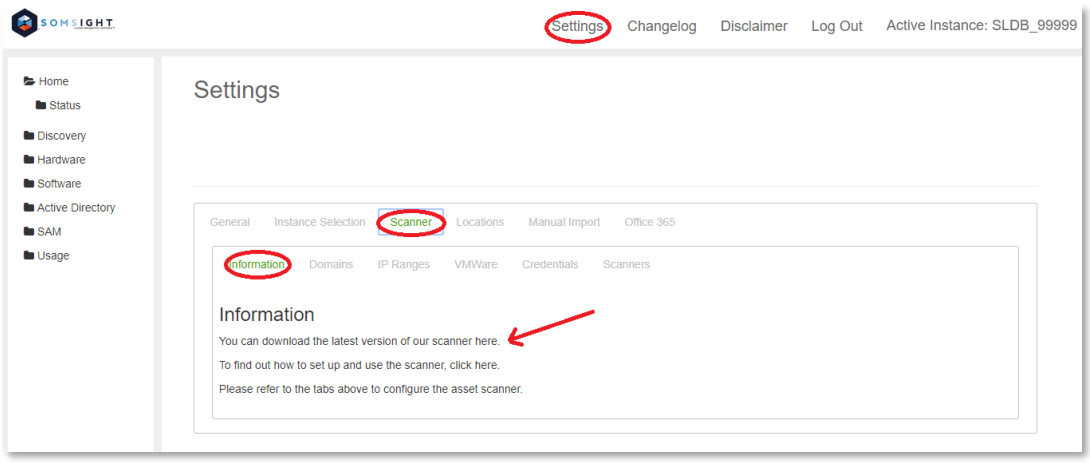
# Scanner install guide

1. You can download the scanner and the guide from the dashboard, *(This is confusing, what are you trying to say regarding the dashboard??* Proceed to "Settings / Scanner / Information" and click on the link for downloading the scanner as shown below.




2. Copy the downloaded file "**SLScanner.zip**" to the machine you want to use as the scan server.

   **Note:** We suggest to deploy the scanner in a server that is powered on 24/7 and running with administrator privileges.

3. On this machine, unzip ***SLScanner.zip*** to any folder

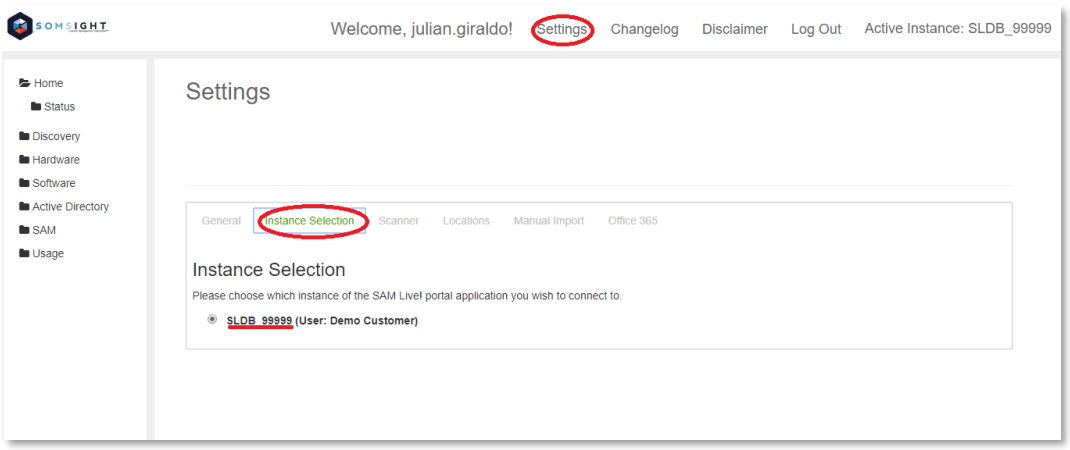
4. Open the folder ***SLScanner*** and run ***SLS_Installer.exe*** like administrator. Follow the instructions until the following dialog box appears:

# Scanner install guide

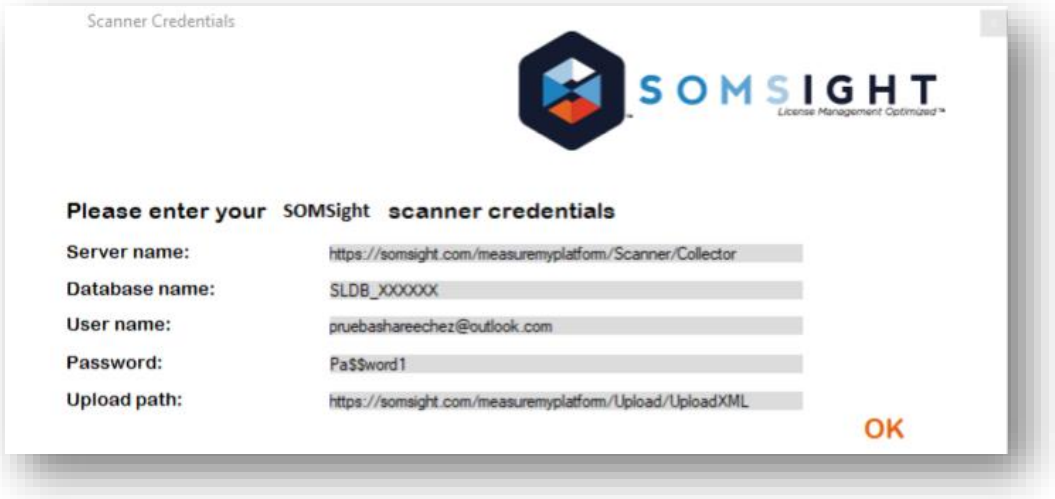
The “Server name” and “Upload path” should appear as follows:

Server name: https://somsight.com/measuremyplatform/Scanner/Collector
Upload path: https://somsight.com/measuremyplatform/Upload/UploadXML

You will find the “Database name” under Settings:




After you fill out all required information, the following should appear on your screen:

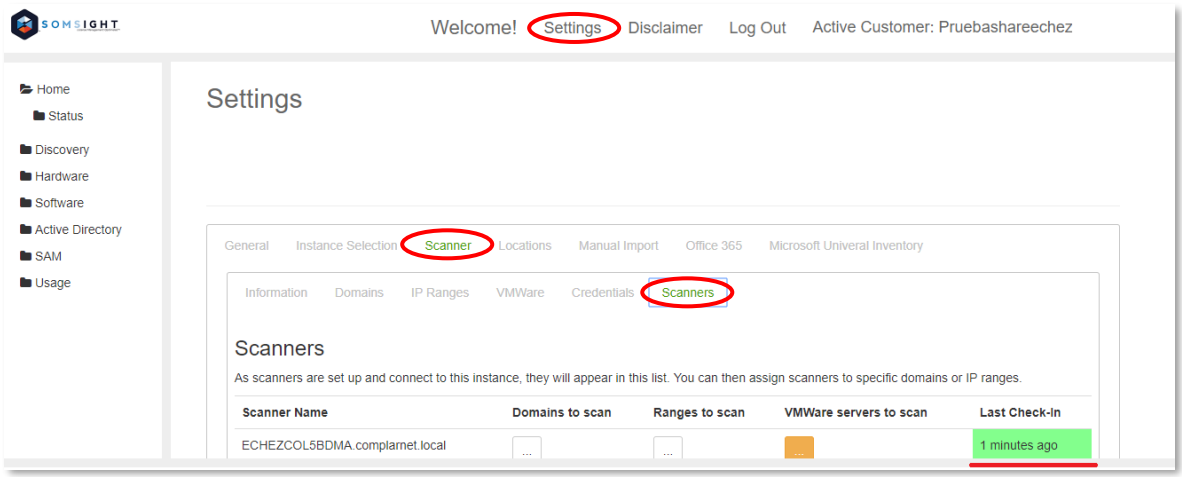



5. Press ***ok*** and ***finish*** and wait 2 minutes for the scanner to restart

**Important: If you use a proxy server or firewall, please make sure to configure it as follows:**

**Set port 443, 80 and 135 (wmi) to allow upload information from on the machine where you install the scanner.**

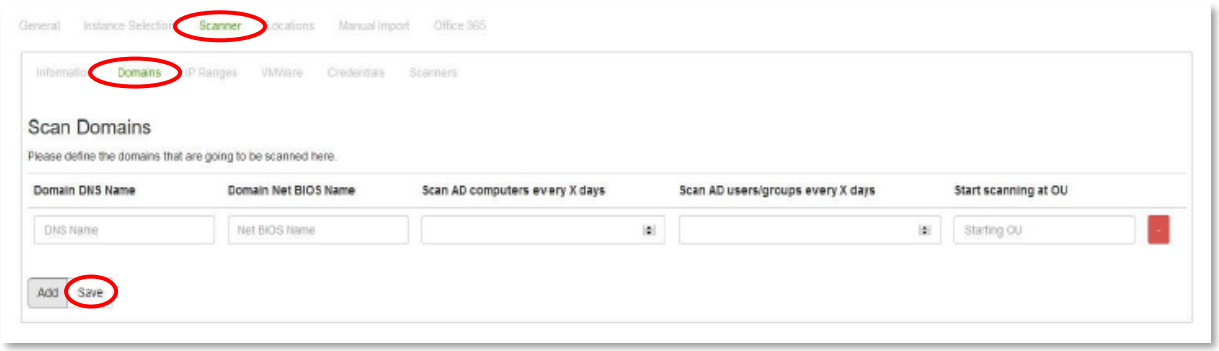
After the scanner has restarted, go to “Settings / Scanner / Scanners”. If there is an entry in the list of scanners and the indicator in the field named “Last Check-in” is green, the scanner is connected and running.




**Note: If the last checking is in read or empty, you need to ensure that you made the process correctly. In case the problem remains please contact us.**

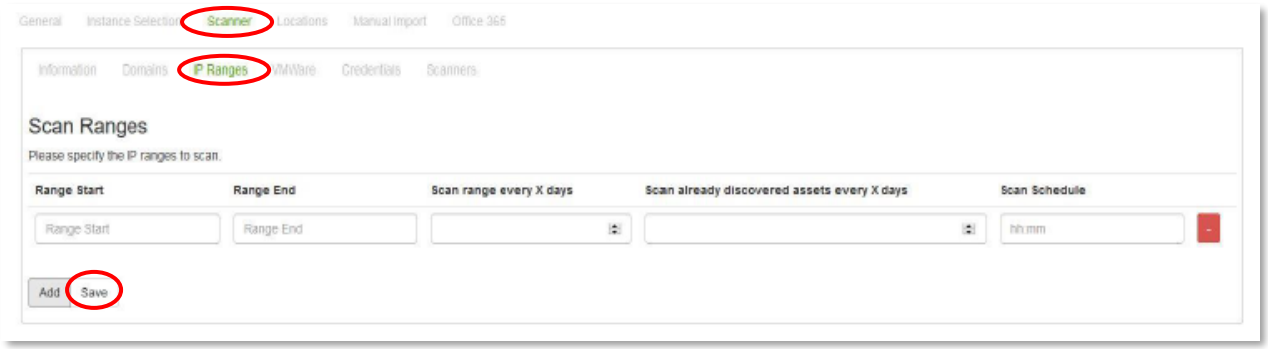
6. Next, select the tab Domain to enter the domains that need to be scanned.

The recommended scanning frequency is 5 days for computers and 1 day for users/groups Enter 5 in “Scan AD computers” and 1 in “Scan AD users/groups”.

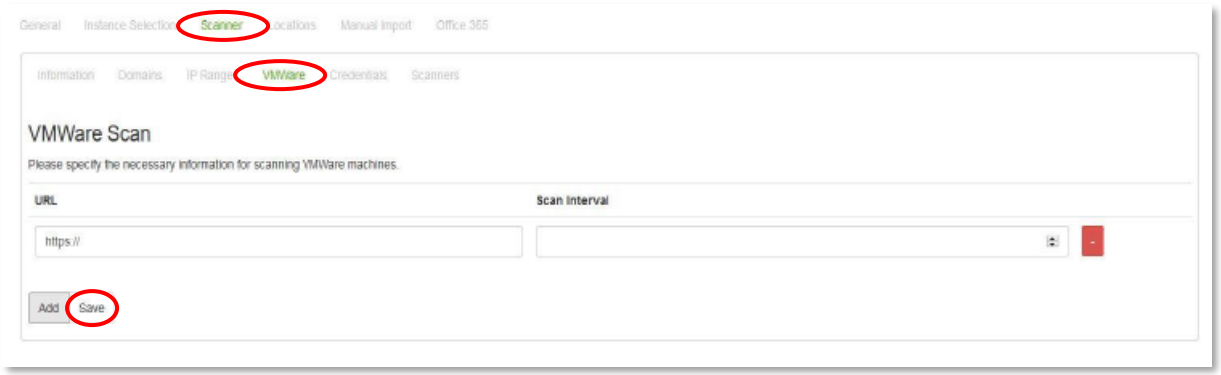



**Optional**: If there are devices that are not members of the domain(s) configured, enter their corresponding IP ranges in the **IP Ranges** tab.

Set up the scanning frequency to 1 day for new devices in the IP address ranges and 5 days for already discovered assets. Enter 1 in “Scan range” and 5 in “Scan already discovered assets”.

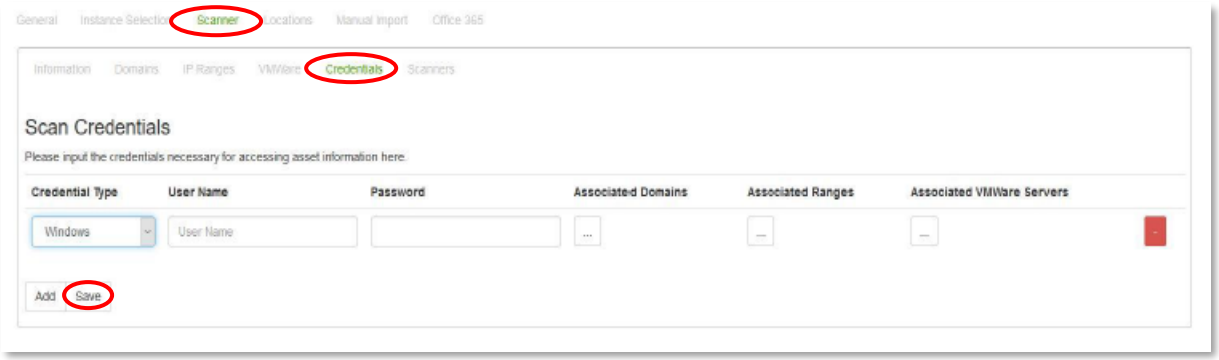



7. Next, enter the vCenter URL(s) in the VMware tab. Usually this is the address that you have typed into the address field of your browser when using the vCenter web application to connect to a vCenter instance followed by “/sdk” (e.g. https://my-vCenter-instance.com/sdk ).

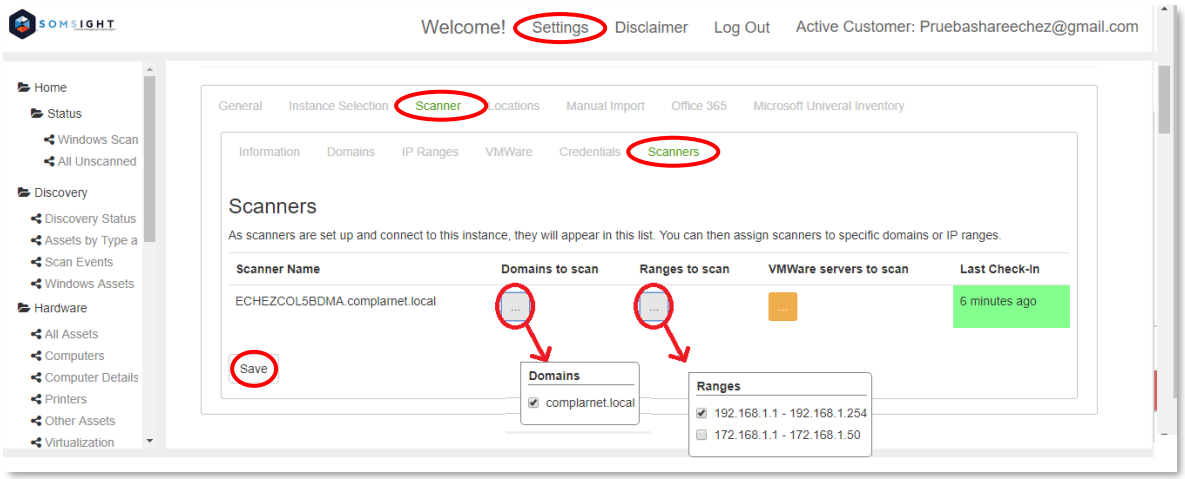



8. The next step is to enter your Credentials. Please make sure that the credentials you enter are correct and that they have administrative privileges on all the devices that will need to be scanned. You may enter as many credential sets as you like and as may be necessary. You can use the assign buttons in the tab Credentials, ensuring that only potentially correct credentials are used for domains and/or IP ranges.

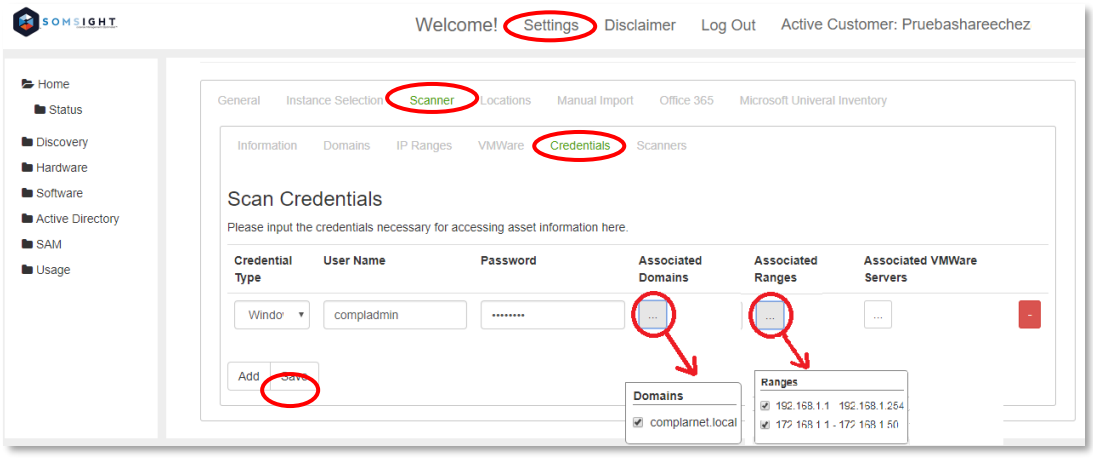
# Scanner install guide




9. Assign domains, IP ranges and vCenters to your scanner(s) to activate the scans. Use the tab Scanners under “Settings / Scanner”.

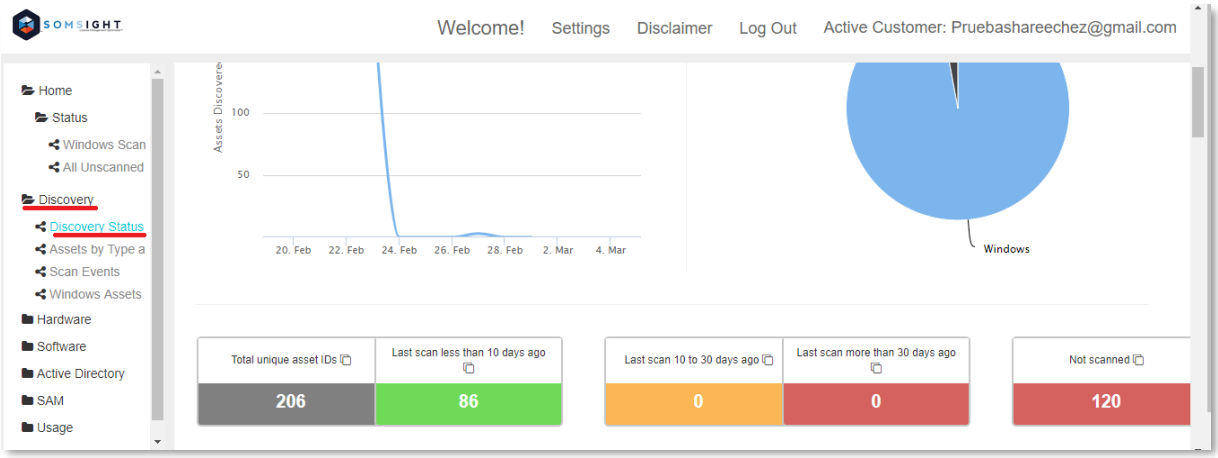



10. Lastly, assign domains, IP ranges and vCenters to appropriate credentials. Go to “Settings/Scanner/Credentials” and fill out the admin credential which allows for the agent execution.

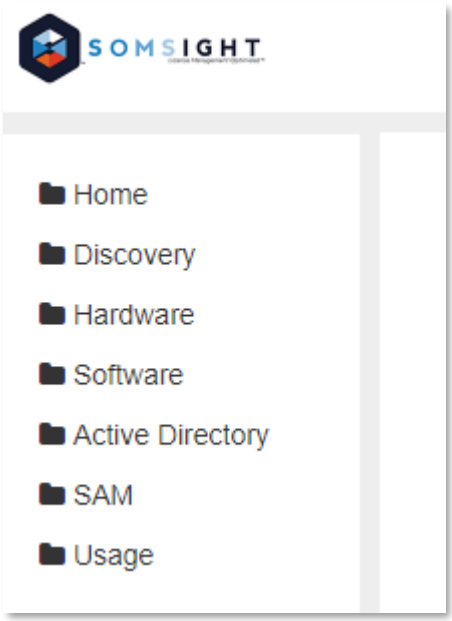


# Scanner install guide

11. After 2 hours you should begin to receive information. To check the scan progress in the left tabs, go to “Discovery/Discovery Status”




12. In the left tabs, you will find information regarding the scan process on your network:




**Home:** Information about the windows devices found by the scanner

**Discovery:** Information about the discover status in your network

**Hardware:** Information about the assets, (i.e. manufacturer)

**Software:** Information about the software and services installed in your network

**Active Directory:** See AD information

**SAM: The best** tool to manage licenses and improve your SAM exercise