Network Discovery Tool

Quick Guide – First Steps

Content

Introduction 3

1. First Steps 4

1.1 Credentials 5

1.2 Scan 5

1.3 Scan process 6

2. Network Discovery Tool Tabs 7

2.1 Asset 7

2.2 Scan 12

2.3 Export 16

3. Contact 17

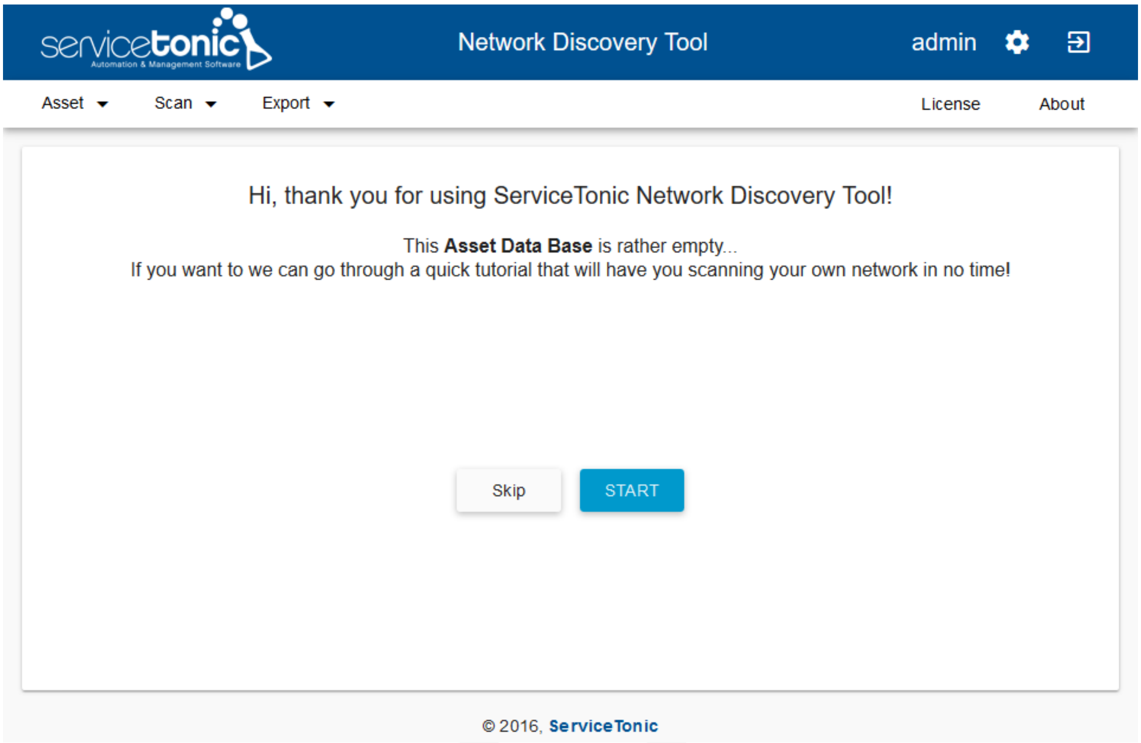
Introduction

ServiceTonic Network Discovery Tool is an enterprise solution that automates asset discovery* and inventory building visual dependency mapping of all the devices and applications used in your company such as computers, servers, monitors, printers and application software.

ServiceTonic Network Discovery Tool seamlessly integrates with ServiceTonic’s CMDB, giving network managers greater control over their IT infrastructure, predicting changes and being ready for audits.

* Windows devices.

1. First Steps



Hi, thank you for using ServiceTonic Network Discovery Tool!

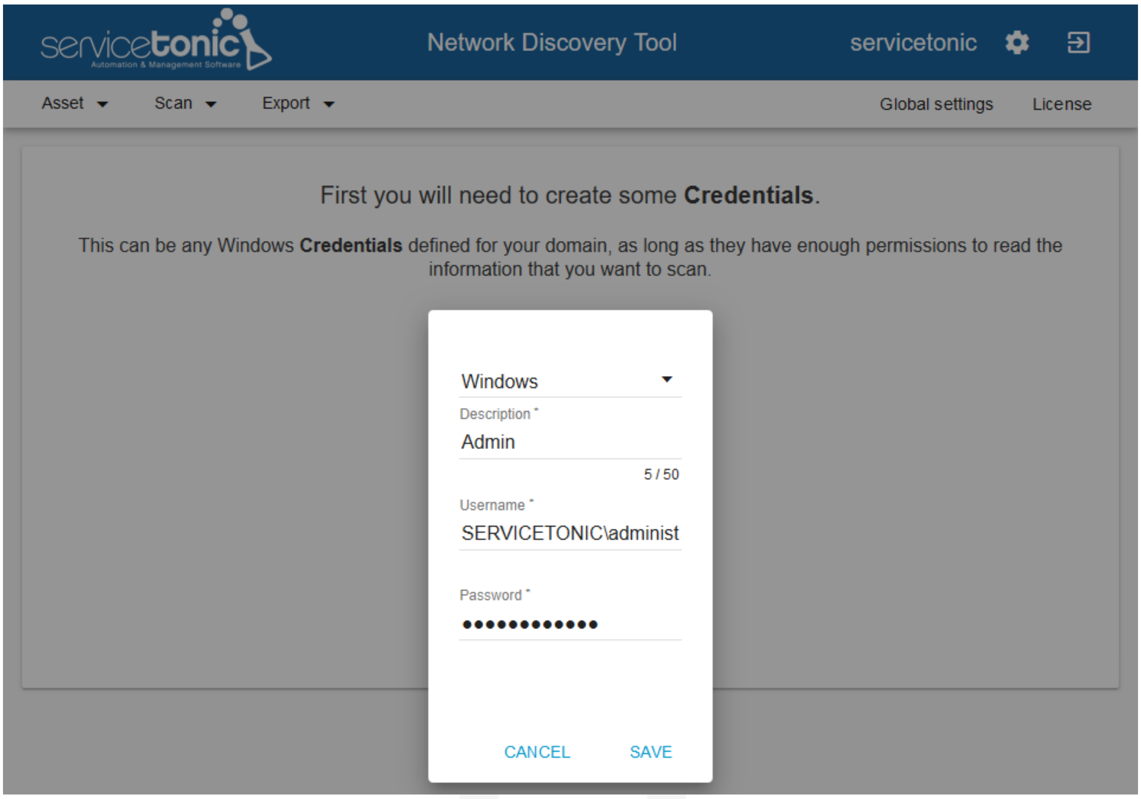
This **Asset Data Base** is rather empty...
If you want to we can go through a quick tutorial that will have you scanning your own network in no time!

© 2016, ServiceTonic

The first time you access ServiceTonic Network Discovery Tool you will be presented a short tutorial to configure the first scan of your network.

It is recommended that you use the tutorial to get started as quickly as possible.

1.1 Credentials



First you will need to create some **Credentials**.

This can be any Windows **Credentials** defined for your domain, as long as they have enough permissions to read the information that you want to scan.

Windows

Description *
Admin
5 / 50

Username *
SERVICETONIC\administ

Password *
●●●●●●●●●●●●

To perform a scan, you have to enter credentials defined for your domain.

- Make sure that with the entered credentials you can access all the computers you are trying to scan.
- Username must be like DOMAIN\USERNAME
- You can define different credentials and use each one on different scans.
- Enter a description to differentiate it from other saved credentials.
- Click on **Save** to keep your changes.

1.2 Scan

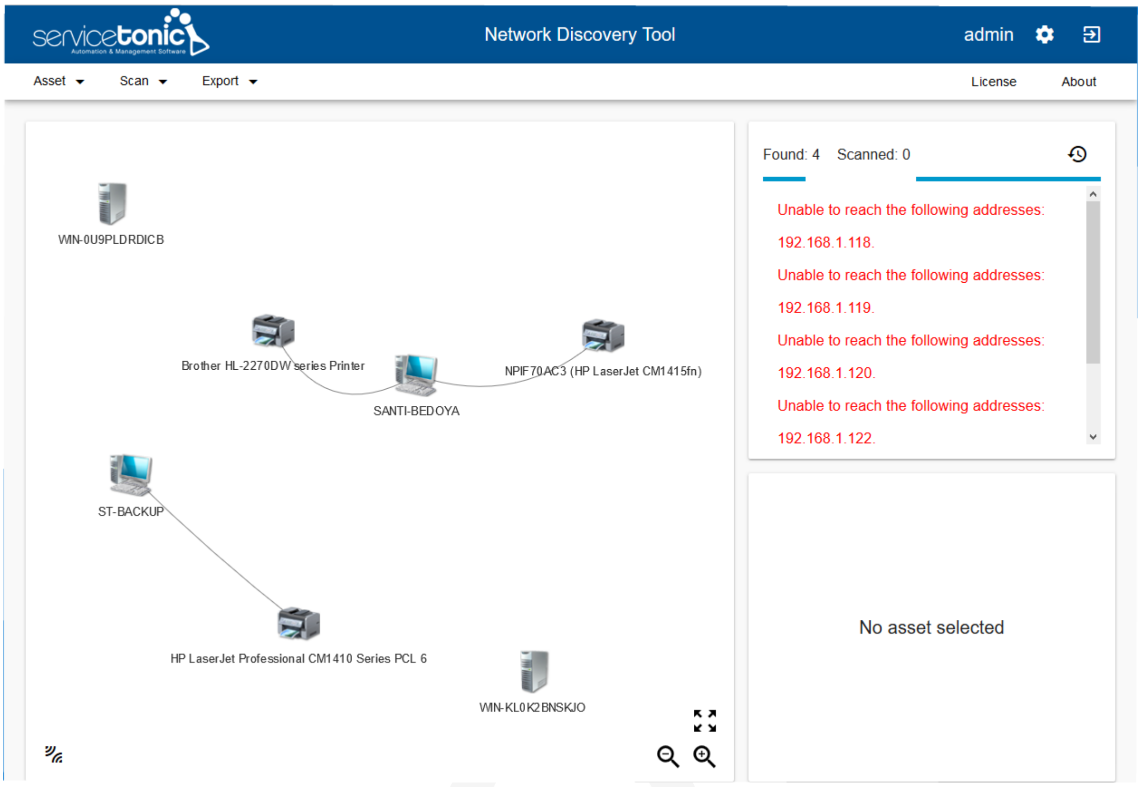
Specify the computers to be scanned.

- Enter a description which will be used to identify the scan process, a valid IP range and click on **Save** to keep your changes.
- It is not necessary to schedule the scan since this scan will be launched manually in the next step.

1.3 Scan process

Click on “Execute” to launch the scan process.

This window will show the information of the different devices found.


Network Discovery Tool
admin
Asset
Scan
Export
License
About
WIN-0U9PLDRDICB
Brother HL-2270DW series Printer
NPIF70AC3 (HP LaserJet CM1415fn)
SANTI-BEDOYA
ST-BACKUP
HP LaserJet Professional CM1410 Series PCL 6
WIN-KL0K2BNSKJO

Found: 4 Scanned: 0

Unable to reach the following addresses:

192.168.1.118.

Unable to reach the following addresses:

192.168.1.119.

Unable to reach the following addresses:

192.168.1.120.

Unable to reach the following addresses:

192.168.1.122.

No asset selected

On the list to the right you can see information in real time about the scan process.

It will indicate if ping fails, if the device connection was successful or if there were any errors (firewall blocking or credential failure).

By clicking on the clock icon, you can see the full detail of the scan.

***Important:** The scan process runs in background-mode so you can let the scan run and surf across other tabs meanwhile.*

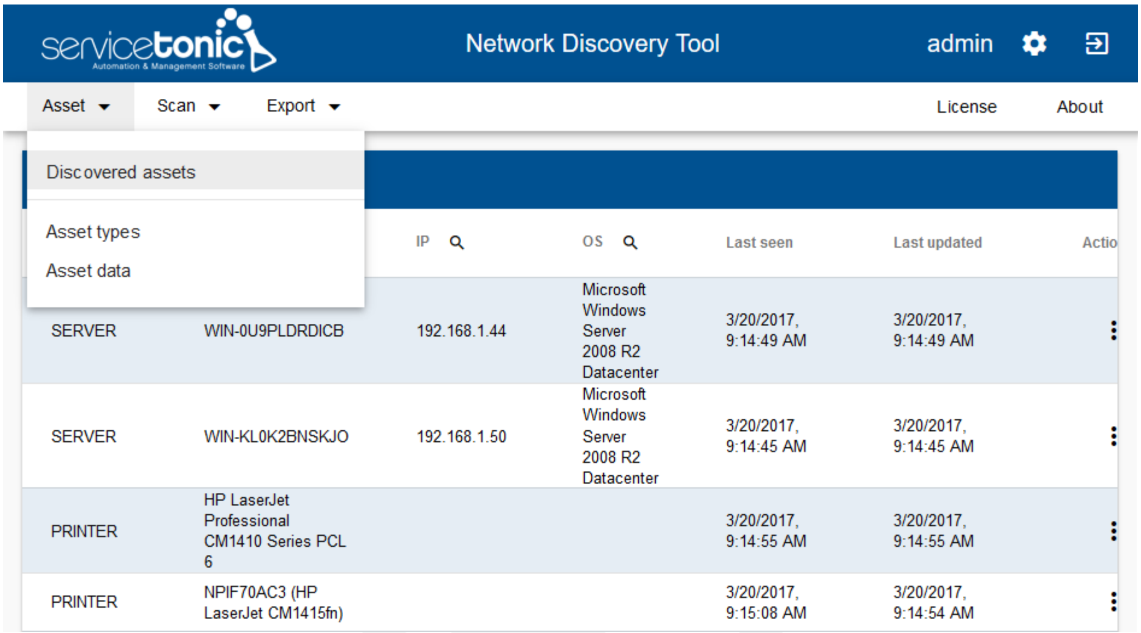
2. Network Discovery Tool Tabs

Each tab that make up Network Discovery Tool is described in detail below.

2.1 Asset

It allows access to the list of discovered assets as well as modify the scan frequency by type and data.

2.1.1 Discovered Assets



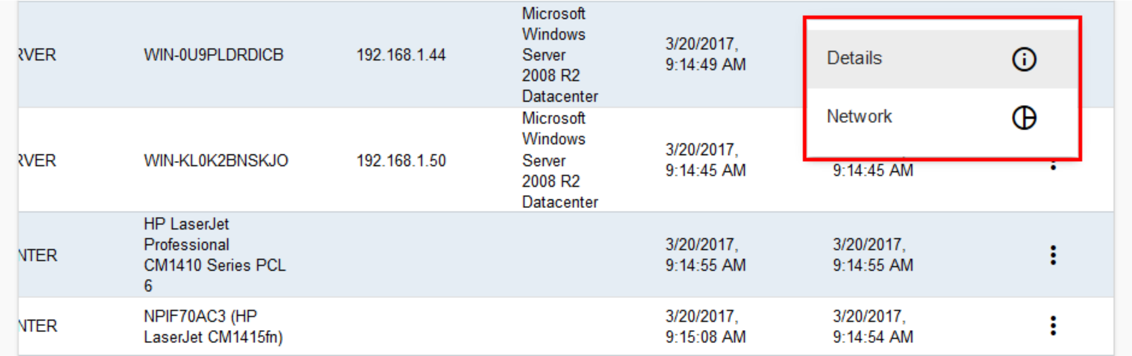
		IP	OS	Last seen	Last updated	Actio
SERVER	WIN-0U9PLDRDICB	192.168.1.44	Microsoft Windows Server 2008 R2 Datacenter	3/20/2017, 9:14:49 AM	3/20/2017, 9:14:49 AM	⋮
SERVER	WIN-KL0K2BNSKJO	192.168.1.50	Microsoft Windows Server 2008 R2 Datacenter	3/20/2017, 9:14:45 AM	3/20/2017, 9:14:45 AM	⋮
PRINTER	HP LaserJet Professional CM1410 Series PCL 6			3/20/2017, 9:14:55 AM	3/20/2017, 9:14:55 AM	⋮
PRINTER	NPIF70AC3 (HP LaserJet CM1415fn)			3/20/2017, 9:15:08 AM	3/20/2017, 9:14:54 AM	⋮

The list shows the most common values such as Device Type, Name, IP Address and Operating System.

You can filter the devices by using the column header to search for a specific IP, machine name, or display only certain types of devices in the list.

Previously applied filters will be maintained each time you access the list of discovered assets.

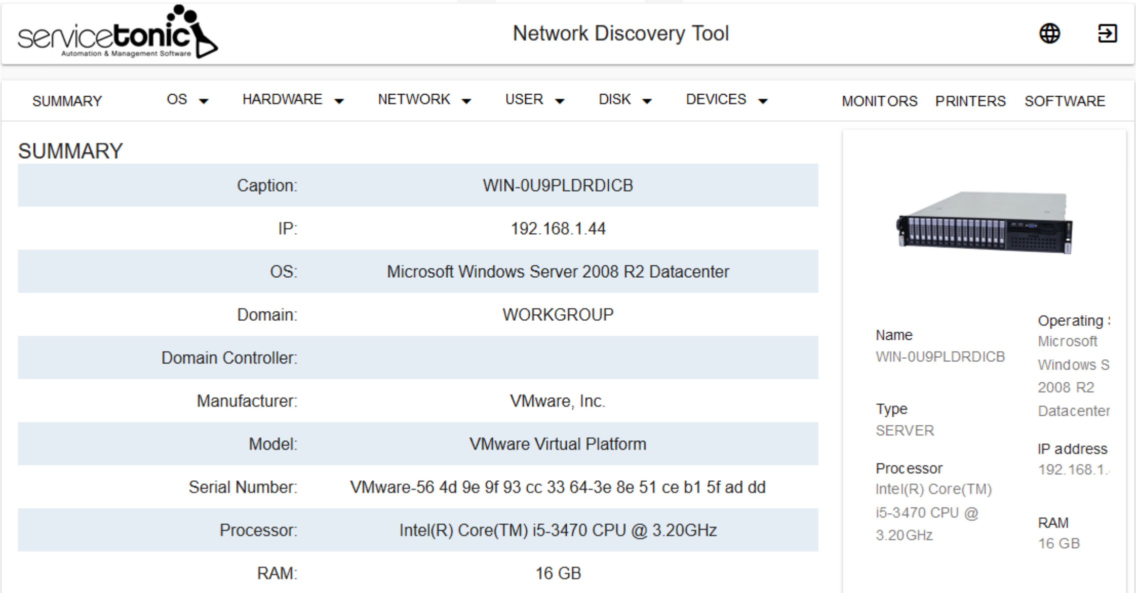
View more information about the asset clicking on Scan > Scanned assets > Actions



RVER	WIN-0U9PLDRDICB	192.168.1.44	Microsoft Windows Server 2008 R2 Datacenter	3/20/2017, 9:14:49 AM		
RVER	WIN-KL0K2BNSKJO	192.168.1.50	Microsoft Windows Server 2008 R2 Datacenter	3/20/2017, 9:14:45 AM	9:14:45 AM	⋮
NTER	HP LaserJet Professional CM1410 Series PCL 6			3/20/2017, 9:14:55 AM	3/20/2017, 9:14:55 AM	⋮
NTER	NPIF70AC3 (HP LaserJet CM1415fn)			3/20/2017, 9:15:08 AM	3/20/2017, 9:14:54 AM	⋮

- **Details:** Shows OS, Hardware, Network Configuration, Users, Relations, etc ...
- **Network:** Shows Connected Network Elements.

Asset Summary



SUMMARY

Caption:	WIN-0U9PLDRDICB
IP:	192.168.1.44
OS:	Microsoft Windows Server 2008 R2 Datacenter
Domain:	WORKGROUP
Domain Controller:	
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-56 4d 9e 9f 93 cc 33 64-3e 8e 51 ce b1 5f ad dd
Processor:	Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz
RAM:	16 GB

Name
WIN-0U9PLDRDICB

Operating :
Microsoft Windows S 2008 R2 Datacenter

Type
SERVER

IP address
192.168.1.

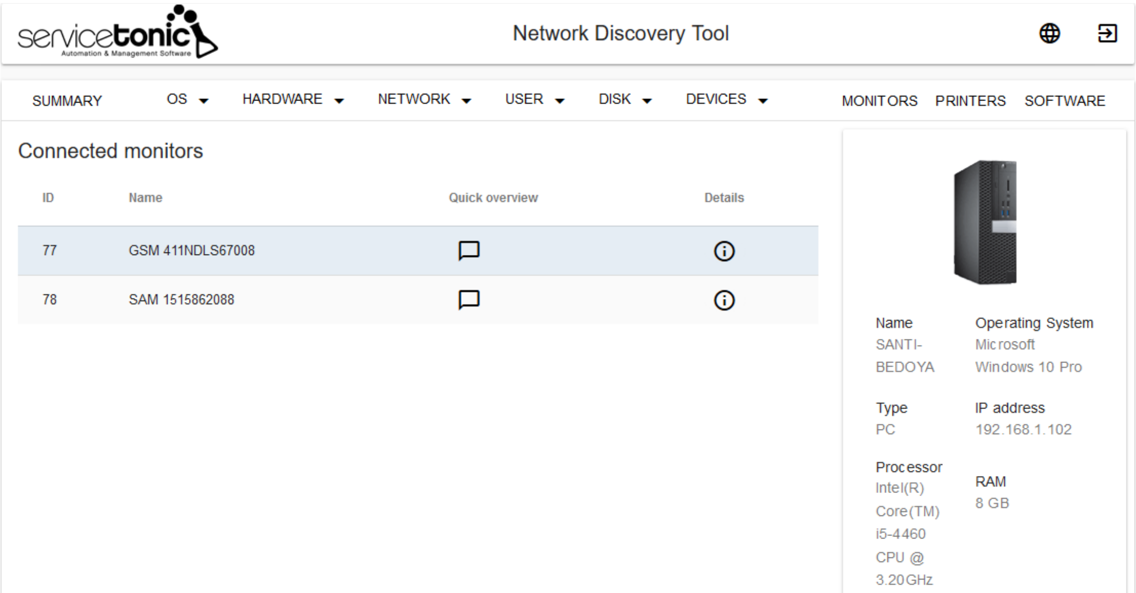
Processor
Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz

RAM
16 GB

In the initial tab, you can see a summary of the most relevant information of the asset as: IP, Operating System and Domain Name.

- You can view more detailed information by accessing:
  - **OS:** Operating System information details.
  - **Hardware**: Hardware details (Processor, RAM, etc).
  - **Net:** Asset Network Adapters details (IP and Mac Address).
  - **User:** Information about the logged user in the asset and on the groups to which it belongs.
  - **HD:** A HD Configuration detail.
  - **Device:** Show other devices like Keyboards & Mice.

- Monitors, Printers and Software buttons show the asset relationship with other existing devices (in the list of assets scanned as independent devices with their own information, you can see the detail by clicking on the corresponding icon).



Connected monitors

ID	Name	Quick overview	Details
77	GSM 411NDLS67008		ⓘ
78	SAM 1515862088		ⓘ

Name
SANTI-BEDOYA

Operating System
Microsoft Windows 10 Pro

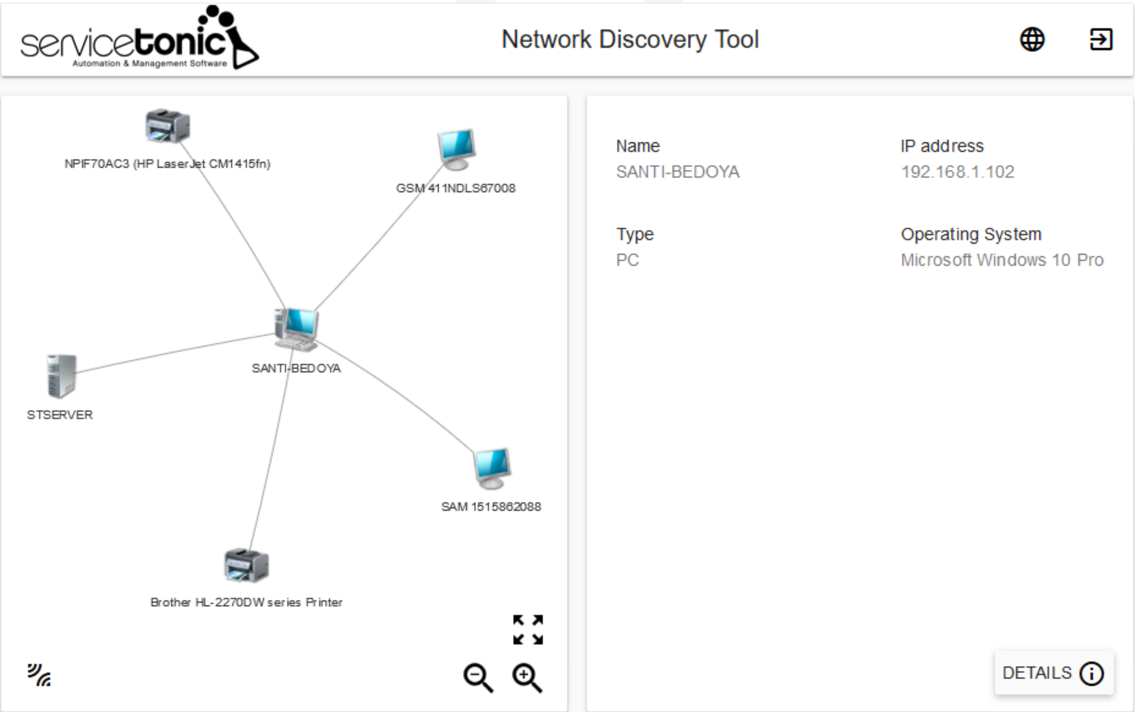
Type
PC

IP address
192.168.1.102

Processor
Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz

RAM
8 GB

- Clicking on the “Details” icon will open a new window displaying graphically the relationships of the selected asset with other devices such as Monitors, Printers, Servers, etc.



Name
SANTI-BEDOYA

IP address
192.168.1.102

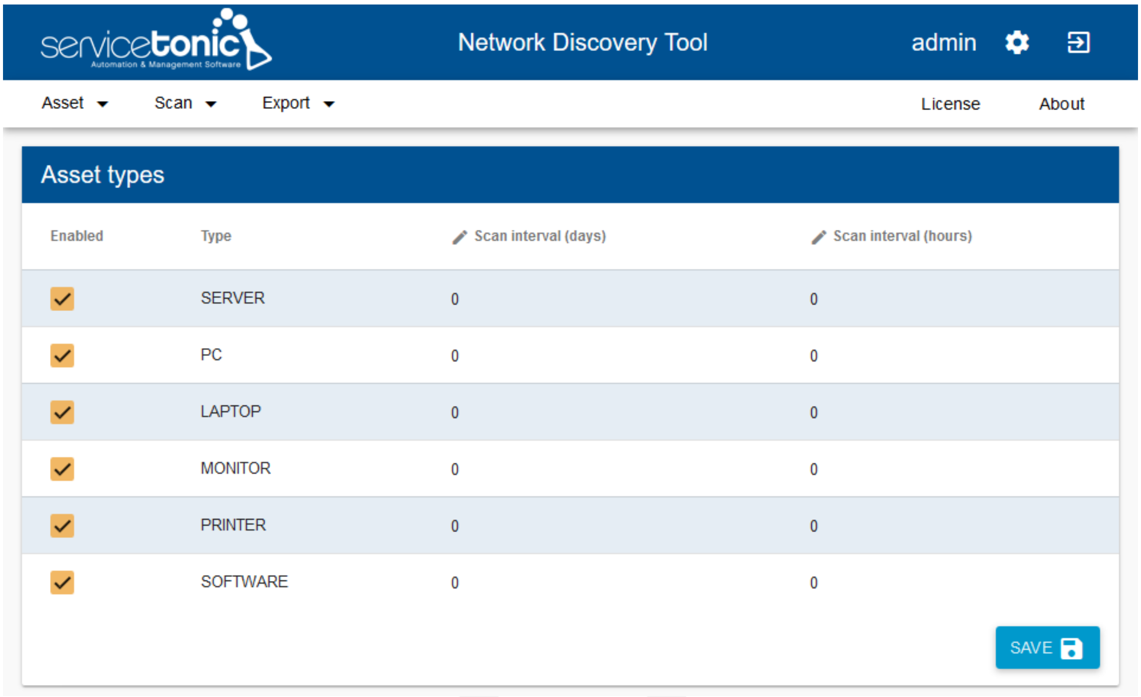
Type
PC

Operating System
Microsoft Windows 10 Pro

In the Network View of the asset you can see all the devices connected to the asset.

- Select a device by clicking on its icon.
- Click on **DETAILS** to see detailed information of the selected device.
- Disable dynamic mode in order to remove graphical animations.

2.1.2 Asset Types



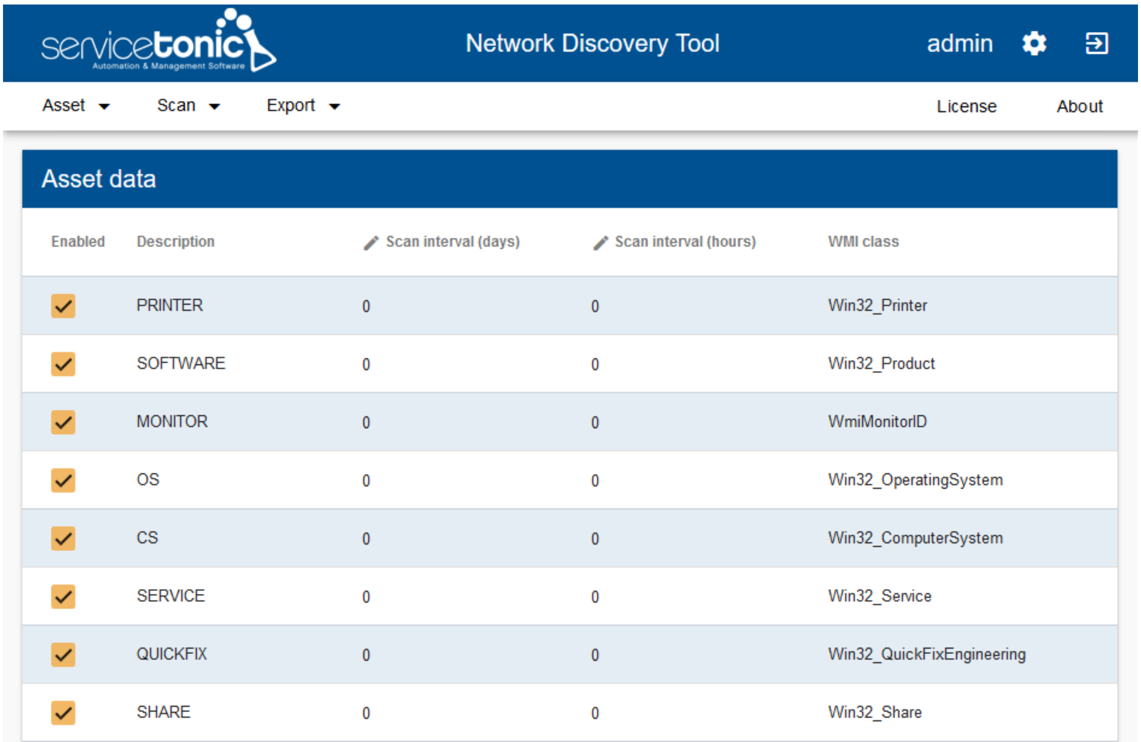
Asset types

Enabled	Type	Scan interval (days)	Scan interval (hours)
☑	SERVER	0	0
☑	PC	0	0
☑	LAPTOP	0	0
☑	MONITOR	0	0
☑	PRINTER	0	0
☑	SOFTWARE	0	0

Enable and disable asset types, manage scan intervals.

- Enable / disable scans for certain types of devices using the checkboxes that are displayed in the window.
- Set a time interval in days / hours by clicking on each column.

2.1.3 Asset Data



Asset data

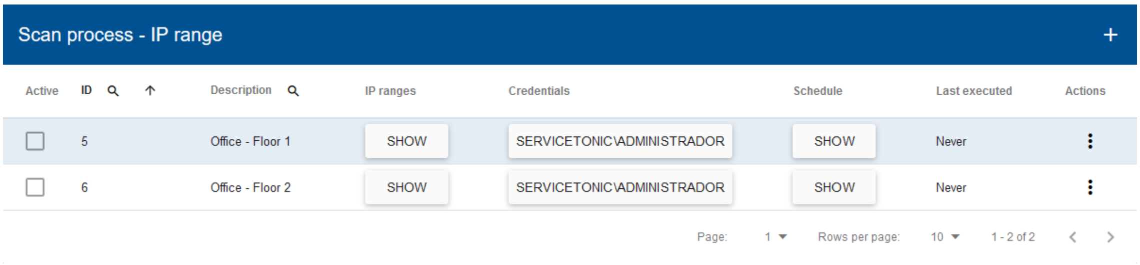
Enabled	Description	Scan interval (days)	Scan interval (hours)	WMI class
☑	PRINTER	0	0	Win32_Printer
☑	SOFTWARE	0	0	Win32_Product
☑	MONITOR	0	0	WmiMonitorID
☑	OS	0	0	Win32_OperatingSystem
☑	CS	0	0	Win32_ComputerSystem
☑	SERVICE	0	0	Win32_Service
☑	QUICKFIX	0	0	Win32_QuickFixEngineering
☑	SHARE	0	0	Win32_Share

Enable / Disable the information to be scanned, configure the scan intervals.

- Enable / Disable scans for certain types of data using the checkboxes that are displayed in the window.
- Set a time interval in days / hours by clicking on each column.

2.2 Scan

Access to credential configuration, scanning processes and historical data.



Scan process - IP range +

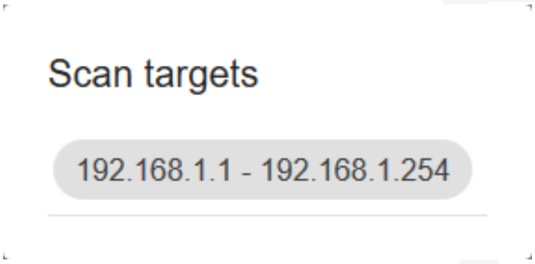
Active	ID	Description	IP ranges	Credentials	Schedule	Last executed	Actions
☐	5	Office - Floor 1	SHOW	SERVICETONIC\ADMINISTRADOR	SHOW	Never	⋮
☐	6	Office - Floor 2	SHOW	SERVICETONIC\ADMINISTRADOR	SHOW	Never	⋮

Page: 1 ▾ Rows per page: 10 ▾ 1 - 2 of 2 ‹ ›

2.2.1 Scan processes

This option will show the configured scanning processes where you can quickly see description, credentials and the last executed scan.

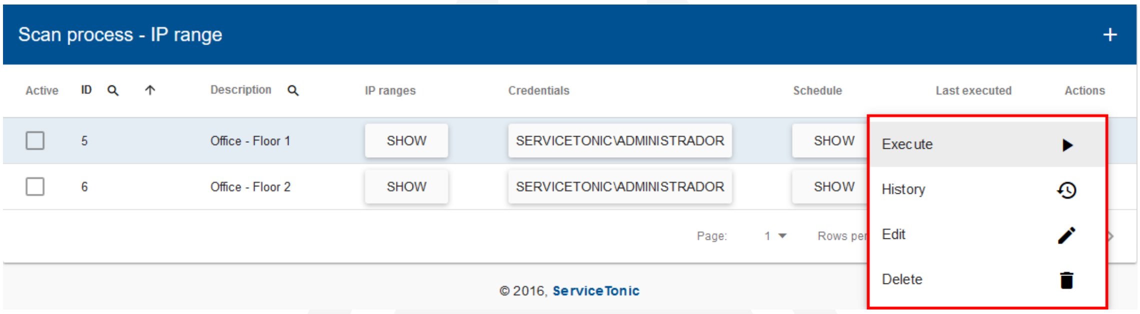
Click the IP Range or Schedule buttons for more details:



Scan targets

192.168.1.1 - 192.168.1.254

Click on the **Actions** icon you to access these options:



Scan process - IP range +

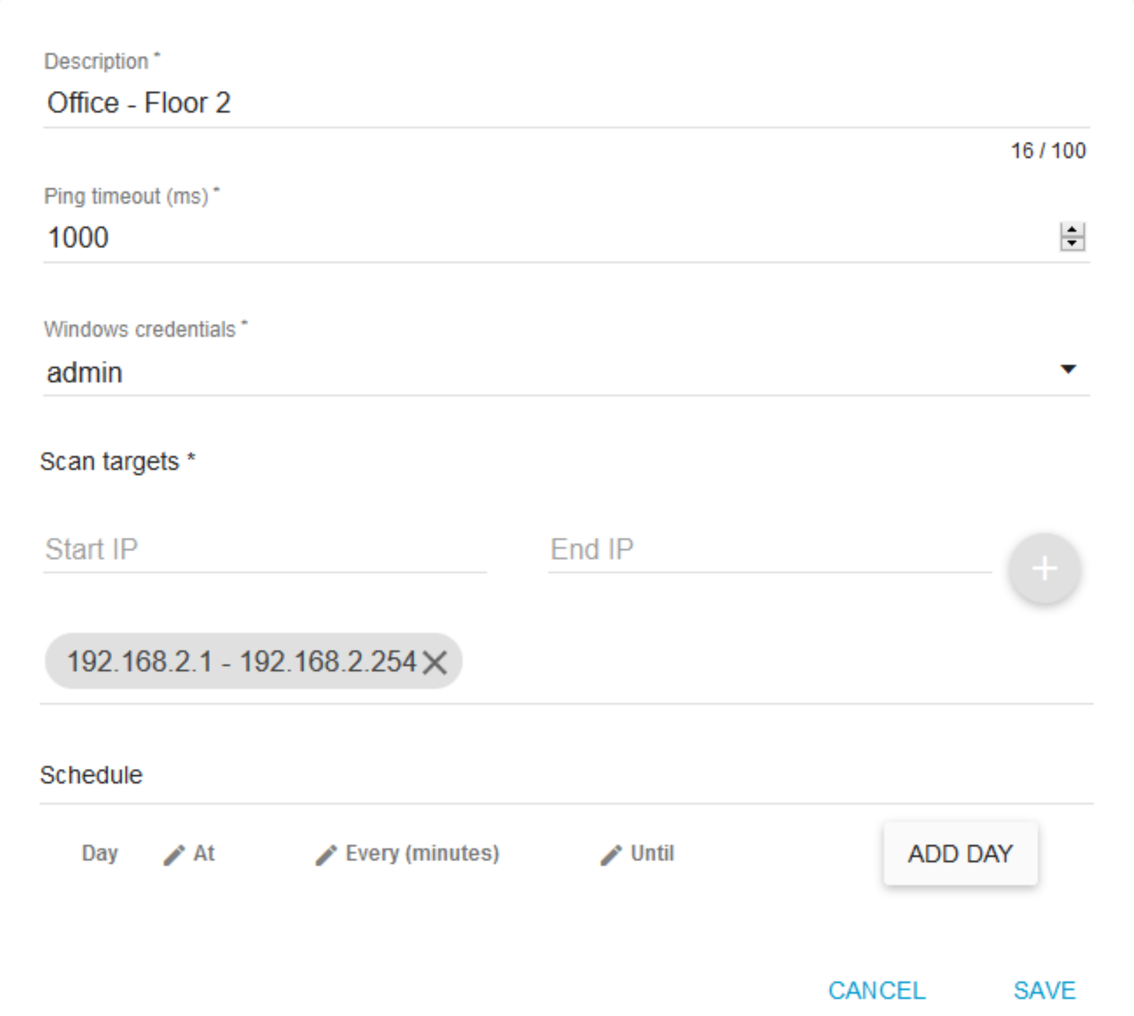
Active	ID	Description	IP ranges	Credentials	Schedule	Last executed	Actions
☐	5	Office - Floor 1	SHOW	SERVICETONIC\ADMINISTRADOR	SHOW		
☐	6	Office - Floor 2	SHOW	SERVICETONIC\ADMINISTRADOR	SHOW		

Page: 1 ▾ Rows per

© 2016, ServiceTonic

- **Execute:** Start the scan process manually.
- **History:** View scan history.
- **Edit:** Modify the scan settings.
- **Delete:** Deletes the scan process.

Clicking on the add (+) icon or edit a scanning process will display the following window:



Description *
Office - Floor 2
16 / 100

Ping timeout (ms) *
1000

Windows credentials *
admin

Scan targets *

192.168.2.1 - 192.168.2.254 ✕

Schedule

You will be able to configure the following features:

- **Description**: Enter a text to identify this scanning process.
- **Ping timeout**: Enter a timeout for the scan. (Min 500ms)
- **Credentials**: Select the credential to use during the selected scan.
- **IP Range:** Enter a valid range of IPs. The **+ (**button**)** will turn blue when you have entered the addresses correctly. Click on it to add the range. You can add multiple ranges of IPs.
- Click **Save** in order to save all the changes.

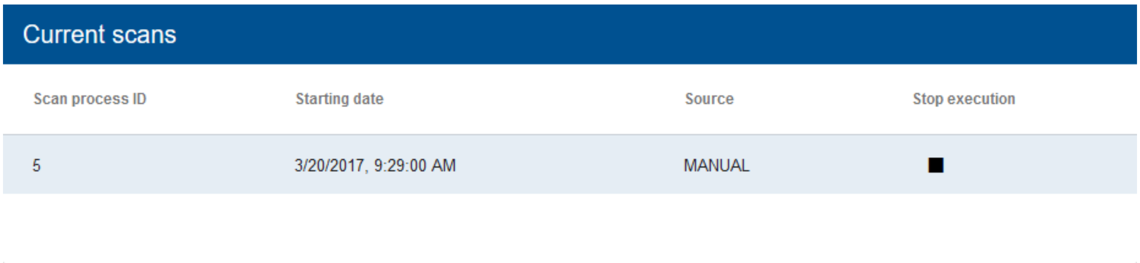
You can also add a schedule to run the scan process automatically.

- **Schedule**: Click on **Add Day** to enter a day/time when the scan process will be launched automatically (allows you to indicate several repetitions per day by selecting **Periodic Execution**). Please enter the time in 24h format.

2.2.2 Current scans

Managing current scans

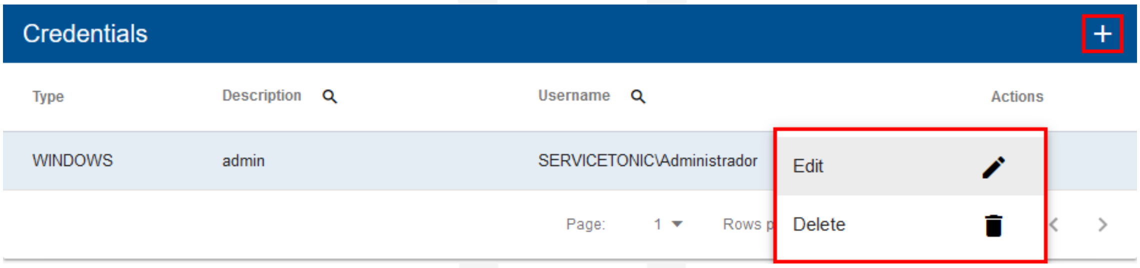
- View the scanning processes in progress.
- Finish a scan by pressing the "**Stop**" button.



Current scans

Scan process ID	Starting date	Source	Stop execution
5	3/20/2017, 9:29:00 AM	MANUAL	■

2.2.3 Credentials



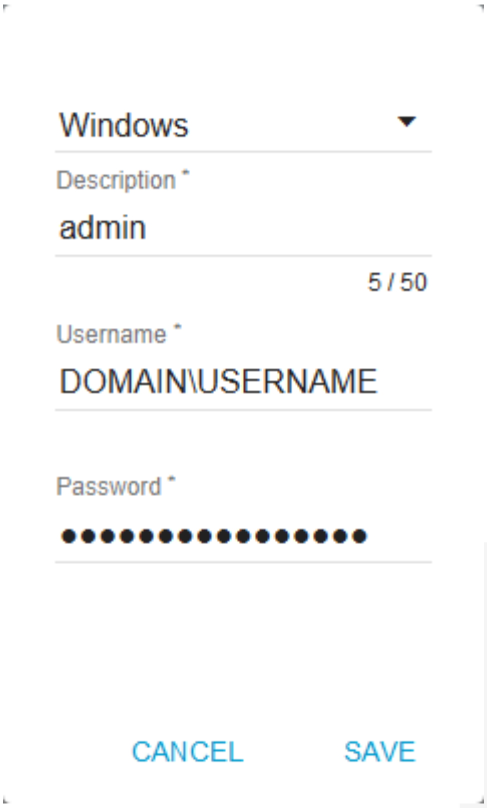
Credentials

Type	Description	Username	Actions
WINDOWS	admin	SERVICETONIC\Administrador	

You can manage your credentials from Scan > Credentials

- You can add new credentials by clicking **+** icon.
- Click the **Actions** button to edit or delete credentials.

When creating / editing the credentials the following screen will be displayed:



Windows

Description *

admin

5 / 50

Username *

DOMAIN\USERNAME

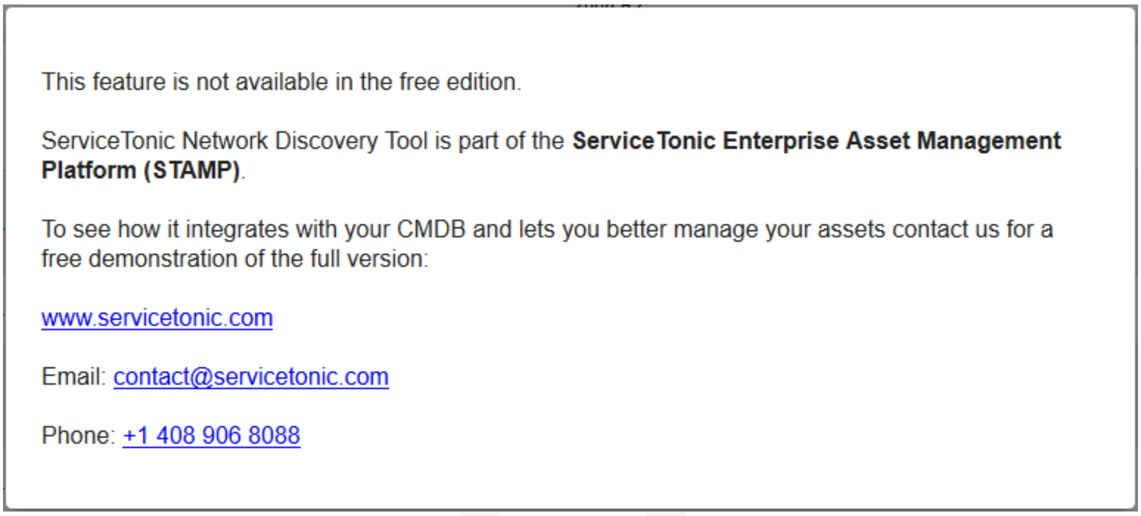
Password *

●●●●●●●●●●●●●●●●

- In the **Description,** you can enter a name to identify this credential.
- In the **Username,** you must indicate the login with which you will try to scan the computers. You must always indicate **DOMAIN \ USERNAME** (it is not necessary for the user to be a domain administrator, it is enough that he can login to the computers).
- Finally enter the **Password** of the previous user.

2.3 Export

2.3.1 Manual



This feature is not available in the free edition.

ServiceTonic Network Discovery Tool is part of the **ServiceTonic Enterprise Asset Management Platform (STAMP)**.

To see how it integrates with your CMDB and lets you better manage your assets contact us for a free demonstration of the full version:

www.servicetonic.com

Email: contact@servicetonic.com

Phone: +1 408 906 8088

The FREE version of ServiceTonic Network Discovery Tool does not have export features so you can't integrate the information into the ServiceTonic's CMDB.

Know more about how you can integrate asset information with your ServiceDesk by contacting ServiceTonic.

3. Contact

For more information please visit us at: https://www.servicetonic.com