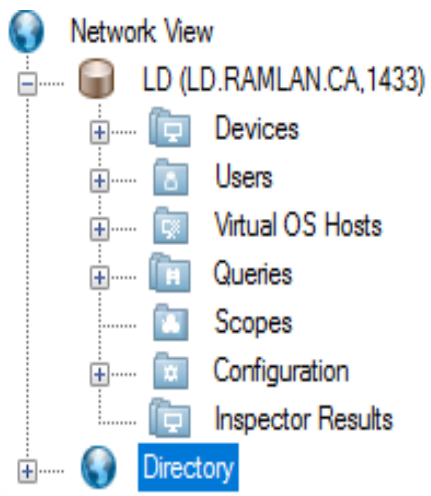
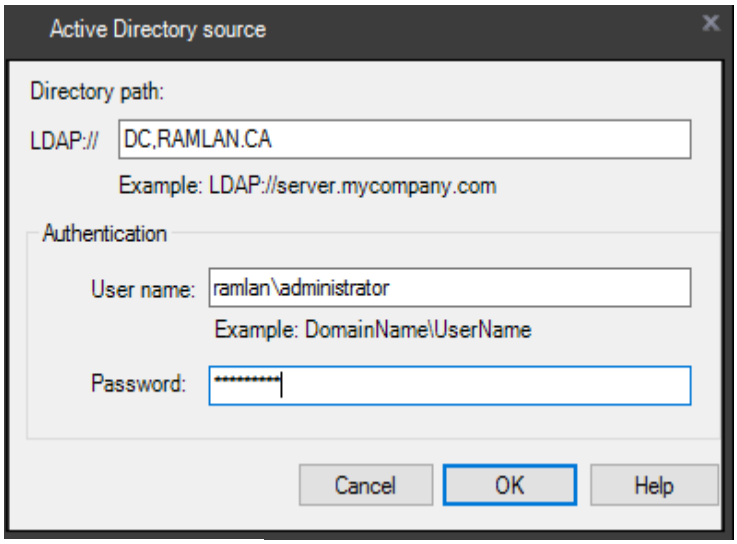
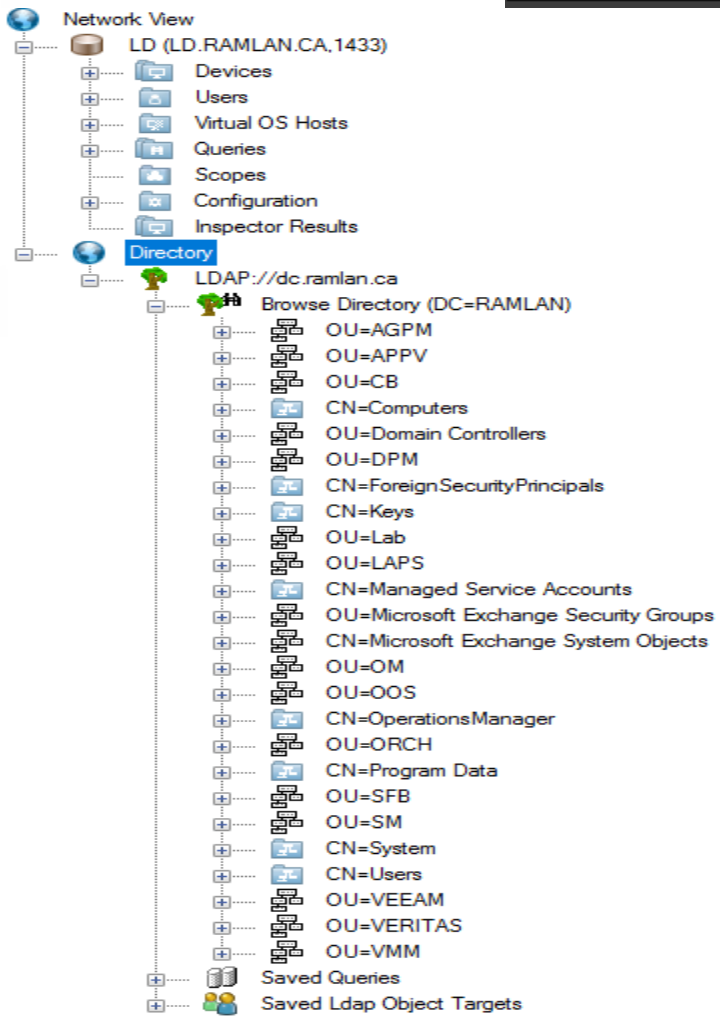
Ivanti Endpoint Manager 2017 – Post Configuration

NETWORK VIEW:

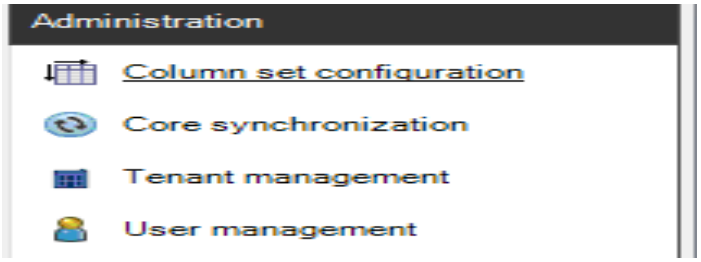
Adding Directory – Right Click Directory – Add





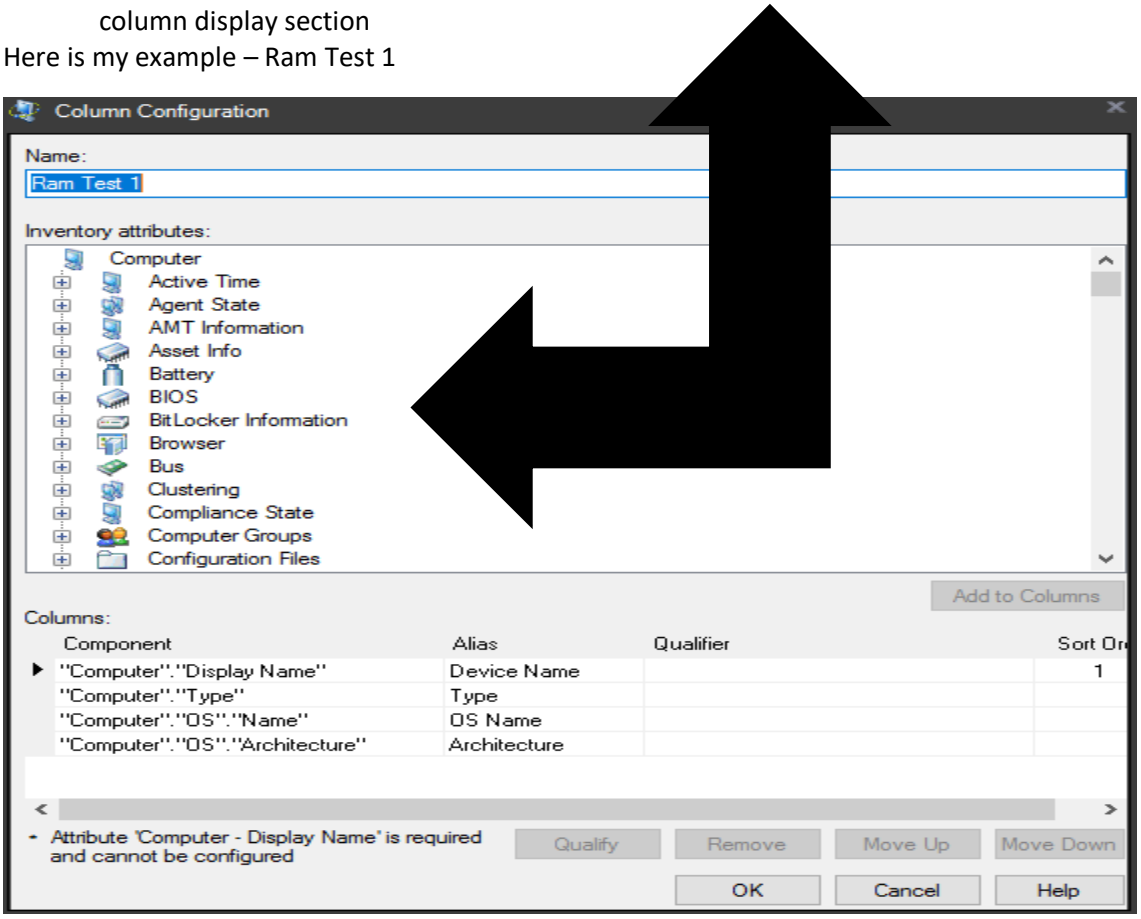


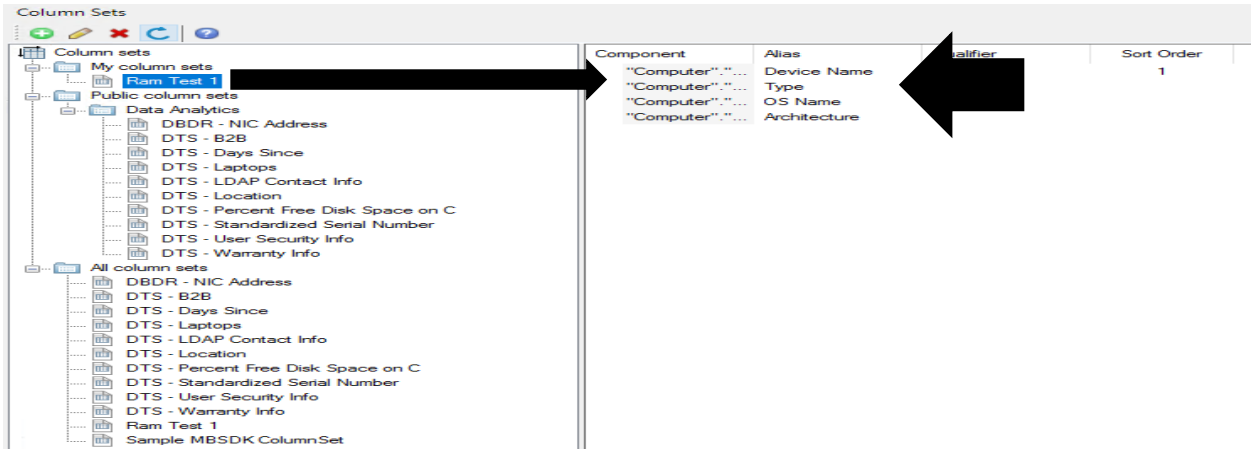
ADMINISTRATION:



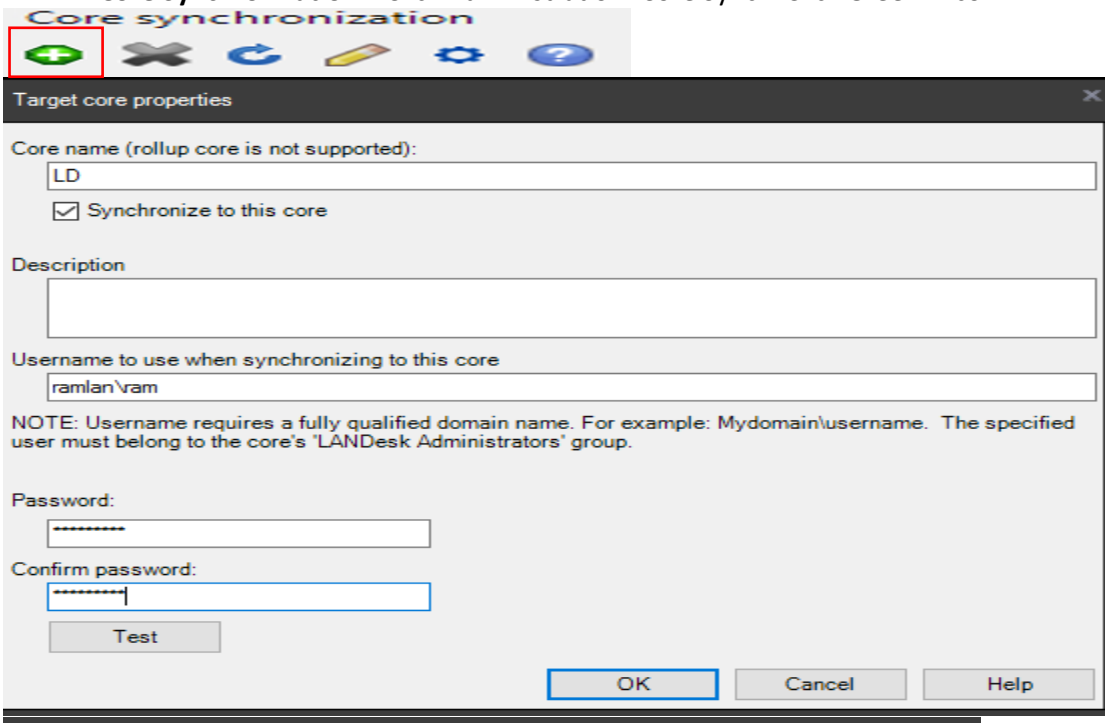
1. **Column Set Configuration** – Click Administration – Column Set Configuration – Select My Column Sets – Right Click – Add – Give a name – From Below select what you want in the column display section

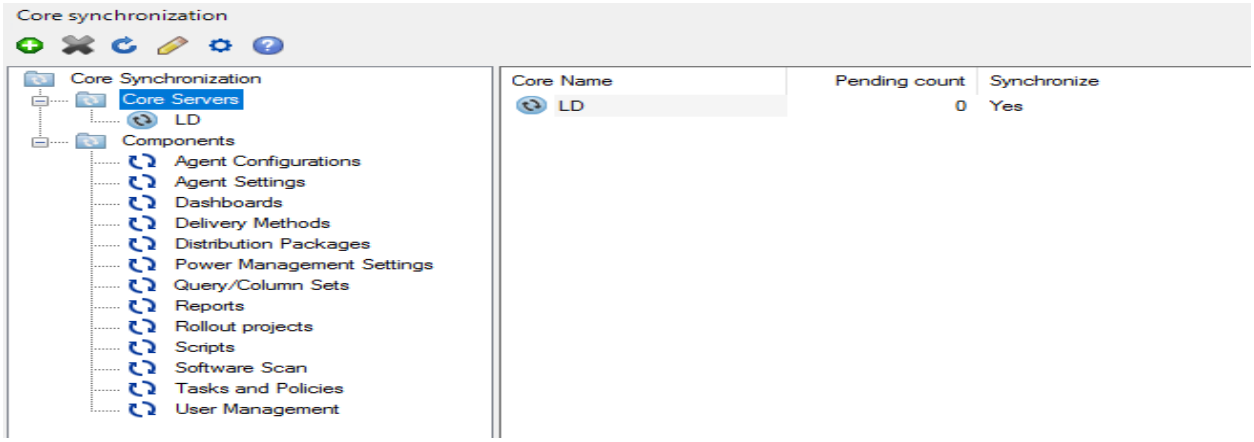
Here is my example – Ram Test 1





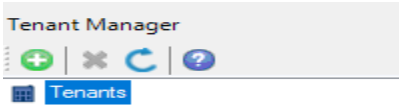
2. **Core Synchronization** – Click Administration- Core Sync – Click Green + icon





Right Click Core Server – You will see below option to enable Auto Sync. This is useful, if you have multiple LanDesk Servers within your environment.

3. **Tenant Management** – Click Administration – Tenant Management



To create a tenant

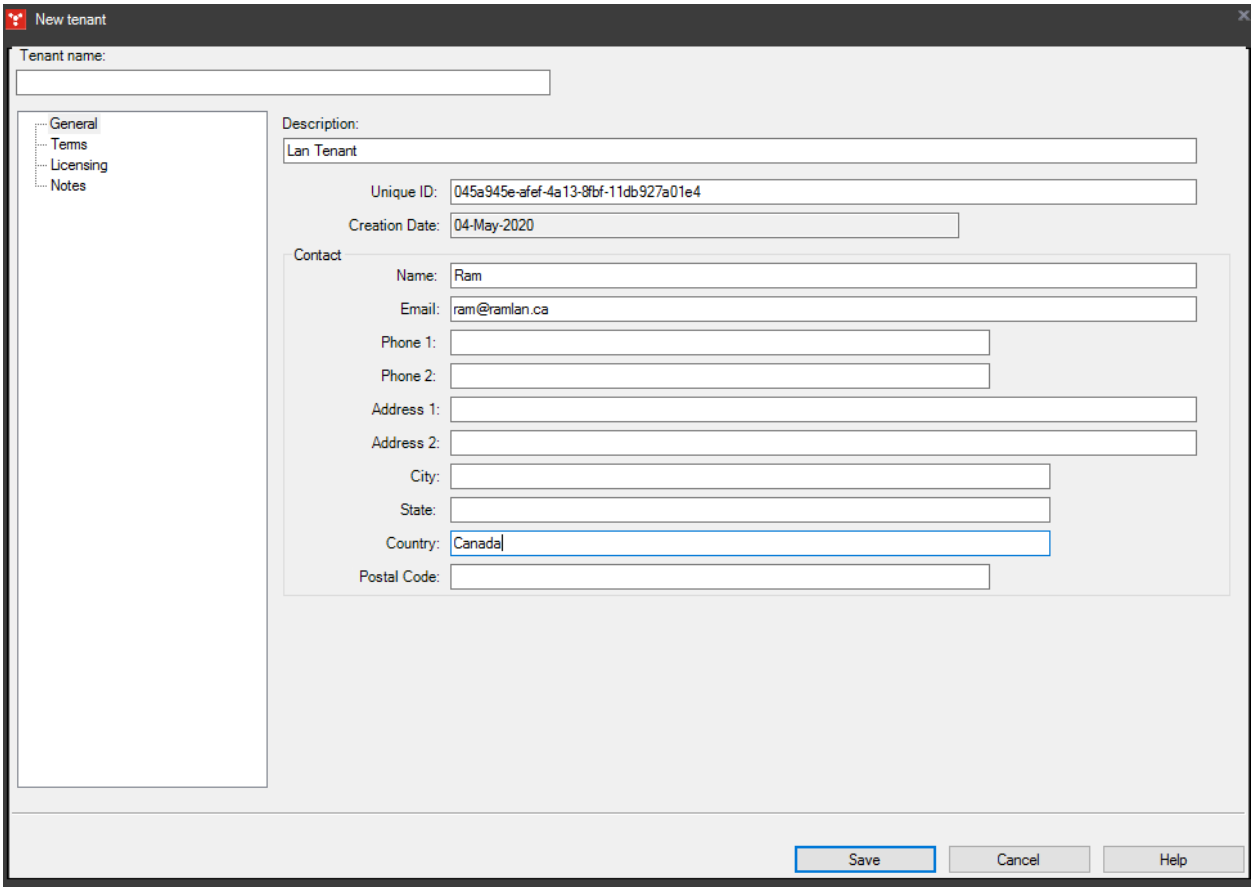
1. Click **Tools** > **Administration** > **Tenant management**.
2. Enter a unique **Tenant name**.
3. Change the **Unique ID** if you don't want to use the random GUID. Valid characters are A-Z, a-z, 0-9, and hyphens.
4. If you want, enter additional data relevant to the tenant.
5. Click **Save**.

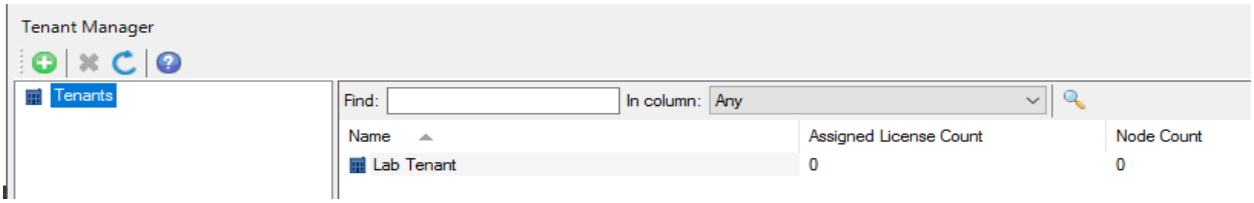
To add console users who will manage the tenant

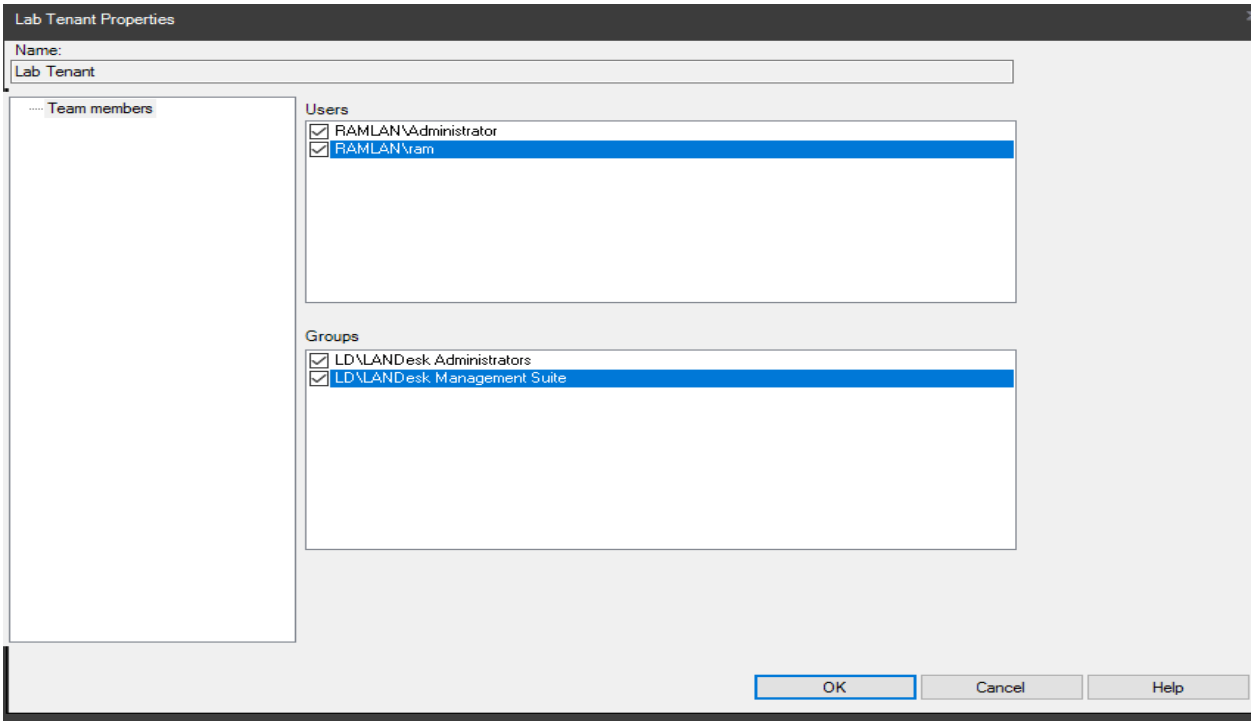
1. Click **Tools** > **Administration** > **User management** > **Teams**.
2. Double-click the new team named after your tenant name.
3. Select the console users who will be managing devices in this tenant.
4. Click **OK**.

To add console users to the tenant's scope

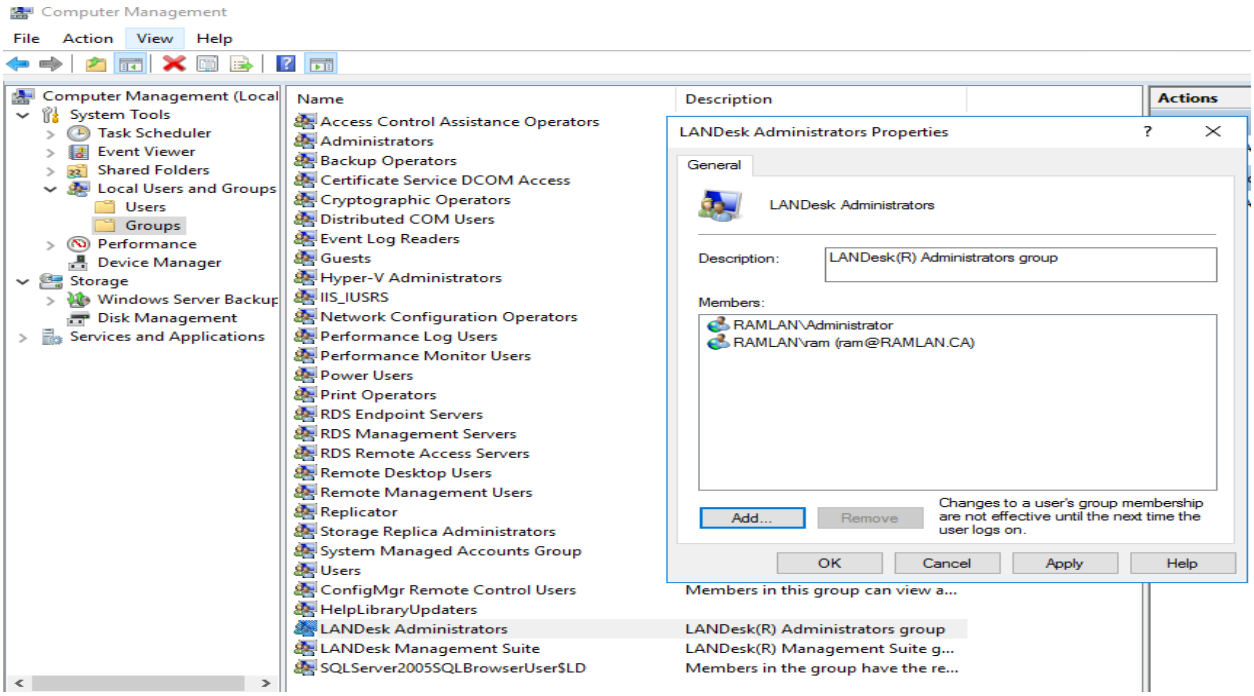
1. Click **Tools** > **Administration** > **User management** > **Scopes**.
2. Right-click the new scope named after your tenant name and click **Properties**.
3. In the **Scope properties** dialog box, select the console users who will be managing devices in this tenant.
4. Click **OK**.







4. **User Management** – Click Administration – User Management

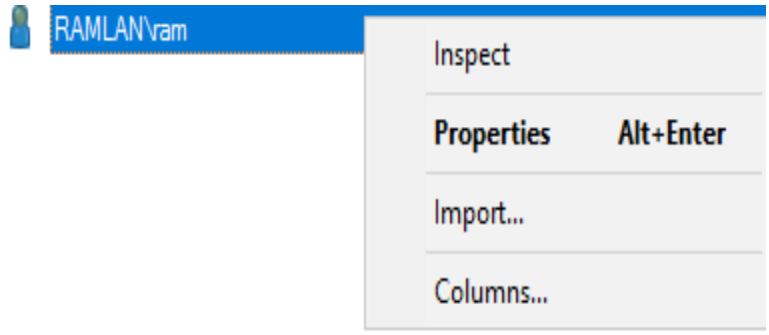


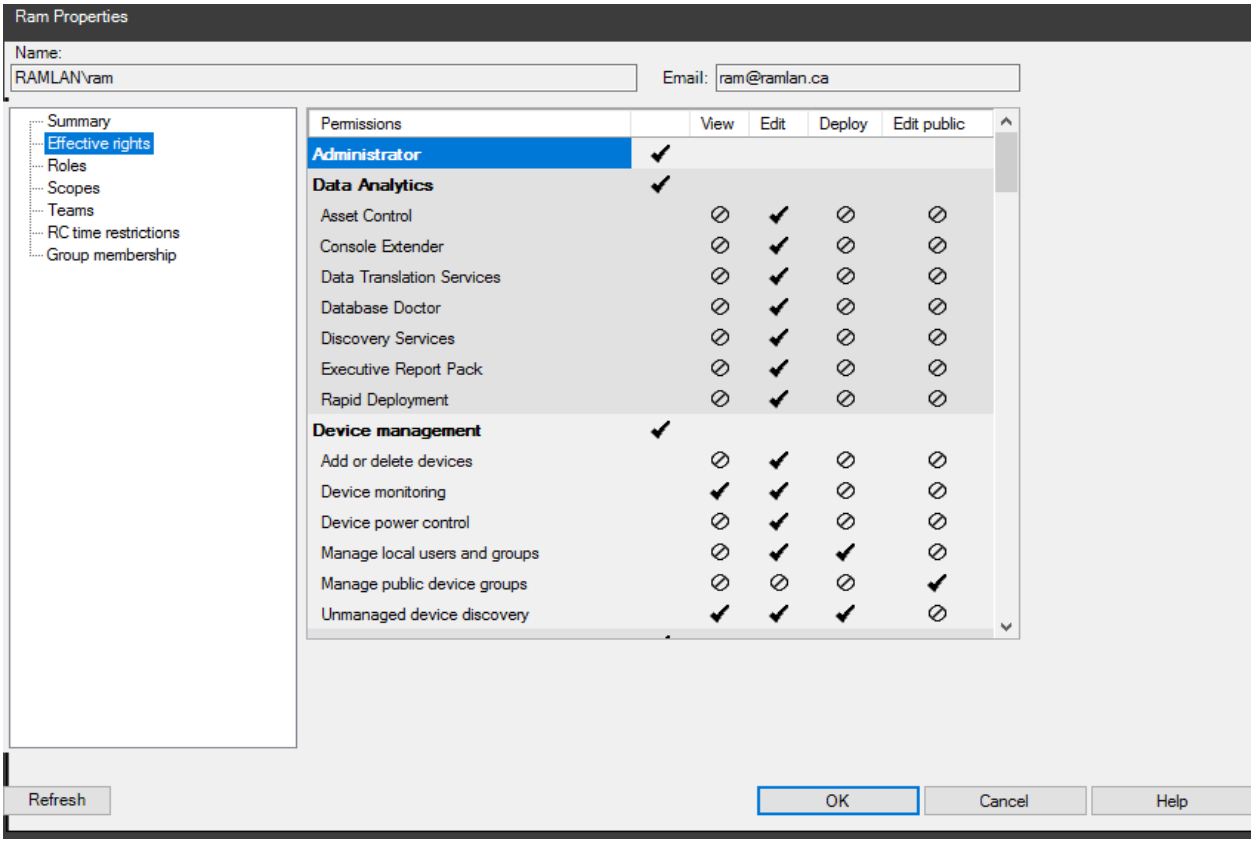
Creating Roles

The following is the basic process for using role-based administration:

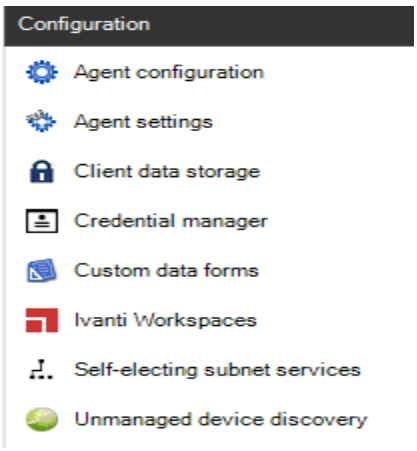
1. Create roles for console users.
2. Use the Windows Local Users and Groups tool to add console users to the appropriate Windows LANDESK groups.
3. Create authentications for each Active Directory you will be using to designate console users.
4. Optionally use scopes to limit the list of devices that console users can manage.
5. Optionally use teams to further categorize console users.

Effective Rights – Select user from User Management – Right Click - Properties

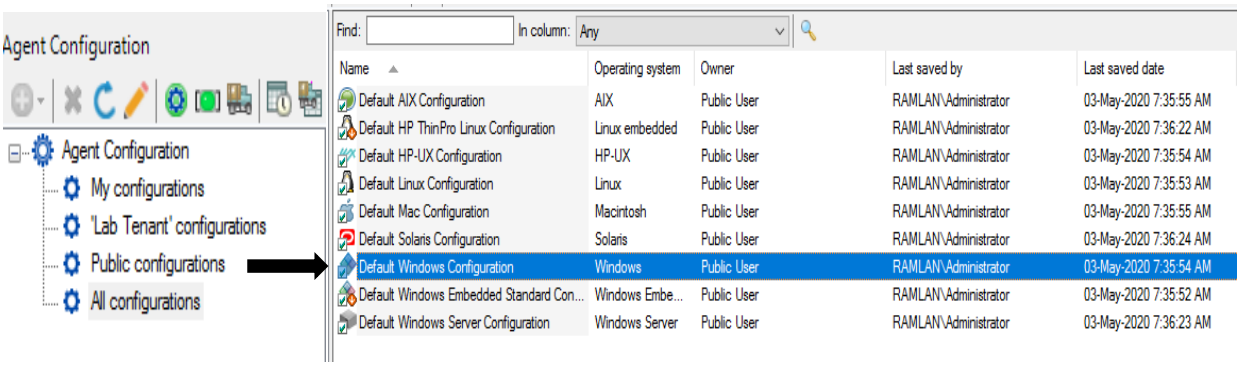


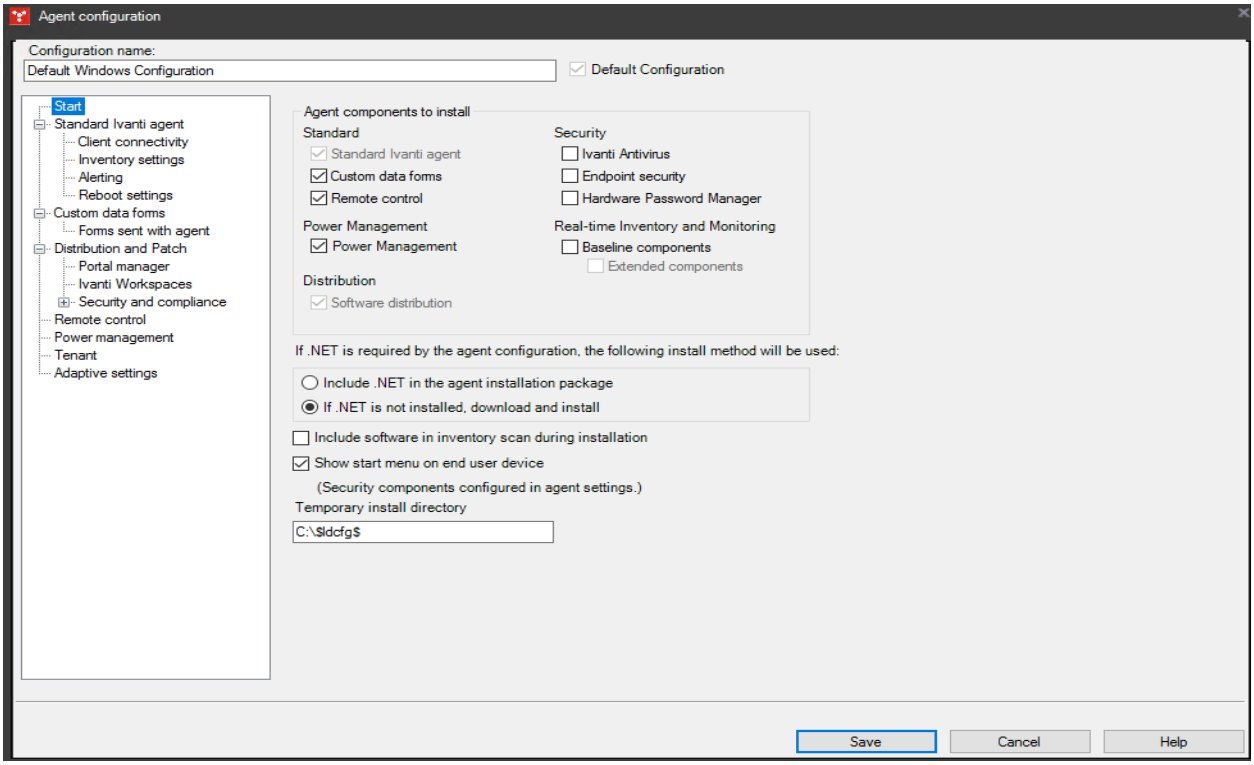


CONFIGURATION:

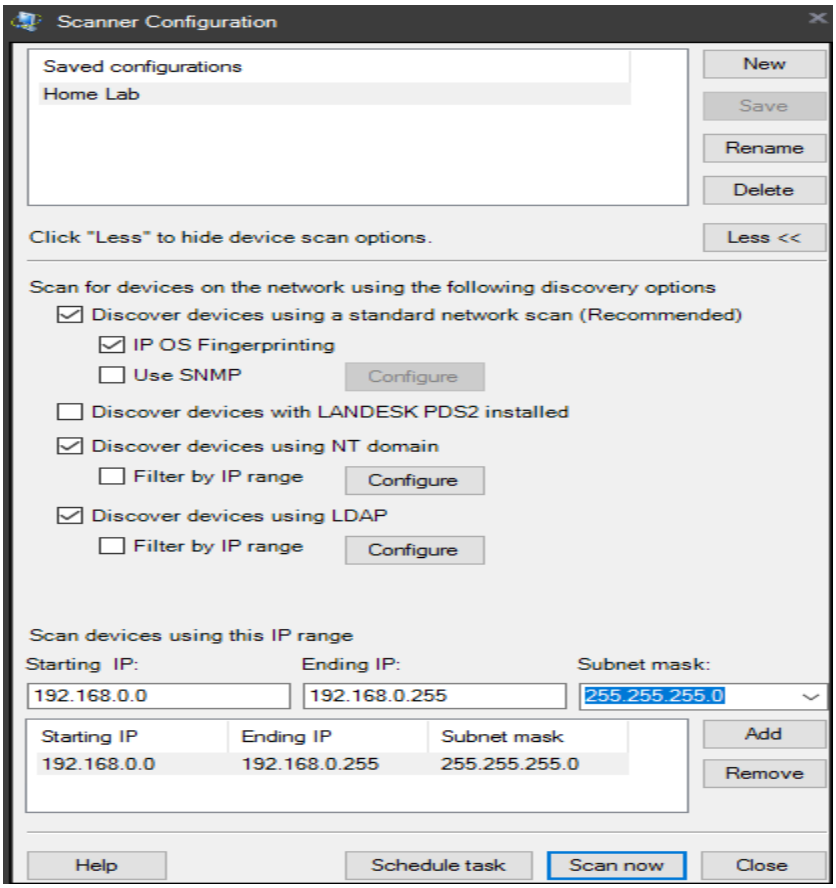


1. **Agent Configuration** – For this, I am going to use default Windows Configuration for workstations only.

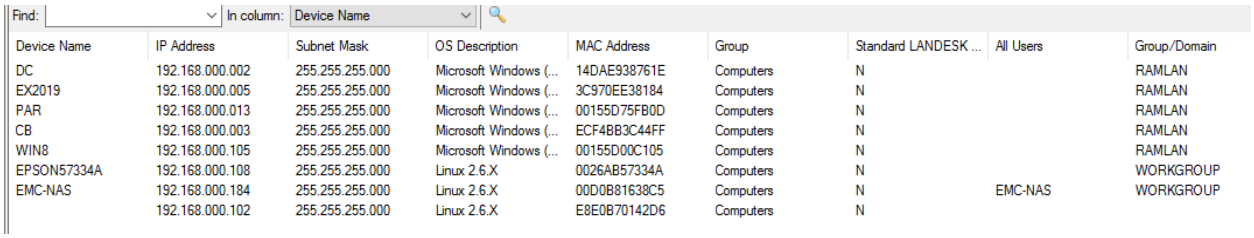




2. **Unmanaged Devices** – Below is my setup to scan the devices on the network



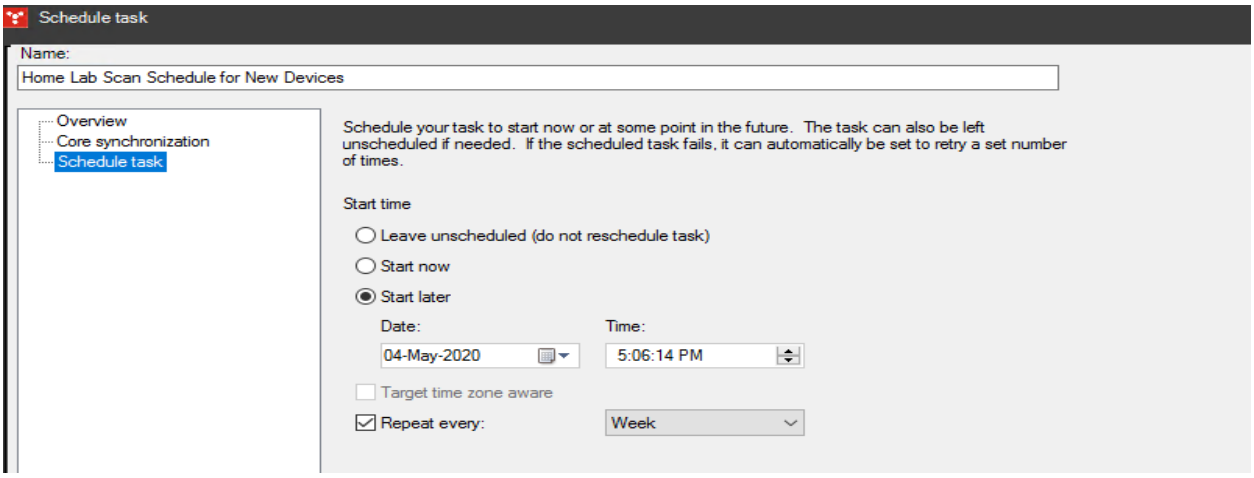
List of devices deducted.



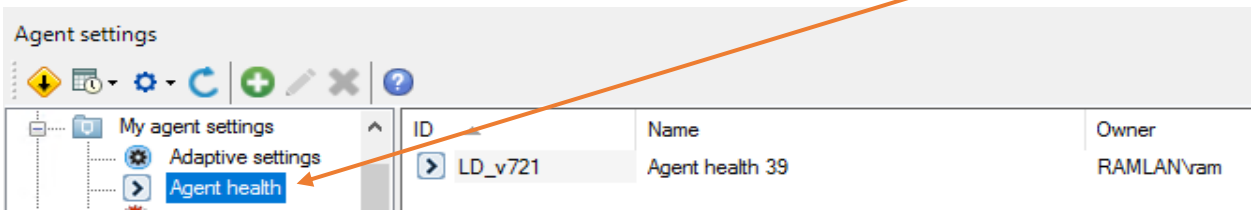
Find: In column: Device Name

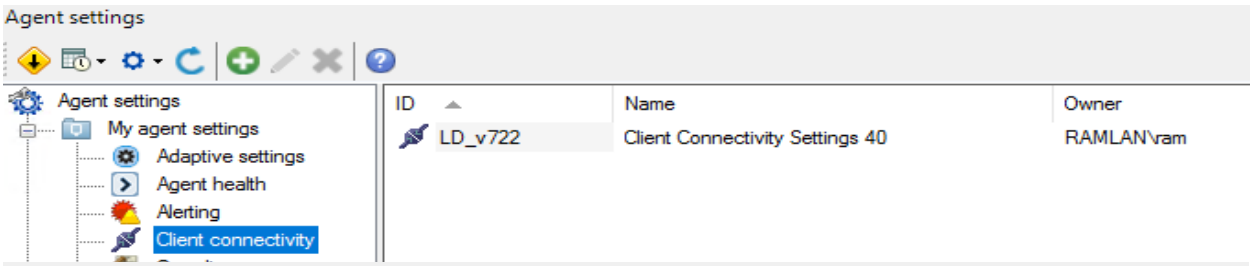
Device Name	IP Address	Subnet Mask	OS Description	MAC Address	Group	Standard LANDESK ...	All Users	Group/Domain
DC	192.168.000.002	255.255.255.000	Microsoft Windows (...	14DAE938761E	Computers	N		RAMLAN
EX2019	192.168.000.005	255.255.255.000	Microsoft Windows (...	3C970EE38184	Computers	N		RAMLAN
PAR	192.168.000.013	255.255.255.000	Microsoft Windows (...	00155D75FB0D	Computers	N		RAMLAN
CB	192.168.000.003	255.255.255.000	Microsoft Windows (...	ECF4BB3C44FF	Computers	N		RAMLAN
WIN8	192.168.000.105	255.255.255.000	Microsoft Windows (...	00155D00C105	Computers	N		RAMLAN
EPSON57334A	192.168.000.108	255.255.255.000	Linux 2.6.X	0026AB57334A	Computers	N		WORKGROUP
EMC-NAS	192.168.000.184	255.255.255.000	Linux 2.6.X	00D0B81638C5	Computers	N	EMC-NAS	WORKGROUP
	192.168.000.102	255.255.255.000	Linux 2.6.X	E8E0B70142D6	Computers	N		

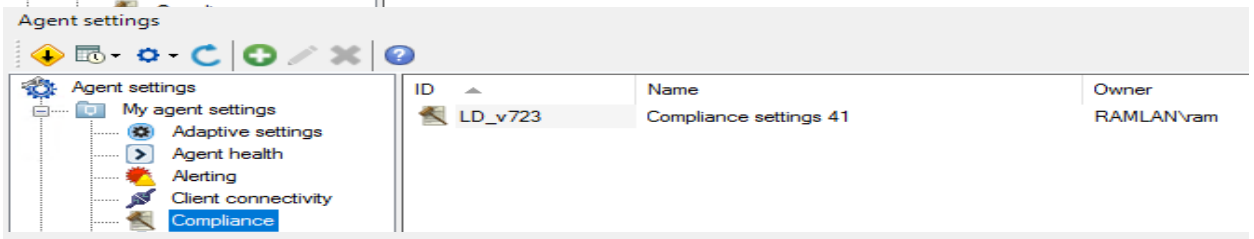
I have scheduled the scan every week

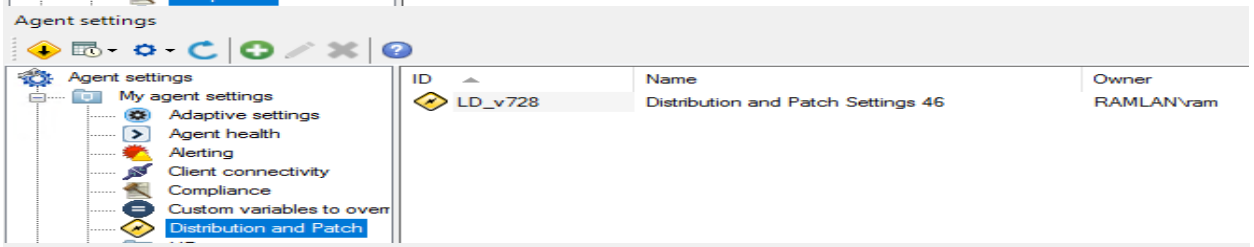


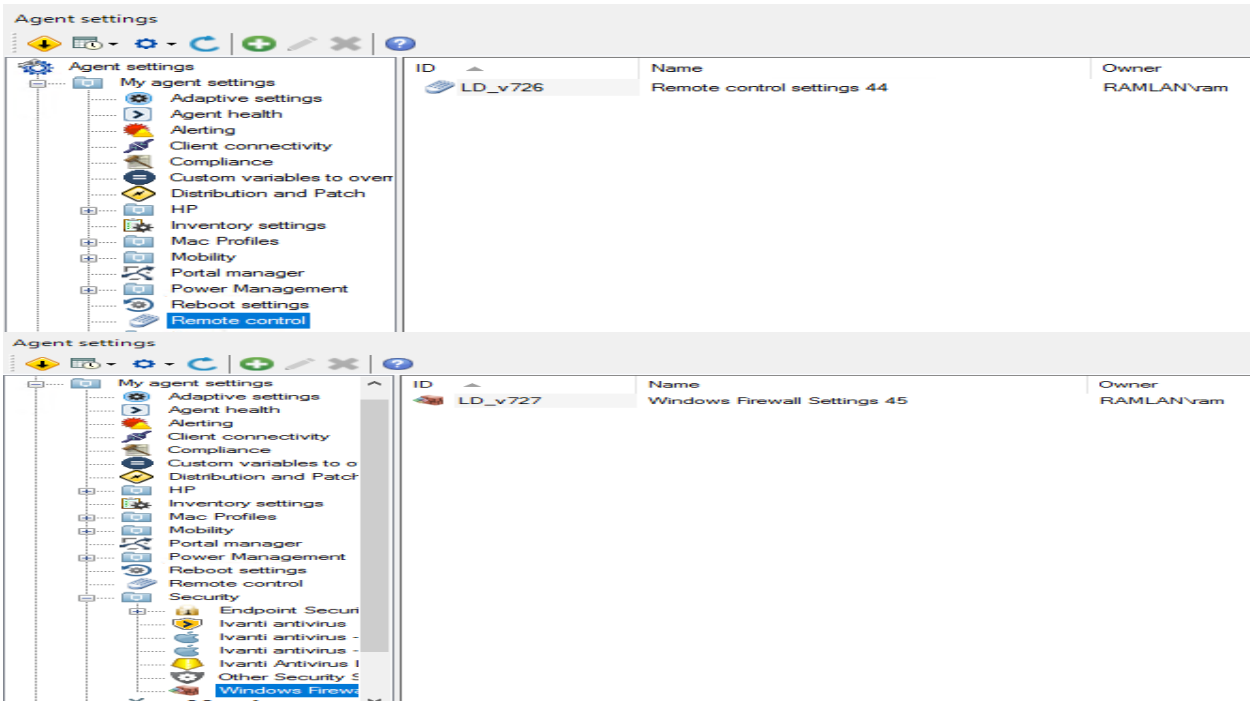
3. **Agent Settings** – These are some of my personal agent settings for workstation. Right click each setting and click New



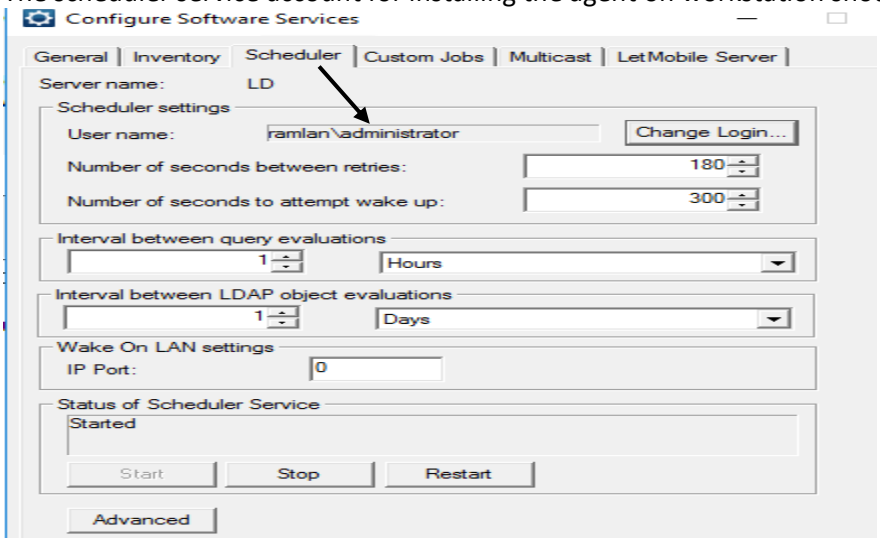




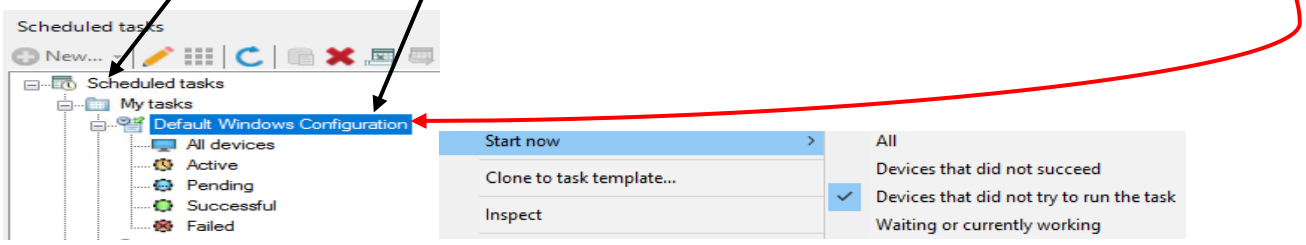


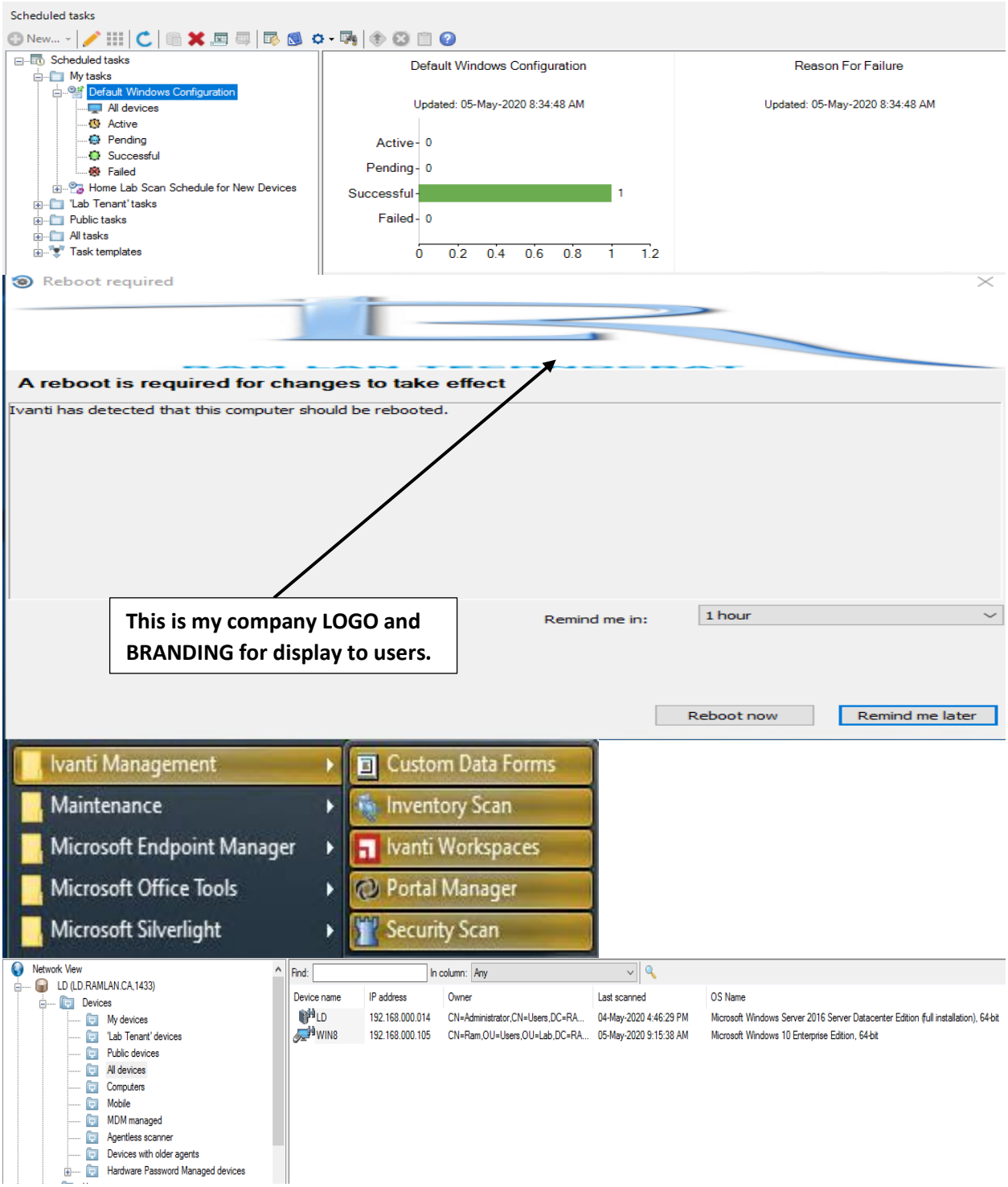


The scheduler service account for installing the agent on workstation should have local admin rights.



Now we are ready to deploy agent. Click Tools - Configure - Unmanaged Devices – Select the device and drag to Scheduled Task Window – Drop it inside Default Windows Configuration. After that right click Start Now – Devices that did not try to run the task. Wait for 10 minutes for the agent to deploy.





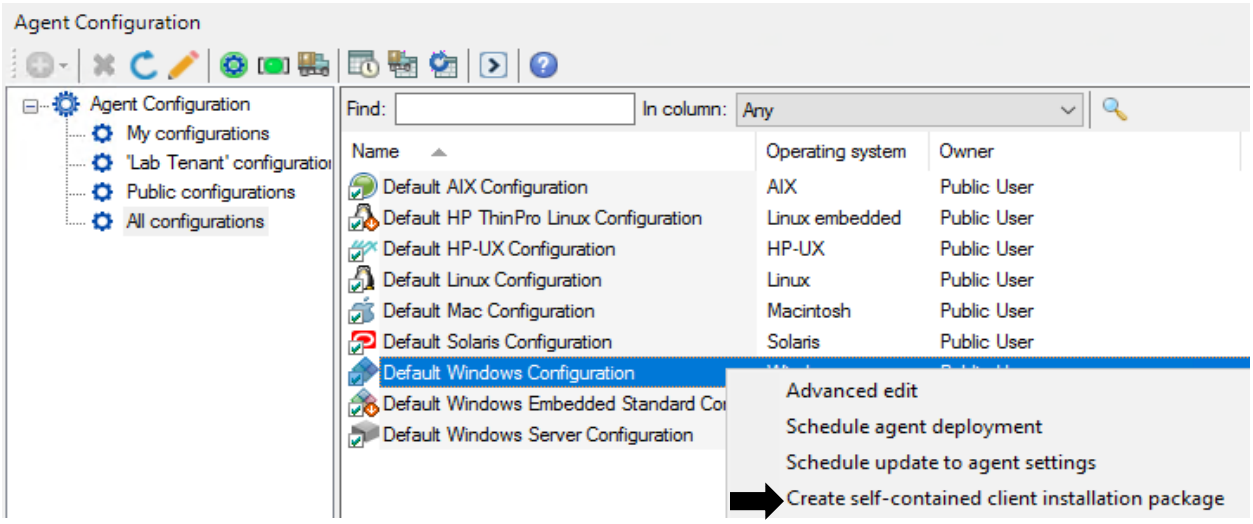
Now we have the agent deployed.

DIFFERENT WAYS TO INSTALL AGENT:

A. Create Self-Contained Executable

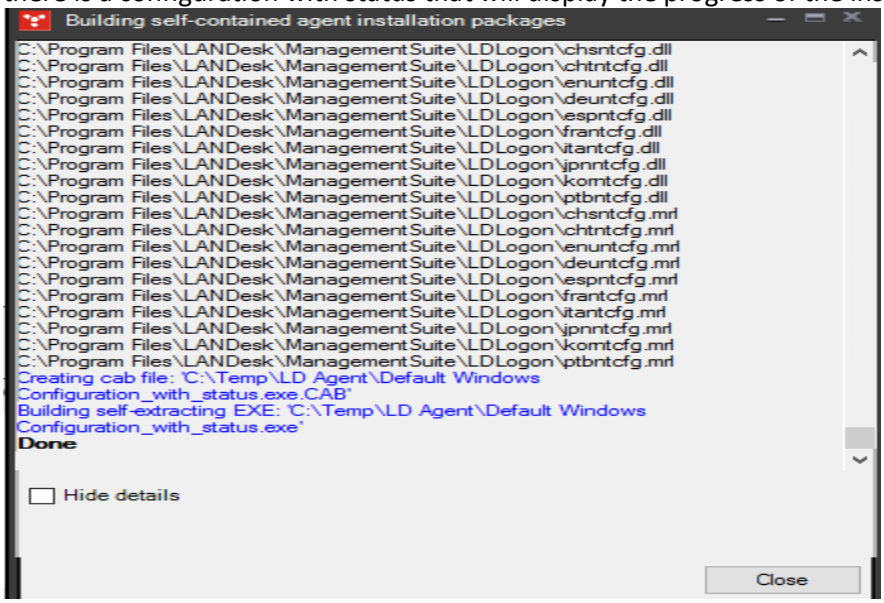
Self-contained agents are ideal, if there are a small number of devices on network, or any number of devices off network that won't have direct communication with the core. This method creates a .exe that can be made available on an internal/external network share and ran manually.

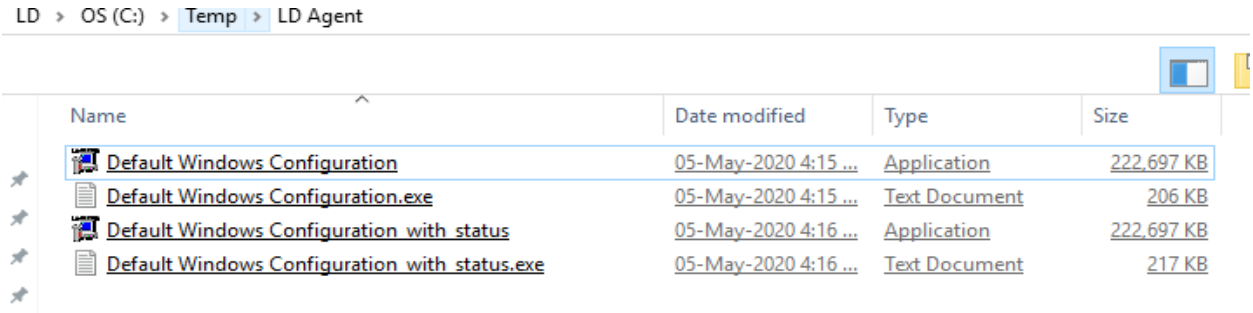
Tools > Configuration > Agent Configuration > Right click on the desired Windows agent configuration > Create self-contained client installation package



I created a network share on LD server at below location to save agent files for manual deployment.

Upon completion, the agent configurations should be found at C:\Temp\LD Agent location. Take note there is a configuration with status that will display the progress of the installer when run.





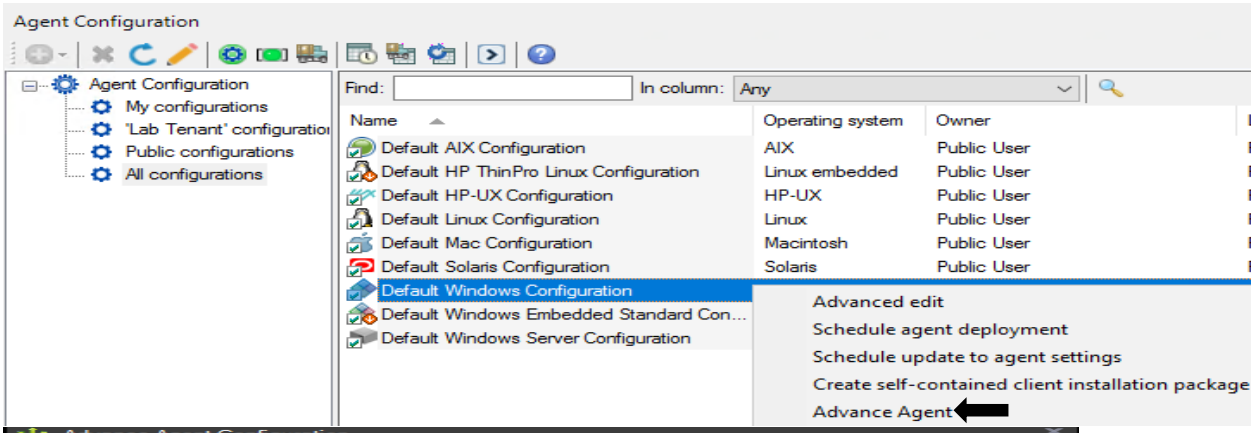
Now you can use above exe from network location and install it manually on workstations

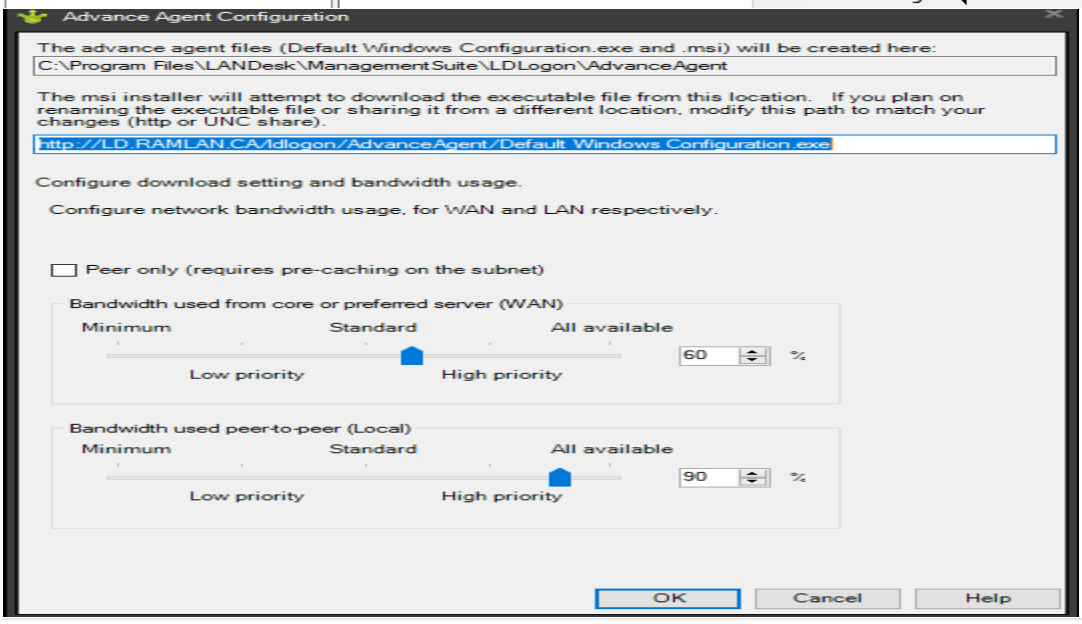
B. Advance Agent Deployment

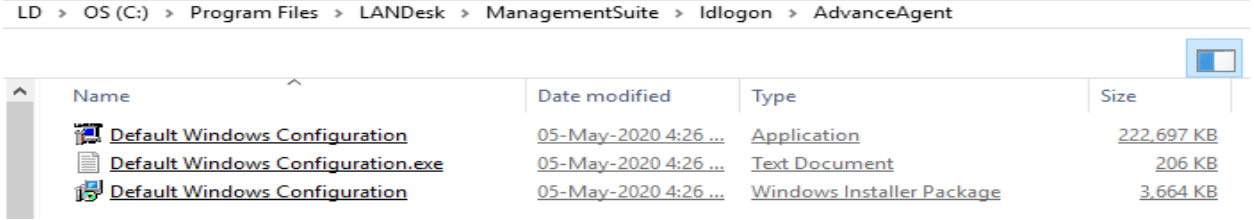
Advance agent deployment works by pushing a .msi to the endpoint devices. The .msi will then install and point to a network location (Usually the core server) to begin downloading the agent configuration. This method is nice for environments with specific bandwidth limitations as it is possible to throttle the download speed. The advance agent is also smart enough to pick up where it left off if the installer gets interrupted unlike other methods of agent deployment.

One common misconception when deploying the advance agent is that the console will return a success message rather quickly. This is because the scheduled task is deploying an advanced agent service, and then having that service copy to the device and start the install of the agent. The success message comes from the service successfully getting installed, not the actual completion of the install.

Tools > Configuration > Agent Configuration > Right click on a Windows configuration > Select “Advance Agent”



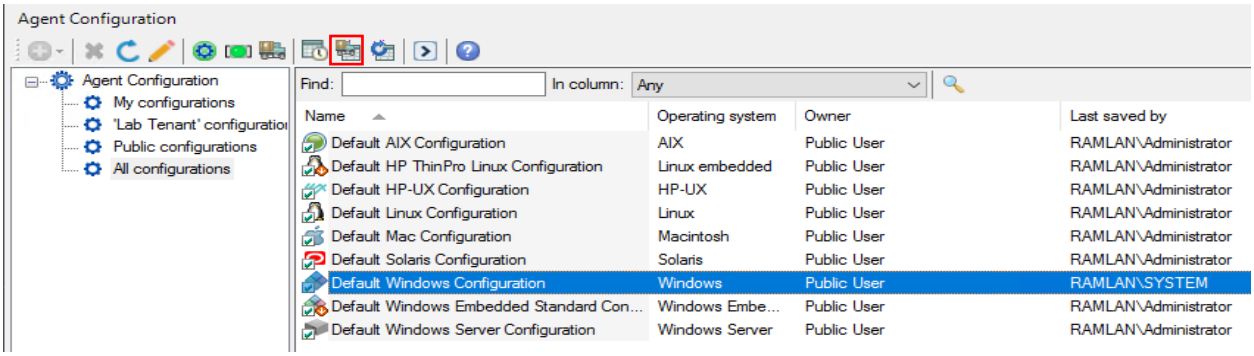


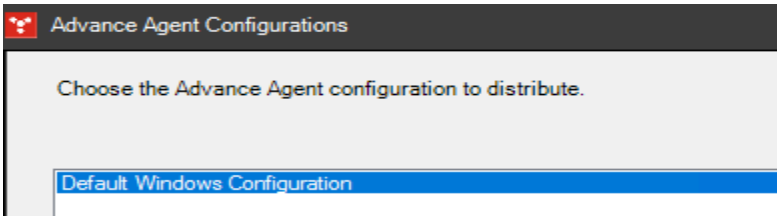


From here, it's possible to manually move the .msi to an endpoint and run it, or create a GPO. It is also possible to schedule the Advance Agent similar to a regular agent deployment.

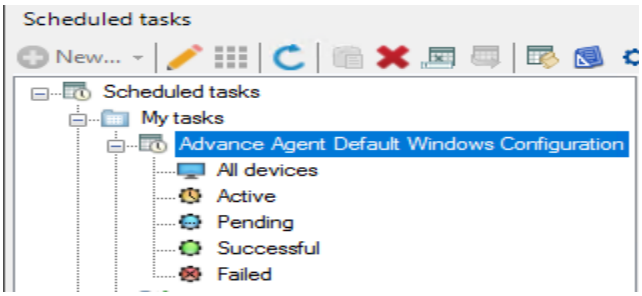
Tools > Configuration > Agent Configuration > Highlight the desired Windows agent configuration > Select the "Schedule push of an Advance Agent configuration" button.

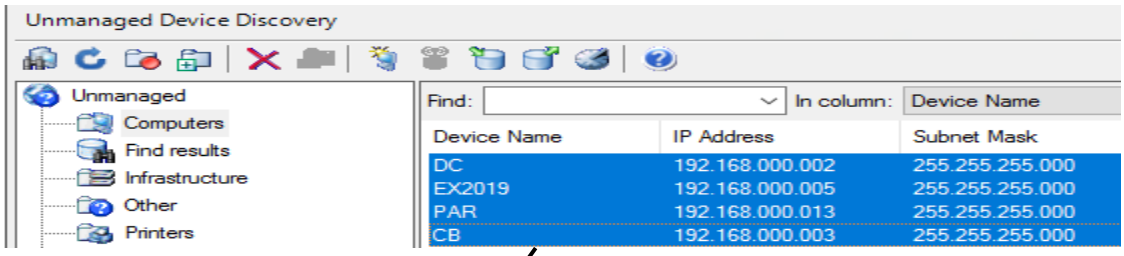
It will provide a list of Advance Agent options. Select the agent that was created previously > Click "OK".

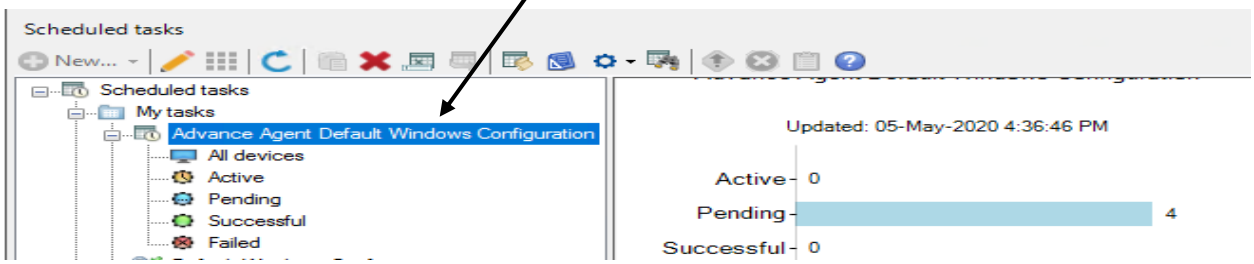


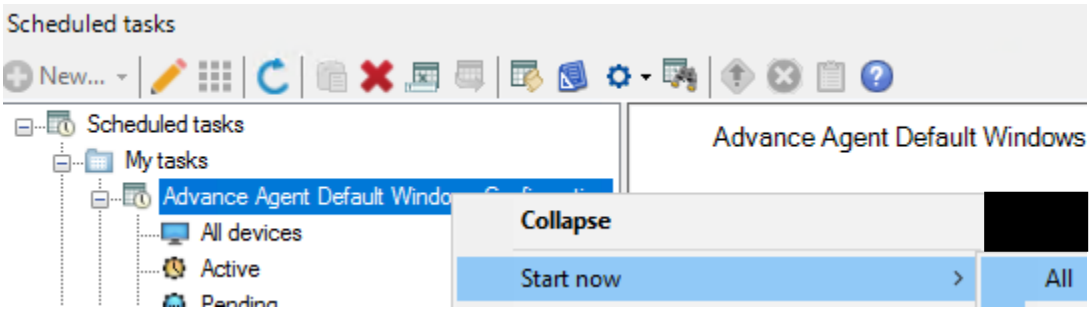


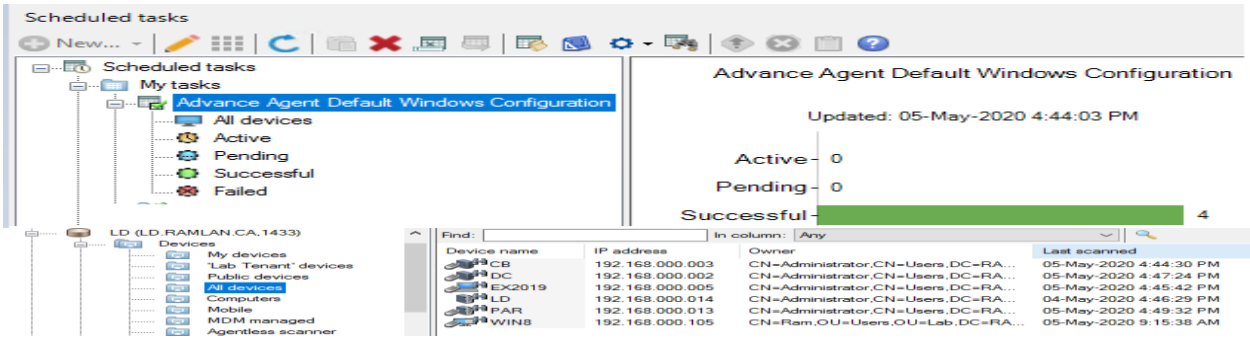
This will create a scheduled task to deploy the Advance Agent. Drag devices into the scheduled task and start the installation when ready.









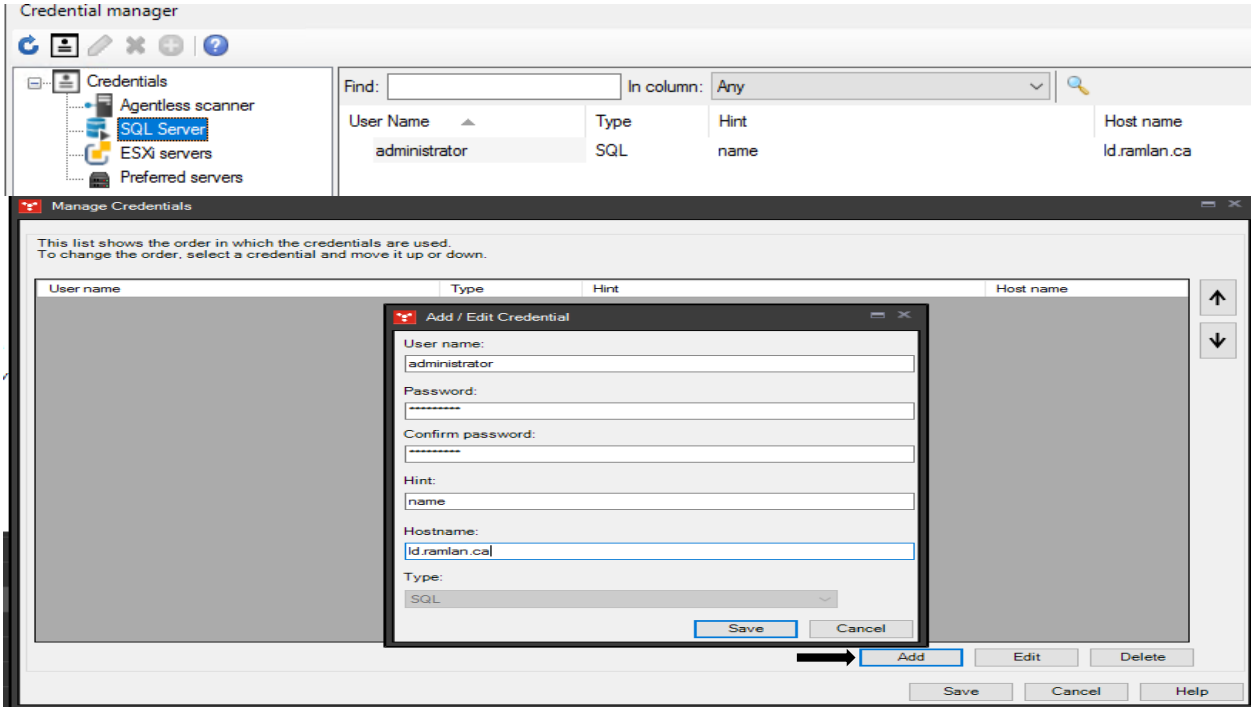


Now we have different ways to install agent. When agent is installed using Advanced method you will see binocular icon and **no reboot for users after agent is installed.**

4. Credential Manager

Use the credential manager tool (Tools > Configuration > Credential manager) to centrally manage credentials for the following:

- Agentless scanner
- SQL servers
- ESXi servers (discovered virtual OS hosts are visible in the Network view under the **Virtual OS Hosts** tree item)
- Preferred servers
- Amazon S3 storage credentials
- Azure storage credentials



5. **Custom Data Form** – I will not go into detail. Just a screen shot for info only.

Create a custom data form

Custom data forms provide a way for you to collect information from users and add it to the core database. Follow these steps to create a custom data form.

To create a custom data form

1. Click **Tools** > **Configuration** > **Custom data forms**.
2. In the Custom Data Forms window, double-click **Add new form**.
3. Enter a name for the form.
4. Enter a description for the form. (The description you enter will appear as a help tip when the user clicks F1 on the field while filling out the form.)
5. Click **Add** to open the **Add question** dialog box.
6. In the Add Question dialog box, type in the **Question text**, **Inventory name**, and **Description.**
7. Select the **Control type.**
8. Select whether you want the field to be required.
9. If you selected the **Edit** control type, click **Finish** to close the **Add question** dialog. The Edit control type lets users type in their own answers to questions in an editable text box. You can add more questions or proceed to step 12.

✚ **Show/Hide image**

10. If you selected either of the **Combo box** control types, click **Next** to open the **Add items** dialog. The Combo box control type lets users select their answers from a drop-down list of pre-defined items.
11. In the Add Items dialog, enter an item name and click **Insert** to place the item in the Items list. These items appear in a drop-down list for that question on the form. You can add as many items as you like, then click **Finish**.
12. When you're done adding questions, click **Close** to save the form.

You can right-click on a form to schedule it for distribution to devices.

6. Client Data Storage

The Client data storage tool (Tools > Configuration > Client data storage) lets you view encrypted client data. Currently, this tool shows data for Windows devices with BitLocker enabled and Mac OS X devices with FileVault enabled via Endpoint Manager. Use this tool if you need to retrieve a device's BitLocker or FileVault recovery key.

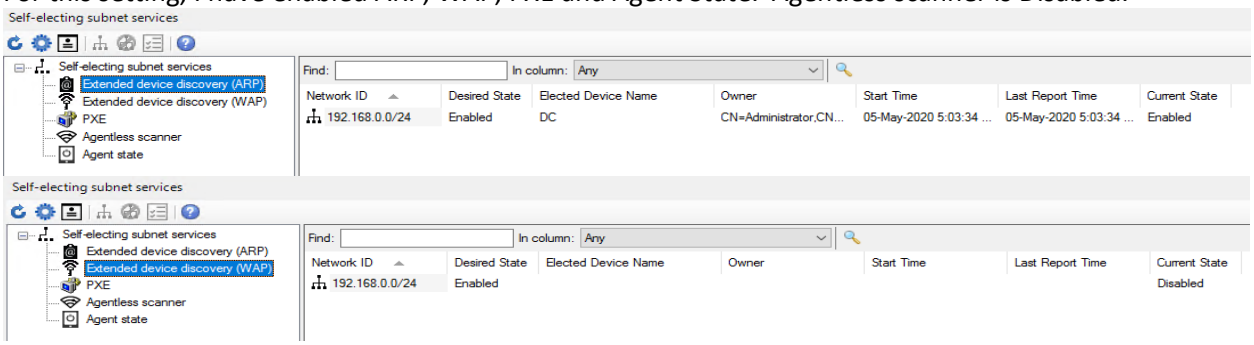
To retrieve a BitLocker or FileVault recovery key

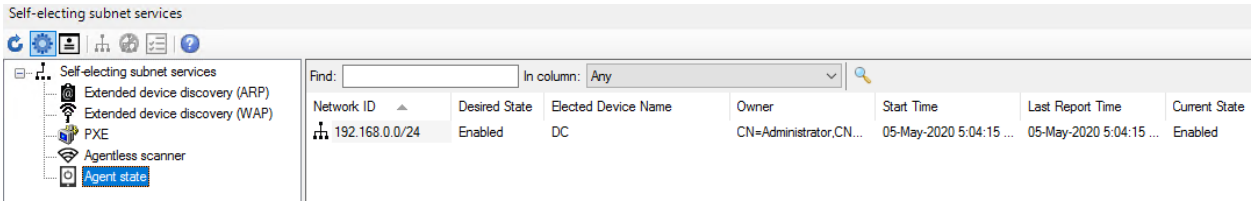
1. Click **Tools** > **Configuration** > **Client data storage**.
2. In the **Devices** tree, double-click the device you want.
3. In the **Client data** dialog box, select the **Client data item** matching the data you want, and click the export toolbar button.
4. Select a location for the resulting text file.
5. Open the text file in an editor and view the recovered key.

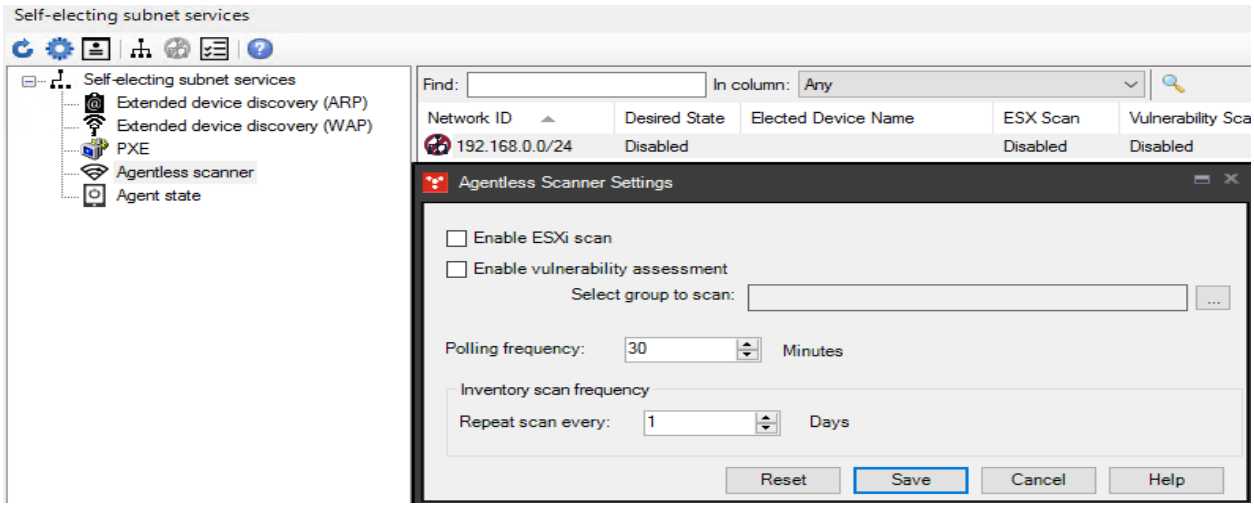
You can also retrieve recovery keys from the **Network view**. In the **Network view**, right-click the device you want, then click **Security and Patch** > **Recover keys** > **BitLocker** or **FileVault**, depending on the device type you selected.

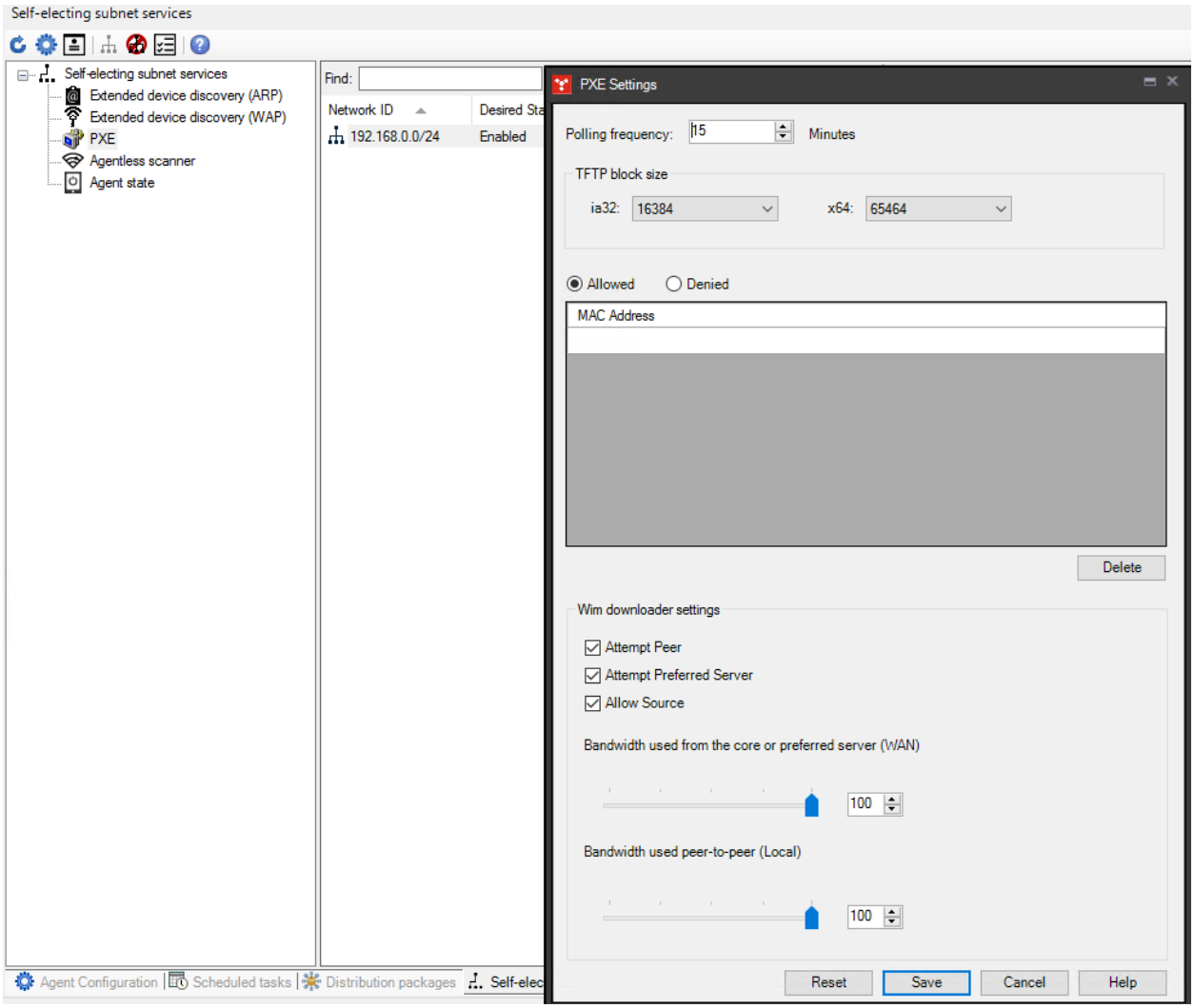
7. Self electing subnet services

For this setting, I have enabled ARP, WAP, PXE and Agent State. Agentless scanner is Disabled.




Self-electing subnet services
Self-electing subnet services
Extended device discovery (ARP)
Extended device discovery (WAP)
PXE
Agentless scanner
Agent state
Find:
In column:
Any
Network ID
Desired State
Elected Device Name
Owner
Start Time
Last Report Time
Current State
192.168.0.0/24
Enabled
DC
CN=Administrator,CN...
05-May-2020 5:04:15 ...
05-May-2020 5:04:15 ...
Enabled


Self-electing subnet services
Self-electing subnet services
Extended device discovery (ARP)
Extended device discovery (WAP)
PXE
Agentless scanner
Agent state
Find:
In column:
Any
Network ID
Desired State
Elected Device Name
ESX Scan
Vulnerability Sca
192.168.0.0/24
Disabled
Disabled
Disabled
Agentless Scanner Settings
Enable ESXi scan
Enable vulnerability assessment
Select group to scan:
Polling frequency:
30
Minutes
Inventory scan frequency
Repeat scan every:
1
Days
Reset
Save
Cancel
Help


Self-electing subnet services
Self-electing subnet services
Extended device discovery (ARP)
Extended device discovery (WAP)
PXE
Agentless scanner
Agent state
Find:
Network ID
Desired Sta
192.168.0.0/24
Enabled
PXE Settings
Polling frequency:
15
Minutes
TFTP block size
ia32:
16384
x64:
65464
Allowed
Denied
MAC Address
Delete
Wim downloader settings
Attempt Peer
Attempt Preferred Server
Allow Source
Bandwidth used from the core or preferred server (WAN)
100
Bandwidth used peer-to-peer (Local)
100
Reset
Save
Cancel
Help
Agent Configuration
Scheduled tasks
Distribution packages
Self-elec

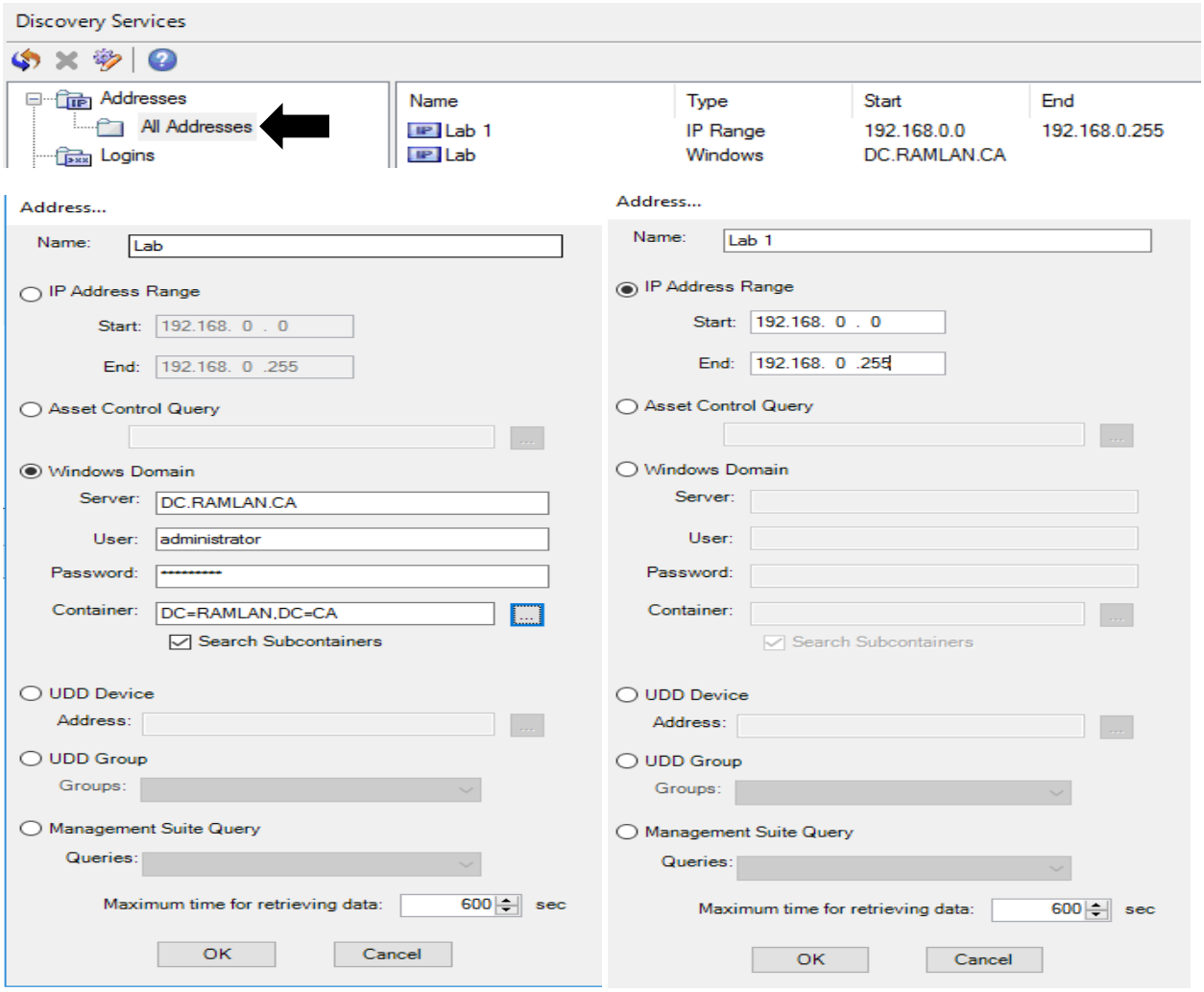
DATA ANALYTICS

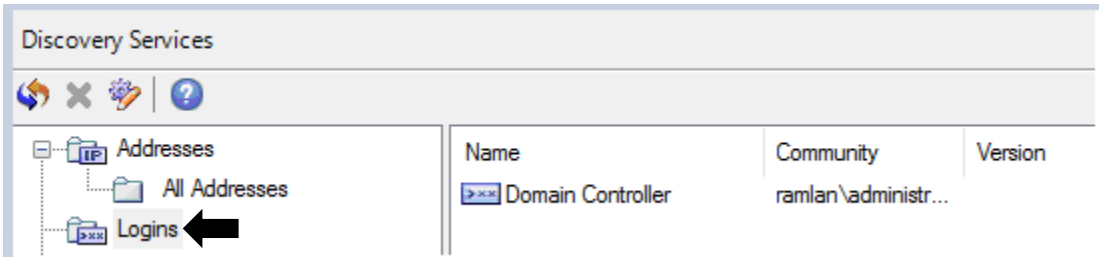
1. Configure Discovery Services

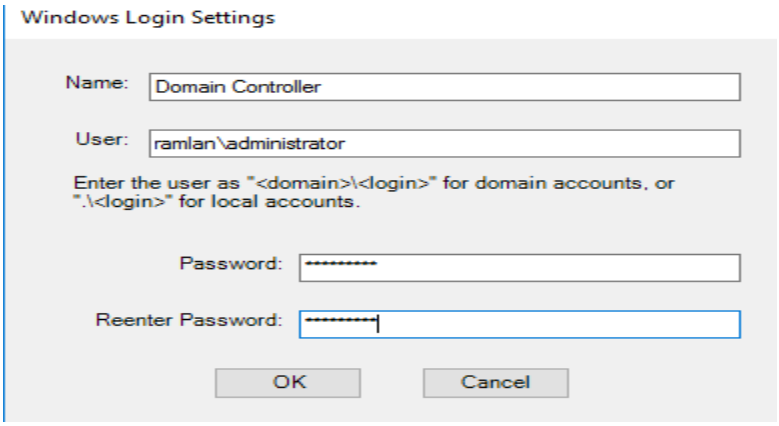
Discovery Services is a Data Analytics tool for Ivanti® Management Suite that helps you gather data about SNMP-enabled devices for which Management Suite has no agent, such as printers, switches, routers, and so on. You can also use Discovery Services to gather inventory data from WMI-enabled devices that you've chosen not to deploy the Ivanti agent to.

Discovery Services uses a scan configuration to connect to these devices, then gathers and stores the available inventory data in either the Asset Control database (for SNMP-enabled devices) or the inventory database (for WMI-enabled devices).

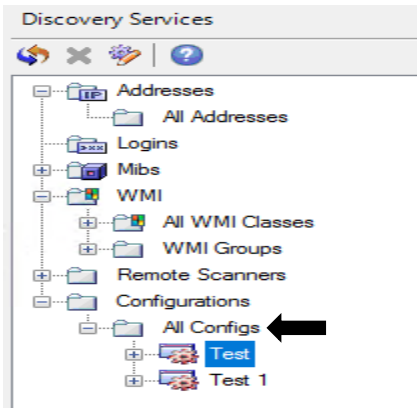
Configure – Discovery Services

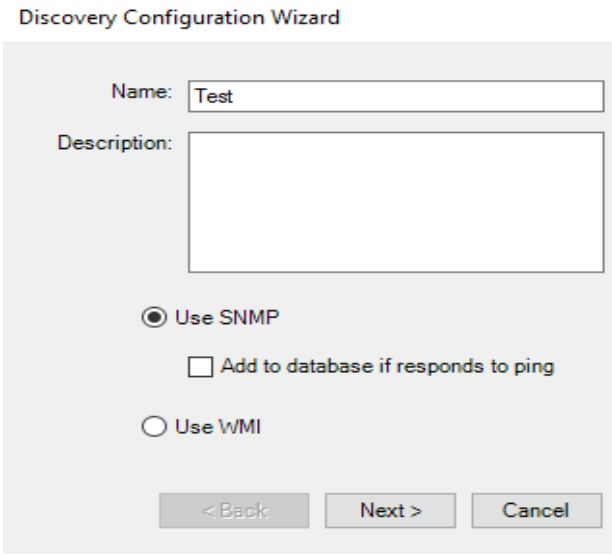


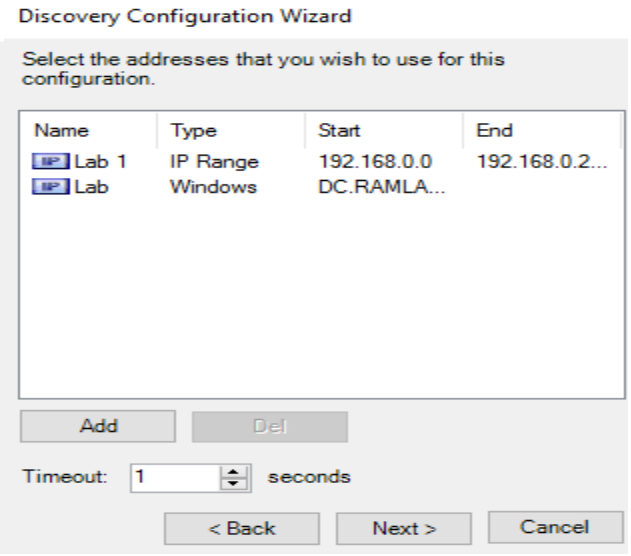


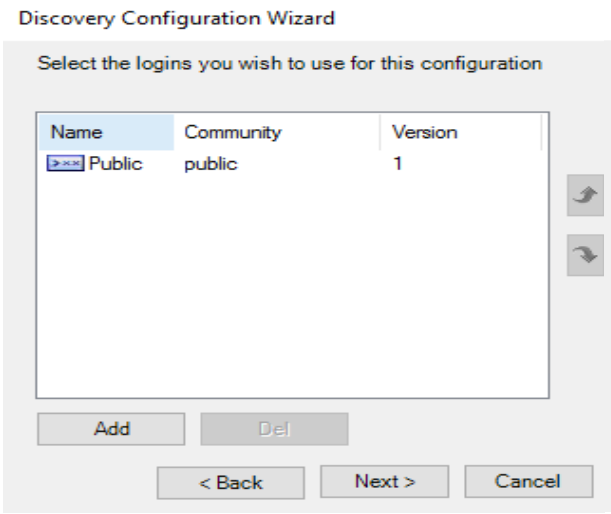


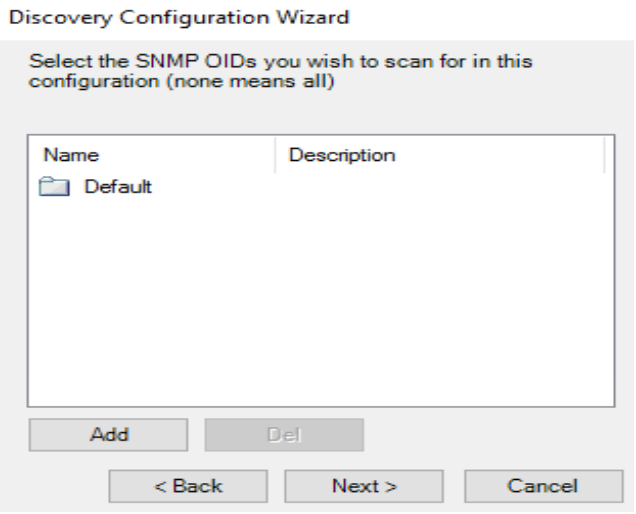
All Configs - Add

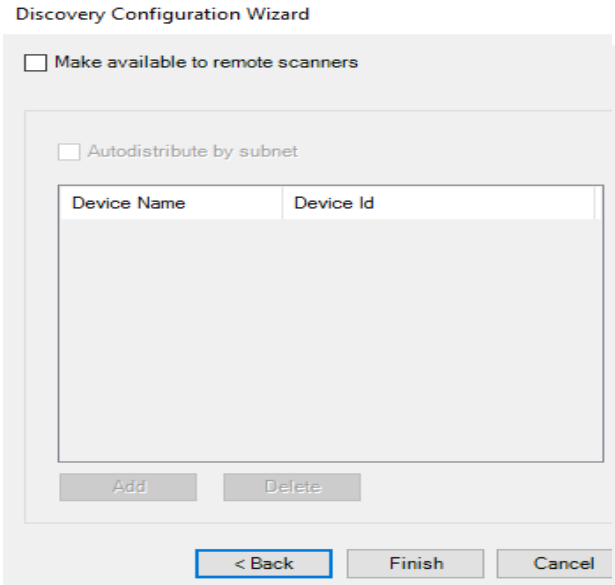


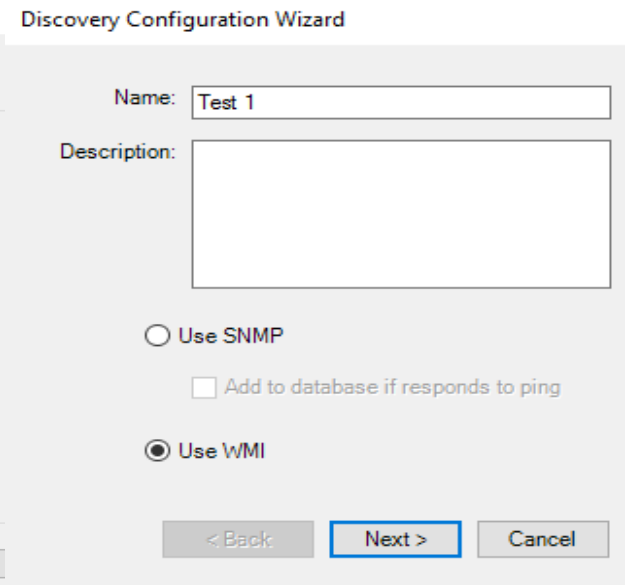


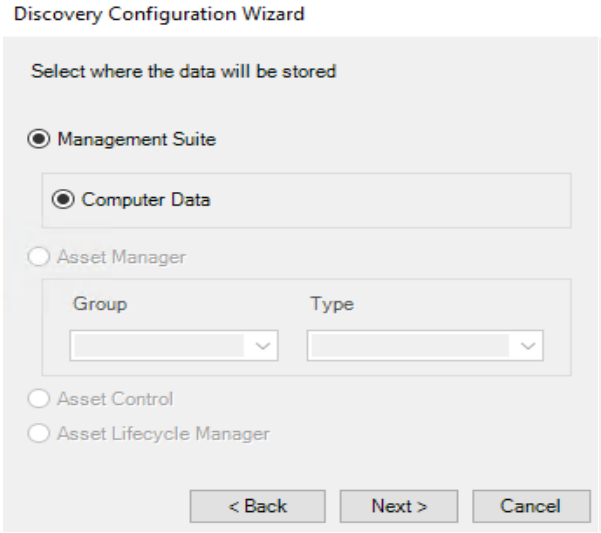


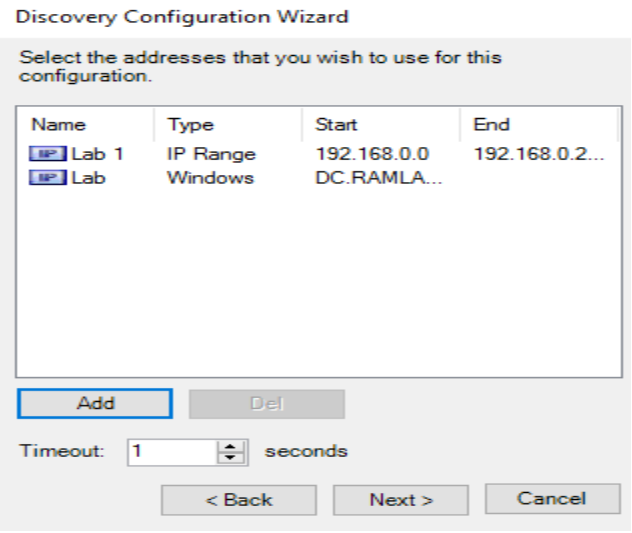

Discovery Configuration Wizard
Select the logins you wish to use for this configuration
Name
Community
Version
Public
public
1
Add
Del
< Back
Next >
Cancel

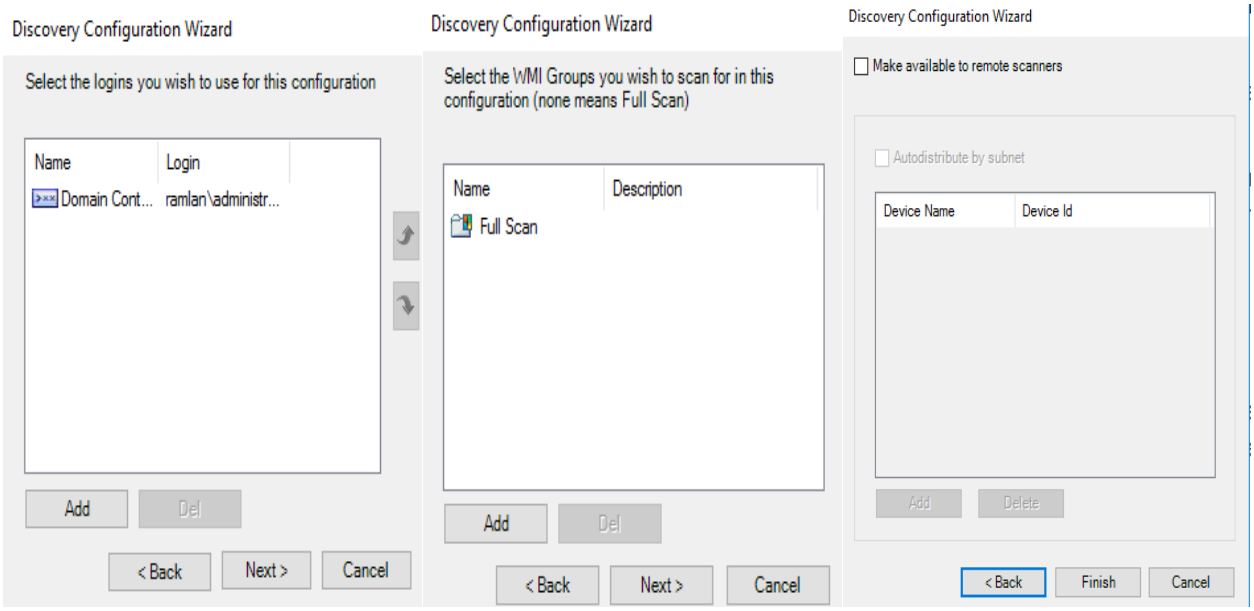

Discovery Configuration Wizard
Select the SNMP OIDs you wish to scan for in this configuration (none means all)
Name
Description
Default
Add
Del
< Back
Next >
Cancel

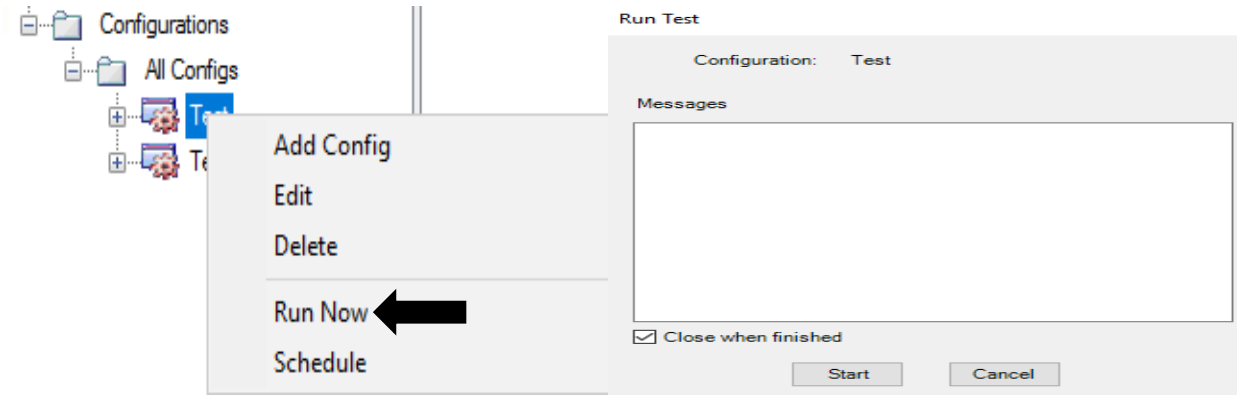

Discovery Configuration Wizard
Make available to remote scanners
Autodistribute by subnet
Device Name
Device Id
Add
Delete
< Back
Finish
Cancel

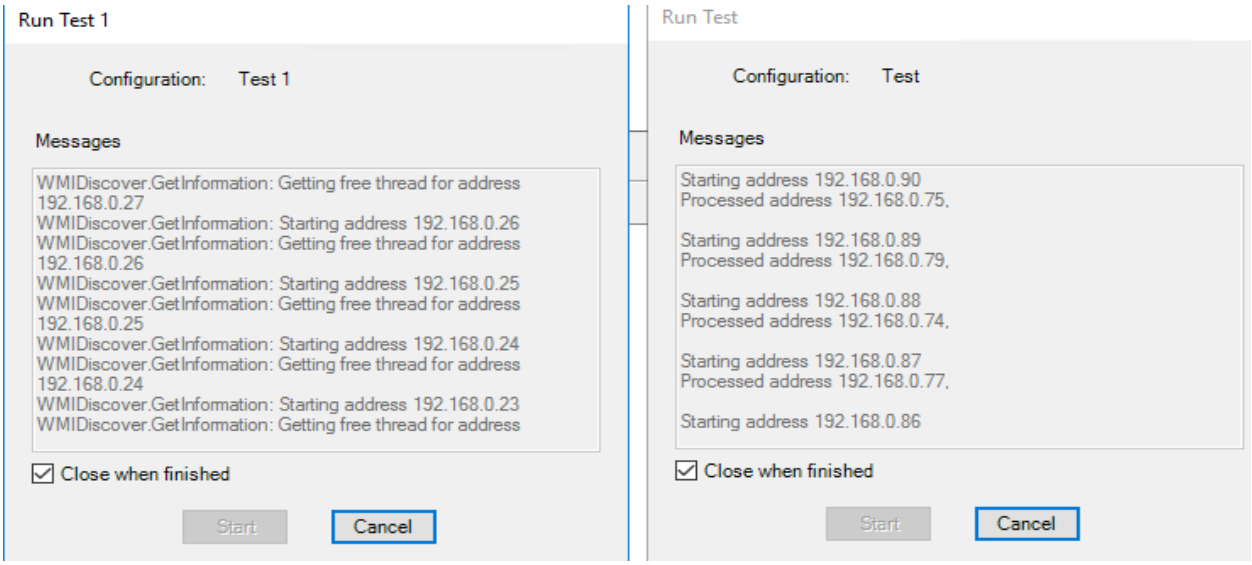

Discovery Configuration Wizard
Name:
Test 1
Description:
Use SNMP
Add to database if responds to ping
Use WMI
< Back
Next >
Cancel


Discovery Configuration Wizard
Select where the data will be stored
Management Suite
Computer Data
Asset Manager
Group
Type
Asset Control
Asset Lifecycle Manager
< Back
Next >
Cancel


Discovery Configuration Wizard
Select the addresses that you wish to use for this configuration.
Name
Type
Start
End
Lab 1
IP Range
192.168.0.0
192.168.0.2...
Lab
Windows
DC.RAMLA...
Add
Del
Timeout:
1
seconds
< Back
Next >
Cancel


Discovery Configuration Wizard
Select the logins you wish to use for this configuration
Name
Login
Domain Cont...
ramlan\administr...
Add
Del
< Back
Next >
Cancel
Discovery Configuration Wizard
Select the WMI Groups you wish to scan for in this configuration (none means Full Scan)
Name
Description
Full Scan
Add
Del
< Back
Next >
Cancel
Discovery Configuration Wizard
Make available to remote scanners
Autodistribute by subnet
Device Name
Device Id
Add
Delete
< Back
Finish
Cancel


Configurations
All Configs
Add Config
Edit
Delete
Run Now
Schedule
Run Test
Configuration: Test
Messages
Close when finished
Start
Cancel


Run Test 1
Configuration: Test 1
Messages
WMIDiscover.GetInformation: Getting free thread for address 192.168.0.27
WMIDiscover.GetInformation: Starting address 192.168.0.26
WMIDiscover.GetInformation: Getting free thread for address 192.168.0.26
WMIDiscover.GetInformation: Starting address 192.168.0.25
WMIDiscover.GetInformation: Getting free thread for address 192.168.0.25
WMIDiscover.GetInformation: Starting address 192.168.0.24
WMIDiscover.GetInformation: Getting free thread for address 192.168.0.24
WMIDiscover.GetInformation: Starting address 192.168.0.23
WMIDiscover.GetInformation: Getting free thread for address
Close when finished
Start
Cancel
Run Test
Configuration: Test
Messages
Starting address 192.168.0.90
Processed address 192.168.0.75,
Starting address 192.168.0.89
Processed address 192.168.0.79,
Starting address 192.168.0.88
Processed address 192.168.0.74,
Starting address 192.168.0.87
Processed address 192.168.0.77,
Starting address 192.168.0.86
Close when finished
Start
Cancel

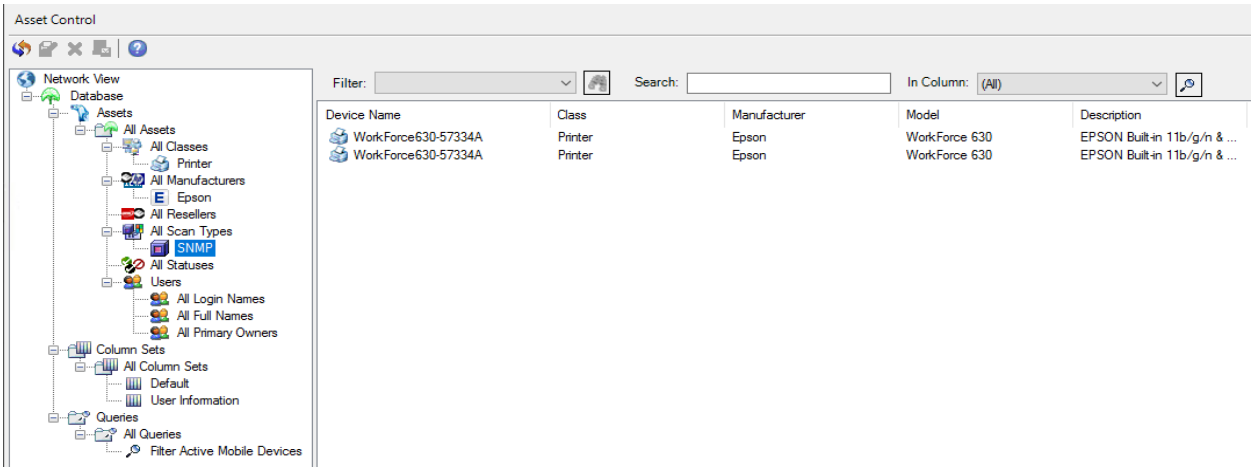
After running a configuration, new inventory data will appear in either the Asset Control view (for SNMP-enabled devices) or the Management Suite network view (for WMI-enabled devices).

Two files are created during the process—a log file, which lets you know if the configuration succeeded or failed and an .XML file, which contains the actual inventory data. By default, the files are located in these directories:

- **Log file**—C:\Program Files (x86)\LANDesk\ManagementSuite\MP_Log. The filename will appear as **Discovery - <configuration name> - <date><time>.log**.
- **.XML file**—C:\Program Files (x86)\LANDesk\ManagementSuite\MP_TEMP\DiscServ\Processed.

2. Asset Control

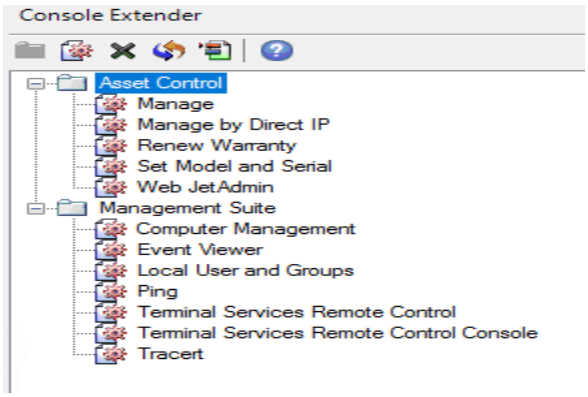
Asset Control is a Data Analytics tool for Ivanti Management Suite that enables you to store and view detailed records for devices lacking the Ivanti agent in a database separate from inventory. For Unmanaged Device Discovery (UDD) devices (such as printers, switches, routers, and so on), only a minimal amount of data is visible in the Management Suite network view. By using Data Analytics' Discovery Services to add these devices to the Asset Control database, you have the ability to view a more detailed inventory record.



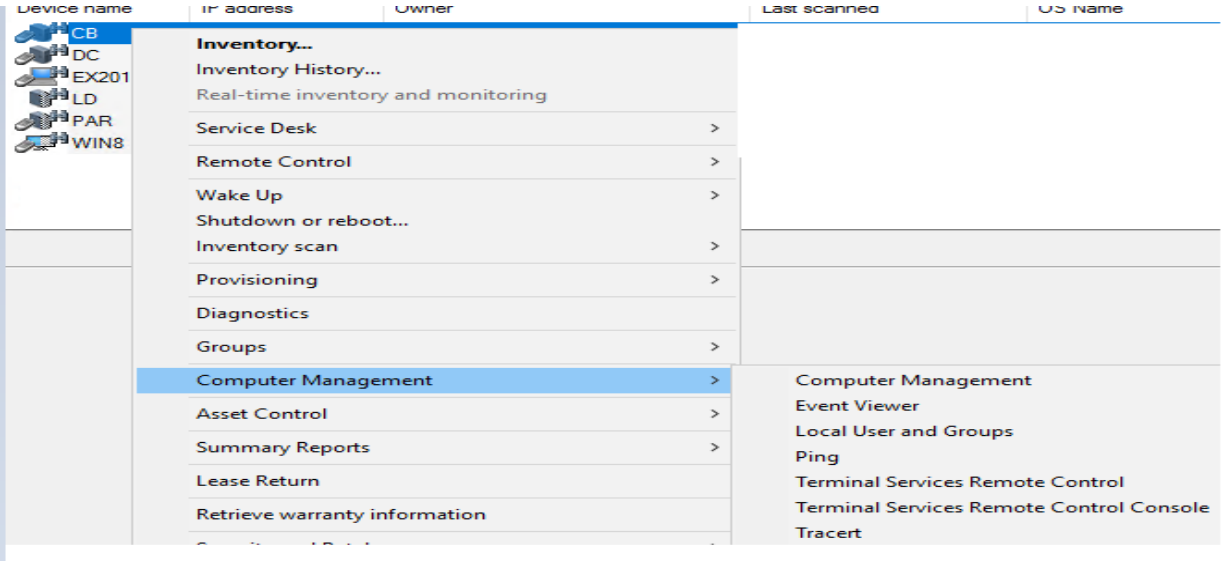
3. Console Extender

Console Extender is a Data Analytics tool for Ivanti® Management Suite that enables you to customize the right-click (context) menu of devices appearing in either the Management Suite network view or the Data Analytics Asset Control view. Console Extender provides a convenient way of customizing right-click menus instead of the more time-consuming method of editing a device's registry.

Console Extender ships with a number of pre-built menu options that automatically appear on the right-click menus of devices in either the Asset Control view or the network view. You can edit these options as needed.

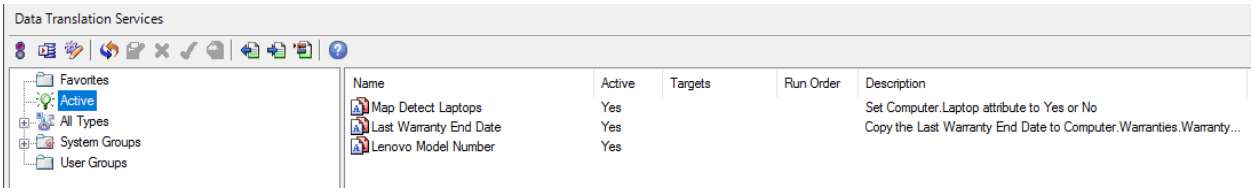


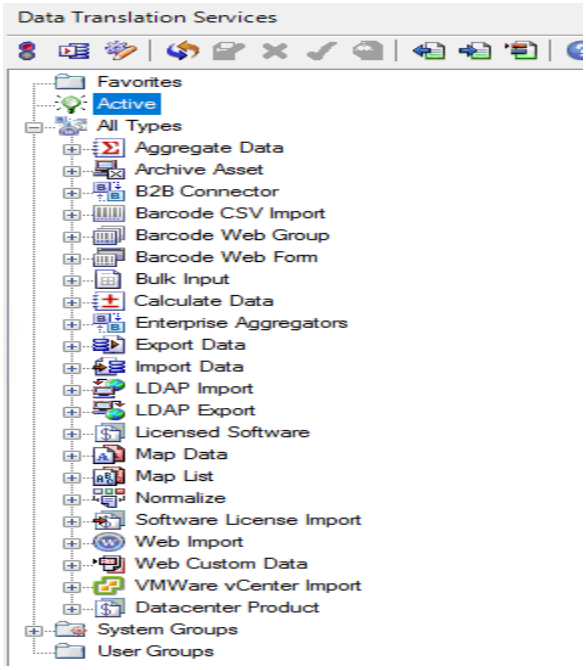
Right click any device

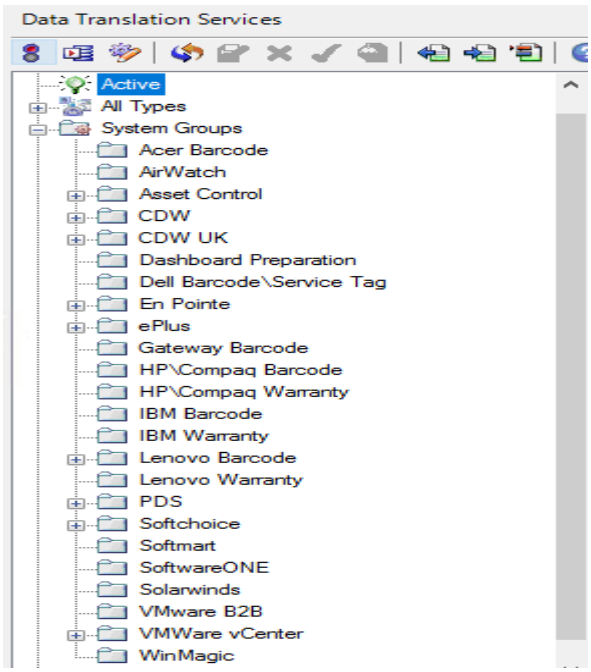


4. Data Translation Services

Data Translation Services (DTS) is a Data Analytics tool for Ivanti® Management Suite that scans your organization's devices for the inventory data you most care about, such as software licensing, warranties, and so on. Once the data is scanned into the inventory database, you can customize, aggregate, and organize it in reports to make informed and practical decisions about hardware and software purchases and needs.







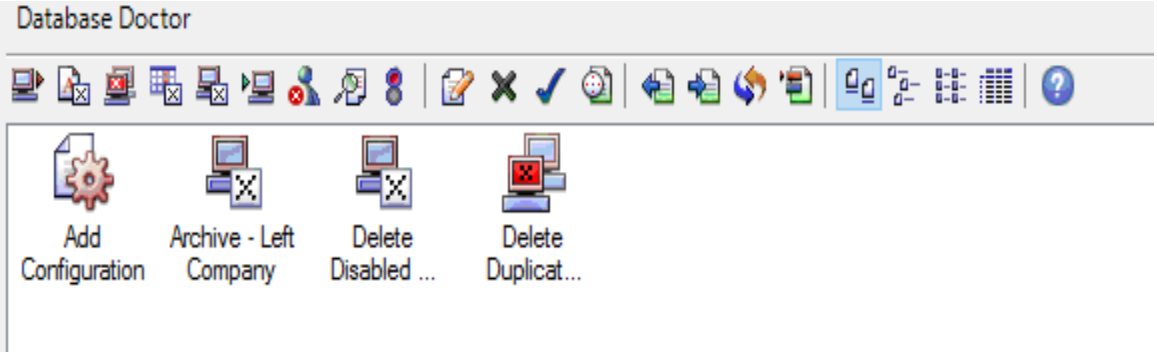
5. **Database Doctor**

Database Doctor is a Data Analytics tool for Ivanti® Management Suite that provides database protection, migration, and lifecycle maintenance to ensure the integrity of your inventory data.

You can use Database Doctor to protect the inventory database by removing corrupt or unwanted fields and classes, as well as removing and archiving duplicate records, all on demand or as scheduled. Once duplicates are removed, you can schedule data-integrity configurations to run on a regular basis, assuring on-going protection from data corruption.

Database Doctor also helps with database migration, preserving key inventory data and settings when you upgrade or restore your Ivanti core server. Before a rebuild, protect your inventory data by exporting (as scan files) inventory records, queries, policy details, and other configuration information. After the rebuild, you can import the data back into the database. This export, rebuild, and import technique not only helps with upgrades and disaster recovery but also avoids the instability of an overlay installation.

Finally, you can use Database Doctor to help with database-lifecycle maintenance. As devices age and require removal from the inventory database, use Database Doctor to archive them to an off-line state by saving device data as scan files in a directory. You'll have a complete record of retired assets that aren't included in Management Suite license calculations.

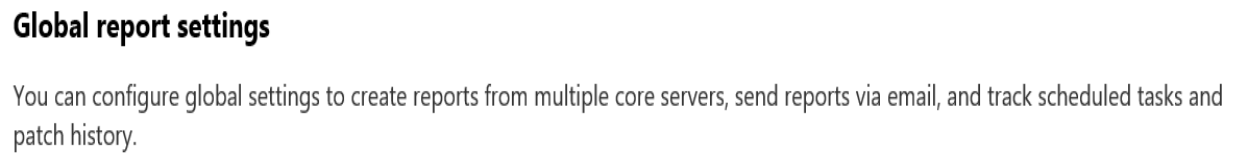


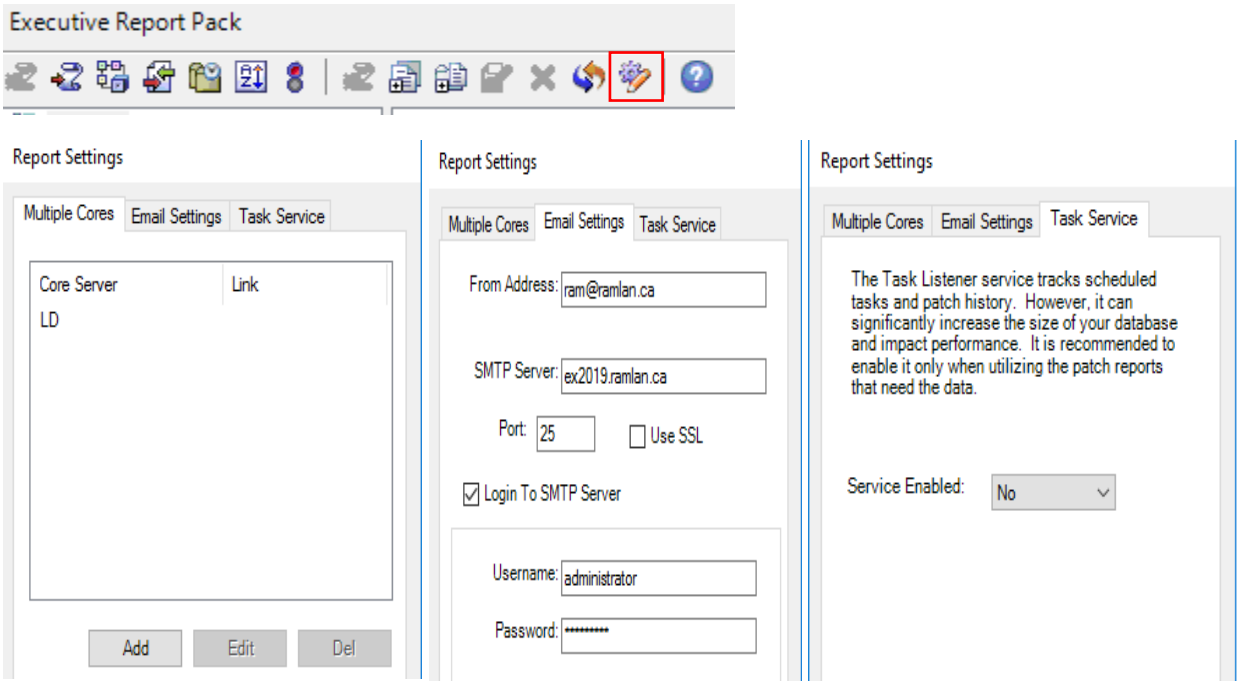
6. **Executive Report Pack**

Executive Report Pack (ERP) is a Data Analytics tool for Ivanti® Management Suite that provides useful, time-saving reporting features such as scheduled report publishing and organization-driven reports.

ERP gives you detailed control over your Management Suite queries, enabling you to edit them with SQL to create reports that contain the data most meaningful to you. ERP installs with a number of reports already defined and ready to run.

To use ERP, your first task should be to configure the global report settings. After these settings are configured, you can run existing reports, create your own, and schedule reports to run at regular intervals.



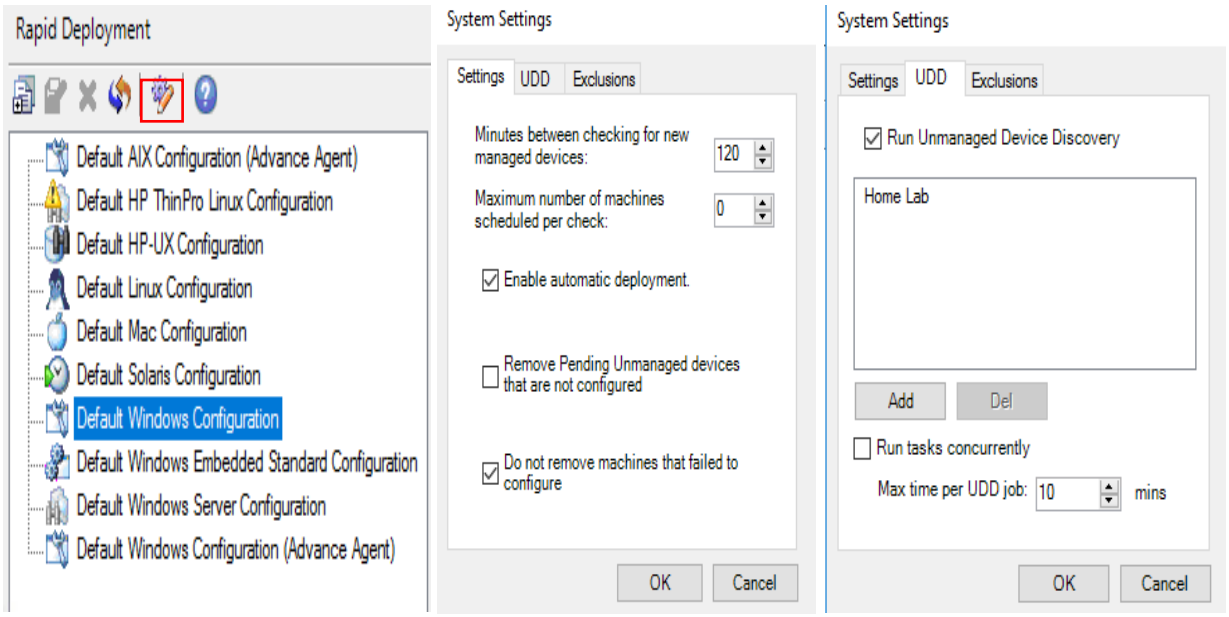


I will not go into any other settings as, I have only one database server for this exercise.

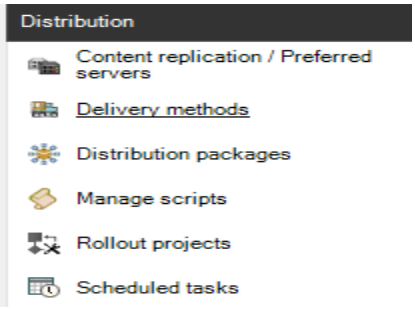
7. Rapid Deployment

Rapid Deployment is a Data Analytics tool for Ivanti® Management Suite that automates the deployment of Ivanti agents to unmanaged devices on your network.

One of the most time-consuming tasks for an Ivanti administrator is to deploy the appropriate Ivanti agent to new or existing devices. The most common way to do this is via Management Suite's Unmanaged Device Discovery (UDD) tool, which requires you to discover new devices on the network, drag and drop those devices to the appropriate scheduled client deployment, and then push the agent out to them. There are other methods as well, but Rapid Deployment helps you automate this process with a client-configuration query that uses UDD to discover devices and install the agent in one procedure.



DISTRIBUTION

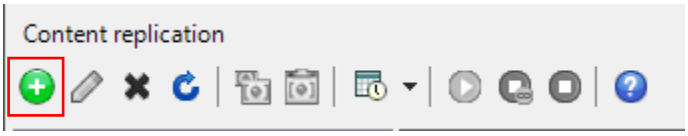


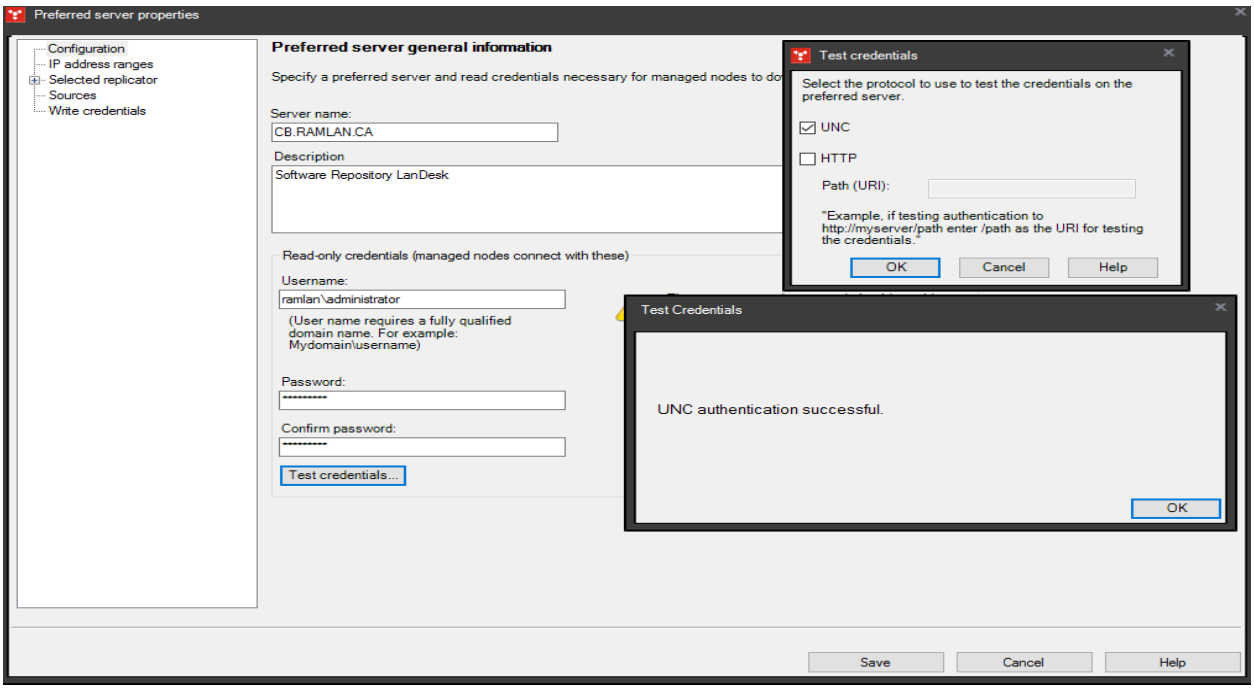
1. Content Replication Preferred Server

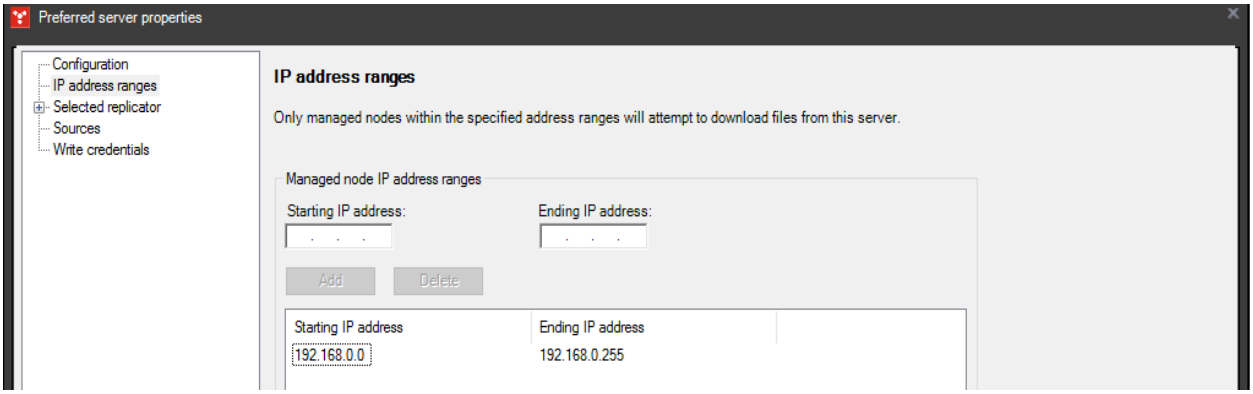
How to configure the Preferred Server (Target) for Content Replication

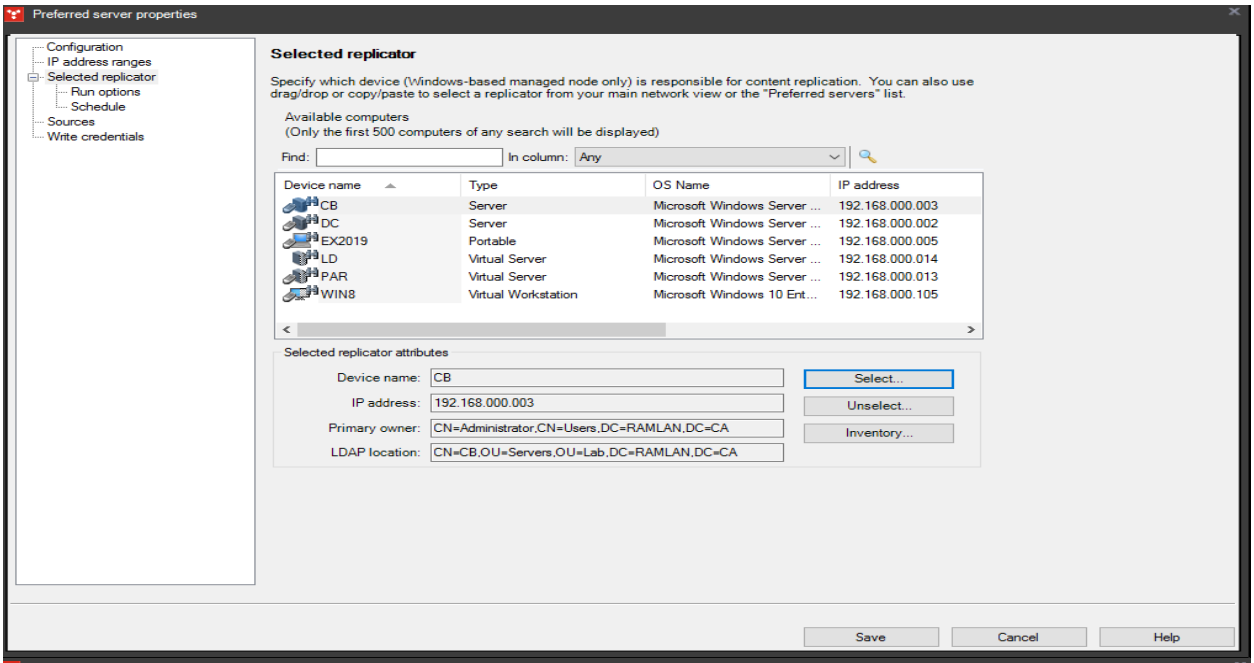
To configure preferred servers

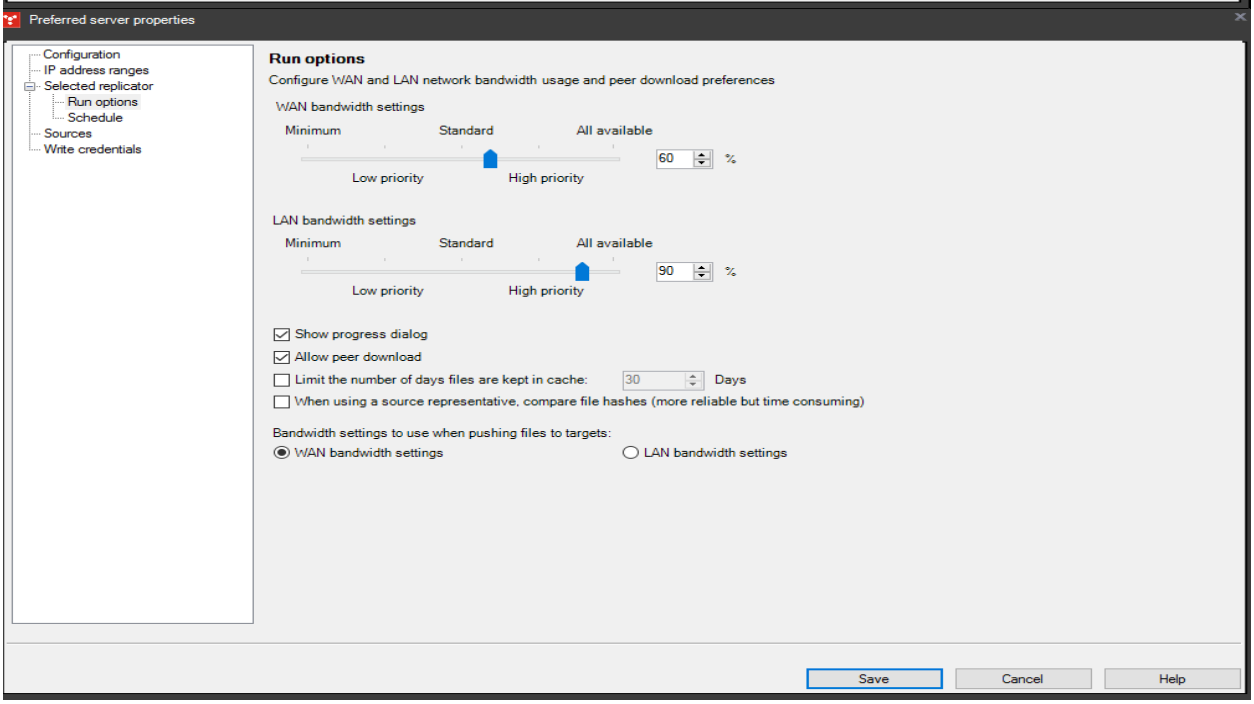
1. Click **Tools > Distribution > Content replication / Preferred servers**.
2. In the **Content replication** tree, right click **Preferred servers (Targets)** and click **New preferred server**.
3. On the Configuration page, enter the server information and read-only credentials. Click **Test credentials** to make sure the credentials are valid.
4. On the IP address ranges page, enter the IP address ranges you want this preferred server to allow.
5. On the **Selected replicator** pages, select the replicator, run options, and schedule. Click **Help** on each page for more information.
6. On the **Sources** page, select the source paths to be replicated.
7. On the **Write credentials** page, enter the credentials the replicator should use to write replicated files on the target preferred servers. Click **Test credentials** to make sure the credentials are valid.
8. Click **Save**.

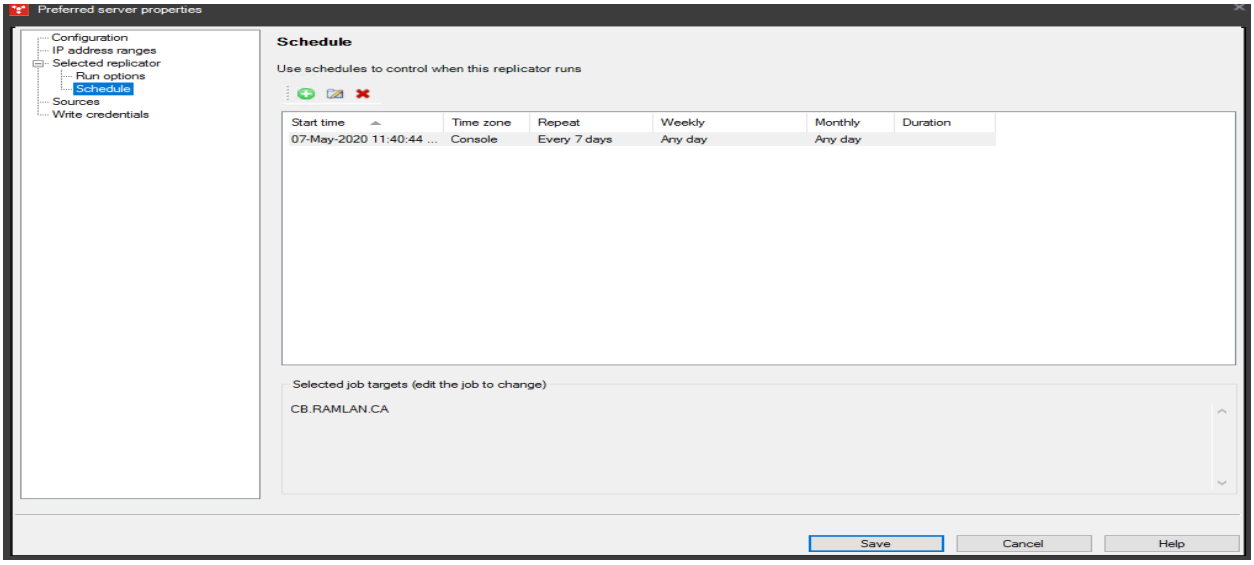


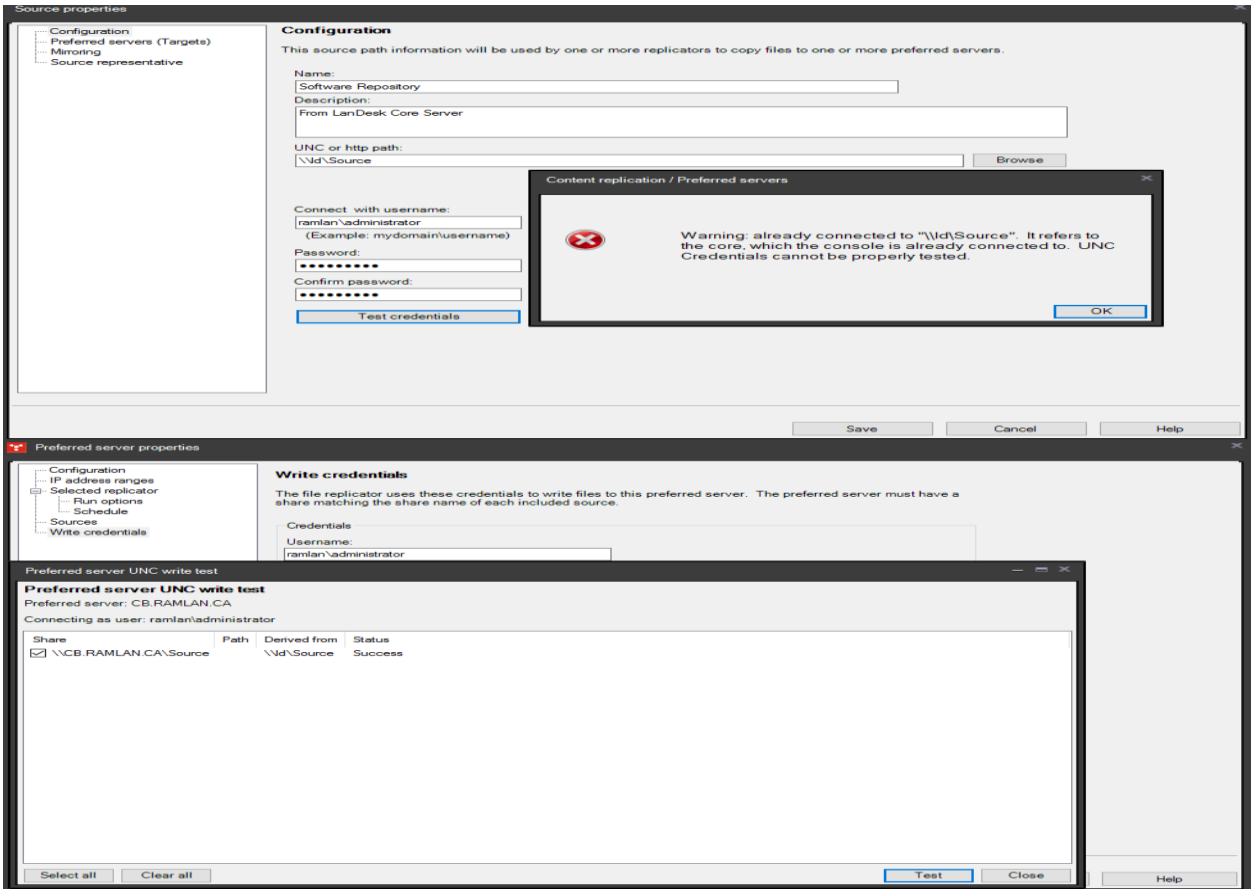



Preferred server properties
Configuration
IP address ranges
Selected replicator
Sources
Write credentials
IP address ranges
Only managed nodes within the specified address ranges will attempt to download files from this server.
Managed node IP address ranges
Starting IP address:
Ending IP address:
Add
Delete
Starting IP address
Ending IP address
192.168.0.0
192.168.0.255

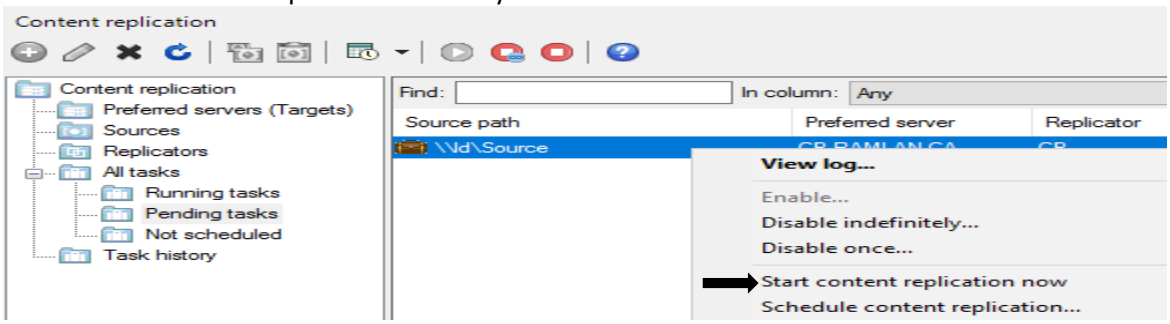

Preferred server properties
Configuration
IP address ranges
Selected replicator
Run options
Schedule
Sources
Write credentials
Selected replicator
Specify which device (Windows-based managed node only) is responsible for content replication. You can also use drag/drop or copy/paste to select a replicator from your main network view or the "Preferred servers" list.
Available computers
(Only the first 500 computers of any search will be displayed)
Find:
In column:
Any
Device name
Type
OS Name
IP address
CB
Server
Microsoft Windows Server ...
192.168.000.003
DC
Server
Microsoft Windows Server ...
192.168.000.002
EX2019
Portable
Microsoft Windows Server ...
192.168.000.005
LD
Virtual Server
Microsoft Windows Server ...
192.168.000.014
PAR
Virtual Server
Microsoft Windows Server ...
192.168.000.013
WIN8
Virtual Workstation
Microsoft Windows 10 Ent...
192.168.000.105
Selected replicator attributes
Device name:
CB
IP address:
192.168.000.003
Primary owner:
CN=Administrator,CN=Users,DC=RAMLAN,DC=CA
LDAP location:
CN=CB,OU=Servers,OU=Lab,DC=RAMLAN,DC=CA
Select...
Unselect...
Inventory...
Save
Cancel
Help

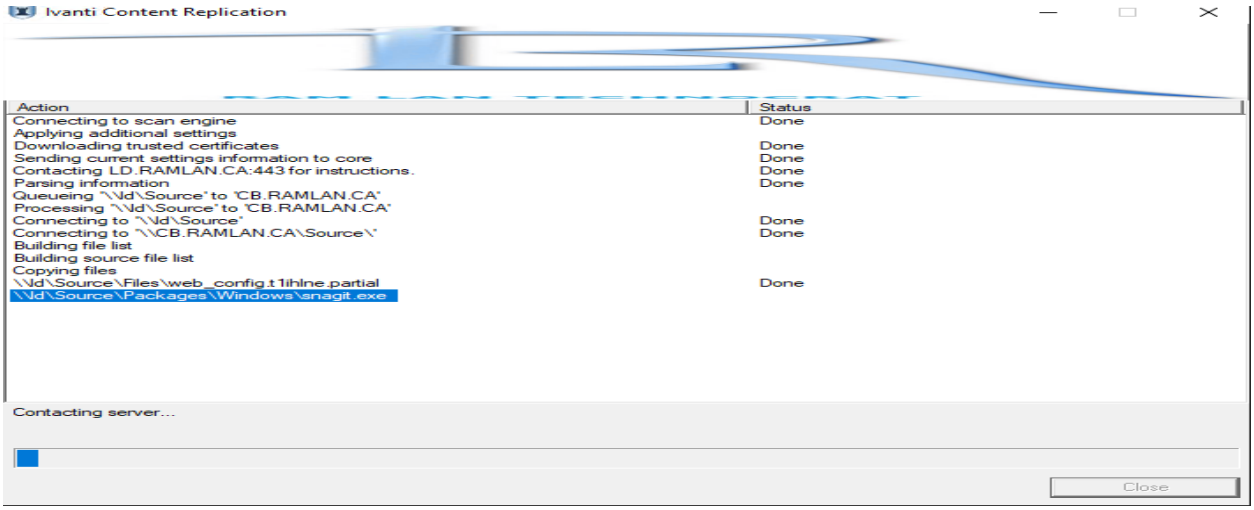

Preferred server properties
Configuration
IP address ranges
Selected replicator
Run options
Schedule
Sources
Write credentials
Run options
Configure WAN and LAN network bandwidth usage and peer download preferences
WAN bandwidth settings
Minimum
Standard
All available
60
%
Low priority
High priority
LAN bandwidth settings
Minimum
Standard
All available
90
%
Low priority
High priority
Show progress dialog
Allow peer download
Limit the number of days files are kept in cache:
30
Days
When using a source representative, compare file hashes (more reliable but time consuming)
Bandwidth settings to use when pushing files to targets:
WAN bandwidth settings
LAN bandwidth settings
Save
Cancel
Help



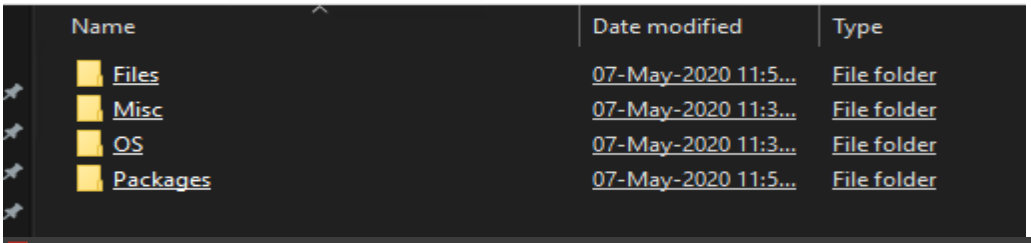


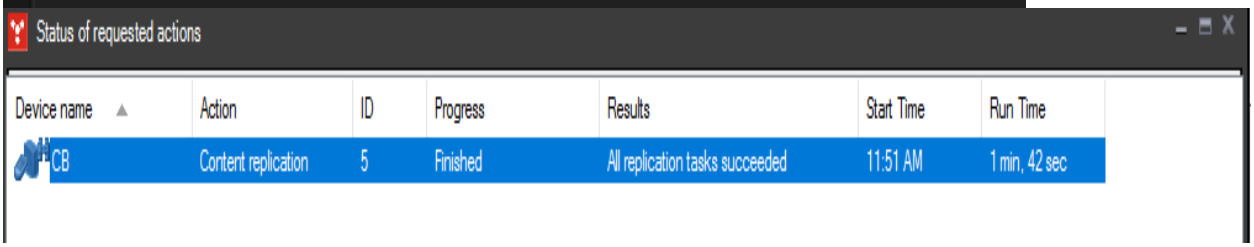
Now we can start the replication manually.

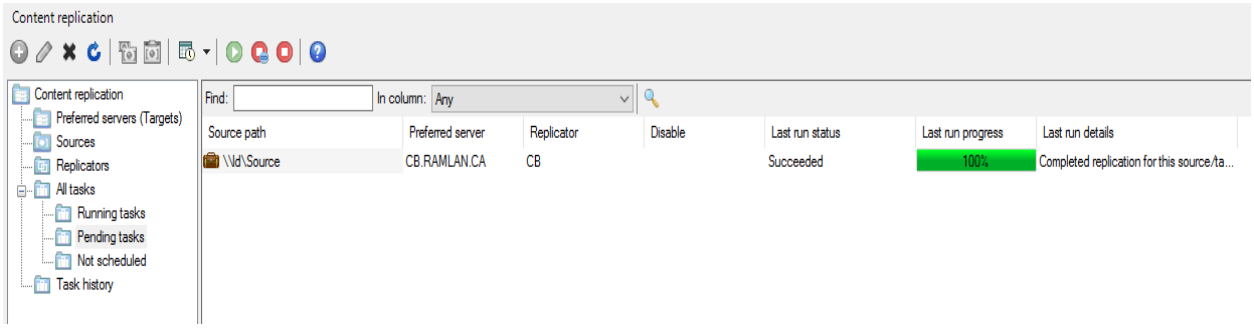


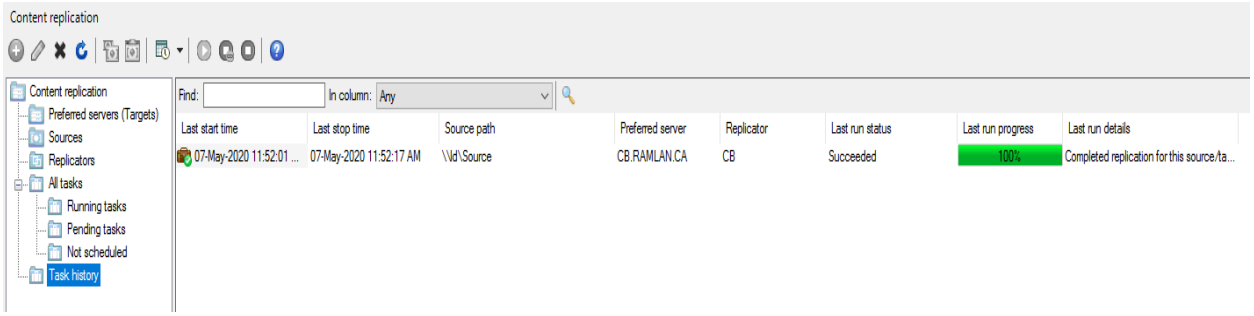

Ivanti Content Replication
Action
Status
Connecting to scan engine
Done
Applying additional settings
Downloading trusted certificates
Done
Sending current settings information to core
Done
Contacting LD.RAMLAN.CA:443 for instructions.
Done
Parsing information
Done
Queueing "\\ld\Source" to "CB.RAMLAN.CA"
Processing "\\ld\Source" to "CB.RAMLAN.CA"
Connecting to "\\ld\Source"
Done
Connecting to "\\CB.RAMLAN.CA\Source\"
Done
Building file list
Building source file list
Copying files
\\ld\Source\Files\web_config.t1ihlne.partial
Done
\\ld\Source\Packages\Windows\snagit.exe
Contacting server...
Close


CB › OS (C:) › Source ›


Name
Date modified
Type
Files
07-May-2020 11:5...
File folder
Misc
07-May-2020 11:3...
File folder
OS
07-May-2020 11:3...
File folder
Packages
07-May-2020 11:5...
File folder


Status of requested actions
Device name
Action
ID
Progress
Results
Start Time
Run Time
CB
Content replication
5
Finished
All replication tasks succeeded
11:51 AM
1 min, 42 sec


Content replication
Content replication
Preferred servers (Targets)
Sources
Replicators
All tasks
Running tasks
Pending tasks
Not scheduled
Task history
Find:
In column:
Any
Source path
Preferred server
Replicator
Disable
Last run status
Last run progress
Last run details
\\ld\Source
CB.RAMLAN.CA
CB
Succeeded
100%
Completed replication for this source/ta...


Content replication
Content replication
Preferred servers (Targets)
Sources
Replicators
All tasks
Running tasks
Pending tasks
Not scheduled
Task history
Find:
In column:
Any
Last start time
Last stop time
Source path
Preferred server
Replicator
Last run status
Last run progress
Last run details
07-May-2020 11:52:01 ...
07-May-2020 11:52:17 AM
\\ld\Source
CB.RAMLAN.CA
CB
Succeeded
100%
Completed replication for this source/ta...

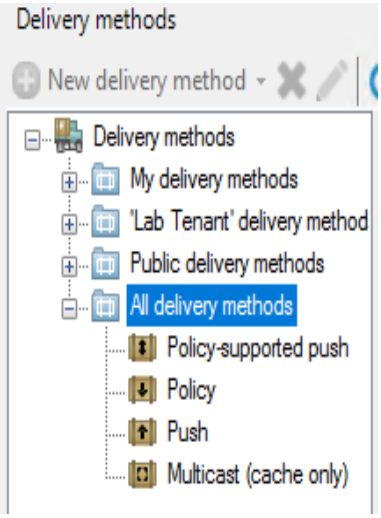
2. Delivery Methods

I did not configure anything for this option. Left with the default configuration.

Understanding the available distribution delivery task types

Once you schedule a package for distribution, you can use one of these delivery task types:

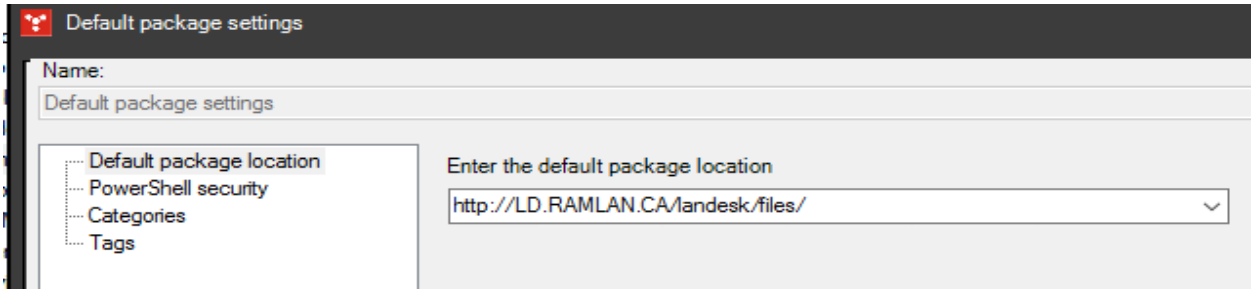
- **Policy-supported push:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it. Generally, this is the recommended delivery method.
- **Policy:** The core server makes the packages available for download. When a managed device checks for available policies, the package will be returned. Depending on the policy type, devices may install the package automatically or make the package available to users for them to install when they want.
- **Push:** The packages may be multicast out to the managed devices. The core server then initiates package installation at the managed devices.
- **Multicast (cache-only):** Copies one or more files to the local distribution cache folder but doesn't install the file or do anything else with it. This option can be useful when you know users will need to install a package soon, and you don't want them to have to wait for the download.



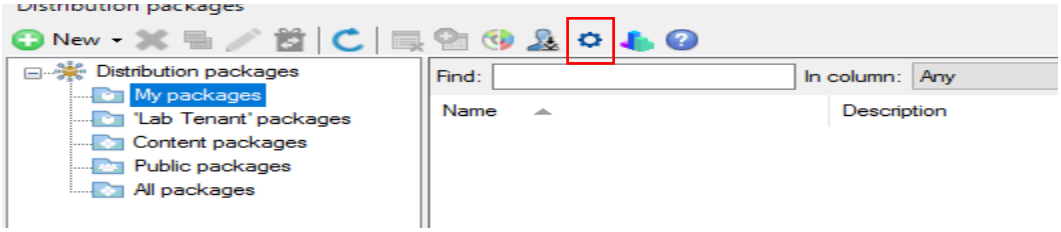
3. Distribution Packages

A. Change default package location for Software Distribution

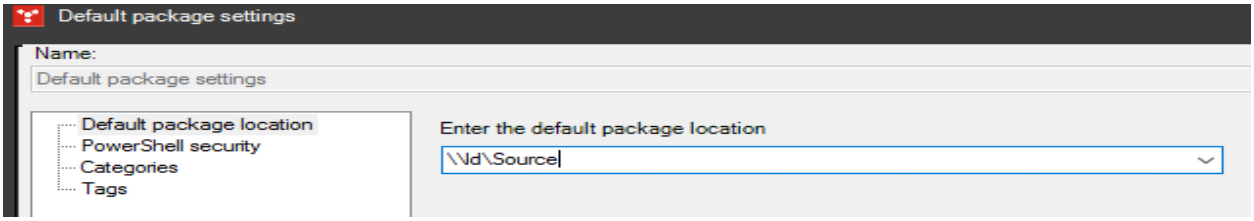
By default, when you install Ivanti Endpoint Manager the software distribution location is http link. It is not the ideal location. So, I would like to change the setting to this \\LD\Source



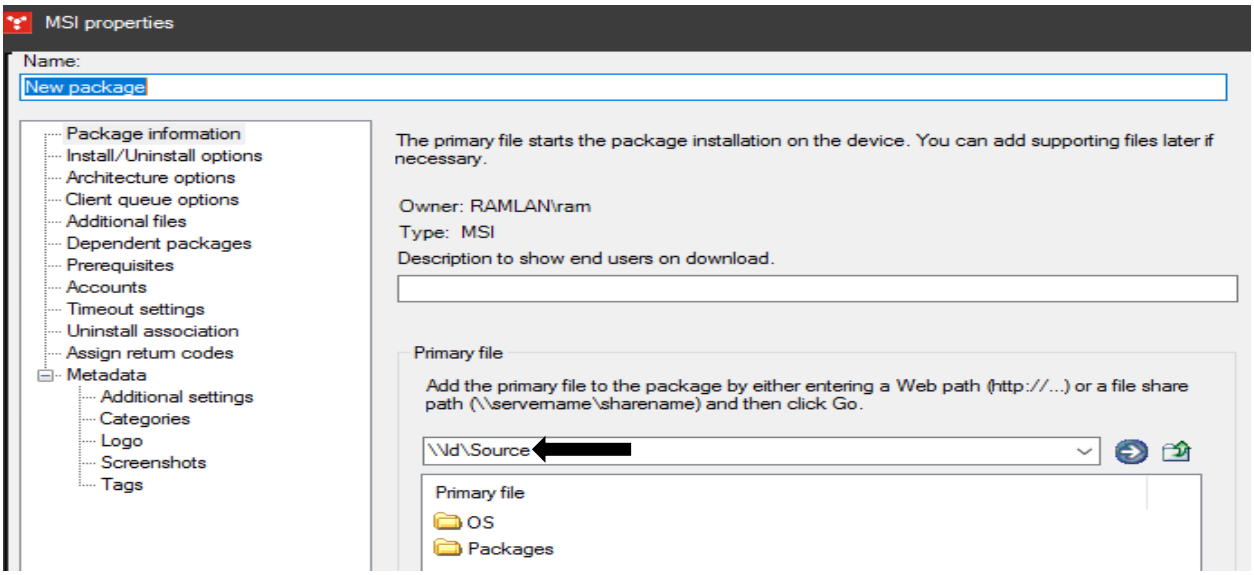
Click Tools > Distribution > Distribution Packages. The Distribution Packages panel will open at the bottom of the Endpoint Manager Console.



http://LD.RAMLAN.CA/landesk/files/ change to \\ld\Source

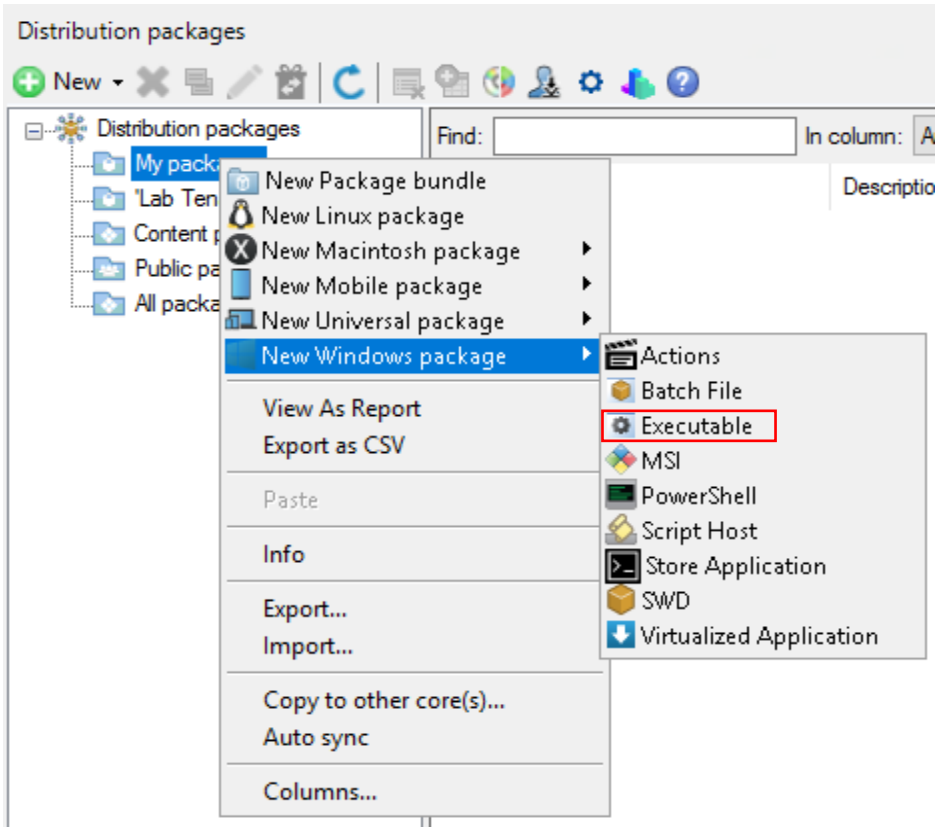


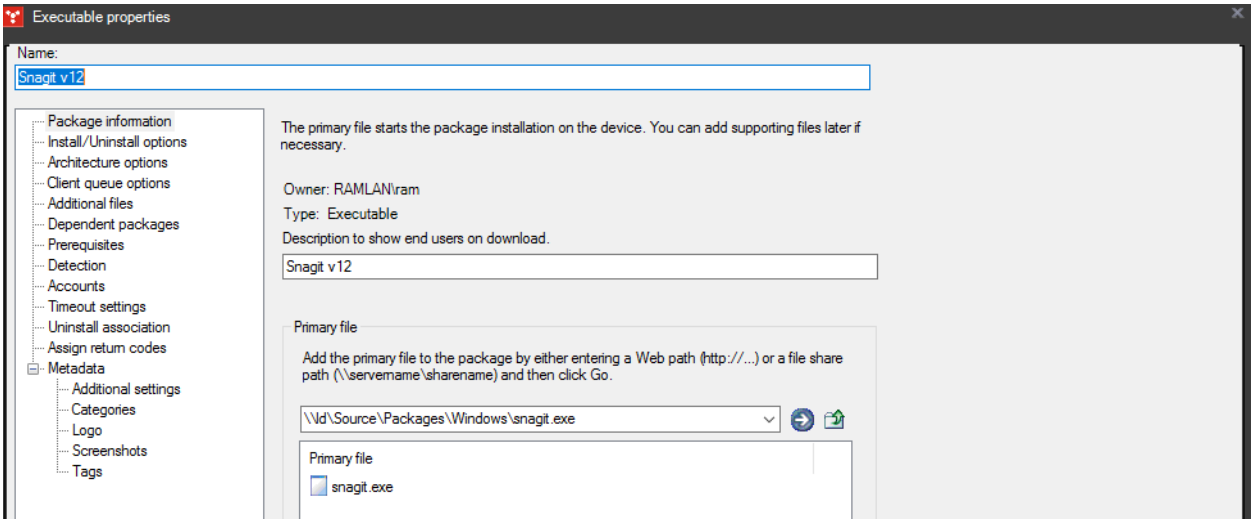
Test by creating New Package. The new source location is updated.

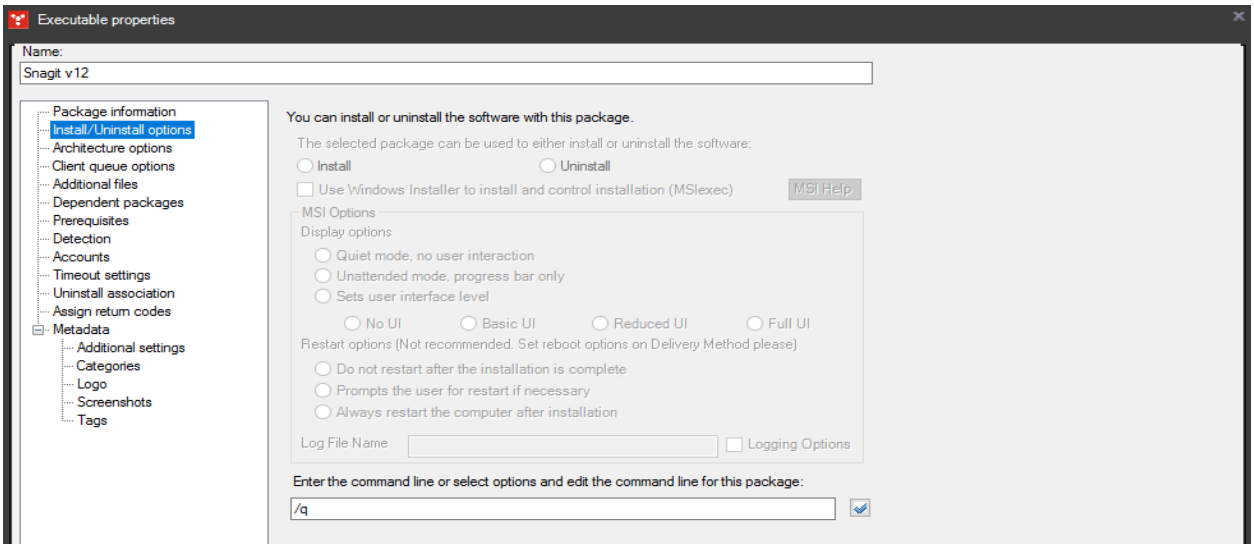


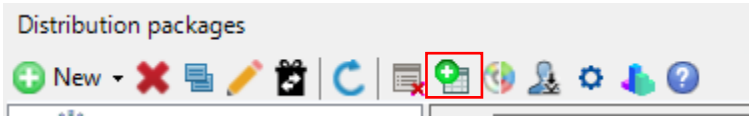
B. Creating EXE Package Deployment

I will show you EXE package creation within Ivanti Endpoint Manager.

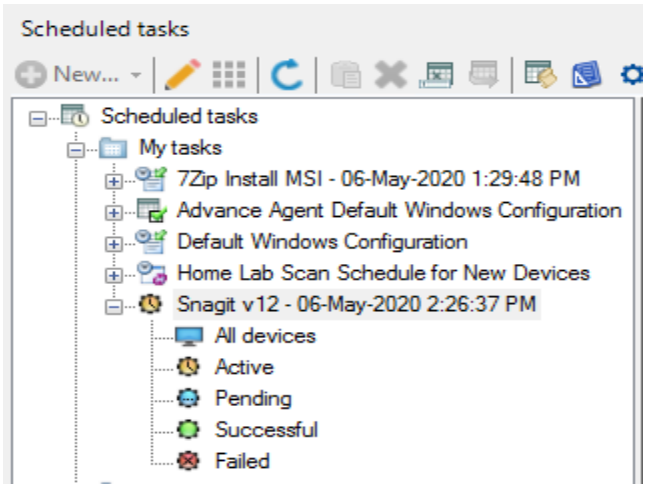




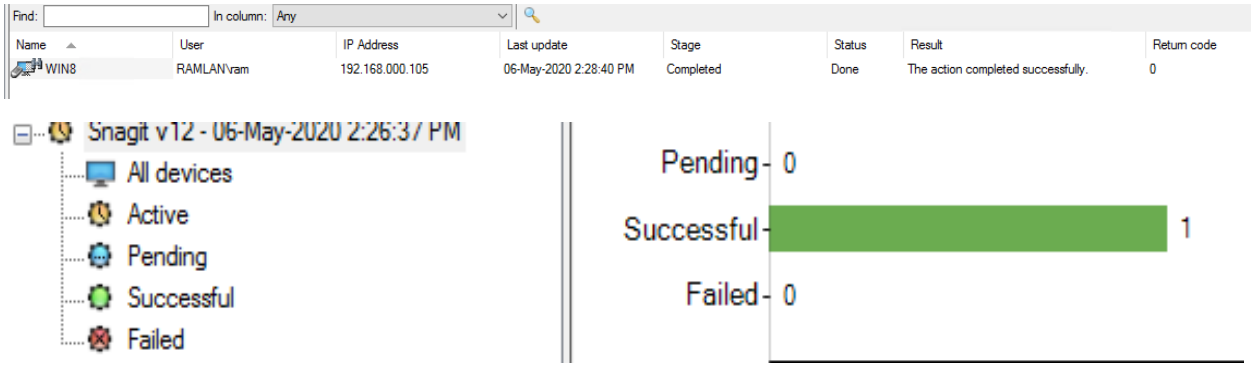




Drag & drop devices that require the package. In my case Win8. Right Click the task and Click Start - All

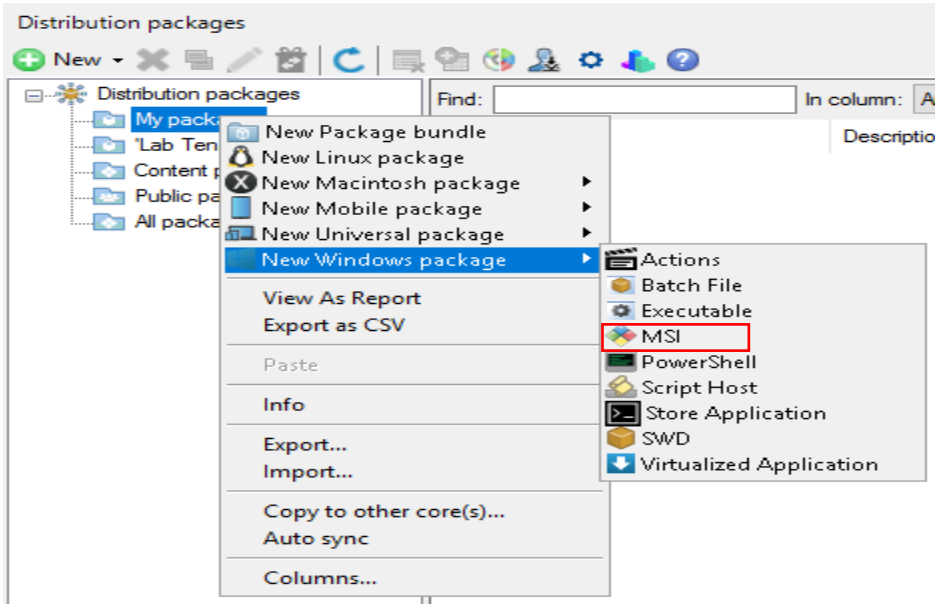


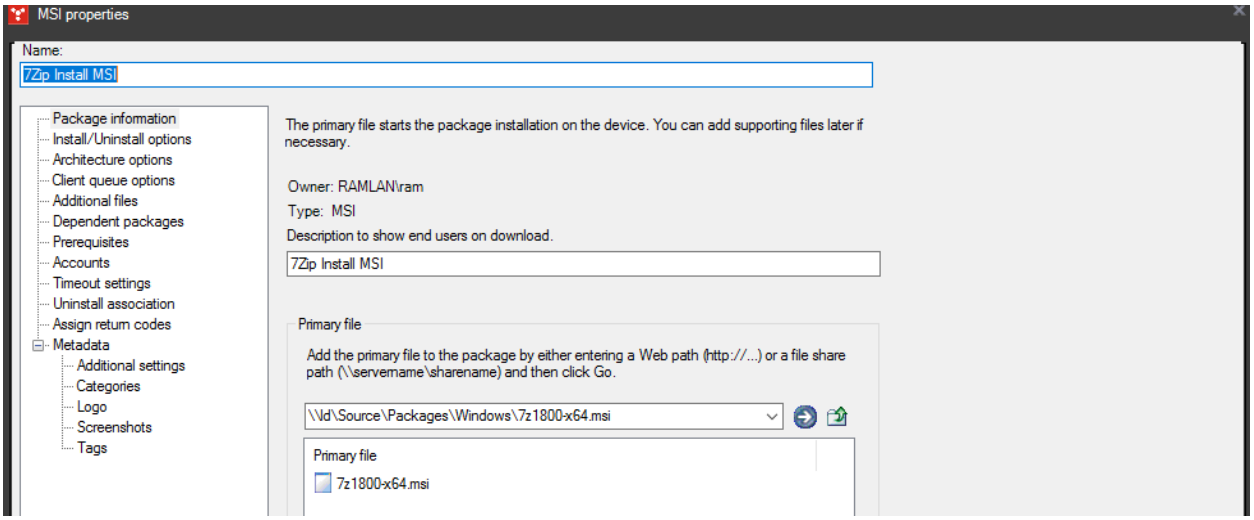
On the workstation open task manager and watch for SDClient process. This is the process that download the file and starts the install.

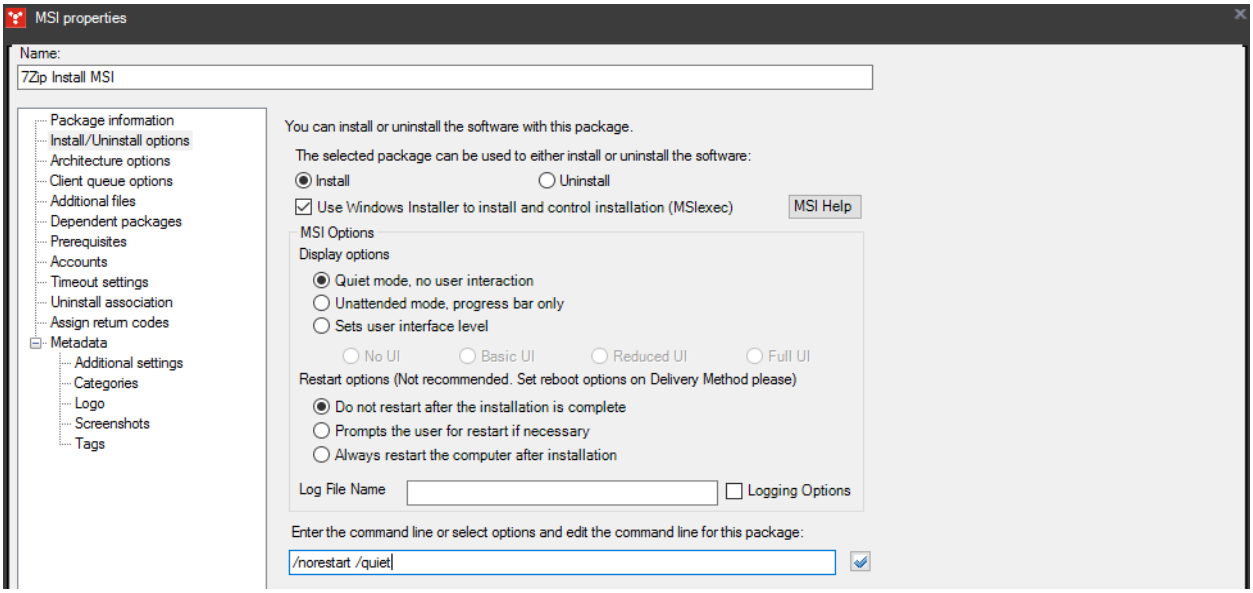


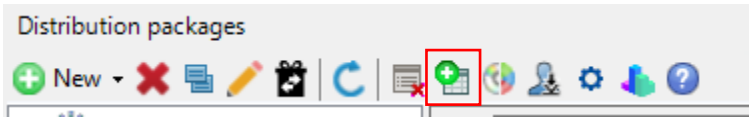
C. Creating MSI Package Deployment

I will show you MSI package creation within Ivanti Endpoint Manager.

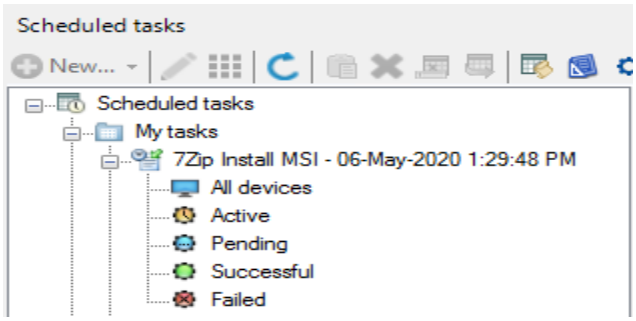




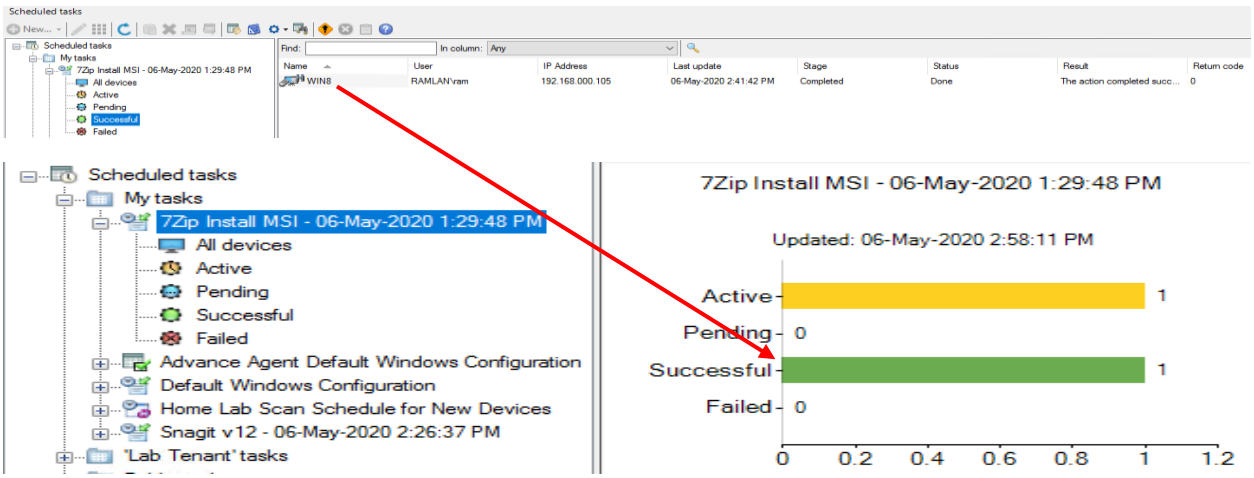




Drag & drop devices that require the package. In my case Win8. Right Click the task and Click Start – All



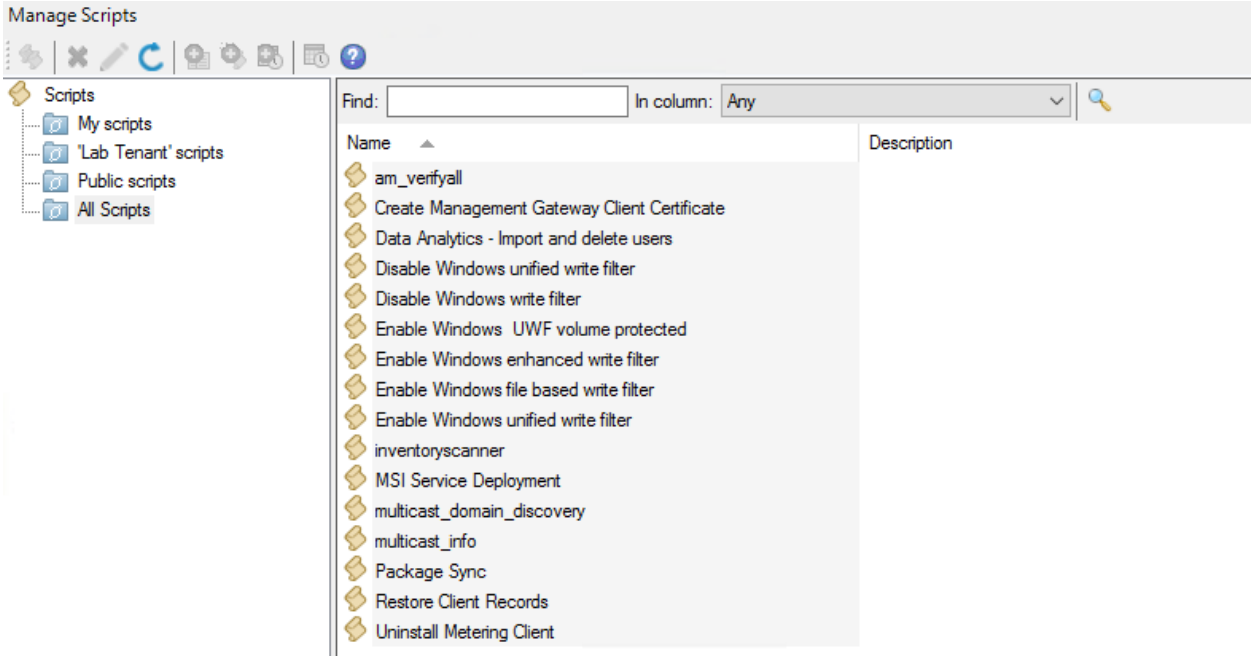
On the workstation open task manager and watch for SDClient process. This is the process that download the file and starts the install.



https://forums.ivanti.com/s/article/How-To-Create-and-test-an-msi-or-exe-software-distribution-package - Interesting link to check

4. Manage Scripts

From here you can create your own script and use pre created scripts for deployment.

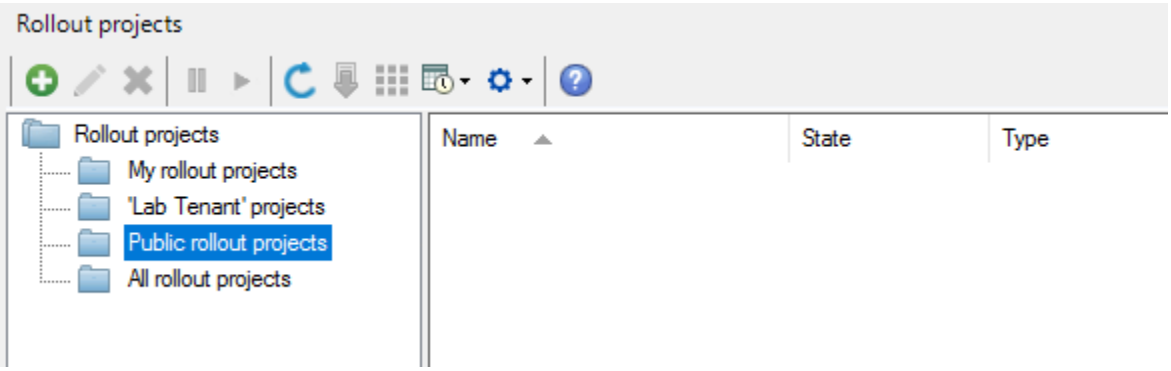


5. Rollout Projects

Rollout projects are a simplified method for managing vulnerability patching or software distribution. A rollout project is a set of steps to automate deployment. For each step, you can perform actions (such as a scheduled task), set criteria for when the content should move to the next step (such as an 80% success rate), and send notification emails.

When the patches or software packages have completed the actions in a step and pass the exit criteria, they are moved to the next step in the project. A project can be completely automatic, or you can require administrator intervention to make sure content doesn't progress until you approve it. And since you can set up email notices when a step succeeds or fails, you may not need to monitor the project as closely.

Use a rollout project for a distribution task that has multiple steps that can be automated. For example, applying patches in phases, or distributing new software to a pilot group before general distribution. Rollout projects are especially useful in situations where the task is frequently repeated or requires minimal oversight.



Example software package rollout project

To perform a staged rollout for new software, you can set up a rollout project to deliver the software to a small group first, and then after it has been installed on 80% or more of those devices, wait for a week to make sure things are working as designed. If the software fails to install on a significant percentage of devices within 2 weeks, set up the rollout project to send an email warning and don't push the software to a larger group. However, if everything works as planned, push the software to a larger group.

This example has two steps:

- Step One
  - Action: A scheduled task that distributes the software package to a small group.
  - Exit criteria: An 80% success rate, meaning that the package cannot move to Step Two until the success rate has been matched or exceeded.
  - Email: You get an email if the package is still in Step One after 2 weeks.
- Step Two
  - Action: A scheduled task that distributes the software package to a larger group.

Example patch rollout project

To create a rollout project to automate deploying Ivanti patches, set up the definition download settings to always add Ivanti patches to the rollout project. Apply the patches to your pilot group, send an email that the patches have been downloaded and applied, then wait until an administrator confirms that the patches are working successfully. Deploy the patches to a larger group, and then when the patches are installed on 85% of the devices, set the patches to Autofix and tag them with an Autofix tag to make them easy to identify.

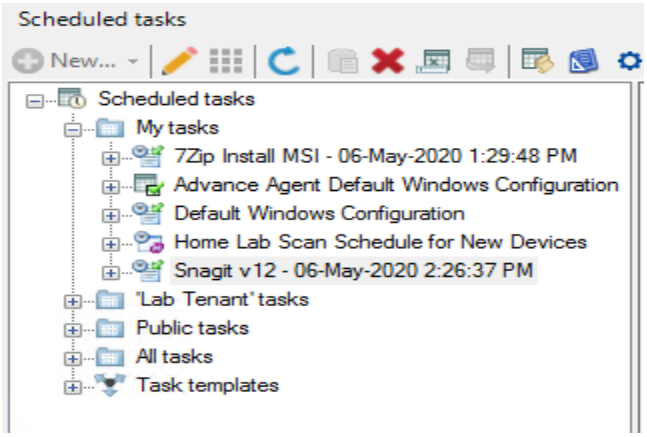
In this example, you change the definition download settings to add content automatically to a rollout project. When you use this feature, the downloaded content is added to the project and automatically begins to move through the project steps the next time the project processor runs. Since this feature requires no administrative oversight after it is set up, you'll probably choose to do this only in situations where you trust the content or you have an approval built into the project.

This example has three steps:

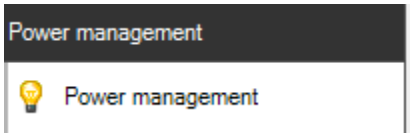
- Step One
  - Action: A scheduled task that applies the patch to your pilot group.
  - Exit criteria: An 85% success rate, meaning that the patch must be installed on 85% of devices.
  - Exit criteria: Administrator approval.
  - Email: After the success rate has been met, you get an email saying that the content is waiting for approval.
- Step Two
  - Action: A policy-supported push task that applies the patch to a larger group.
  - Exit criteria: An 85% success rate, meaning that the patch must be installed on 85% of devices.
- Step Three
  - Action: Set the patch to Autofix.
  - Action: Tag the patch as Autofix.

6. Scheduled Tasks

Here you will see all the task you have created and deployed so far.



POWER MANAGEMENT



1. Power Management

The Ivanti power management tool allows you to monitor power usage on your managed computers from a central location. You can easily create and deploy power management policies and generate reports to evaluate financial and power savings. You control the conditions under which computers and monitors stand by, hibernate, or power down.

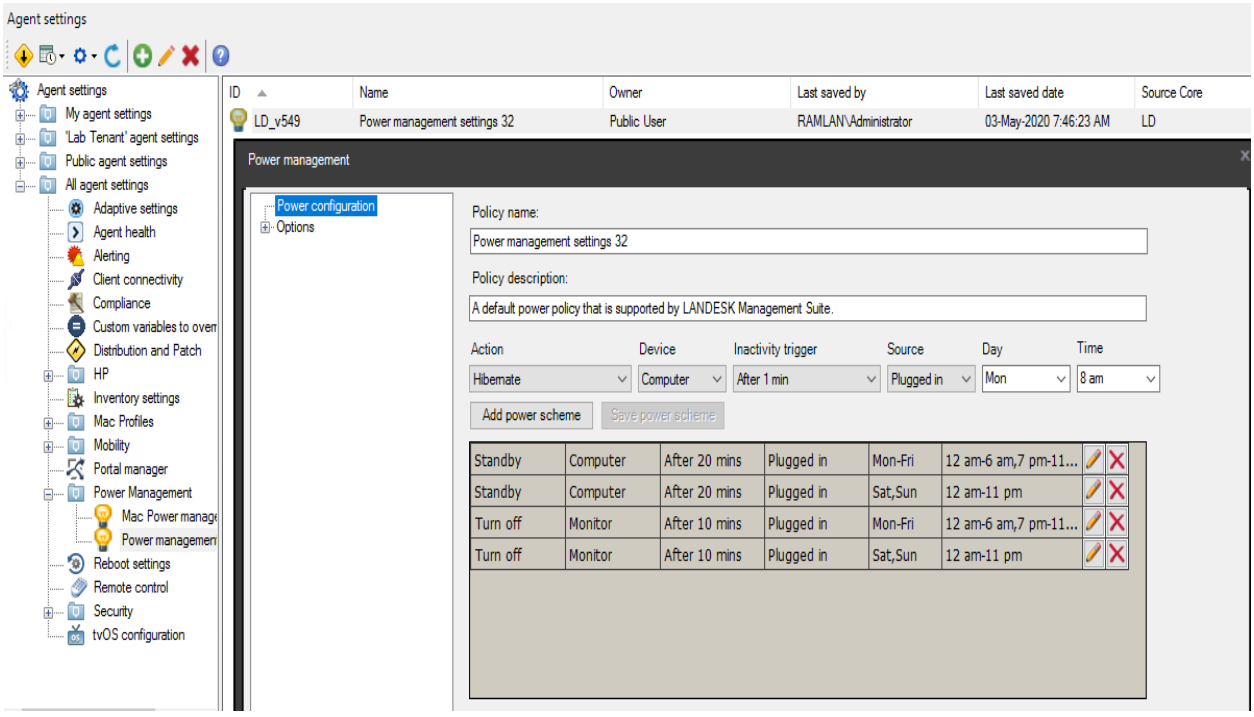
Power management includes a feature that lets users avoid specific power management actions (such as a hard shut down) using a client-side user interface. The avoided action will take place the next time the policy runs or is updated on that computer.

How it works

The Ivanti agent that is deployed to every managed device includes a power management option. When you choose to deploy a power management policy to a device, it is enabled as part of the agent.

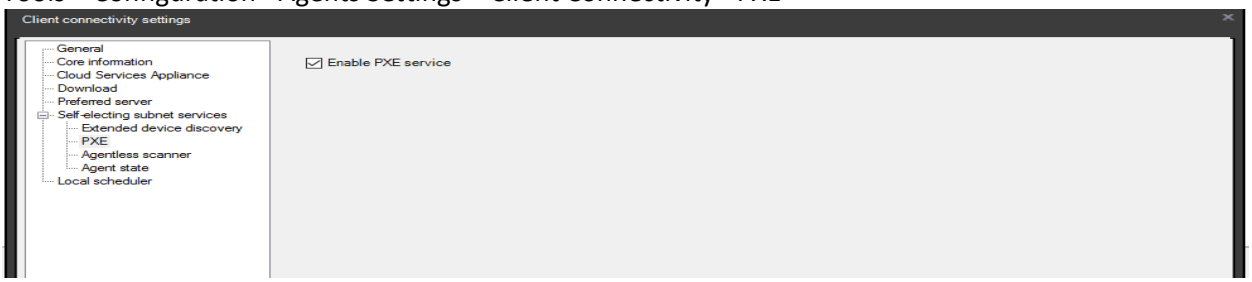
You define policies based on the specific needs of different types of managed devices. You can then deploy the policies to groups of devices in your organization. For example, you would define one policy for servers that need to be running continuously and a different policy for desktops that are typically not in use overnight and on weekends.

Below is the default power management that is part of Agent settings that is deployed to machines. I did not make any changes to this setting. Accepted default.

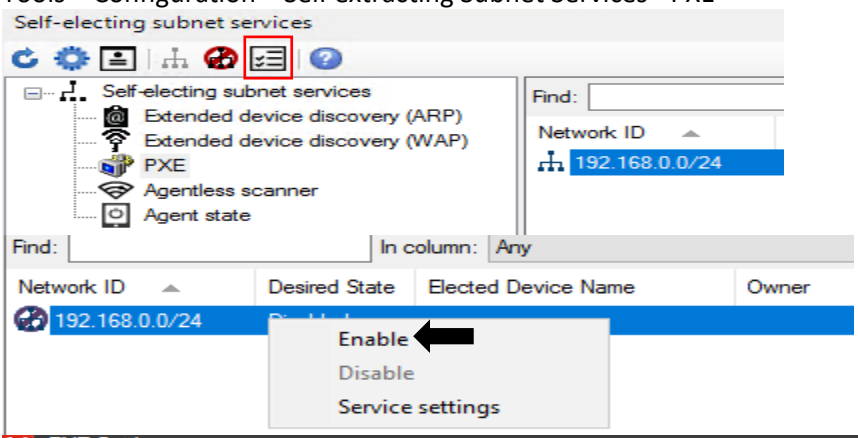


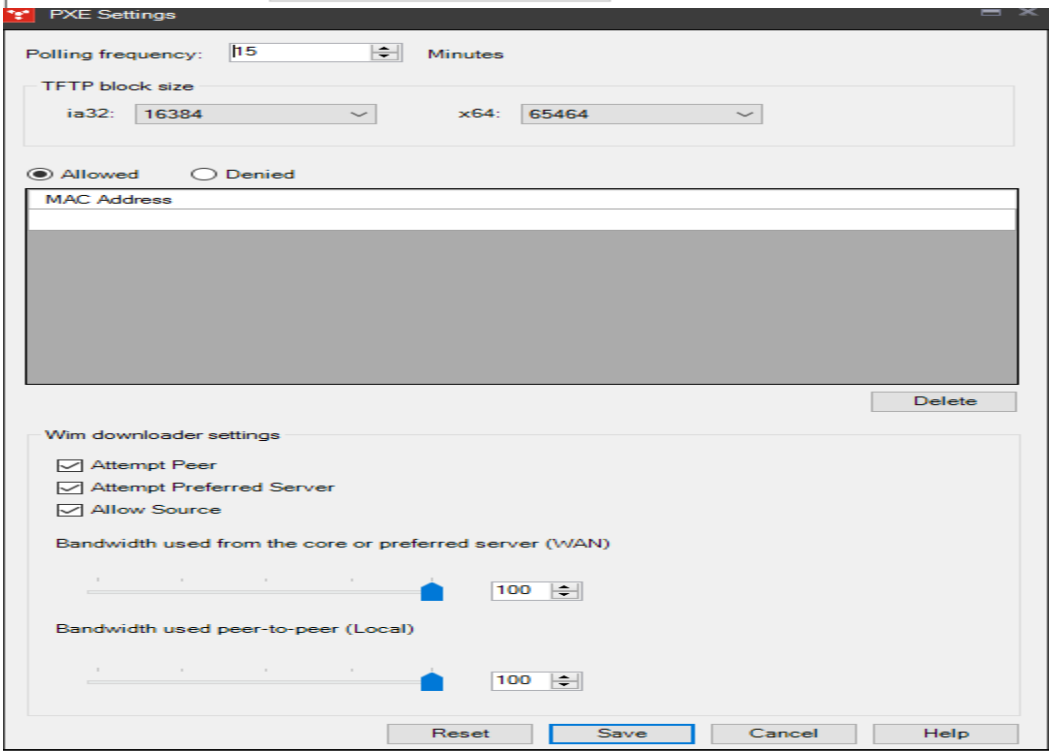
Enable PXE Service and Configure

Tools – Configuration - Agents Settings – Client Connectivity - PXE



Tools – Configuration – Self extracting Subnet Services - PXE





This concludes all the configuration with Ivanti Endpoint Manager. In the next blog, I will cover OS provisioning and deployment.

Thanks

Ram Lan
8th May 2020