



Network Discovery and Agentless Inventory Best Practices and Troubleshooting



Table of Contents:

Table of Contents

Network Discovery and Agentless Inventory Best Practices and Troubleshooting	1
Introduction	4
Network Discovery and Computers	4
Credential Management	5
Troubleshooting Tips:	7
Pluggable Protocol Architecture	8
Troubleshooting Tips	10
Initial Network Discovery	10
Considerations:	12
Troubleshooting Tips:	12
Device Classifications	12
Troubleshooting Tips	14
Advanced Settings	14
Discovery Engine	14
Main Engine	14
Port Scan	14
Master Browse List	15
PPA Connection Profile	15
ICMP	15
SNMP	15
AMT	15
Other Protocols	15
Network Discovery Task	16
Considerations:	17
Task Results	17
Discovered Devices Reports	18
Resource Manager	19
Network Discovery to Agentless Inventory	20
MIB Imports	21
Troubleshooting Tips	22
SNMP Data Mapping Tables	22
Troubleshooting Tips	24
Agentless Inventory Task	25



Troubleshooting Tips	25
Troubleshooting	26
SNMPutilg.exe	26
Conclusion	28

Introduction

This document is meant to help provide users guidance in using both Network Discovery and Agentless Inventory, and to provide details, processes, and tips to avoid issues and troubleshooting problems. In way of explanation, the engine that collects data for both Network Discovery and Agentless Inventory is the same engine. Before the technology was acquired by Altiris some time ago, the two products were one in the same. Much iteration later they are two distinct products, but Agentless does use the same engine for gathering data.

Note that Network Discovery must run successfully on a device before an Agentless Inventory can be collected for that device. Without a Network Discovery, Agentless does nothing. Consider Agentless an SNMP extension of Network Discovery.

Additional NOTE! Network Discovery is first and foremost a network device inventory/discovery tool. While it is capable of finding computers, there are other methods that may be better suited for that purpose, such as an AD Import of computer objects, or the Domain Discovery provided by the Platform in relation to finding systems to install the Symantec Management Agent.

Network Discovery and Computers

An often hot topic in support is the way Network Discovery handles computer discovery. When used alongside AD Import, Domain Discovery, and Symantec Management Agent installation, often duplicates can be created. These duplicates cause problems with reporting, target and filter management, and any aspect or picker in the Console where these duplicates may show up.

To combat duplication of computer records, consider the following:

- Avoid discovery of computers by Network Discovery.
- Run Network Discovery after the Symantec Management Agent has been installed.
- Clean up DNS so that Discovery gets the correct Name.Domain primary key. This primary key is the main way computers are identified uniquely in discovery circumstances.
- Use AD Import or Domain Discovery instead of Network Discovery for the purpose of finding systems to install the Symantec Management Agent on.
- Do not use AD Import or Domain Discovery if Network Discovery is meeting your needs. The three different discovery methods are redundant in a lot of cases so it may be best to choose one of the three to use.
- Delete duplicates after a Network Discovery if the situation cannot be avoided.

Not all of these items are doable depending on the circumstances. Network Discovery is looking to help the duplicate issue by reevaluating the items used to identify unique machines already registered in the Symantec Management Platform.

The following process is used when looking up existing systems within the Symantec CMDB Database.

There are 2 primary keys used by Network Discovery in order to avoid creating duplicates and instead updating existing records in the database. These keys are:

- NetBios Name, Domain (name.domain key)
- MAC Address

This comparison is done against the results from the stored procedure tmBuildTargetDeviceCache which uses the vTaskTargetDevices view which obtains MAC addresses from the Inv_AeX_AC_TCPIP table. This table is populated



by the Symantec Management Agent as part of Basic Inventory, or is populated by Stand-alone Inventory, AD Import, or Domain Discovery. Most discovery or agent inventory pieces contain this data class.

Note: `vTaskTargetDevices` returns information about only one NIC for each computer. So relevant information may be ignored for computers with multiple NICs. While certain dummy NICs are ignored (those with IP addresses 0.0.0.0 or 127.0.0.1). Of the remaining NICs, the NIC about which information is returned is arbitrarily selected. So a different NIC may be returned by `vTaskTargetDevices` each time it is run.

With Network Discovery using ICMP or SNMP, ND creates and/or modifies the following resource keys

- hostname = CL-XP-01
- nbname.domain = CL-XP-01.EPM
- macaddress = 00-50-56-05-41-76

Additionally Network Discovery creates and/or modifies the FQDN resource key with the devices short name, for example:

- fqdn = CL-XP-01

Whereas the Altiris agent also creates and/or modifies the FQDN resource key with a longer name, for example:

- fqdn = CL-XP-01.EPM.LOCAL

Note: This discrepancy causes the resource key to alternate between these two values. I am not aware of any adverse effects of this discrepancy.

Thus if the MAC address or netbiosname.domain values do not match up, a duplicate will be created.

See more in the Troubleshooting section to understand how to troubleshoot duplicate issues. Also see the section on the Discovery Engine to see how Network Discovery is finding and capturing data on computers.

Credential Management

Before we dive into Network Discovery, we need to ensure that the proper credentials are setup. These credentials will be used by Network Discovery to gather data on a specific device. While not all credentials are necessary, it is good to have as many available to allow the best results with the Discovery.

To review what credentials are provided by default, follow these steps:

1. In the Symantec Management Console, browse under Settings > All Settings > Monitoring and Alerting > Credential Settings > and select Credentials Management.
2. The list of credentials will be listed. Note that some credentials may only be set to default and will not show up at this location.

Add what credentials are necessary. The subsequent steps will walk you through the most typical credentials used for a Network Discovery. Again not all need to be used.

1. Click the Add Credentials button.
2. Under the Credential type, select SNMP V1 V2 Read Credentials.
3. Provide a Name for the credentials (this will be the label for the credentials provided).
4. Provide all Community Strings used in your environment. Multiple strings can be added using space delimited.

- If needed, set the Expiration date and limit who can use the credentials.

Add Credential

Select the credential type and enter information

Credential type:

*Name:

*Read:

Expiration date: 

Who should be allowed to use this credential:

Only me

Let me select which users

- Click OK to save the credentials.
- Click Add Credentials.
- Choose WMI Credentials from the Credential type dropdown.
- Provide a Name.
- Provide a Domain for the credentials to use. As WMI is a Windows-based protocol this should be the Domain your Windows systems belong to.
- Provide a Username and Password that has local administrator rights on your target Windows computers. Admin rights are generally required for WMI interaction.
- If needed, set the Expiration date and limit who can use the credentials.

Add Credential

Select the credential type and enter information

Credential type:

*Name:

*Domain:

*Username:

Password:

Confirm Password:

Expiration date: 

Who should be allowed to use this credential:

Only me

Let me select which users

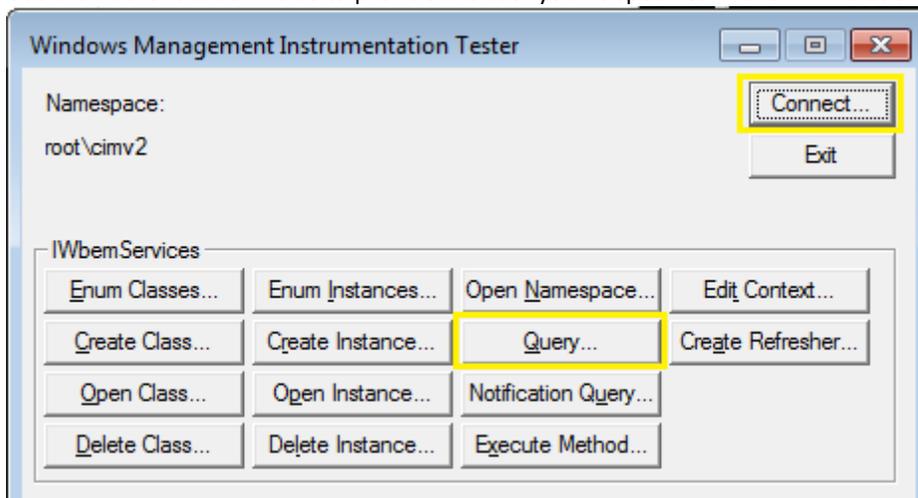
- Click OK to save the credentials.
- Click Add Credentials.

15. Choose SSH Credentials from the Credential type dropdown.
16. Provide a Name.
17. Provide a Username and password that has access to your Mac systems.
18. If needed, set the Expiration date and limit who can use the credentials.
19. Click OK to save the credentials.
20. Not all available credentials are used by Network Discovery, but the above are the most common.

Now that we've setup the proper credentials for use with Network Discovery, we can now configure a Connection Profile to use the set of Credentials.

Troubleshooting Tips:

- If SNMP Community strings are not working, try using the default, which is public only. "public" is the default community string for all network devices and will work unless it has been changed.
- Try specifying only one community string at a time if authentication and SNMP gathering does not appear to be working. This allows you to test specific credentials.
- WMI credentials use Windows-based authentication, typically via AD. If WMI information is not being gathered, check your WMI credentials against a system to ensure that user has rights to the local system. You can test WMI with the following process:
 - o Log onto the Symantec Management Platform server.
 - o Launch Windows WMI utility by going to Start > Run > type wbemtest > and click OK.
 - o Click the Connect button.
 - o The Namespace was given \\computersname\root\cimv2, so type this into the Namespace area if it is not already set.
 - o Use the Authentication fields to provide the user you've specified in the WMI credentials.



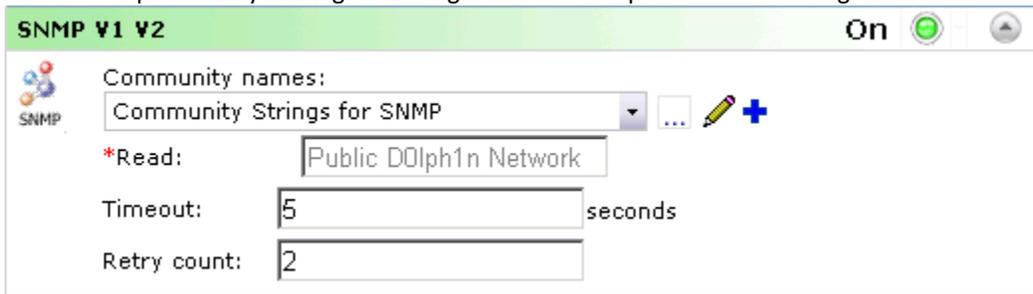
- o Click Connect. By using the Computer Name in the Namespace and providing the authentication, this utility will attempt to connect via WMI, and we can see if WMI is working properly from the NS to the target computer.
- o You can run a WMI query using the query button for further testing, such as querying `SELECT * FROM Win32_Processor`
- Make sure to add Public if you create your own SNMP credential as it will catch any devices that have not had their community strings updated.

Pluggable Protocol Architecture

Pluggable Protocol Architecture, or PPA, provides a profile that allows you to use multiple credentials and protocols for tasks needed by the Notification Server. Network Discovery requires the use of a connection profile from PPA in order to authentication and use the various protocols it supports. In the previous section we created the credentials needed, and now we'll tie them together using a connection profile in PPA.

The following steps walk through setting up a Connection Profile for use with Network Discovery.

1. In the Symantec Management Console, browse under Settings > All Settings > Monitoring and Alerting > Protocol Management > Connection Profiles > and select Manage Connection Profiles.
2. Click the Add settings button.
3. Provide a Connection profile name, such as "Network Discovery Protocols".
4. In the list of protocols, use the arrow to expand the section for ICMP.
5. Increase the Timeout to 1000 milliseconds.
6. Increase the Retry count to 2.
NOTE: Increasing the timeout and retry count will increase the time it takes for a Discovery to run
7. Turn on the protocol by clicking the red light indicator dropdown and selecting "On".
8. In the list of protocols, use the arrow to expand the section for SNMP V1 V2.
9. From the community names: dropdown, select the credentials created previously for SNMP V1 V2. Note that if you did not need to create a credential for this, *i.e.* public is the correct community string for all devices, the default credential will work.
10. Review the Read field to ensure you have the correct community strings listed.
11. Timeout and Retry count values are generally sufficient.
12. Turn on the protocol by clicking the red light indicator dropdown and selecting "On".



13. In the list of protocols, use the arrow to expand the section for SSH.
14. In the dropdown, select the credentials you created for SSH.
15. Check the details to ensure the Username is the one you intend for the Discovery process.
16. Change the Port if needed, and increase the Timeout only if timeouts are suspected.
17. Turn on the protocol by clicking the red light indicator dropdown and selecting "On".
18. In the list of protocols, use the arrow to expand the section for WMI.
19. In the dropdown, select the credentials you created for WMI.
20. Check the details to ensure the Domain and Username is the one you intend for the Discovery process.
21. Timeout and Retry count values are generally sufficient.
22. Authentication Level is generally sufficient being unchecked.
23. Enable and check the settings for any other protocol you may be using, such as AMT.
24. Click OK to save the connection profile.

When complete, ensure all desired protocols are turned on. The following screenshot shows an example of the completed profile, without SSH since no Mac systems were to be discovered:

Define Group Settings

Connection profile name:

[Access permissions to protocols settings](#)

Network protocols

Protocols can be turned on or off

ICMP	On
 Timeout: <input type="text" value="500"/> ms Retry count: <input type="text" value="1"/>	
IPMI	Off
SNMP V1 V2	On
 Community names: <input type="text" value="Community Strings for SNMP"/>	
*Read: <input type="text" value="Public D0lph1n Network"/>	
Timeout: <input type="text" value="5"/> seconds Retry count: <input type="text" value="2"/>	
SNMP Trap Sender	Off
SSH	Off
MD Array	Off
VMware	Off
WMI	On
 <input type="checkbox"/> Runtime credentials <input type="text" value="Windows Authentication"/>	
*Domain: <input type="text" value="MyDomain"/> *Username: <input type="text" value="Administrator"/> Password: <input type="password" value="....."/> Confirm Password: <input type="password" value="....."/> Timeout: <input type="text" value="5"/> seconds Retry count: <input type="text" value="1"/>	
<input type="checkbox"/> Use authentication level Authentication level: <input type="text" value="Default"/>	

You are now ready to run a Network Discovery!

Troubleshooting Tips

- If you are getting inconsistent results, where some devices are discovered and others are not, increase the timeout settings for both ICMP and SNMP. If latency on the network causes a timeout to occur, we may not gather data on a device. For ICMP triple the numbers, and for SNMP double them. Play with these settings as it will increase the time it takes to run a Network Discovery, so you can find the lowest timeout value possible that will work in the environment.
- For WMI if it is not working as you would suspect, and you've successfully used wbemtest to connect to it, you may need to enable Use authentication level. There are a number of values so they will need to be tested in order to find the right one. It is recommended to test against a single Windows computer as you work to find a valid setting.
- Disable protocols not being used. If all Protocols are enabled, each protocol will be attempted against each IP Address found as part of the Discovery process. This will increase the amount of time it takes to complete a Network Discovery.

Initial Network Discovery

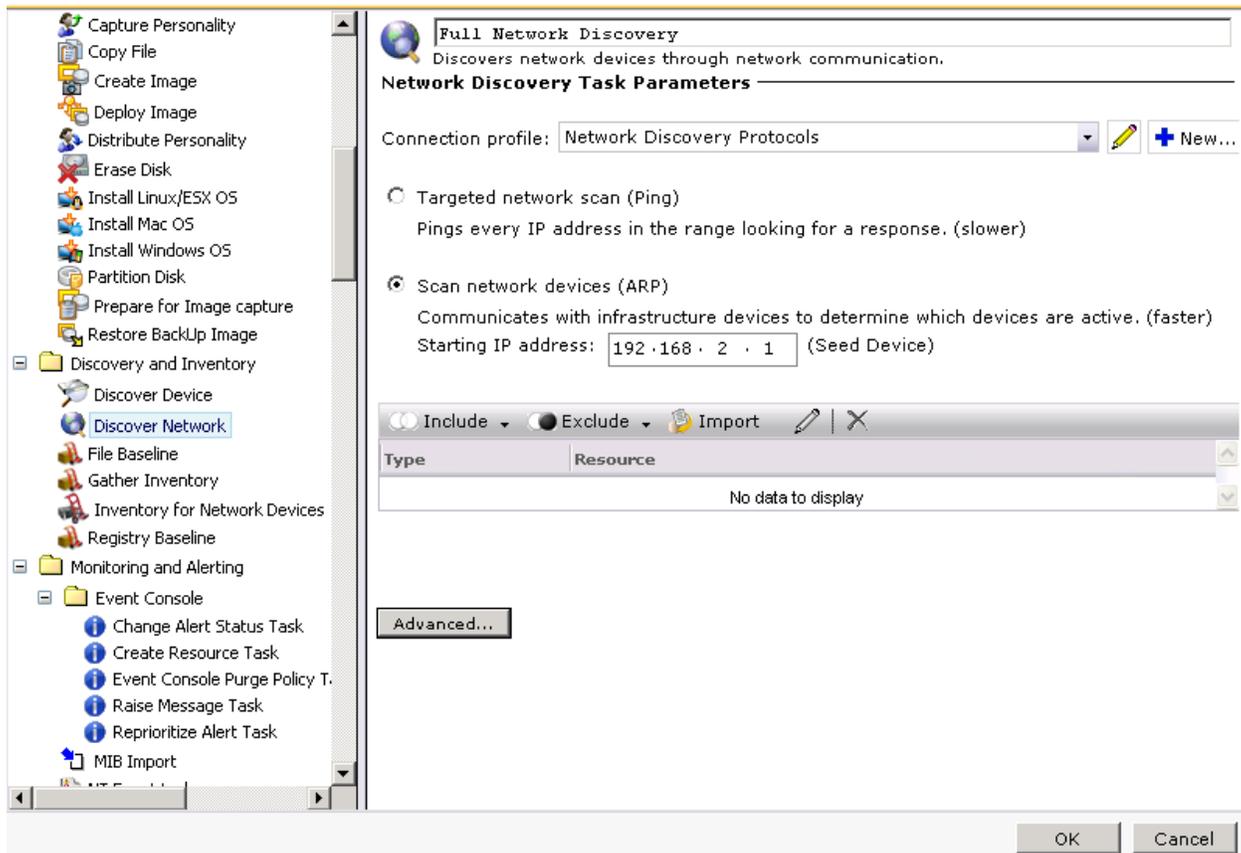
Unless you already know all the make and model information for your network devices, often an initial Network Discovery needs to take place. This allows the discovery to return information on devices which will then allow us to properly add Device Classifications. If you've already run a Network Discovery, then this part is complete.

Steps to run through the initial discovery are listed here:

1. In the Symantec Management Console browse under Manage > Jobs and Tasks > in the left-hand tree browse under System Jobs and Tasks > Discovery and Inventory > and select Network.
NOTE: You can create a Network Discovery Task from whatever location you wish within the Jobs and Tasks tree. The above is just a typical place to create such a task.
2. Right-click on the containing folder and select New > Task.
3. From the left-hand tree, locate the folder for Discovery and Inventory, and select Discover Network.
4. Provide a name for the discovery, such as "Full Network Discovery".
5. From the Connection profile dropdown select the connection profile we created previously, or that you have configured separately.

- Configure the scan type, either Targeted (Ping), or ARP or seed device. This can be edited later after creating the Task. For this example I selected Seed Device (Scan network devices (ARP)).

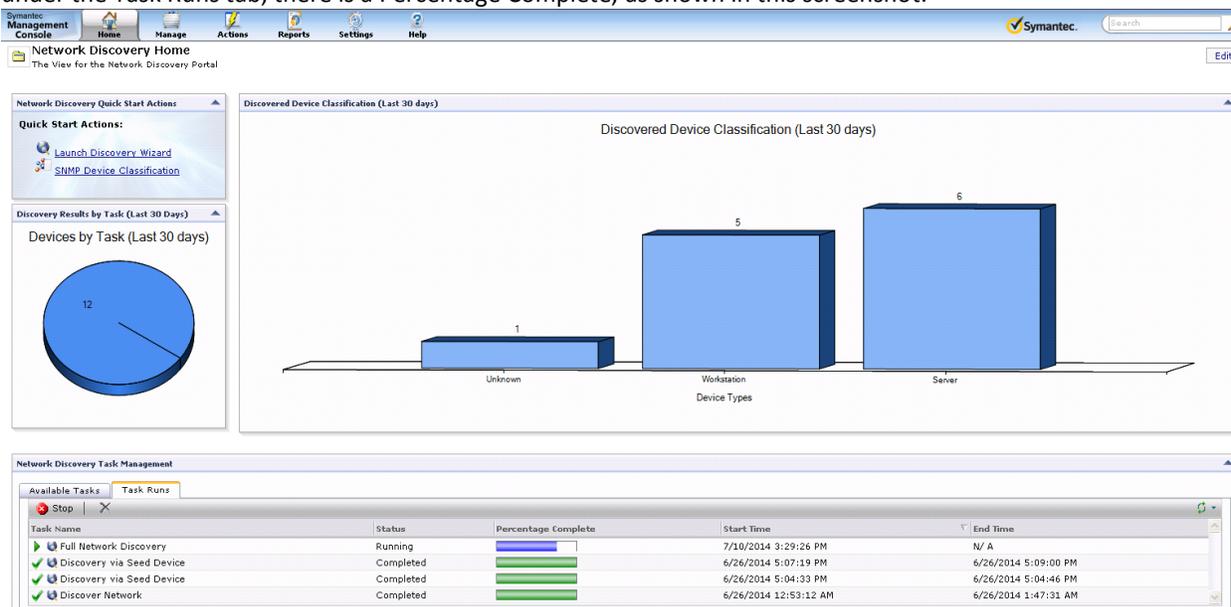
Create New Task



- Click OK to save the Task.
- In the main console the task will now load in the tree and the details within the right-pane.
- Check the considerations listed below before scheduling the discovery.
- Click the New Schedule option.
- If you choose the Now radial, the discovery will execute immediately. It can also be set to a Schedule to run during off-peak times, if that is required.
- Click the Schedule button.
- Done!

To check progress, in the Symantec Management Console browse under Home > Discovery and Inventory > and select Network Discovery. This will provide an overview of all Discoveries, but note that at the bottom webpart,

under the Task Runs tab, there is a Percentage Complete, as shown in this screenshot:



Considerations:

- IP Ranges will take considering longer if a large range is included. We will start by pinging every IP Address, waiting for the timeout and executing the retry count. Take this into mind when scheduling a range.
- A huge range, such as a class B subnet, is not recommended. A class B subnet has thousands and thousands of IP Addresses in the range so a discovery will take a very, very long time.
- Find out what specific ranges are being leased on the network so that those ranges can be added.
- When selecting a Seed Device the ARP table, or every device and its IP that it knows about, will be used to check what IP Addresses to query against. Most Seed devices will provide what is directly connected to them, and will have the ARP tables of other routers and switches it knows about. This may create a very large discovery, so IP ranges may be needed in very large environments.

Troubleshooting Tips:

- If a Discovery does not kick off, Try restarting the Altiris Object Host Service. This is the Task Server service that Network Discovery uses. Task Server executes the Discovery engine, so if Task Server is having problems restarting that service may allow the Discovery to execute.
- If a Network Discovery instance is not starting and you wish to try and schedule another, it is recommended to delete the first instances so they do not overlap, or the previous one kicks off later.
- When Network Discovery Tasks perpetually do not kick off typically this can be a Server task or Job Task Server issue. Please refer to the following KB for possible cause and resolution: www.symantec.com/docs/TECH209754.
- Trace logging can be very useful in troubleshooting problems with the Discovery process. Check the section for Troubleshooting Network Discovery for more details.

Device Classifications

Specifying device classifications allows you to set not only the device type, make and model, but also the resource type The Symantec Management Platform will use to classify the device within the Altiris framework. Classifications are based solely on SNMP, so a device must be capable and SNMP must be enabled to be able to

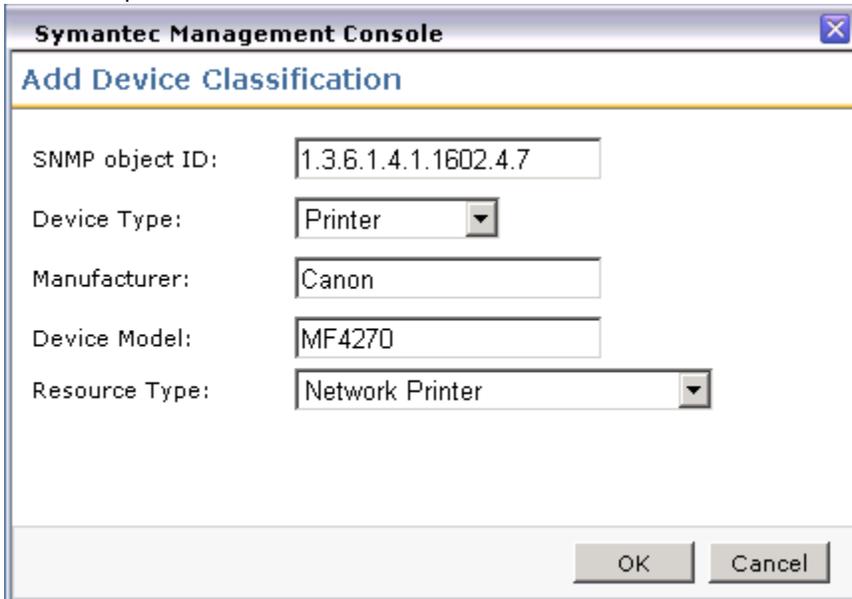
classify a device. The proper community string must also be provided in order to authenticate and fetch the necessary data. Lastly, the SysObjectID of the device needs to be known in order to setup a classification.

The following points should be used when discovering what the SysObjectID of a device is:

- The SysObjectID is specific to the make and model of the device. All devices of that make and model will have the same ID.
- The manufacturer knows what the SysObjectID is for a device.
- An Internet search can provide that ID to you. Be sure to not take the first instance of the ID you find unless it is the manufacturer's definitive website.
- Running an initial Network Discovery (covered in a previous section) can provide you the SysObjectID of a device.
- MIB or .my files are not required for classification. Only knowing the SysObjectID is.
- Without a classification, many devices will be specified as a Network Resource (generic), or unknown. This limits how easily the device can be identified in the console.

The following steps you through setting up a Classification.

1. In the Symantec Management Console, browse under Settings > All Settings > Discovery and Inventory > SNMP Settings > and select SNMP Device Classification.
2. Do a search on the SNMP object ID, Manufacturer and Device Model to ensure an entry doesn't already exist. If it does, you can edit the existing entry to make any corrections or adjustments.
3. Click the Add button.
4. Provide the following details:
 - a. SNMP object ID: this will be unique to the device make and model. This is not a unique ID to the specific device, but to the make and model of the device. This means it will apply to the same make and model you have out in the environment.
 - b. Device Type: This is for classification purposes for Reporting and filtering.
 - c. Manufacturer: This field is a label for the manufacturer and can be used for reporting purposes.
 - d. Device Model: This field is a label for the Device Model. Check your documentation for the device to ensure you input the correct model information.
 - e. Resource Type: This dropdown correlates directly with the Resource Types available in the Symantec Management infrastructure. For example if you look under Manage > All Resources when you browse the views the Type selected here will determine where in this tree the device will show up. Note that Routers and Switches are considered Infrastructure Devices.



Symantec Management Console

Add Device Classification

SNMP object ID:

Device Type:

Manufacturer:

Device Model:

Resource Type:

OK Cancel

5. Click OK to add the classification.

6. Repeat this process for every device you need to classify. This is a manual process required for every device type that is in your environment; that is not already covered by the predefined classifications.

Classification is important to get the most out of Network Discovery. It is also essential when moving to Agentless Inventory as the Device Type and Resource Types determine what types of SNMP calls are made to those devices by default.

Troubleshooting Tips

- When Network Discovery is running the SNMP routines against a discovered device, it will fetch the SNMP Object ID from the device. It will then compare the ID against what is known in the classifications table. If the wrong Object ID has been provided in the classification, it will not use that classification.
- If a device isn't classified, check to see if SNMP was successful. If no SNMP data class exists, likely SNMP was not fetched. Open Resource Manager for the device and check under View > Inventory to see if SNMP data classes are listed.
- Check timeout and retry values for SNMP if you feel it should be working correctly in the Connection Profile.
- You can test SNMP using the SNMPUtilg utility, covered in the Troubleshooting section.

Advanced Settings

This section will be remarkably short. In two places you have Advanced Settings, both as a global in the Symantec Management Console under Settings > All Settings > Discovery and Inventory > Network Discovery Settings, and within the Advanced Settings button per Network Discovery Task. The one setting is for the threads used for the discovery task.

As a general rule, this setting should be left alone. If you are having resource problems on the Notification Server when a discovery runs you can try lowering this amount. If the lowering does not change the behavior, set it back to 40.

Discovery Engine

Network Discovery uses a myriad of ways to find devices. Understanding what methods are used can help troubleshoot issues that may arise when using the product. There are two main categories for discovery. The first is labeled Main Engine, or those items done that are not exposed through the Connection Profile. The second are those exposed and configured through PPA's Connection Profile. Each section is covered below.

Main Engine

Many of the original protocols the engine used exclusively have been broken out into the connection profile. There are a few items Discovery uses as part of its discovery that does not show up in the list.

Port Scan – This is not configurable, but Network Discovery scans the open ports on a device to try and determine what that device is. Based on what is returned, it can deduce if a device is a switch, router, or other device based on what ports are available. As this is not configurable, there is no visibility into this process.

Master Browse List

For Windows systems the Master Browse List is queried in order to get a list of known systems and their NetBios Names and IP Addresses. This allows the engine to check known names against the IP Addresses it has in its list to discover. Almost all other protocols supersede the use of this method so often the end result is not factored by the MBL data.

PPA Connection Profile

These are configured via the PPA Connection Profile covered in a previous section. Each Protocol interacts differently with the devices and are unique to that protocol.

ICMP – When ND uses the ICMP protocol; ND queries the device using ICMP (echo(8)); ND queries the device using NetBIOS status (UDP 137); and ND queries the DNS server (UDP 53) with forward and reverse lookups. The forward lookup is based on the name returned from the device and the NS's NIC's DNS Suffix Search List. Here are DOS commands that simulate these actions:

- - Ping request: `ping 192.168.2.15`
- - NetBIOS query: `nbtstat -A 192.168.2.15`
- - DNS forward lookup: `nslookup -type=a sql-w2k8-01.epm.local`
- - DNS reverse lookup: `nslookup -type=ptr 192.168.2.15`

SNMP – When ND uses the SNMP protocol; ND queries the device using SNMP (UDP 161), authenticating using the community string provided by the connection profile; next ND queries device using NetBIOS and the DNS server as described above; finally ND queries the device using SNMP for additional information. Essentially the ND with SNMP includes everything from ND with ICMP, plus some SNMP items.

The SNMP calls are made using the GET command specifying a specific SysObjectID. These IDs are garnered from the MIB files already pre-loaded. MIBs represent Object IDs and what values they represent. A collection of standard MIBs (RFC), or specifically SNMP SysObject ID calls, are supported by virtually all network devices. Network Discovery uses these calls to fetch basic data from all devices it comes into contact with that supports SNMP.

AMT – AMT, or Intel vPro technology, must be configured and setup in order to be used by Network Discovery. The connection profile entry for AMT must also be setup properly for it to be utilized. This is not an easy process, so if you are unsure if you have AMT capable and enabled systems, you probably don't. Prior to AMT 9, AMT uses soap-http (16992); AMT-soap-https (16993)

The process of setting up AMT is difficult. Please refer to the following links when looking to use AMT:

- <https://www.secure.symantec.com/connect/articles/best-practices-configuring-intel-vpro-capable-system-within-out-band-management-70>
- <http://www.symantec.com/docs/HOWTO99719>

Other Protocols

The following are a list of protocols and what calls/ports they use:

- ASF > asv-rmcp (udp:623)
- IPMI > asv-rmcp (udp:623)
- SSH > ssh (tcp:22)
- VMWare > https (tcp:443)
- WMI > netbios-ns (udp:137) & epmap (tcp:135)
- WS-MAN > oob-was-http (tcp:623)

Network Discovery Task

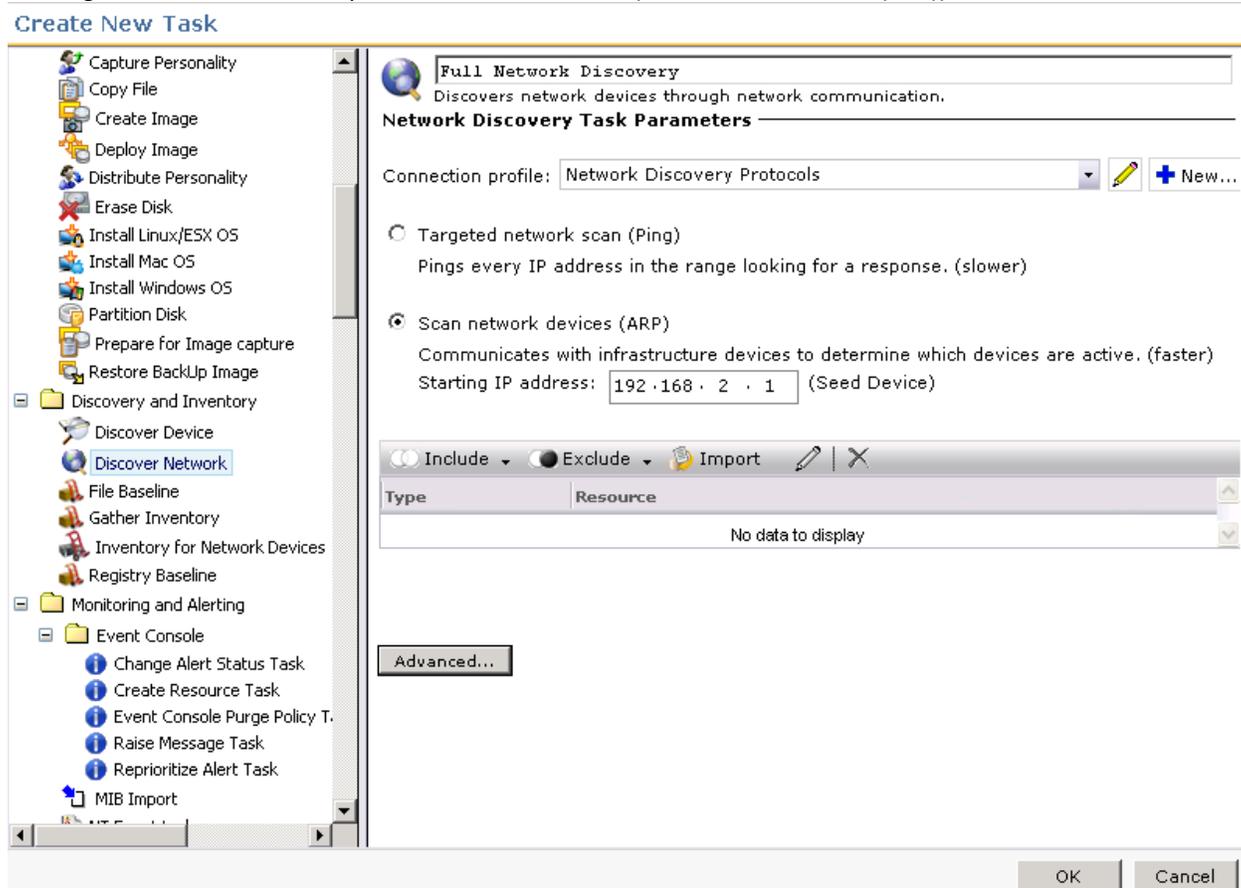
After all the preliminary work is done, it is simple to run a Network Discovery. If an initial Discovery was run, you can kick off the same task again to now run the discovery with the proper classifications in place.

Steps to run through the discovery are listed here:

14. In the Symantec Management Console browse under Manage > Jobs and Tasks > in the left-hand tree browse under System Jobs and Tasks > Discovery and Inventory > and select Network.

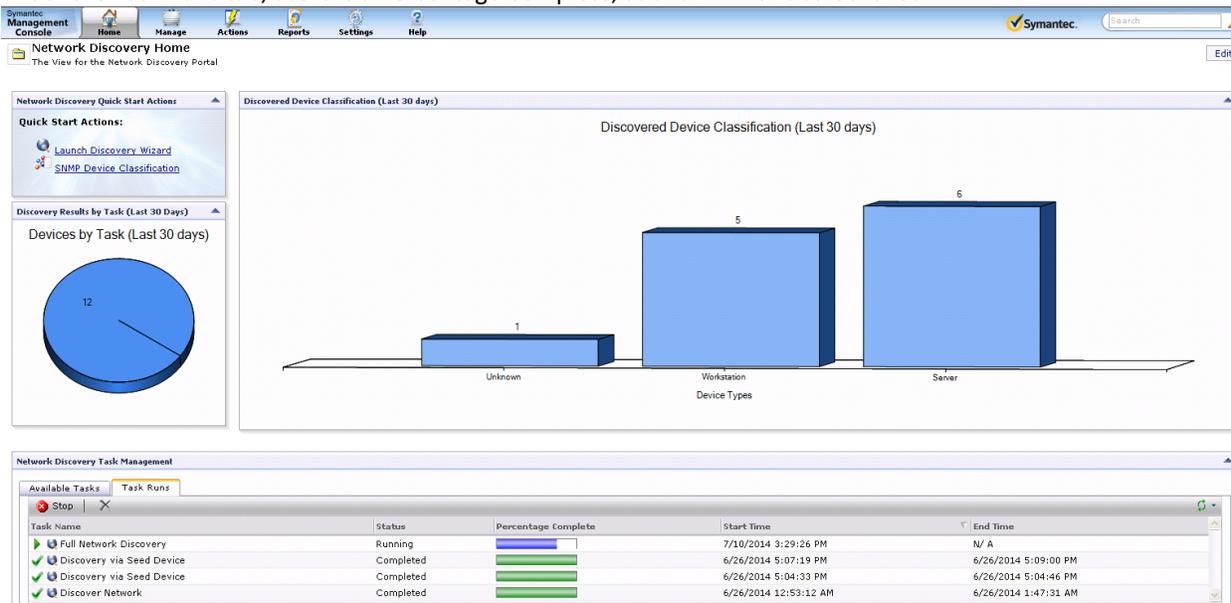
NOTE: You can create a Network Discovery Task from whatever location you wish within the Jobs and Tasks tree. The above is just a typical place to create such a task.

15. Right-click on the containing folder and select New > Task.
16. From the left-hand tree, locate the folder for Discovery and Inventory, and select Discover Network.
17. Provide a name for the discovery, such as “Full Network Discovery”.
18. From the Connection profile dropdown select the connection profile to use for this task.
19. Configure the scan type, either Targeted (Ping), or ARP or seed device. This can be edited later after creating the Task. For this example I selected Seed Device (Scan network devices (ARP)).



20. Click OK to save the Task.
21. In the main console the task will now load in the tree. The details will show within the right-pane.
22. Check the considerations listed below before scheduling the discovery.
23. Click the New Schedule option.
24. If you choose the Now radial, the discovery will execute immediately. It can also be set to a Schedule to run during off-peak times, if that is required.
25. Click the Schedule button.
26. Done!

To check progress, in the Symantec Management Console browse under Home > Discovery and Inventory > and select Network Discovery. This will provide an overview of all Discoveries, but note that at the bottom webpart, under the Task Runs tab, there is a Percentage Complete, as shown in this screenshot:



Considerations:

- IP Ranges will take considering longer if a large range is included. We will start by pinging every IP Address, waiting for the timeout and executing the retry count. Take this into mind when scheduling a range.
- A huge range, such as a class B subnet, is not recommended. A class B subnet has thousands and thousands of IP Addresses in the range so a discovery will take a very, very long time.
- Find out what specific ranges are being leased on the network so that those ranges can be added.
- When selecting a Seed Device the ARP table, or every device and its IP that it knows about, will be used to check what IP Addresses to query against. Most Seed devices will provide what is directly connected to them, and will have the ARP tables of other routers and switches it knows about. This may create a very large discovery, so IP ranges may be needed in very large environments.

Task Results

When a task is complete, you can check the results by double-clicking on the scheduled line in the policy. This will bring up statistics for the task, including what new devices were discovered, what devices were updated, etc. The quick view allows you to know if things are completing as expected.

This shows a view of these statistics:

Task Instance Details (SMP-W2K12-01 - 8/7/2014 11:38:45 AM)

 Refresh

Status: Completed
Return code: 1

Start time: 8/7/2014 11:38:45 AM
End time: 8/7/2014 11:40:40 AM
Total run time: 2 min 54 sec

Completed

Output Properties

Discovery statistics: Total devices processed: 12
New devices added: 1
Devices updated: 11
Device add failures: 0
Device update failures: 0

With this view you can determine:

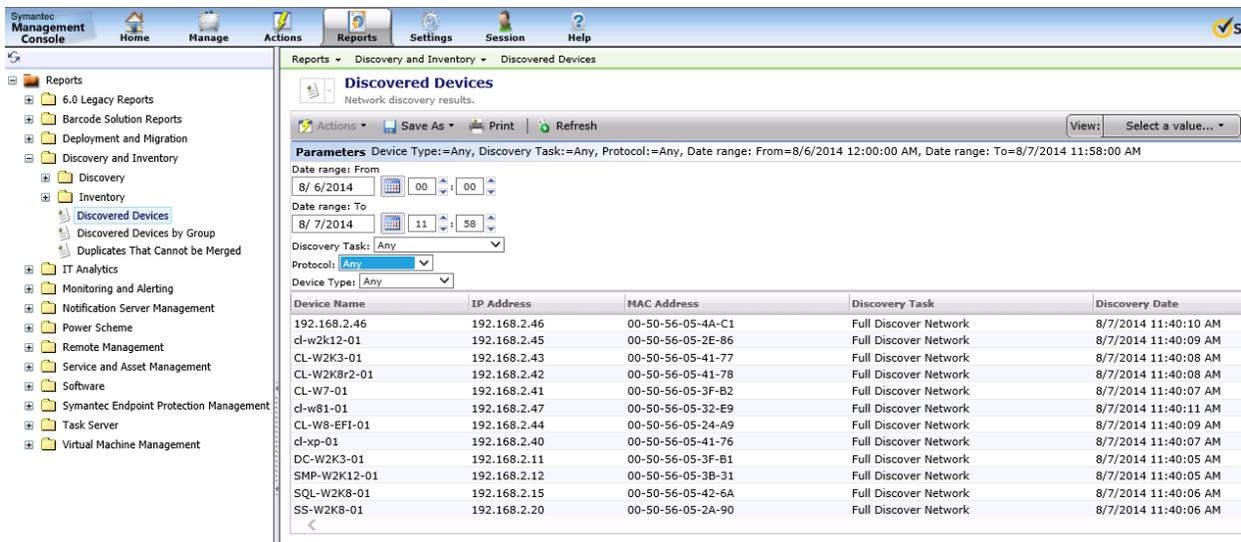
1. If the number of expected devices were seen (Total devices processed)
2. Number of new devices found by the discovery (New devices added)
3. What devices were already known to the Notification Server (Devices updated)
4. Any failures, and the type (Devices add failures, Device update failures)
5. How long the discovery took. The start and end times allow you to understand the impact of the discovery on the network, and how much time it took to go through the various protocols against found devices. Review the Considerations section for possible explanations of short or long times reported.
6. Return code can help determine if something is wrong. If it is not a 1, generally something failed within the discovery and the logs should be checked.
7. In the future, you can review the last time the scan ran. NOTE: This is important if troubleshooting problems with duplicate computer records, etc.

Discovered Devices Reports

The Discovered Devices report allows you to review all devices discovered via Network Discovery. The parameters allow you to see a holistic view, or narrow down to very specific results. The Parameters include:

- Date Range – Show devices discovered within a specific date range, from all those discovered regardless of task, method, or type, or narrow down further.
- Discovery Task – See the results for a specific Task, or leave at Any for all.
- Protocol – Select a specific Protocol if you want to see devices discovered specifically by that protocol. Any is typically the best option.
- Device Type – Refine the view to only include specific device types.

The following shows a typical display of this report:



Discovered Devices
Network discovery results.

Parameters Device Type:=Any, Discovery Task:=Any, Protocol:=Any, Date range: From=8/6/2014 12:00:00 AM, Date range: To=8/7/2014 11:58:00 AM

Device Name	IP Address	MAC Address	Discovery Task	Discovery Date
192.168.2.46	192.168.2.46	00-50-56-05-4A-C1	Full Discover Network	8/7/2014 11:40:10 AM
cl-w2k12-01	192.168.2.45	00-50-56-05-2E-86	Full Discover Network	8/7/2014 11:40:09 AM
CL-W2K3-01	192.168.2.43	00-50-56-05-41-77	Full Discover Network	8/7/2014 11:40:08 AM
CL-W2K8r2-01	192.168.2.42	00-50-56-05-41-78	Full Discover Network	8/7/2014 11:40:08 AM
CL-W7-01	192.168.2.41	00-50-56-05-3F-B2	Full Discover Network	8/7/2014 11:40:07 AM
cl-w81-01	192.168.2.47	00-50-56-05-32-E9	Full Discover Network	8/7/2014 11:40:11 AM
CL-W8-EFI-01	192.168.2.44	00-50-56-05-24-A9	Full Discover Network	8/7/2014 11:40:09 AM
cl-xp-01	192.168.2.40	00-50-56-05-41-76	Full Discover Network	8/7/2014 11:40:07 AM
DC-W2K3-01	192.168.2.11	00-50-56-05-3F-B1	Full Discover Network	8/7/2014 11:40:05 AM
SMP-W2K12-01	192.168.2.12	00-50-56-05-3B-31	Full Discover Network	8/7/2014 11:40:05 AM
SQl-W2K8-01	192.168.2.15	00-50-56-05-42-6A	Full Discover Network	8/7/2014 11:40:06 AM
SS-W2K8-01	192.168.2.20	00-50-56-05-2A-90	Full Discover Network	8/7/2014 11:40:06 AM

You can drill down into a network resource by double-clicking on the row. This will launch Resource Manager for that resource, which provides you a lot of information about what was discovered, what data gathered, etc.

Other reports provide good information as well. These reports include:

Discovery and Inventory > Discovery > Computers:

1. Network Computers – Computers discovered by Network Discovery. For computers with records already in the Notification Server, Network Discovery appends Network-specific tables to the record.
2. Novell NetWare Computers – Used to review data on Novell Netware systems.

Discovery and Inventory > Discovery > Devices:

3. Chassis and Module – For devices such as blade enclosures or other multiple-device structures, you can view the chassis and included modules.
4. Device Interfaces – For devices with multiple interfaces, this report provides data on them.
5. Network Devices – A pie graph of all discovered devices by manufacturer, with the ability to drilldown.
6. Network Routers – A report for routers.
7. Network Switches – A report for switches.

Discovery and Inventory > Discovery > Printers

8. Network Printers – A report for printers.

Discovery and Inventory > Discovery

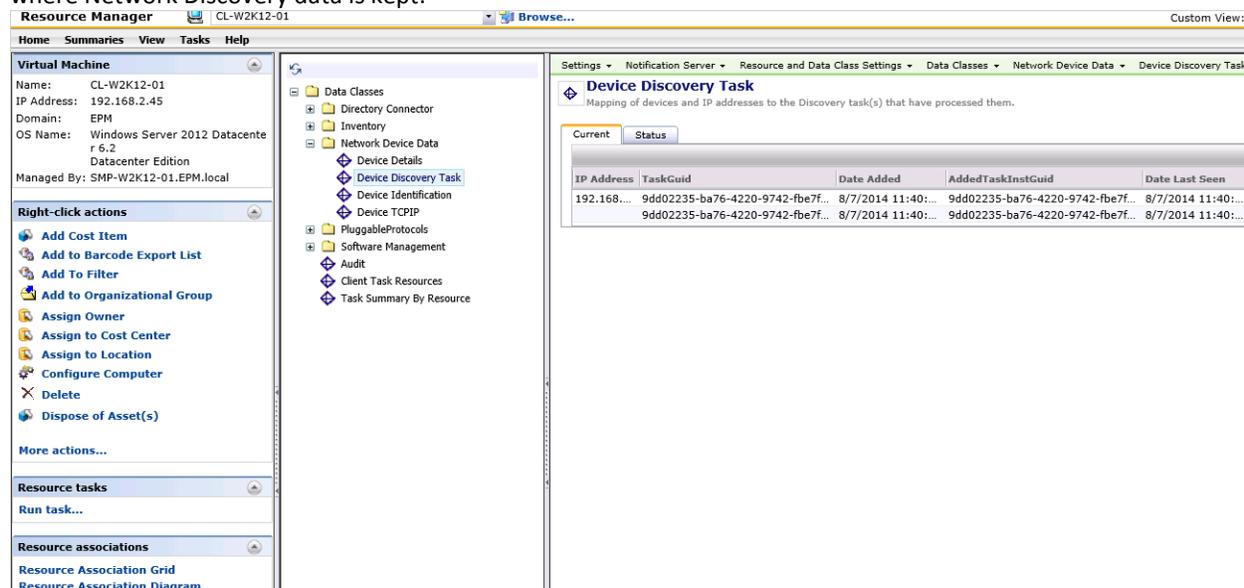
9. Discovered Devices by Group – Unlike the Discovered Devices report, this one displays in a pie graph, grouped by device type. The graph can be used to drill down into each type for a list.
10. Duplicates That Cannot be Merged – Use this when troubleshooting duplicate device problems.

Another view of network devices by Resource Type can be viewed in the Symantec Management Console under Manage > All Resources > Asset > Network Resource > and all subgroups. These views do not filter on other criteria, including how the device came into the system. While Network Discovery reports are all based off of results from discovery tasks, the Resource views will show all, including those that came in via other methods such as Connector, AD Import, Domain Discovery, Asset Management.

Resource Manager

When reviewing what was captured on a system, the reports only provide partial information based on what the report is for. To get a full view, Resource Manager can be viewed. This can also help you understand what was captured, and if Agentless Inventory is needed to inventory additional details.

The most useful place in Resource Manager to look is the Inventory section. You can reach this by browsing under View > Inventory. The Inventory tree will appear in the middle pane. The pane is populated by data classes (typically understood as tables in the database), grouped by the type of data class. The following example shows where Network Discovery data is kept:



The screenshot shows the Symantec Resource Manager interface. The left pane displays 'Virtual Machine' details for 'CL-W2K12-01'. The middle pane shows a tree view of 'Data Classes' with 'Device Discovery Task' selected. The right pane shows a table of 'Device Discovery Task' data.

IP Address	TaskGuid	Date Added	AddedTaskInstGuid	Date Last Seen
192.168.2.45	9dd02235-ba76-4220-9742-fbe7f...	8/7/2014 11:40:...	9dd02235-ba76-4220-9742-fbe7f...	8/7/2014 11:40:...
192.168.2.45	9dd02235-ba76-4220-9742-fbe7f...	8/7/2014 11:40:...	9dd02235-ba76-4220-9742-fbe7f...	8/7/2014 11:40:...

Note the following data classes and what useful information can be found therein:

- **Device Details, Device Identification, Device TCP/IP** – These data classes contain basic information for the device, and most devices discovered via Network Discovery will have these data classes present.
- **Device Discovery Task** – This contains the information for the Discovery Tasks that discovered this system, whether initially or with subsequent network scans.
- **AeX AC Discovery** – This basic inventory data class contains when the device was discovered, and what method was used. If Network Discovery was used, the Discovery Method will indicate such.
- **SNMP%** – The SNMP data classes contain specific SNMP data. **SNMP Identification**, for example, contains the SysObjectID of the device. This is useful when reviewing discovered devices and pulling the OID in order to properly classify a device.

Network Discovery to Agentless Inventory

Now that the discovery is done, Agentless Inventory can now be used against SNMP discovered devices. The following items should be considered when moving to an Agentless Inventory

1. Agentless Inventory is SNMP only. A device must have returned SNMP information in order for us to gather Inventory for Network Device data.
2. Computers are not good candidates for Agentless without a lot of customization, the intended purpose is for SNMP driven devices such as routers and switches. This was covered earlier. Inventory Solution for Windows or Unix, Linux, Mac provides better information and does not require a lot of customization, so it is recommended to use the Agent in those cases.
3. For credentials we use the known good community string used during the Network Discovery. This means it is not necessary to do any security, protocol, or credential configuration with a Network Inventory task.
4. Network Discovery is REQUIRED for Agentless Inventory. The two use the same engine, and Agentless is designed as an SNMP extension of Network Discovery.
5. All calls for Network Discovery and Agentless are made via Task Server

Just like Network Discovery, there are a number of items that need to be considered before running it. Out of the box Agentless Inventory provides standard information about systems via our SNMP data classes, but the real

ability of Agentless is to configure the engine to pick up whatever SNMP has to offer. In order to do this, the following steps need to be followed:

1. Import MIB files that contain the SysObjectIDs needed for the data you wish to be collected.
2. Create a table / data class to house the collected data.
3. Create columns for the table that contain a data type, length, name, and the OID used to capture the data.
4. Select what device types will try to collect this data.

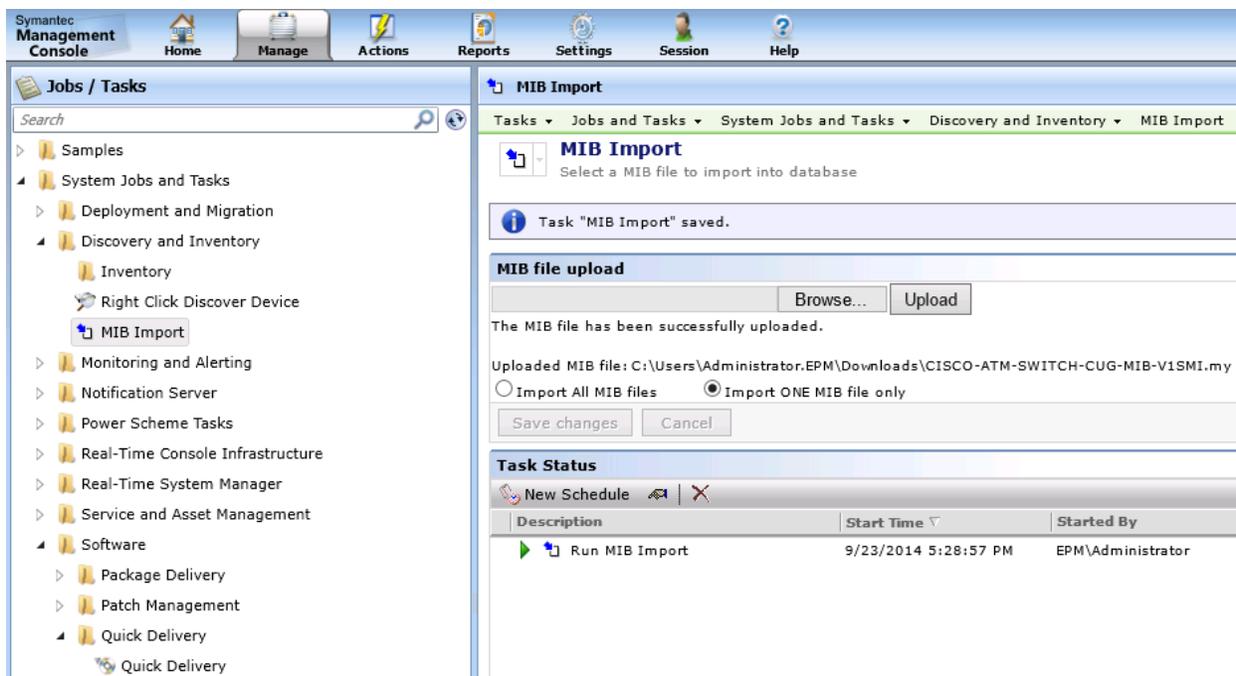
By following all the steps the custom data can be collected upon completion of the Inventory for Network Devices (Agentless) Task.

MIB Imports

Agentless requires a manufacturer's MIB file in order to make a proper call to the device to gather each column value of a custom data class. The process must be followed in order to gather custom data if the SNMP values are not available in the MIBs we provide by default. The following process walks through how to import MIBs, using the MIB Importer from the Event Console.

NOTE: At this time the All MIB files import does not appear to be functional, so individual MIBs must be imported individually. Note that the entire process below must be followed for each MIB import.

1. In the Symantec Management Console, browse under Manage > Jobs and Tasks > and in the left-hand tree browse under System Jobs and Tasks > Discovery and Inventory > Right-click on Discovery and Inventory and choose New > Task.
2. In the left-hand task tree, look under the Monitoring and Alerting section and choose MIB Import.
3. Provide a Name (default works as this task can be reused for multiple MIB Imports) and click OK. The steps to import the MIB will be done after the task is created.
4. The following steps must be followed to properly upload a MIB. It is not intuitive, so please make special note of the order of steps.
 - a. Click Browse.
 - b. Select the MIB you've obtained and downloaded from the manufacturer or elsewhere on the internet and click Open.
 - c. Select the radial for Import ONE MIB file only.
 - d. Click the Upload button. Ensure that the message "The MIB file has been successfully uploaded" is displayed below the browse field.
 - e. Click the Save changes button.
 - f. Click the New Schedule button.
 - g. Select Now, or if desired schedule a time, and click Schedule.
 - h. Let the schedule complete.
5. The MIB is now imported.



Once the MIB is imported, it is available to use when setting up the Data Mappings for custom tables.

Troubleshooting Tips

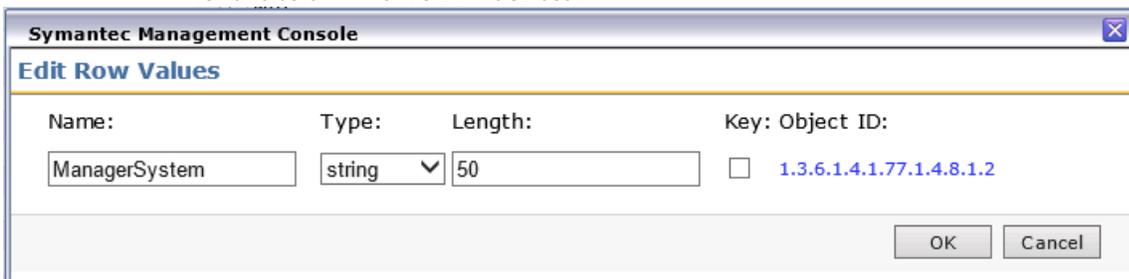
- If a MIB shows as importing successfully, but does not show up when using SNMP Data Mapping Tables, then the MIB might not be in a format supported by Agentless Inventory. Seek an alternative MIB, or contact the manufacture. The MIB should support SNMP v1 or v2, not v3 which is not supported at this time.
- Review the steps taken if a MIB does not import. Make sure all steps are taken from Step 5, A through H for each MIB to be imported.
- Double-check the list as the MIB name might not be the same as the file name of the MIB. Review the values to see if it matches what is expected.

SNMP Data Mapping Tables

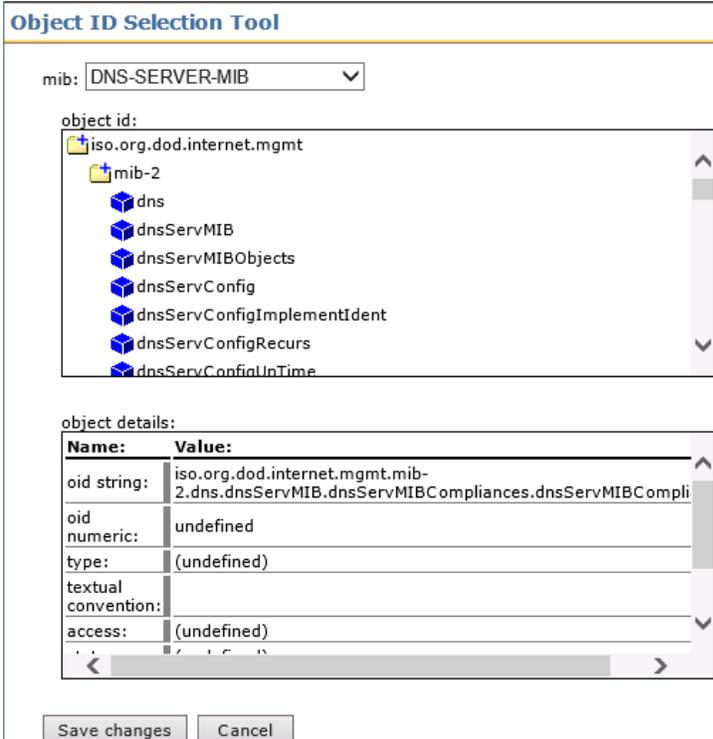
The heart of Agentless Inventory (sometimes known as Inventory for Network Devices) is custom values available via SNMP. By setting up new tables and columns, these values can be collected and stored, available in reporting and filtering on Network Devices. Setting up these tables and columns is important, and there are several gotchas to be aware of to ensure success. The following process walks through setting up a customer table to be captured by SNMP devices.

1. In the Symantec Management Console, browse under Settings > All Settings > and in the left-hand pane browse under Discovery and Inventory > SNMP Settings > and select SNMP Data Mapping Tables.
2. Click the New icon to create a new table.
3. Provide a Name. This name will become the table name is the following format:
Name provided: SNMP Cisco 8540 Switch
Resulting SQL table name: Inv_SNMP_Cisco_8540_Switch
4. Click OK to move to the configuration step.
5. Click New under Table columns.
6. Provide the values as applicable, following the guidelines below:

- Name: This will become the column name. Note that while spaces are supported, it will require the underlining reporting or filtering SQL to bracket the column name.
- Type: This will be the data type for the column in SQL. An appropriate value for what is being captured should be selected. The common selecting (and default) is “string”.
- Length: This should be long enough to contain any expected values. Adding extra typically does not hurt anything.
- Key: Only select this option if the value captured will be specifically unique for each device reporting it. If it is not, two devices with the same value cannot reside in the table at the same time. Data can be overwritten and/or rejected. If in doubt, do not select this option.
- Object ID: This will open up the MIB browser, allowing a user to select the value they wish to capture. The select must be accurate as this is the OID the engine will use when fetching data for this column from SNMP devices.



7. When selecting the MIB value for a column, use the following guidelines:
 - Double-click on the folders in the UI to expand them.
 - Select a value to populate the properties fields below.
 - Review the properties field to ensure you have selected the value you require.



Object ID Selection Tool

mib: DNS-SERVER-MIB

object id:

- iso.org.dod.internet.mgmt
 - mib-2
 - dns
 - dnsServMIB
 - dnsServMIBObjects
 - dnsServConfig
 - dnsServConfigImplementIdent
 - dnsServConfigRekurs
 - dnsServConfigUnTime

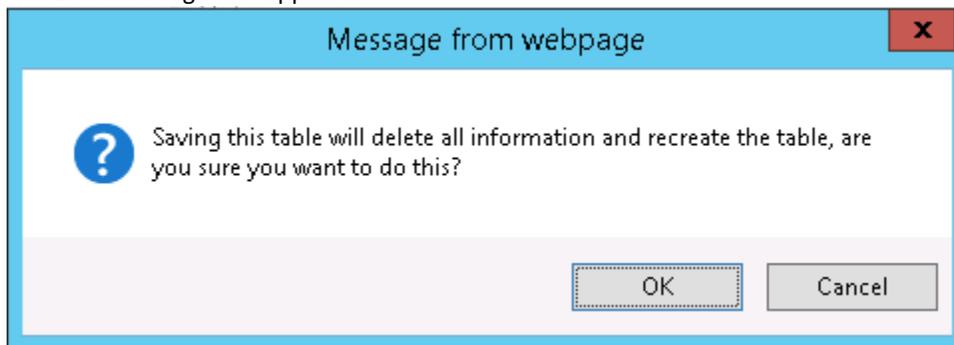
object details:

Name:	Value:
oid string:	iso.org.dod.internet.mgmt.mib-2.dns.dnsServMIB.dnsServMIBCompliances.dnsServMIBCompli
oid numeric:	undefined
type:	(undefined)
textual convention:	
access:	(undefined)

Save changes Cancel

8. Click OK to save the column.
9. Repeat the process of creating columns until you have the columns you desire. Note that the ID column and Resource GUID of the device will be created but not shown in this section of the user interface.

10. NOTE! When going through this process, the ASPX session may timeout, so be ready to save changes as you go. Alternatively you can refresh the console and start again once you've identified what values and MIB selects to use.
11. Click Save changes to save the current progress.
12. Click on the Device mappings tab. (NOTE! This step is often forgotten, ensure that it is followed or no device will collect inventory for the new table)
13. These are the same Device mappings used when working in Network Discovery. Any device you wish to run the new SNMP calls against, and thus capture the custom data, must be checked in this list.
14. If you sort by Manufacturer it can make it easier to select the devices you need.
15. Once you've checked all applicable devices, click Save changes again.
16. NOTE the message that appears:



- Saving this table will delete all information and recreate the table, are you sure you want to do this?
17. This will happen any time the table mapping is saved, whether merely adding a device mapping or adjusting, modifying the columns. This means all previously captured data WILL BE ERASED. In this way it is highly recommended to have all device mappings and intended columns configured. If you do need to adjust it, run an Agentless Inventory again to repopulate the table.
 18. The process is now done!

NOTE: The Test on Device button has defects which render its effectiveness null. Please see the section in Troubleshooting for SNMPUtilg.exe for the alternative way to test.

Repeat the above steps for any data class (table) you wish to create. Be sure to follow all the steps so that mistakes don't cause failure to gather the data, or the need to adjust the configuration and thus delete and recreate the table.

Troubleshooting Tips

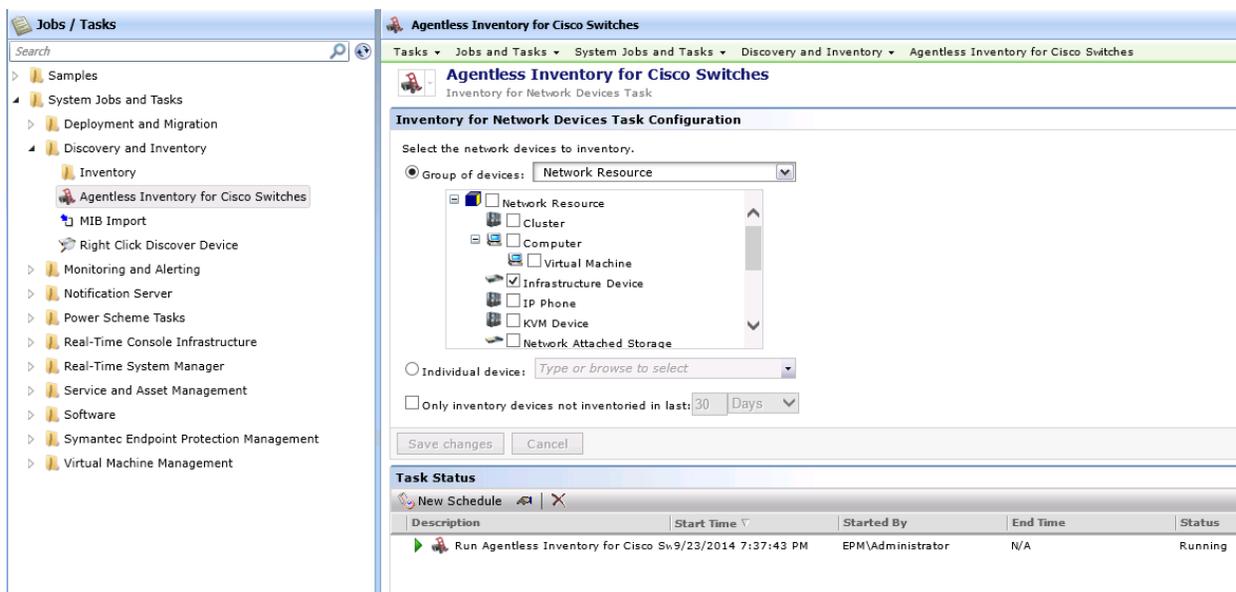
If data is not gathered, note the following items:

- Have you selected the device mapping for the device being inventoried? You can review this in the Discovered Devices report in Network Discovery. The Manufacturer, Model should match what is placed in the mappings.
- Do you have more than one device mappings that might apply to this device? Make sure all are checked.
- Does the machine respond to the OIDs you have selected to be queried via SNMP? See the section for troubleshooting that covers the SNMPUtilg.exe utility for how to test this.
- Check the Notification Server logs at the time the Discovery completed as the engine will drop the NSEs with the data into the queue for processing. Look for errors relating to the processing of that data. If no errors or warnings are seen, the data was likely processed correctly.

Agentless Inventory Task

Now that all the preliminary work has been completed, the task can now be run. Most of the work is done on the back end, so running the task is fairly painless. Follow these steps to run the task:

1. In the Symantec Management Console, browse under Manage > Jobs and Tasks > and in the left-hand tree browse under System Jobs and Tasks > Discovery and Inventory > Right-click on Discovery and Inventory and choose New > Task.
2. In the task tree, look under the section for Discovery and Inventory and select Inventory for Network Devices.
3. Provide a name, such as “Agentless Inventory for Cisco Switches”.
4. Select the group of devices to Inventory. Note that the default organizational groups will not allow a lot of specific targeted. For example I selected Infrastructure Device, which will include all Cisco Switches, but will also include any other Infrastructure device found in that group. If you want to be more specific, create your own Organizational Group to select.
5. Alternatively you can select an individual device. This is recommended when testing the Task to limit how much activity the Task causes.
6. You also have the option to check the box for inventory devices not inventoried in a defined number of days. Use this as necessary to limit the traffic on the network if needed, otherwise it is recommended to keep this unchecked so to ensure data integrity.
7. Ignore the Advanced button.
8. Click OK to save the Task.
9. Once back to the main console, click on the New Schedule button.
10. Set a scheduled time or choose now to run the Agentless Inventory.
11. When complete, the new inventory should be appended to the targeted devices, including the new custom data classes configured previously (if applicable via device mappings).



Jobs / Tasks

Search

- Samples
- System Jobs and Tasks
 - Deployment and Migration
 - Discovery and Inventory
 - Inventory
 - Agentless Inventory for Cisco Switches
 - MIB Import
 - Right Click Discover Device
 - Monitoring and Alerting
 - Notification Server
 - Power Scheme Tasks
 - Real-Time Console Infrastructure
 - Real-Time System Manager
 - Service and Asset Management
 - Software
 - Symantec Endpoint Protection Management
 - Virtual Machine Management

Agentless Inventory for Cisco Switches

Tasks > Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory > Agentless Inventory for Cisco Switches

Agentless Inventory for Cisco Switches
Inventory for Network Devices Task

Inventory for Network Devices Task Configuration

Select the network devices to inventory.

Group of devices: Network Resource

- Network Resource
 - Cluster
 - Computer
 - Virtual Machine
 - Infrastructure Device
 - IP Phone
 - KVM Device
 - Network Attached Storage

Individual device:

Only inventory devices not inventoried in last: 30 Days

Save changes Cancel

Task Status

New Schedule

Description	Start Time	Started By	End Time	Status
Run Agentless Inventory for Cisco Sw	9/23/2014 7:37:43 PM	EPM\Administrator	N/A	Running

Troubleshooting Tips

- When you've selected a group, does the device you expect to inventory reside in that group? Check by browsing under Manage > All Resources and browsing to and selecting the group. Look for the device in the right-hand list. Alternatively you can test the task against the device specifically using the “Individual device” radial option.

- Did the task complete successfully? Double-click on the Task Status row for the instance you ran. This will provide statistics and statuses for the task, and you can review if the task has completed and what the outcome was.
- Double-check data mappings if a device is not inventoried as expected (for example it collects the standard default tables but not the custom one).

Troubleshooting

The most important tool for troubleshooting not already covered in the individual sections is the SnmpUtilg.exe utility. This utility provides the interface to test using the same methods we will use when running Network Discovery or Agentless Inventory.

SNMPutilg.exe

You can obtain this utility from the following location:

- <http://www.symantec.com/connect/downloads/snmputilgexe-testing-against-devices-same-method-inventory-solution-network-devices>
- Alternatively you can search the Web as it is available elsewhere.

You can use SnmpUtilG to perform the basic SNMP operations such as GET, GET-NEXT, and SET from a graphical interface. SnmpUtilG also supports saving SNMP data to the clipboard, as well as saving data to comma delimited text files.

This utility is provided as is. This utility was originally released as freeware from Microsoft, but since it follows the same SNMP calls/methods that Altiris employs it is good for testing.

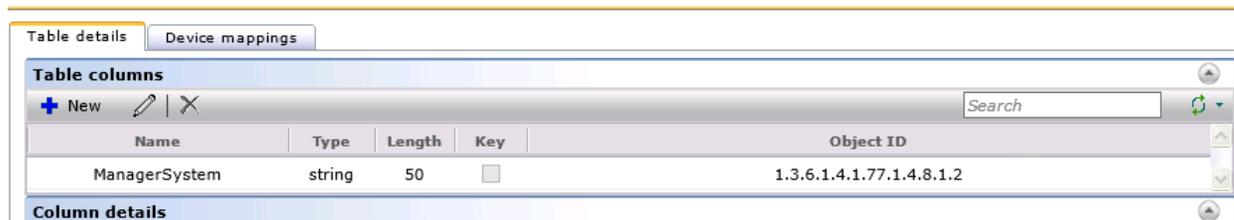
Use the 'Get' method to see if the OID you are supplying returns any data. If not, switch to the 'Get Next' method to see what the next OID is. If it's outside of the current branch, Altiris will not capture that OID. You can see the results, and if it's the value you're looking for, use the returned OID.

Note: Using this utility you need to put a '.' at the beginning of the OID you are querying, and a .0 at the end. This is usually required!

Use the following steps to test against a device to see if the SNMP SysObjectID will work for the device in question.

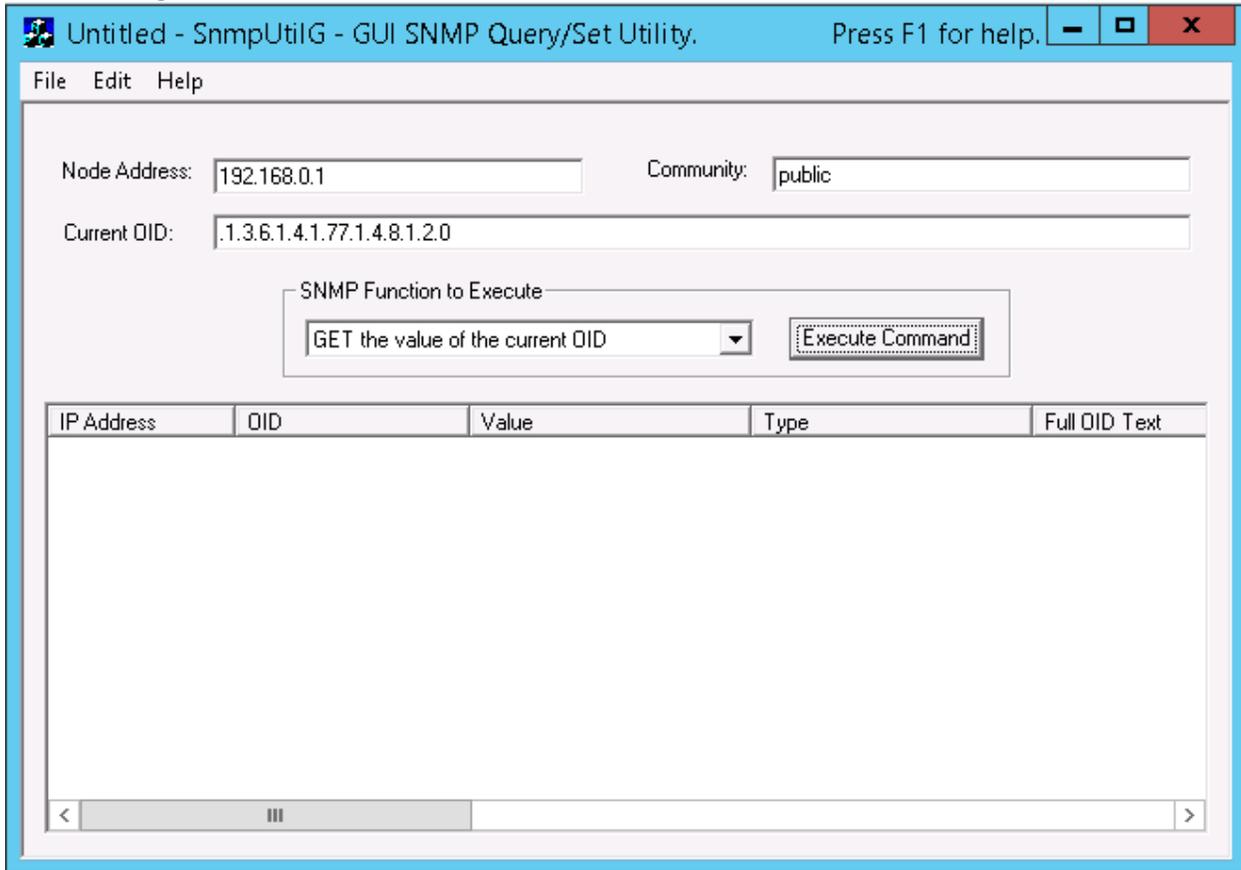
1. Download the utility to the Notification Server. Since the calls are being made from the NS, this is the location you will want to run the utility for proper testing. This is a stand-alone EXE and does not require installation.
2. Right-click on the EXE and select Run as Administrator.
3. In the Node Address field, put in the IP address of the device you wish to test against.
4. In the Community field, put in the community string of the device. This will be the "password" that allows SNMP to fetch data.
5. In the Current OID field, put in the SysObject ID in question. This will be the OID that shows up in the column mappings for the table, as shown in this screenshot:

SNMP Cisco 8540 Switch



Name	Type	Length	Key	Object ID
ManagerSystem	string	50	<input type="checkbox"/>	1.3.6.1.4.1.77.1.4.8.1.2

- Be sure to add a period '.' at the beginning of the OID, and end it with a '.0'
6. Change the SNMP Function to Execute to "GET the value of the current OID".



IP Address	OID	Value	Type	Full OID Text
------------	-----	-------	------	---------------

7. Click the Execute Command to test against the device.

The result should show up in the list below the options. If an error is thrown, check the error to see what may be the problem. If data is shown, generally it means this OID should work, but check the value.

- Does the error indicate it can't reach the IP? Perhaps SNMP is being blocked on its way to the selected device.
- Is the Community string correct? It must be correct in order to be successful (Community Strings are CASE sensitive).
- Is no data returned? The device is contacted and authenticated to, but the OID selected is not returning data. This means the device will not return the desired data. Check with the manufacturer to see what may be the problem. Also you can switch the SNMP Function to "Get the NEXT value after the current OID" to see if the OID might be a little off. Check the value found and what the next OID is. If it's correct, you have a new OID to aspire to! That's where the difficulty comes in as we need the MIB that corresponds to that OID.

All in all it may be up to the Network Team or Manufacturer to figure out the issue. As long as we are making the call successfully but are not getting results, it often is an environmental/manufacturer issue.



Conclusion

I hope this article has helped when troubleshooting and using Network Discovery and Agentless Inventory (aka Inventory for Network Devices). If none of these things helps with your problem, and you are unsure if the issue is with the network or manufacturer, consider contacting Symantec Endpoint Management Support for assistance.