



netTerrain 9.7

Integration Toolkit Guide



Contents

1 About this guide	9
1.1 Who should use it	9
1.2 Assumptions	9
2 Integration Toolkit basics	9
2.1 Main user interface components	11
2.2 Nodes vs devices	12
2.2.1 Can I use node connectors in the ITK to represent devices in netTerrain?	13
2.3 Device connectors	13
2.4 Node and link connectors	14
2.5 Monitoring	15
2.6 Architecture	15
2.7 Setting up the ITK for first time use	17
2.8 Setting up the ITK as a service	19
2.8.1 Installing and starting the ITK service	19
2.8.2 Uninstalling the ITK service	21
2.9 Obtaining the ITK version	21
3 Built-in device connectors	22
3.1 Viewing available connectors	22
3.2 Deleting connectors	23
3.3 Setting up a built-in connector	24
3.3.1 Using device connector "drop-ins"	24
3.3.2 Setting up the connection to the data source	27
3.3.2.1 Source Database	29
3.3.2.2 Testing the connectivity	29
3.3.3 Mappings tab	30
3.3.3.1 Source table	30
3.3.3.2 Device type field	30
3.3.3.3 Default diagram	31
3.3.3.4 Parent locator field	31
3.3.5 Name field	31
3.3.3.6 Rack position field	32
3.3.3.7 WHERE clause	32
3.3.4 Reconciliation settings	33
3.3.4.1 Updates	33
3.3.4.2 Inserts	34

3.3.4.3 Deletes	34
3.3.4.4 Preventing deletes for low record counts	34
3.3.4.5 Pre and post import functions	35
3.4 Additional mapped fields	36
3.4.1 Adding and removing mapped fields	37
3.4.1.1 Mapping fields when they already exist in netTerrain	37
3.4.1.2 Mapping fields when they don't exist in netTerrain	38
3.5 Device discovery	39
3.5.1 Viewing the results	41
3.6 Device reconciliation	42
3.6.1 Type mappings	43
3.6.1.1 The role of the object identifier	43
3.6.1.2 Viewing existing type mappings	44
3.6.1.3 Adding new type mappings	46
3.6.2 Preventing device imports without a mapped type	48
3.6.3 Previewing a reconcilation process	49
3.6.3.1 Copying the output window contents to the clipboard	51
3.6.4 Reconciling data with netTerrain	52
3.6.5 Mapped fields missing in netTerrain	54
3.7 Automating the process	56
3.7.1 Setting up the scheduler	56
3.7.2 Real-time status polling	57
3.7.2.1 Mapping the status field in the source	58
3.7.3 Discovery order and passes	61
3.7.4 Starting the scheduling process	62
3.7.5 Activating connectors	63
3.8 Analyzing the results	64
3.8.1 Device states and their corresponding color codes	64
3.8.2 Refreshing views	66
3.8.3 Filtering devices based on color code	67
3.8.4 Mapping types from the device view	68
3.9 Logs and data purging	69
3.9.1 Truncating (or purging) connector tables	71
3.9.1.1 Truncating all device tables	73
4 Creating custom device connectors	73
4.1 Prerequisites	73
4.1.1 Proxy or source database?	74
4.1.1.1 Proxy set up use-case: OTDR readings	74
4.1.1.2 Setting up the proxy database using SQL Server	75

4.1.1.3 Setting up a proxy database using MS Access	80
4.2 Step 1: Creating the device connector	83
4.2.1 Connection information	84
4.2.2 Mappings tab	86
4.2.2.1 Source table	86
4.2.2.2 Device type field	86
4.2.2.3 Default diagram	87
4.2.2.4 Parent locator field	87
4.2.2.5 Name field	87
4.2.2.6 Rack position field	88
4.2.2.7 WHERE clause	88
4.2.3 Reconciliation settings	89
4.2.3.1 Updates	89
4.2.3.2 Inserts	89
4.2.3.3 Deletes	90
4.2.3.4 Pre and post import functions	91
4.3 Step 2: Mapping additional fields	91
4.4 Tying it all together with an example	93
4.5 Next steps	95
4.6 Deleting and suspending a device connector	97
4.7 Cloning a connector	97
5 Node connectors	98
5.1 Viewing node connectors	99
5.2 Prerequisites for creating node connectors	99
5.2.1 Proxy or source database?	99
5.3 Step 1: creating the node connector	100
5.3.1 Connection information tab	100
5.3.1.1 Database engine	100
5.3.1.2 Database credentials	102
5.3.1.3 Source Database	102
5.3.2 Mapping tab	102
5.3.2.1 Source table	102
5.3.2.2 netTerrain Type	102
5.3.2.3 Default diagram	103
5.3.2.4 Parent locator field	103
5.3.2.5 Name field	103
5.3.2.6 X and Y coordinate fields	103
5.3.2.7 WHERE clause	104
5.3.3 Reconciliation	105

5.3.3.1 Updating existing nodes in netTerrain	105
5.3.3.2 Inserting new nodes into netTerrain	105
5.3.3.3 Deleting nodes without matches	106
5.3.3.4 Pre and post import functions	106
5.4 Step 2: Mapping custom fields	107
5.4.1.1 Mapping fields when they already exist in netTerrain	107
5.4.1.2 Mapping fields when they don't exist in netTerrain	108
5.5 Next steps	109
5.6 Discovering and reconciling nodes	110
5.6.1 Viewing the results	111
5.7 Node reconciliation	113
5.8 Deleting and suspending node connectors	114
6 Link Connectors	115
6.1 Viewing link connectors	115
6.2 Step 1: creating the link connector	115
6.2.1 Connection information tab	116
6.2.1.1 Database engine	116
6.2.1.2 Database credentials	118
6.2.1.3 Source Database	118
6.2.2 Mapping tab	118
6.2.2.1 Source table	118
6.2.2.2 netTerrain Type	119
6.2.2.3 Name field	119
6.2.2.4 Endpoint locator fields	119
6.2.2.5 Endpoint separator (and how to create connections between ports)	119
6.2.2.6 WHERE clause	120
6.2.3 Reconciliation	121
6.2.3.1 Updating existing links in netTerrain	121
6.2.3.2 Inserting new links into netTerrain	121
6.2.3.3 Deleting links without matches	122
6.2.3.4 Pre and post import functions	122
6.3 Step 2: Mapping custom fields	123
6.3.1.1 Mapping fields when they already exist in netTerrain	123
6.3.1.2 Mapping fields when they don't exist in netTerrain	123
6.4 Next steps	123
6.5 Discovering and reconciling links	124
6.6 Deleting and suspending link connectors	125
7 Monitoring	126
7.1 General parameters	127

7.1.1 Timeout and threads	127
7.1.2 Device properties	128
7.2 SNMP auto-discovery	129
7.2.1 Built-in MIBs	131
7.2.1.1 System MIBs	133
7.2.1.2 Interface MIBs	134
7.2.1.3 IP address table and routing table MIBs	134
7.2.2 Configuring SNMP parameters	136
7.2.3 SNMP device connector settings	138
7.2.4 Configuring SNMP: IP address manager	139
7.2.4.1 Manual IP address entry	140
7.2.4.2 Setting devices with SNMPv3	141
7.2.4.3 Uploading IP addresses from a text file	142
7.2.4.4 Editing the settings of an IP address	144
7.2.4.5 Adding and removing addresses	145
7.2.4.6 Enabling and disabling addresses	146
7.2.4.7 Outputting a csv report of your IP addresses	147
7.2.4.8 Running a ping sweep for an IP address range	149
7.2.5 Mapping device types for native SNMP	152
7.2.6 Starting the SNMP device discovery	154
7.2.7 Viewing discovered device details	156
7.2.8 Previewing a reconcilation process	157
7.2.9 Reconciling SNMP devices with netTerrain	159
7.2.10 Viewing ports	160
7.2.11 Mapping port types	162
7.2.12 Viewing ports in netTerrain	166
7.2.13 SNMP link discovery	167
7.2.13.1 Discovering Layer 3 link data	170
7.2.13.2 Running the layer 3 link discovery and reconciliation	170
7.2.13.3 Discovering Layer 2 link data	171
7.2.13.4 Running the layer 2 link discovery and reconciliation	173
7.2.14 Using custom MIBs	174
7.3 WMI Discovery	177
7.3.1 Initializing the WMI connector	178
7.3.2 Registering WMI hosts	179
7.3.3 Setting WMI discovery parameters	182
7.3.4 Discovering WMI host data	186
7.3.5 Setting up and troubleshooting WMI in your environment	188
7.3.5.1 Adding a user to the WMI namespace	189
7.3.5.2 DCOM permissions	191

7.3.5.3 Testing a WMI connection	193
7.4 AWS Discovery	195
7.4.1 Initializing the AWS connector	196
7.4.2 Configuring AWS for first time use	197
7.4.2.1 Storing the AWS account settings	197
7.4.2.2 Configuring AWS parameters	198
7.4.3 Discovering from AWS	199
7.5 SQL Server Monitoring	200
7.5.1 Initializing the SQL monitoring connector	201
7.5.2 Registering SQL Servers	202
7.5.3 Discovering SQL Server data	203
0 Other settings and commande	204
8 Other settings and commands	204
8.1 Commands	204
8.2 Other application settings	209

Document Code. GN_D_nT9-04 Last revision: 03/24/2023

© 2023 Graphical Networks LLC. All rights reserved (but some wrongs are still available).

Our "keep the lawyers happy" disclaimer: Graphical Networks and netTerrain are registered trademarks of Graphical Networks LLC. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

This document was created with 100% recycled electrons.

Before printing, please be mindful of that PC load letter and consider the environment when hitting the printer with a baseball bat.

Image: Azores, Portugal.

Graphical Networks LLC Telephone: +1-240-912-6223 Fax: +1-240-912-6339 (where you can send us the purchase orders)

1 About this guide

1.1 Who should use it

The Integration Toolkit (ITK) is an application for importing data from third-party systems or home-grown databases and files into netTerrain. It also has a built-in discovery engine supporting several protocols such as Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI).

The ITK is part of the netTerrain application installer, and it is deployed on the netTerrain application server. Upon request, Graphical Networks can also provide a separate installer for the ITK, which can be deployed on individual computers. In those cases, a database connection from the computer to the netTerrain database will be required.

This guide is intended advanced users that want to automate the data entry into netTerrain by setting up discovery processes or creating and managing connectors to external systems. In short, geeks like us.

1.2 Assumptions

This guide assumes basic knowledge of database queries, Microsoft Office tools and netTerrain end-user and power-user functions.

Discovery functions may require the user to have knowledge about WMI, SNMP and the Management Information Base (MIB) structure.

2 Integration Toolkit basics

The Integration Toolkit (or ITK) is an application that provides users with the ability to import and synchronize data into netTerrain from external databases or files, as well as auto-discovery functions. The ITK is a .NET based fat-client application that runs on the netTerrain application server. As mentioned above, upon request, Graphical Networks can also provide a separate installer for the ITK, which can be deployed on individual computers. In those cases, a database connection from the computer to the netTerrain database will be required.

The toolkit includes several methods for pulling data from the network:

- Built-in device connectors: predefined connectors that read device data from external data sources
- Custom device connectors: user defined connectors that read device data from external data sources
- Node connectors: user defined connectors that read generic node data from external data sources
- · Link connectors: user defined connectors that read link data from external data sources
- An SNMP discovery engine
- A WMI engine
- An AWS connector
- IPMI and other protocols using Intel's DCM API (separate module required)
- A SQL Server database discovery utility

The first four methods (connectors) support native database connections to SQL Server, Oracle, PostgreSQL, MySQL and Microsoft Access. If the data is stored in a different database engine or file format, you can implement a "proxy database" to gain access to those data sources and still import the data into netTerrain.

All connectors support the three basic database operations for inserting, updating and deleting records (the infamous CRUD operations). What this means is that nodes and links can be automatically created in netTerrain, based on new records coming from the original data source and existing nodes and links in netTerrain can be updated or deleted, if the records experienced a change or were removed from the source database.

The SNMP discovery tool supports SNMPv1 and SNMPv2c for discovering devices, ports, IP address tables and layer 2 and layer 3 links (by means of bridging and routing tables) from the network and SNMPv3 for device discovery.

The WMI discovery tool can discover hardware and software characteristics from WMI enabled devices, as well as application and IIS data.

The ITK also ships with a predefined connector for discovering data from AWS instances. This connector uses the AWS API and can import regions, groups, rules, instances, volumes, health checks and buckets, among other things.

With the adequate license, the ITK can also include the Intel DCM module that can monitor power and temperature variables from select devices. This module is outside the scope of this manual.

The SQL Server monitor uses an ADO.NET native SQL connection to read database and instance information from registered SQL database engines.

2.1 Main user interface components

The ITK is a thick client application with a User Interface (UI) that simplifies the process of creating and maintaining connectors, as well as importing data into netTerrain. The main ITK UI components are accessed from a switchboard, as shown in the image below.

	1: Me 2: Too	enu bar olbar								
	A Shet I Cruzel									G
the state of the	the face	lighted .	antelly	Address	Centre 10	Cathole (C	Logia			1,000
ve 1966		US Ballions	Taken 1	1000 Fed Times	101	26.16	31.67			
LCIS-2800-244 LCIS-8-2011-2-3		US Backborn	Terms.	ALC Malaman		42.37	71.82			
LCS-#26110424		US Backbone	Annes	CO. Javaille Re.		41.5	104.40			
L05828122		Austa	Panan	SH Long Time	11	41.3	-87.66			
LCI5-8-2990-26-1		US Baldows	Parata .		28	18.28	:08.07			
1-015-0-0580-34-7	Los Ropel	US Backborn	Penan	All lie Ave.	21	10.00	2011			
LCI5-5-2550-40-5	Marc Se.	US Balkhove	. Person	12 Sat Avenue	28	25.02	40.12			
L/049/T2105-4		US Backborn	- Penary	TO CALL Harbor PM	27	44.33	-40.22		Determination of the second of	
SearGanag		US Buildone	Penang	ST7 Yellow Call.	30	40.77	25.00	4:	: List views	
A Mar Debine		UE Boltone	Paners 1	ST7 Sender Ave	34	36.00	55		and the second	
A Man Distance Installance		Cavola	Ponary	723 Sun Deol Pet		32.43	-11242			
va DMP Saana Pa		US Backboos	Privacy	3 floor fel	н	40.5	-80.22			
Contraction and Contraction		US Backbore	(Inter	254 Meeter St.	42	25	100			
Satrow		US Baldone	Panato -	21 October Lane	40	1740	322.8			
fineur Ontwine	and the second s	CO BARRIER	- Percent	ETC hash Dear	-	1.1				
Dicage Las Vegas Las Replac										
In Veps In Argens New Sent	0 0 2 2				Pager (H	41 TO 14 H				
Las Vegas Las Angelas Mart Ramit -			•		Page (H	41)) H H				
Ler Veges In Argens New Deart FREE-VIEW New Yok Private	Inanto Pare Records)				Page (H	41]] b H				
Lar Vegal Ian Kepala Kana Kepal Pada VieW Nasagine Resea Resea					Page (1)	41 E] IP H		-		
Ler Veget Ler Angele Norei Reach PROCUMPIEN Processor Reducto	Inanto Pare Records)				Page (H	4 ⊡нн		•		
Lar Vegal Ian Kepala Kana Kepal Pada VieW Nasagine Resea Resea	Frank Park Records 11/24/2014 12 13/21				Page (1)	4 <u> </u>] b H		•		
Les Veges Mans Search Pages - Mark Pages - M	Frank Park Records 11/24/2014 12 13/21	M 2,34 i.in	Arigebes		Page (H	41 <u> </u>] +		•		
Les Vegets Ins Regites Non Stant Pare Tun Nonni Nonni Nonni Nonnin Nonni Nonni Nonnin N	Insets (Rev Records) 11/04/2014 (213/27) Test records: 1 New Records with real 11/04/2014 (215/2014)	M Like La ang panat a nafi	Argeles eren							
Les Veges Mans Search Pages - Mark Pages - M	Frantis Plans Records 11/24/2014 12 13 201 Tinial records: 1	M Like La ang panat a nafi	Argeles eren				e output	# \	6: Command input	
Les Viges lans faute Tans Tans Tans Tans Tans Tan Tans	Insets (Rev Records) 11/04/2014 (213/27) Test records: 1 New Records with real 11/04/2014 (215/2014)	rie 2,3e Les regueres a sel rie 2,3e De rie 2,3e Ro	Argeles eren				e output	*	6: Command input	
Les Vigne lans Septie Nano Start Pare Yan Nano	Francis (Face Records) 11/24/2014 (2/13/07) Tinal seconds: 1 New Records with real 11/24/2014 (2/15/07) 11/24/2014 (2/15/07)	M 2,3e Les equerit i ref M 2,3e De M 2,3e Ro Nami 2	Angeles anan ang				e output		6: Command input	
In Yope In Yope In Sopher State Sam? State Sam? Same Rebury Rebury Rebury Rebury Same	Interfer (New Records) 11.04 (2014 12 13 07) Tind records 1 New Records of the sec 11.04 (2014 13 13 08) 11.04 (2014 13 13 08) Tind records (2014 13 13 08)	PH 2,344 Los ang parent a real PH 2,544 Dec PH 2,544 Po PH 2,544 P	Angeles anan ang				e output		6: Command input	
In Yope In Yope Tao Suite Tao Suite Tao Yuk Nasarine Nasarine Tao Yuk Nasarine Tao Yuk Nasarine Tao Suite Tao Suite Suit	Interfer (Fase Records) 11.29(2016-12.12.027) Tanal records: 1 New Records with res 11.29(2016-12.12.027) 11.39(2016-12.13.007) Tanal records (Fase) Tanal records (Fase)	PH 2,344 Los ang parent a real PH 2,544 Dec PH 2,544 Po PH 2,544 P	Angeles anan ang				e output		6: Command input	

ITK switchboard and UI

The Menu bar (1) provides easy access to common functions for managing the ITK (File), viewing objects (View), discovering records from external systems (Discover), managing the application, connector and auto discovery settings (Settings), creating new connectors and administering the log files (Tools) as well as accessing the guide and software version (Help).

The toolbar (2) includes a few shortcuts to common functions for accessing the connector lists, creating new connectors and starting and stopping the automatic discovery with the scheduler.

The tree view (3) shows all connectors and their discovered objects.

The list views (4) can display all device, node and link connectors set up in the system, their discovered objects, as well as other lists such as mapped types.

a a	Type Mappi	ings - Count: 4830		
Mon Devices	id	Type Name in Source	Type Name in netTerrain	Data Source
enter Trig	19704	13614110213	NO_NAME	Native SNMP
onfig Files	23782	13614110122521	NO_NAME	Native SNMP
ME	23783	1.36.1.4.1.1012.2.5.2.2	NO_NAME	Native SNMP
f eHeath	20827	1.3.6.1.4.1.10213.1.1	NO_NAME	Native SNMP
A MOM	21848	1.3.6.1.4.1.1022.9	NO_NAME	Native SNMP
At SCOM	21451	1.3.6.1.4.1.1027.1.2.1	NO_NAME	Native SNMP
SNMP	20996	1.3.6.1.4.1.1027.1.2.2	NO_NAME	Native SNMP
PM	20904	1.3.6.1.4.1.1027.1.2.3	NO_NAME	Native SNMP
	21474	1.3.6.1.4.1.10418.10.1.1	NO_NAME	Native SNMP
	21475	1.3.6.1.4.1.10418.10.1.2	NO_NAME	Native SNMP
27	21486	1.3.6.1.4.1.10418.10.1.3	NO_NAME	Native SNMP
129	21477	1.3.6.1.4.1.10418.10.1.4	NO_NAME	Native SNMP
1	20826	1.3.6.1.4.1.10418.13.1.2	NO_NAME	Native SNMP
12	20678	1.3.6.1.4.1.10418.13.1.3	NO_NAME	Native SNMP
A3	20844	1.3.6.1.4.1.10418.2.1.1	NO_NAME	Native SNMP
4.4	20843	1.3.6.1.4.1.10418.2.1.3	NO_NAME	Native SNMP
45	20716	1.3.6.1.4.1.10418.7.1.10	NO_NAME	Native SNMP
AS	20718	1.3.6.1.4.1.10418.7.1.11	NO_NAME	Native SNMP
47	20719	1.3.6.1.4.1.10418.7.1.12	NO_NAME	Native SNMP
11	20788	146141104187114	NO_NAME	Native SNMP
42	IFOO	solarwinds	🔛 Page: 14 44 1 1 🕪 陆	

List view showing the filter text box

The message output (5) provides the user with the status of finished or ongoing discovery and reconciliation processes as well as output messages from commands issued from the command input window (6).

Attention!

The command input window is mainly used for development and consulting purposes, but several commands (see chapter 7) are available to end users.

2.2 Nodes vs devices

Throughout this guide we will be working a lot with device and node connectors, which are responsible for automatically creating and reconciling nodes and devices in netTerrain. It is important then, to know the difference between nodes and devices before choosing which type of connector to work with.

A node is a very unassuming yet flexible object in netTerrain: it can represent anything from a building to transportation equipment, a data center object, location or even a chair or person. Nodes can, of course, be connected with each other or to a device. Yet nodes are rather modest compared to their cousins, the smart devices. Nodes, as opposed to devices are not aware of sub components they may contain, their physical dimensions, let alone more sophisticated properties like weight or power usage.

If you are a user of netTerrain DCIM you probably want to use device connectors in case you need to import entities like routers or switches via the ITK. That way, you can take advantage of some of the business rules and automation that netTerrain offers. These business rules and features include:

- An extensive predefined library of makes and models
- Automatic creation of subcomponents (ports and slot)
- Automatic creation of a background image
- Awareness of physical size and weight
- Easy "snap in" for rack mounting
- Awareness of power consumption
- Ability to receive automatic alarms from the ITK
- More comprehensive modeling capabilities such as the ability to specify reference node location
- Ability to restrict which card types can be positioned under which slot
- Pre-defined reports in the dashboard

Generic nodes (or simply nodes) have none of these capabilities. They are basically just modeled as objects that have an image, a set of fields, and visual overrides.

2.2.1 Can I use node connectors in the ITK to represent devices in netTerrain?

You certainly can, but those device representations in netTerrain are generic nodes that only look like devices, but lack most of the smart business rules described above.

To make it clear: none of the features that come with smart devices prevents a user from utilizing generic nodes to represent actual devices. In those cases, netTerrain really doesn't see a difference between your "nodes as devices" and any other node. You can certainly create a node type that looks like a router and later connect it to another instance of a generic node type that looks like a switch. The caveat is that netTerrain will treat these objects as any other generic node.

When using nodes as devices you can still overcome the lack of automatic business rules by documenting things a bit more manually. For example, if you want to document the ports of a router or switch using generic nodes, you will need to create those ports manually, and if you want to rack mount the node, you will have to resize it and fit it inside a rack diagram manually.

2.3 Device connectors

Device connectors are hooks into external databases or files designed to specifically import and reconcile device data into netTerrain. These external databases are usually back-end data stores of a Commercial-Off-The-Shelf (COTS) product. Some examples of COTS products are described in the bulleted list below.

Records that are imported from the external system using a device connector will be mapped to smart devices in netTerrain. A type field must be used to associate each device type with its corresponding type in netTerrain without having to create a specific connector for each device make and model.

Besides the built-in device connectors that already ship with the netTerrain software, a wizard allows you to create their own device connectors, enabling real-time or near real-time import and reconciliation of device data into netTerrain.

Graphical Networks has created several device connectors to external systems for different customers in the past, including:

- Solarwinds Orion Network Performance Monitor (NPM)
- VMWare VCenter / Virtual Center
- Ipswitch What's Up Gold
- Castle Rock SNMPc
- Cisco RME
- CA Unicenter Tng
- CA Concord eHealth
- Microsoft MOM and SCOM
- HP Open View Operations
- CA Spectrum
- Red Hat Linux Network
- Zenoss

Many of these predefined device connectors are made available as part of an ITK build or through XML drop-ins (explained later in this guide).

Attention!

Built-in device connectors usually bring in basic data fields. If a more in-depth integration between the third-party system or COTS product and netTerrain is needed, then it may be more convenient to create a custom device connector from scratch using the ITK wizard. If your organization has an active maintenance license you can request Graphical Networks to create the connector free of charge, provided it is to a COTS product.

2.4 Node and link connectors

Node or link connectors are hooks into external databases or files to pull in records and map them to new or existing generic nodes and links in netTerrain.

Users can create any number of node and link connectors and each one will be mapped to a predefined type in the netTerrain catalog. To create a connector, a wizard to connect to the data source and map source fields to custom fields in netTerrain is available.

Attention!

For netTerrain DCIM or netTerrain Enterprise users we recommend using device connectors to bring in device data into netTerrain. That way you can take advantage of the built-in intelligence associated with smart devices (such as automatic port creation).

2.5 Monitoring

The netTerrain ITK currently supports various monitoring mechanisms: an SNMP discovery engine, WMI, Website monitoring (static sites and WMI-based IIS discovery), a built-in IPMI environmental monitoring engine (for licensed users that purchased a license of netTerrain with the Environmental Monitoring module, such as netTerrain DCIM-EM) and a SQL Server monitoring utility.

The SNMP discovery module provides a simple way to discover devices within one or more IP address ranges using SNMPv1, SNMPv2c and SNMPv3. Using SNMPv1 and SNMPv2c the ITK can discover device data, interface data, IP address tables and layer 2 and layer 3 links (by means of bridging and routing tables). With SNMPv3 the ITK currently only supports device discovery.

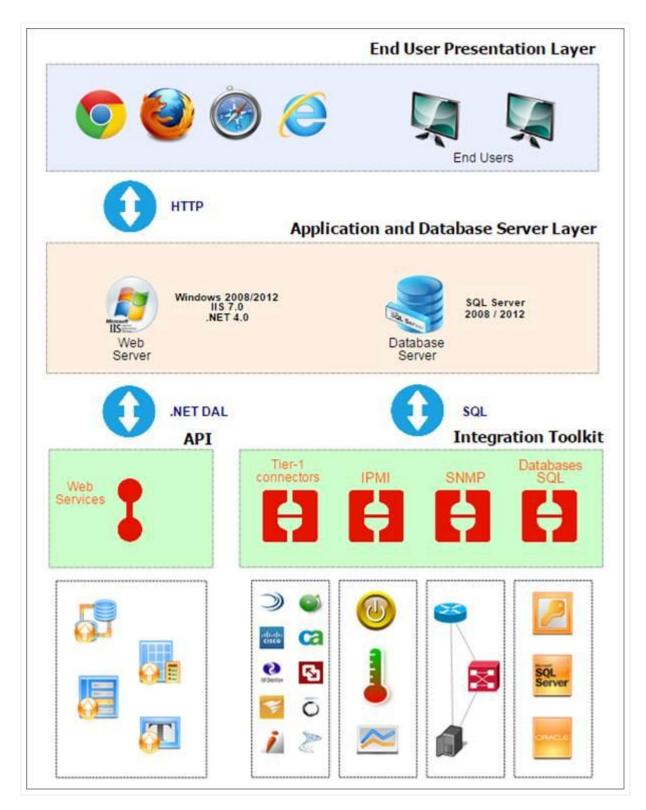
The WMI discovery tool can discover hardware and software characteristics from WMI enabled devices, as well as application and IIS data.

The netTerrain Environmental Monitoring module can provide environmental data such as power and temperature variables from select devices using the IPMI protocol.

The SQL Server monitor can discover SQL Server instance statistics, as well as statistics for each database that resides in one of the monitored instances.

2.6 Architecture

The following diagram represents the system architecture, along with the components of the ITK.



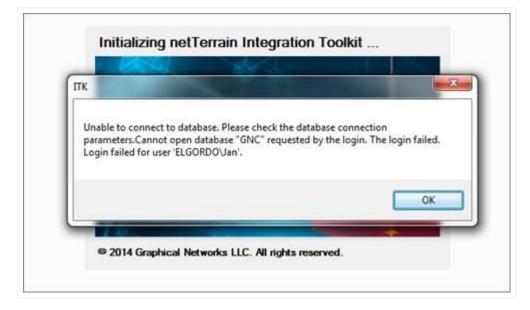
netTerrain and ITK architecture

The ITK components are represented on the bottom right corner.

2.7 Setting up the ITK for first time use

The ITK is installed on the application server and launched from the Program Files->netTerrain shortcut folder.

When launching the ITK for the first time the connection to the netTerrain database may fail since the connection string stored in the ITK xml file has the default (factory shipped) credentials.



Failed connection dialog

By clicking 'OK' the system will prompt the user to enter the credentials to the netTerrain database:

onnection	
DB Engine	SQL Server *
Server	•
Database	GNC
Trusted	Yes 💌
User	vis
Password	
Connection Timeout [s]	300 🚖
	Test Connection

Dialog to enter the netTerrain database credentials

The ITK needs a valid user set up in the netTerrain SQL Server. This user can log in via SQL Server or Windows authentication and it requires a permission level enough to modify table structures in the netTerrain database (such as db_owner or a combination of db_datareader, db_writer and db_ddladmin).

A connection timeout parameter can also be set. Usually 30 or 60 seconds is sufficient for normal ITK operations. However, because this parameter not only controls the timeout between the ITK and the netTerrain database but also the timeout between the ITK and source database engines, if you suspect that certain connectors may have long processing times during data querying you may want to increase that timeout value.

After testing for a proper connection, click on 'Submit' and the application will try to connect again. If the connection has been correctly set, you should see the ITK Main switchboard.

yew Djoovery Settings Inste B									
00000000									
	_								
ectory 🍓 📽	# line - Court	116							40.1.001
Devices	Site Name			Address	Center ID	(inter-	1000000		1000000
-sill Names Statem	200 10010	tiplevel.	ptody				Longkule		
LC/5-3550-24-6	Editor in	UE Bachbone	C. Perage 1.	1000 Fel Street	101	38.18	3.67		
LOS-6281520	Bottom	US Beltore	Paras .	ALC Notamen	1	40.12	-71.62		
LCIS-R2010003-8	Departe	US Buildone	Penan	ESS Januaries The	10	#15	- 47.68		
LC15.6.2980.261	Overage Las Verage	Assis US Backtone	Panas	M Ling Dive	22	31.08	1111.17		
LC15-5-3950.247		US Bathtone	Paras -	CT he he		111	118.1		
LCI5-5-3510-45-5	Hart Do.		(Annal)	U for here	2	25.42	40.13		
L 004 12105-4		US Baltions	Parat .	SECOL Party Rd		4.5	4522		
Seran/General		US Backborn	Percent	\$17 Nation Call	22	41.77	-73.54		
Notes .		US Backborn	(Annual)	ATT Groder Ave.	5	31.00	-8.8		
3 SQ, Mr. Sealer	Puerte	Casinta	Permit	203 San Devil Par.		12.42	-112.02		
30, No. Otherwisiania	Fildungh	US Backborn	Frank	2 Row Pd	12	40.5	40.27		
II Notice DOMP_External_Ph	See Dept		Parate	254 Maxico 18	42	12.79	1412		
in State	Sai Fran	UC Balldore	Penan	179 Hillion Lana	-	3742	(122.2)		
- A finite	faults	US Baddone	Ferme	34-the lines	44	14745	122.5		
- 2 Deceme	The second se	U.S. Barblana		arti sale Deal	100		100.00		
Organ		2110 250							
Ovrap Ovra		84.00	•		tope [1]	et 200 et 1			
Orcept Orcept Orcepte Orcepte UnitApple UnitApple MonitApple MonitApple MonitApple Orcepte Orcepte Orcepte Orcepte	O 2 d	88.00			Tope 11	et <u>213</u> in 141			
B Change Bongen B Les Regetes D Les Regetes D Les Regetes D' Les Regetes D' Les Regetes D' Les York D' Résetes D' Résetes D' Résetes D' Résetes D' Résetes	O C Z	88.00			Tope 11	e 🖂 in 14			
Orcago Occago Occarope	O 2 d	88.00			Page 11	н <u>П</u> н н			
Orapp O	Control New	8 ið 🗖 🖬 6 799 3,54 1.64	Argene		tope 11	et 🖂 to ot			
Orange Orange	Control (Control (Contro) (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro)	0 18 0 0	Argeise arrar		tope (1)	et 2000 et 1		*	
Bonape Banape Banape	Alter Receil Transite States Receiled Transite States Receile	0 10 0 0 6 779 2,34 10 199 2,34 10 199 2,34 00 199 2,34 00	Argeise arrar		Page 11	et <u>1</u> . 10 oc			
Oncap O	Control (Control (Contro) (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro)	0 10 0 0 6 779 2,34 10 199 2,34 10 199 2,34 00 199 2,34 00	Argeise arrar		Page 11	et <u>20</u> 10 oc	T		
	Alter Receil Transite States Receiled Transite States Receile	C al C C	Angeles lange ange		Page 11	n <u></u> 10 m.	I		
	Partie New Point Scale Team New Point Scale S	C III C III C III C III C III C III C III C III C III C III C III Accord I Accord I Accord I	Angeles lange ange		тур (45 <u>2 - 1</u> 80 48	I		
	Construction C	C III C III C III C III C III C III C III C III C III C III C III Accord I Accord I Accord I	Angeles lange ange		тур 11	КШН Н	I		

Main switchboard

If you still get an error after trying to relaunch the ITK, then the connection parameters are wrong. You may need to consult with your netTerrain DBA what the proper connection parameters are.

2.8 Setting up the ITK as a service

The ITK can run as a service on the machine it is installed on. This has the following advantages:

1) The service account can start the ITK

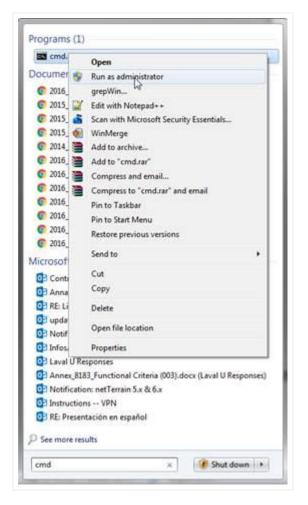
2) If the machine is restarted, then the ITK will launch automatically

Also, it is worth noting that if the ITK had a scheduler running and the server restarts, upon restart, the scheduler will be active and the timer will resume where it left off.

2.8.1 Installing and starting the ITK service

To install the ITK as a service you need to follow these steps:

1) Open a command prompt with elevated permissions



2) Execute the following command: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" "C: \ProgramData\Graphical Networks\netTerrain\ITK\netTerrainITKService.exe"

a. Note that the first folder may vary for different versions of windows, so consult with your system admin as to where the install utility for the .NET framework is installed.

b. The second folder is the installer folder for the ITK, which also may vary depending on your netTerrain installation.

3) Go to the services utility, and start the ITK service

· ·	: Hep 2					
Services (Local)	C Services Glocall					
	netTerrain ITK Service	Name	Description	Status .	Startup Type	Log On As
Statt the service Description netTemain Integration Toolkit service	Microsoft Office ClickToRun Service Microsoft SharePoint Workspace Audi	Manages resource coordination, backgroun	Started	Automatic Manual	Local Syste Local Service	
	Overcription	Microsoft Software Shadow Copy Pro Mosilla Maintenance Service	Manages software-based volume shadow c The Mopila Maintenance Service ensures th		Manual Manual	Local Syste Local Syste
	Automedia Class Scheduler	Enables relative prioritization of work based Receives activation requests over the net ma	Started	Automatic Disabled	Local Syste Network S	
		C. Net Pipe Listener Adapter	Receives activation requests over the net pi	Started	Automatic	Local Service
		Q Net.Tcp Listener Adlepter	Receives activation requests over the net.tz	Started	Automatic	Local Service
		Net. Top Port Sharing Service	Provides ability to share TCP ports over the	Started	Manual	Local Service
		G Netlogon O Testanti Manual	Maintains a secure channel between this co		Manual	Local Syste
		Q. Network Start	The Network Access Protection (NAP) agen		Manual	Network 5.
		Q Network they Q	Manages objects in the Network and Dial-U	Started	Manual	Local Syste
		Q Network Passe	Identifies the networks to which the compu-	Started	Manual	Local Service
		Charles and the second s	Collects and stores configuration informati	Started	Automatic	Network 5
		C Network	This service delivers network notifications (s_		Automatic	Local Service
		G NTRUTS Restart	TCS service for accessing the TPM	0.000	Automatic	Network S.,
		CORASI All Tasks +	2012 2020 2012 2012 2012 2012 2012	Started	Automatic (D_	Local Syste-
		G 025010#	02Micro 500 service	Started	Automatic (D_	Local Syste
		Coffice Se Refresh	Seves installation files used for updates and	Started	Manual	Local System
		Q Office Sc Properties	Enables the download, installation, and enf	Started	Menual	Network S
		Coffice Fi	The Offline Files service performs maintena	Started .	Automatic	Local Syste
		CracleRe Help			Manual	Local Syste
		Q Parental Controls	This service is a stub for Windows Parental		Manual	Local Service
		Peer Name Resolution Protocol	Enables serverless peer name resolution eve		Manual	Local Service
		Q Peer Networking Grouping	Enables multi-party communication using _		Manual	Local Service
		Reer Networking Identity Manager	Provides identity services for the Peer Name		Manual	Local Service
		Renformance Counter DLL Host	Enables remote users and 64-bit processes t		Manual	Local Service
		C Performance Logs & Alerts	Performance Logs and Alerts Collects perfor		Manual	Local Service
		C. Plug and Play	Enables a computer to recognize and adapt _	Started	Automatic	Local Syste
	Extended (Standard /	TI Doll, X H. Roy Enconarcher	The Deb, I have an orderative cancer a managed		B.Barrowell	Annal firste

The ITK is now installed as a service and activated. To stop the service simply use the services utility as shown above.

2.8.2 Uninstalling the ITK service

To uninstall the ITK service you need to follow these steps:

1) Open a command prompt with elevated permissions

2) Execute the following command: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /u "C:\ProgramData\Graphical Networks\netTerrain\ITK\netTerrainITKService.exe"

2.9 Obtaining the ITK version

In case of problems, if you contact Graphical Networks support we may request the ITK version number. This can be obtained from the Help->About menu.

About netTerrain Int	egration Toolkit 🛛 🔀
	netTerrain Integration Toolkit Version 7.1.720 Copyright © Graphical Networks LLC Graphical Networks netTerrain Integration Toolkit

About dialog

3 Built-in device connectors

netTerrain has a UI to create new device connectors for any third-party data source that uses an Oracle, PostgreSQL, MySQL, SQL Server or MS Access backend database. netTerrain also includes a series of builtin device connectors that require basic connection and reconciliation parameters to perform automated imports. These device connectors are sometimes referred to as built-in (or tier-1) connectors, as they were created in advance by a Graphical Networks engineer and are already available in the ITK, either as part of the factory installation or as a drop-in XML file.

3.1 Viewing available connectors

To see which device connectors are currently included in your ITK configuration, go to the View-> Device connector list (Ctrl-A) and a list view of all the tier-1 device connectors will show up.

Ele View Discovery Setting								
Connectors 🧠 🖉	Device Con	sector List - Countril	i.					
Devices CA Unicenter	ы	alas	doEngin	e server	database	status	lastDiscovered	lastReconciled
Castlerock SNMPc	P 1001	Native SNMP	SQL Se		GNCORE	1		7/13/2015 4:44
Geco RME	P 1004	SolarNewProdu	SQL Se		the second s	1	7/10/2015 12:4.	7/9/2015 1:41:
Moresoft SCOM	1005	CA Unicenter	SQL Se	2 C	TNG	2		
Native SNMP SolarNewProduction	P 1006	Castlerock SNM			SNMPc mdb	1		
Solarwinds	P 1007	Caco RME Microsoft SCOM	MS Acc SQL Se		CacoRME mdb SCOM	1		
What's Up Gold	F 1009	What's Up Gold	SQL Se		WhatsUp	1		
🖶 📑 Nodes	1010	Solanimda	a statistical data	and the second se	The second	110		
ii) 👗 Links	- V &	- W		Suspend		a	- 64	
				Activate				
			. 8	Clone				
			3	Edit				
			0	Delete				
			1.1	1. The second				
			1	View Becords	2			
			E	Mapped Fields				
				Create New Device Con	nector			
			1	Status Mappings				
				and the second se				
			68	Refresh View				

Device connector list view

Your initial ITK deployment may not have any tier-1 device connectors available, in which case netTerrain provides a feature to "drop" new tier-1 device connectors into the database, which is reviewed later.

The current list of drop-ins includes the following device connectors:

- CA Unicenter
- Castlerock SNMPc
- Cisco RME
- Concord eHealth
- Microsoft MOM
- Microsoft SCOM
- Solarwinds NPM
- Whats Up Gold

You can request additional drop-ins from Graphical Networks by logging a drop-in ticket request in the customer support portal.

3.2 Deleting connectors

You can easily delete a connector by selecting it from the connector list and clicking on the 'Delete' button (or right clicking on the connector and hitting delete).

Connectors 👒 📽	Device Com	vector List - Counti	E.					
CA Unicenter CA Unicenter Cantineols SNM/s Cece RME Monosth SCOM Native SNMP StartiereProduction Solamends When be Geld	4 1001 1005 1005 1005 1005 1005 1005 1005 1005	alas Native SNMP SolarNewProdu CA Uncenter Castlerock SNM Dato RME Microadt SCOM	dolingne SQL Server SQL Server SQL Server	server 113 163 1 4213 - Iocalhoet	database GNCORE SolarWinde/New TVG S1MIPC mdb CecoRME mdb SCOM	status 1 2 1 1 1	latDacovend 7/10/2015 12-4	
ar il Noden in â Linka	P 1010	Solarunda		Suspend Activitie Clone Delete Traw Apports Mapped Frields Create New Device Co Status Mappings Refresh View	intraction			

Deleting a connector

Attention!

Once a device connector is deleted you can only bring it back by creating it manually, using a drop-in or restoring the netTerrain database. It may be better to not delete the connector and simply mark it as suspended if you think you may use it later.

Also note that when you delete a device connector, any type mappings (more on that later) associated with that connector will also be deleted!

3.3 Setting up a built-in connector

When importing data from a third-party system that is included in the tier-1 connector list, you typically just need to set up the backend connectivity and specify a series of basic parameters for proper data reconciliation.

3.3.1 Using device connector "drop-ins"

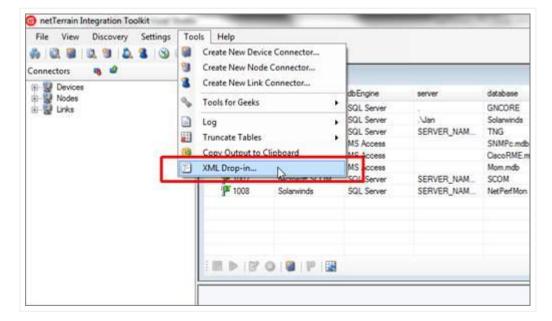
Your initial ITK deployment may not have any tier-1 device connectors available, in which case netTerrain provides a feature to "drop" new tier-1 device connectors into the database. This feature can also be used for creating new device connectors or even cloning existing ones.

Drop-ins are XML files that can be imported into the ITK via the drop-in import menu option. netTerrain already ships with several XML files (essentially the tier-1 device connectors displayed on our website). These XML files include a section that specifies the connectivity and main mapping and another section that includes all the extra fields that will be mapped into netTerrain. Below is an example of the Solarwinds drop in:

```
<?xml version="1.0" encoding="utf-8"?>
<Main>
<Connector>
  <ConnectorName>Solarwinds</ConnectorName>
 <DatabaseEngine>SQL Server</DatabaseEngine>
  <DatabaseServer>localhost</DatabaseServer>
  <DatabaseName>NetPerfMon</DatabaseName>
  <Table>Nodes</Table>
  <NameField>Caption</NameField>
  <DeviceType>sysObjectId</DeviceType>
  <ParentNetworkField>Location</ParentNetworkField>
  <Icon>Orion.ico</Icon>
 </Connector>
 <Fields>
  <Field1>
     <Source>DNS</Source>
     <nT>Dns</nT>
  </Field1>
  <Field2>
     <Source>IP Address</Source>
     <nT>Ip Address</nT>
  </Field2>
  <Field3>
     <Source>Status</Source>
     <nT>Status</nT>
  </Field3>
  <Field4>
     <Source>SysName</Source>
     <nT>sysName</nT>
  </Field4>
  <Field5>
     <Source>SystemUpTime</Source>
     <nT>sysUpTime</nT>
  </Field5>
  <Field6>
     <Source>Description</Source>
```

```
<nT>sysDescr</nT>
</Field6>
<Field7>
<Source>Contact</Source>
<nT>sysContact</nT>
</Field7>
</Fields>
</Main>
```

The screenshot below shows how to import a drop-in into netTerrain.



Device connector drop-in feature

Once you click on the XML Drop-in menu option a new dialog prompts the user to browse for the drop in XML files. The default directory is the DropIn folder in the ITK installer folder, which already includes several predefined XML drop-in files. After selecting the drop-in and clicking OK, you will be asked a few basic

questions about how to connect to the data source. The ITK will then restart and the new device connector should be registered in the tool.

Attention!

XML drop-in files only include basic field mapping information. For a deeper integration you may need to add more mapped fields or switch from a raw source table to a custom view.

Tip:

Use your GN maintenance! We can deliver a new XML drop-in for you or simply help you in creating a connection to any COTS product at no charge. This is another good reason to be current on your netTerrain maintenance!

3.3.2 Setting up the connection to the data source

Device connectors can communicate with any third-party tools that store the data in an accessible Oracle, PostgreSQL, MySQL, SQL Server or MS Access repository. If the third-party tool uses a different repository, the device connector can still be created by setting up an intermediate SQL Server or MS Access repository that establishes an ODBC connection to the source. This intermediate database is sometimes referred to as a 'proxy database'. We discuss proxy databases later in the guide.

Since built-in connectors include a lot of predefined data, setting them up in your environment essentially consists of just editing some basic parameters in the connector settings dialog.

Go to the Settings tab and hover over 'Device Connectors' and click on the particular device connector that needs to be set up.

File View Discovery	Sett	ings T	ools Help						
		Device 0	onnectors		_DCM_Mon_Devices.	- 1			
Connectors o o Devices I I Nodes Links	8	Node Connectors Link Connectors Monitoring		;	CA Unicenter Castlerock SNMPc	Ì		server	dat GN TN SN Os
	8 T 2 S			1011 1011000	Cisco RME		P = 4		
		Set Disc	Mappings liscovery Order		Concord eHealth Microsoft SCOM Native SNMP				
	Q	Applicat	ion Cbf+H ₱ 1006 ₱ 1008 ₱ 1009 ₱ 1010 ₱ 1011	1	Solarwinds () What's Up Gold Zenoss Solarwinda	SUL Serve		locahost locahost locahost locahost .UAN_SQL_2014	SO Wł Ok Re
			(III))	7.0	19 17 19 19 19				

Device connector settings menu

The settings dialog includes a series of input fields to set up connectivity parameters, such as database credentials, mapping parameters and reconciliation rules.

nnection Mapping Re	econciliation
d	1002
Connector name:	Orion NPM
Database engine:	SQL Server 🗸
Server:	.Wan
Windows authentication:	Yes 🔻
Jser:	vis
Password:	*******
Database:	Solarwinds 👻
	Test Connection

Device connector settings

The connection tab includes fields to specify the database server, database name and credentials for connecting to the third-party system. Note that certain fields may be enabled or disabled depending on the database engine that is chosen. For example, server, user and password do not apply for an MS Access database.

3.3.2.1 Source Database

If the database engine is SQL Server, then the database field does provide a drop-down box of all the databases available on that engine. For MS Access-based connectors use the ellipsis '..' button to browse for the file (.accdb and .mdb extensions are supported). For Oracle-based connectors you must type in the TNS reference. For PostgreSQL-based connectors the Server field turns into a 'DSN' field. You must then make sure there is a DSN to the PostgreSQL database (from the machine hosting the ITK) and then reference that DSN in the DSN field.

3.3.2.2 Testing the connectivity

To test the connectivity after filling out the proper credentials, you can click on the 'Test connection' button.

Connection	Mapping	Reconciliation
Ы		1002
Connector	name:	Orion NPM
Database e	ngine:	SQL Server
Server:	Conn	ector Connection t
Windows a User:	and the second	nnection Successful!
Password: Database:		Ск
	-	Test Connection

Testing for database connection

3.3.3 Mappings tab

The mapping tab includes several important fields that need to be properly filled out for the connector to discover data from the data source correctly.

Attention!

It is important to understand the structure of the data source you want to import data from. For example, you need to know what table or view contains the devices to be imported as well as which fields contain the unique naming convention and device type information.

Also, if you change any fields in the mapping tab currently associated with an additional mapped field (see additional mapped fields section), then the mapped field will be removed from the mapped field list.

3.3.3.1 Source table

The source table represents the table or view where the records that need to be pulled from the data source are stored.

Tip:

If you need to modify some of the data being imported into netTerrain or need to correlate more information that is available in other tables, create a view that "massages" that data for you and point the source table field to that view.

3.3.3.2 Device type field

The device type field is the data field in the source table that holds the identifier for the type of device that will be mapped with the corresponding type in netTerrain. netTerrain uses a name field in the node catalog

table to identify a device type. In other words, netTerrain will try to map the type name from the source with the node type library name in netTerrain.

Tip:

The most accurate descriptor of a device type is the system object id (usually called sysObjectId or sysOID). This is the SNMP discovered unique make and model identifier for a device and can be nicely mapped to netTerrain's existing table of OID to device type information (more on that later)!

3.3.3.3 Default diagram

When importing devices from a third-party data source, netTerrain can assign a default diagram for the device. This is especially important when the source table has no fields that can provide information about the parent diagram containing each device. This default diagram in netTerrain will serve as the initial repository for newly imported devices. You can assign different diagrams for different device connectors instead of searching for devices from multiple device connectors in one generic diagram. To specify a default diagram, at least one diagram needs to exist in netTerrain beforehand.

3.3.3.4 Parent locator field

An alternative to using a default diagram is to automatically place devices under a specific parent object. This is possible if the source table contains a field that stores that parent ancestry data. This can be specified in the parent locator field.

Attention!

For the automatic placement to work, the parent diagrams must exist in netTerrain prior to importing the devices. We recommend creating a separate connector that pulls the parent objects in advance, which will then guarantee that the devices will be placed under the corresponding parent objects. This is yet another way to further automate your network documentation process.

3.3.3.5 Name field

The name field should contain the name or unique identifier for each device, and it will be mapped to the name field in netTerrain. Technically, it is not necessary for this field to pull values that are unique, but it is highly recommended. If the name field is mapped to a field in the source table that does contain repeated

values, then any devices with the same name field value will throw an error during the update process. Also, if devices do not have unique names in netTerrain, then if later on you decide to also import links using the ITK, any links that have any repeated devices as endpoints will not be imported.

3.3.3.6 Rack position field

Rack coordinates can be used to automatically place devices on a given rack and rack unit. In other words, this field can be used to import rack positioning information from the source data and avoid placing a device on a rack manually. Naturally, this requires the source data to contain the proper rack unit information for the imported devices. This field assumes that the parent for each device is a rack and is specified in the parent locator field. To summarize, the rack positioning in the ITK must comply with the following:

- The parent object type must be a rack and must exist.
- The source table must contain a field for the rack unit.
- The rack unit for each record in the source data must be consistent with the size and rack unit availability for the corresponding parent rack.

If no coordinate information is available, use the value from the drop-down box.

3.3.3.7 WHERE clause

The last field of the second tab contains a WHERE clause. This can be used as a mechanism to filter certain records from the source table. The syntax of the WHERE clause must correspond to the flavor of SQL that the source database uses and must start with the 'WHERE' keyword (see the screenshot for an example).

Attention!

If the syntax in a WHERE field is incorrect, the discovery process will fail. When writing the clause, you must start the filter with the 'WHERE' keyword itself (for example 'WHERE location=1'). Also, mind that SQL syntax as it may differ from different database engines. SQL Server uses T-SQL, Oracle uses PL/SQL and MySQL, PostgreSQL and MS Access also have slightly different flavors of SQL so there may be minor differences in the syntax. If you want to avoid all this hassle don't use the WHERE clause and instead connect to a custom view where the information is already pre-filtered.

Device Connector Se	ettings
Connection Mapping	Reconcilliation
Source table:	Nodes 👻
Device Type Field:	Machine Type 👻
Default diagram:	Sandbox_Physical
Parent locator field:	<null></null>
Name field:	Caption -
Rack Position	<null></null>
WHERE clause:	
	Cancel Submit

Mappings tab settings

3.3.4 Reconciliation settings

The last tab deals with the mechanism for device reconciliation into netTerrain.

3.3.4.1 Updates

If you want to update any field changes for devices that already exist in netTerrain, then set the 'update existing devices' combo box to 'Yes'.

3.3.4.2 Inserts

New devices that do not exist in netTerrain and were discovered by the device connector will be inserted into netTerrain, if the following criteria apply:

- The 'Use generic devices for unmatched types' application setting is checked or the device type can be mapped to a type in netTerrain (see type mapping later in this chapter)
- A default diagram has been assigned for the device connector (defined in the mappings tab) or a parent container field exists, and the proper parent object also exists in netTerrain
- The 'Insert new devices' combo box is set to 'Yes'

3.3.4.3 Deletes

Devices that exist in netTerrain but no longer exist in the source can be processed in two different ways:

- They can be deleted from netTerrain by setting the 'Delete devices without matches' combo box to 'Yes'
- The can be kept in netTerrain by setting the combo box to 'No'

Attention!

When the 'Delete devices without matches' combo box is set to 'Yes' only devices that were originally inserted by that same connector will be deleted from netTerrain. For instance, a router called '123' that no longer exists in the data source but still exists in netTerrain, will only be deleted if it was originally inserted by that same connector. Internally, any devices that are inserted in netTerrain by the ITK are tagged with the connector id. Then, when a delete process occurs, only devices with that connector id will be deleted (provided they no longer exist in the source).

3.3.4.4 Preventing deletes for low record counts

Notice a field underneath the delete drop down box that includes a counter. This counter can be used to restrict a delete operation to cases where the number of discovered elements is greater than a certain number. Set that counter to any integer between 0 and 10 million.

The default value for this counter is always 0, in which case the delete reconciliation process (when the combo box is set to yes) will always occur.

Tip!

Use the delete counter when the data being discovered goes through a process that may not always be robust and could yield an empty table. In those situations, if the delete combo box was set to yes, you can prevent all records that were imported from that connector from being deleted in netTerrain by setting the counter to a number greater than 0.

Update Existing Devices: Yes Insert New Devices: Yes Delete Devices without Matches: Yes Only delete if count >= 0 Pre import function:	onnection Mapping Reconcilliation	5
Delete Devices without Matches: Yes Only delete if count >= 0 Pre import function:	Update Existing Devices:	Yes 🔻
Only delete if count >= 0	Insert New Devices:	Yes 🔻
Pre import function:	Delete Devices without Matches:	Yes 🔻
	Only delete if count >=	0
Partiment functions	Pre import function:	
rost import function.	Post import function:	

Reconciliation tab

3.3.4.5 Pre and post import functions

These fields are used to place advanced functions that are processed before and after an import occurs. An example of a pre-import function could be a call to execute a stored procedure in the source data, which

massages the records to be imported. An example of a post import function could be a layout algorithm that is triggered after the import to automate node positioning.

Attention!

The Pre and Post import function fields are currently reserved for Graphical Networks consultants. If you think you need a function to perform a specific action, please enter a ticket in the support portal.

3.4 Additional mapped fields

In addition to the main fields that comprise the device connector settings, extra fields can be mapped to the connector (such as the IP address, DNS name, location and so on). To find out which fields have been mapped for a built-in connector, go to the device connector list, right click on the connector and click on 'Mapped Fields'.

id 1001 1004 1005 1005 1006	alas Native SNMP SolarNewProdu CA Unicenter Castlerock SNM	dbEngine SQL Server SQL Server SQL Server MS Access	server 192.168.1.42\.5 locathost	database GNCORE SolarWindsNew TNS SNMPc mdb	status 1 2	lastDecovered 7/10/2015 12.4	lastReconciled 7/13/2015 4.44 7/5/2015 1.41
₹ 1007 ₹ 1008 ₹ 1009 ₹ 1010	Conce NME Microardt SCOM What's Lie God Safarwinds	MSRcsee SQL Server SQL Server	Suspend Activate Clone Clone Edt Delete Mapped Fiel Status Mappi Refresh View	ngs			

Accessing additional mapped fields

A new 'Mapped fields' dialog will pop up, which will show any mapped fields in the list view and provide a mechanism to remove any mapped fields or add new ones.

Attention!

If your connector doesn't have valid credentials to connect to the source (i.e. a connection failure) then you will not be able to see the mapped fields. You can always check if your connection is valid by first opening the connector settings in edit mode. Use the test connection button to see if you have a valid connection to the source database.

3.4.1 Adding and removing mapped fields

In addition to the basic fields that are used in the source to properly import data into netTerrain, such as name or type, the ITK allows you to map any other fields in your source to custom fields in netTerrain. So, for example, if you are importing sites from a sites table in your database, and those sites include an address field, it is easy to map that field to an address field in netTerrain.

In short, mapping fields between the source and netTerrain is establishing a correspondence between a field in the source table and a field for a specific type (or for all devices, in the case of device connectors). As a result, during a reconciliation process, all the records in the source that have a value for that field, will append that same value to the corresponding instance in netTerrain.

There are several ways to map fields in netTerrain. The ITK even lets you create the field in netTerrain on the fly, if it doesn't exist there yet. This saves you the extra work of going to the netTerrain catalog and creating the field there.

3.4.1.1 Mapping fields when they already exist in netTerrain

When the destination fields in netTerrain already exist, you can simply map fields one by one or also use the option to map all fields with matching names.

To map a field from the source to an existing field in netTerrain, simply choose it from the source table and then select the corresponding destination field in netTerrain that you want the source field mapped to. Finally click on 'Map Selected Fields' and you are done.

Notice that the fields do not have to have the same names.

Once added, the new mapping will show up in the 'Fields currently mapped' list view.

To remove a mapping, simply select it and hit 'Remove'.

ap New Field				
Field in source data	abase: ntName			
		Create + Map All	Create + M	Лар
Field in net Terrain:	Owner			•
	1	Map Matched Fields	Map Selected	Fields
elds Currently Mappe	d			Map se
nTld	Source Field	ne	tTerrain Field	
28000000147109 28000000147101 28000000147102 28000000147104	createDate database_id databaseName dataFileName	da da	eateDate tabase_id tabaseName taFileName	E
28000000147101 28000000147102 28000000147104 28000000147105 28000000147106	database_id databaseName dataFileName dataFileSize dbEngine	da da da da db	tabase_id tabaseName taFileName taFileSize Engine	E
28000000147101 28000000147102 28000000147104 28000000147105	database_id databaseName dataFileName dataFileSize dbEngine dbServerInstand	da da da da db	tabase_id tabaseName taFileName taFileSize	-

Adding a new mapped field

When many of the fields in the source match the names of the fields in netTerrain, you can map them all in one simple process by clicking on the 'Map Matched Fields' button.

You can also clear all mappings from the connector by clicking on the 'Clear mappings' button.

Any changes in the mapping will be reflected in the corresponding connector table view but notice that if the connector view is currently active you may need to refresh the view. Also, to see the values associated with the new mapped field you must run a device discovery first (see below).

3.4.1.2 Mapping fields when they don't exist in netTerrain

As mentioned before, in case one or more of the source fields do not yet exist for the type in netTerrain, you can map and create them in the catalog, at once, straight from the ITK.

To map and create just one field from the source, select it first from the drop-down list, and then click on 'Create + Map' button. If you want to Create and map all the fields in the source, click on the 'Create + Map All' button.

Notice that these options are not available for device connectors.

3.5 Device discovery

Once the connector is properly configured the fun part begins. To run a discovery for the first time simply go to the 'Discovery' menu and click on the device connector you configured in the previous step.

File View Discovery Settings Tools Help	_				
Manual Device Discovery Manual Node Discovery Manual Link discovery Manual Link discovery Manual Link discovery Manual Link discovery Start Scheduler Concord eHeath Microsoft MOM Microsoft MOM Microsoft SCOM Mat's Up Gold Mat's Up Gold Modes J SQL_Mon_Database J SQL_Mon_DbServerInstance Mative SIMP_Edema_IPs Solar_indes Swtches Swtches Links	Count: 1 NMP ME enter sk SNM ds eHealth t MOM soft SCOM 's Up Gold	dbEngine SQL Server MS Access SQL Server	server - localhost localhost localhost	database GNCORE DiscoRME.mdb TNG SNMPc.mdb Solarwinds Mom.mdb SCOM WhatsUp	statu 2 1 1 1 1 1 1 1 1

Initiating device connector discovery

Tip:

You can also start a discovery by double clicking on the connector entry and then clicking on the 'Refresh List (Discover)' button, as displayed below.

Connectors 👒 🥔	Solarwinds	Court 21					
🕀 👹 Devices	Caption		ocation priority	DNS	IP_Address	Status	s
- CA Unicenter	and the second s	and the state of t			and the later of t	- Sealone	
 Casterock SNMPc 	51A27		25 Primary	\$1A27	192,168,7,3	1	
Geco RME	S1A29		S6 Primary	\$1A29	192.168.7.4	-12	
Concord eHealth	52A1 52A2		42 Pimary	52A1	192.168.7.5	-12	
Mcrosoft SCOM			39 Primary	\$2A2	192 168 7.6	+	
III III Native SNMP	\$2A3		25 Pamary	\$2A3	192,168.7.7	11	
B-III Stewards	S2A4		25 Pemary	52A4	192 168 7.8	-12	
What's Up Gold	5245		25 Pilmary	\$245	192.168.7.9	_!!	
- Nodes	S2A6		25 Primary	\$2A6	192.168.7.10	-12	
III Noose IIISQL_Mon_Database IIISQL_Mon_Db ServerInstance IIISQL_Mon_Db ServerInstance IIINotive SNMP_Extend IPs	\$2A7		39 Primary	\$2A7	192.168.7.11	1	
	S3At		39 Pimary	\$3A1	192,168.7.12	11	
	5342		39 Plinary	5342	192.168.7.13	11	
H- III Stee	\$3A3		42 Pimary	\$3A3	192.168.7.14	-13	
H- II Sola_nodes	S3A4		42 Penary	\$3A4	192.168.7.15	1	
R- B Swtches	\$345		42 Primary	\$3A5	192,168.7.16	1	
🗄 👗 Links	S3A6		56 Pimary	5346	192.168.7.17	1	
	\$3A7		56 Ptimary	\$3A7	192.168.7.188	1	
	\$3A8		56 Primary	S3A8	192.168.7.19	1	1
	\$4A1		51 Primary	S4A1	192,168.7.20	1	
	54A2		79 Pimary	\$4A2	192 168 7 21	1	
	6443	1101112016		C113	103 100 7 93		
	033	030000		P	sge: 14 40 1 100	M	

Running a discovery from the connector view

By clicking on this submenu, netTerrain will start the process of importing the raw data from the third-party data source and will display the results under the corresponding view menu. Note that the devices are not yet imported into netTerrain. The latter involves the execution of the reconciliation process. The output window will also show the start and end times of the discovery process.

S4A2 S4A3	Catalyst 37xx St Primary Catalyst 37xx St Primary	2	
02301		4 1 H H	
6/27/2014 9:19:12 AM: Starting	discovery process for Sola2. This process can take seve	ral minutes	
6/27/2014 9:19:12 AM: Starting 6/27/2014 9:19:13 AM: Finishe		ral minutes	
6/27/2014 9:19:13 AM: Finishe			
6/27/2014 9:19:13 AM: Finishe	f process.		

Discovery process messaging in output window

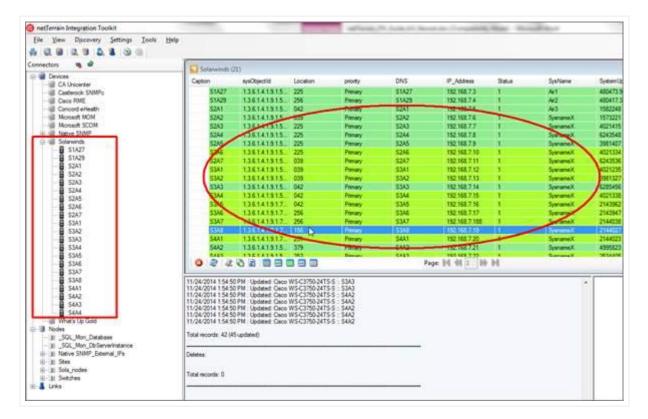
As opposed to discovery with SNMP, WMI and IPMI where the ITK has to actually poll the network, all other processes are usually fast. In certain cases though, the discovery could take several minutes:

- The source is on a slow network.
- The amount of data to discover is extremely large (tens or hundreds of thousands of records).
- The query that pulls the records from the source is very complicated or badly designed.

In sum: mind the network connectivity, preferably filter any unwanted data in the source and make sure that the source data is not using an inefficient query.

3.5.1 Viewing the results

Once devices have been imported as raw data into netTerrain, you can view these devices and associated columns by clicking on the 'View' menu and the corresponding device connector, or by double clicking on the connector in the connector list.



List of discovered devices

Each device will be represented by a row and will contain values for several columns that will depend on the tier-1 connector backend setup.

The list view uses specific color codes to identify the status of the device in netTerrain. We will review these color codes later in this chapter as well as some tricks and tips on how to analyze the results.

Devices can also be viewed from the tree view. In addition, if a user wants to view a device in more detail, by double-clicking on the row entry the ITK will display a dialog box with each attribute for the device.

Caption: S3A6		
Department: R15		
Machine Type: Cisco Catalyst	3560-8PC	
priority: Primary		
AvgResponseTime:		
IP_Address: 192.168.7.17		
LastBoot: 6/3/2010 3:10:00 i	РМ	
Record exists in net Terrain (d	scovered by the ITK)	
	Т	
	5 4 5	
		-
	Show on Diagram	ОК

Device details

3.6 Device reconciliation

So far, the discovery has simply pulled the data from the source into a raw table in the ITK, but it is not yet in netTerrain. To import devices into netTerrain, we need to reconcile the discovered items with the netTerrain database. This reconciliation process includes the insert, update and/or delete of devices from the data source into netTerrain, according to the rules specified in the device connector mapping settings.

The ITK can reconcile devices in two different ways: create a specific device type in netTerrain based on some sort of type identifier available in the source data or create a generic device type in netTerrain. The obvious advantage of providing specific type information to netTerrain is that we can take advantage of the netTerrain catalog and automatically create the slots and ports of the devices as well as obtain the size,

power and other specs of the device. That is, the ITK will create these devices automatically and they inherit all the good stuff from the netTerrain catalog.

If we want specific device types to be created in netTerrain we should make sure that the types are properly mapped. This is known as 'Type mapping'. By default, if during the reconciliation process, there is no proper way of knowing which specific type a certain device is, the ITK will create an instance of a generic type in netTerrain. However, we can prevent the ITK from creating a device in netTerrain unless the type is mapped and force a 'device reconciliation'.

3.6.1 Type mappings

In order for device reconciliation to work for a given device, a type mapping is required between the name of that device type in the source and netTerrain. This type mapping process enables the ITK to determine the netTerrain type a device needs to be mapped with. So, for example a device type in the source may be called Cis_6509, which could map to the corresponding Cisco 6509 in the netTerrain catalog.

3.6.1.1 The role of the object identifier

In one of the tips above we mentioned the object identifier as the recommended source field to identify the device type. Let's review this again.

Usually the most accurate descriptor of a device type is the system object id (called sysObjectId, sysOID or just OID). The OID is a so-called MIB value that many systems (including netTerrain itself) can discover via SNMP and it uniquely identifies the make and model for a device. Conveniently enough, the ITK includes a table that maps OIDs to potential netTerrain types, as described below

Later in this guide we will review the sysObjectId as part of our native SNMP discovery engine, but it is important to note that many device connectors can also have this field available. The advantage of using this field not only lies in the fact that it ensures a univocal identification of the device type, but it can also be used as a hint to find what is the most likely type in netTerrain that matches that OID.

OID	Model	Vendor
1.3.6.1.4.1.2879.1.1.1	Sanus GSX9000	Sonus
13.6.1.4.1.2879.1.1.2	G5X9000HD	Sonus
1.3.6.1.4.1.2379.1.1.2	Sanus GSX9000HD	Sonus
1.3.6.1.4.1.289	EMCConnectrixSwitch	EMC
1.3.6.1.4.1.299.2.1.1.2	ED-6064	MODATA
1.3.6.1.4.1.289.2.1.1.2	McDATA ED-6064	McDATA
1.3.6.1.4.1.290.7.1.1.0	HarrisheDQness	Harris
1.3.6.1.4.1.290.7.1.1.1.1	HarrisSCM	Harris
1.3.6.1.4.1.2925.4	AlterPath ACS48	Cyclades
13.6.1.4.1.2925.4	AvocentACS48	Avocent
1.3.6.1.4.1.2925.4	Cyclades AlterPath ACS48	Cyclades
136.14.1.2944.1.18	Attack Mitigator	Top_Layer_Networks
136.14.12944.1.18	Top_Layer_Networks Attack Mit	Top_Layer_Networks
1.3.6.1.4.1.298.2.2.18	Asante Technology Intra5witch	Asante Technology
1.3.6.1.4.1.298.2.2.18	IntraSwitch 622404	Asante Technology
136.14.1.298.2.2.24	Asante Technology IntraCore 65	Asante Technology
1.3.6.1.4.1.298.2.2.24	IntraCore 6524-2G	Asante Technology
13.6.1.4.1.298.2.2.27	Asante Technology IntraCore 3524	Asante Technology
1.3.6.1.4.1.298.2.2.27	IntraCore 3524	Asante Technology
136.1413.11		HDS
136.1413.11	HDS .	HDS
136.1413.11	HDS NA	HDS
136.14.13.1.1	NA.	HDS
1.3.6.1.4.1.300.1	Digilink DL 3100	Digilink
1.3.6.1.4.1.300.1	DL 3100	Diglink
1.3.6.1.4.1.300.102	DL3800	Quickeagle
1.3.6.1.4.1.300.102	Quickeagle DL3800	Quickeagle
1.3.6.1.4.1.300.200	4300/5800	Quick_Eagle
1.3.6.1.4.1.300.200	Quick_Eagle 4300/5800	Quick_Eagle
1.3.6.1.4.1.3003.2.2.2.1	Alcatel OnniCore 5200	Alcatel
1.3.6.1.4.1.3003.2.2.2.1	Alcatel OmniCore 5052	Alcatel
1.3.6.1.4.1.3003.2.2.2.1	Alcatel PR-5200 Gigabit Switch R	Akatel
1.3.6.1.4.1.3003.2.2.2.1	AlcatelGigabitSwRt	Alcatel

Embedded OID to type suggestions table

As mentioned before (and shown in the screenshot above), the ITK includes a table with several thousand OIDs and the most likely make and model it is associated with. By taking advantage of this embedded table, you can speed up the process of finding the netTerrain type that should be mapped with the OID.

3.6.1.2 Viewing existing type mappings

To view the list of existing type mappings, click on Settings->Type mappings->View.

The ITK includes a few thousand mappings that are used for the native SNMP discovery. To filter the mappings for a specific device connector, simply type the name of the connector into the filter box and press enter.

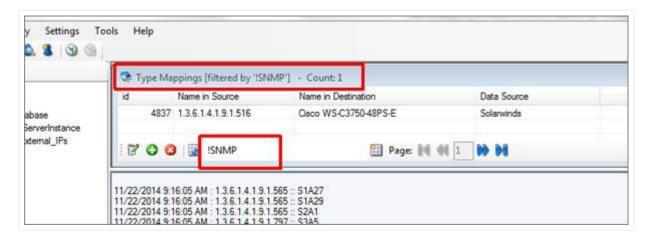
•	Type Mappi	ngs - Count: 4830		
Mon Devices	id	Type Name in Source	Type Name in netTerrain	Data Source
center Tng	19704	13614110213	NO_NAME	Native SNMP
onfig Files	23782	13614110122521	NO NAME	Native SNMP
ME	23783	13614110122522	NO_NAME	Native SNMP
d eHealth	20827	1.3.6.1.4.1.10213.1.1	NO_NAME	Native SNMP
A MOM A	21848	1.3.6.1.4.1.1022.9	NO_NAME	Native SNMP
oft SCOM	21451	1361411027121	NO_NAME	Native SNMP
SNMP	20996	1361411027122	NO_NAME	Native SNMP
PM	20904	1.3 6 1 4 1 1027 1 2 3	NO_NAME	Native SNMP
	21474	1.3.6.1.4.1.10418.10.1.1	NO_NAME	Native SNMP
5	21475	136141104181012	NO_NAME	Native SNMP
427	21486	1.3.6.1.4.1.10418.10.1.3	NO_NAME	Native SNMP
A27 A29	21477	1.3.6.1.4.1.10418.10.1.4	NO_NAME	Native SNMP
A29 A1	20826	136141104181312	NO_NAME	Native SNMP
12	20678	1.3 6 1 4 1 10418 13.1.3	NO_NAME	Native SNMP
A3	20844	1.3.6.1.4.1.10418.2.1.1	NO_NAME	Native SNMP
44	20843	13614110418213	NO_NAME	Native SNMP
45	20716	1.3.6.1.4.1.10418.7.1.10	NO_NAME	Native SNMP
AG	20718	1.3 6 1 4 1 10418 7 1 11	NO_NAME	Native SNMP
47	20719	136141104187112	NO_NAME	Native SNMP
11	20788	106141104187110	NO_NAME	Native SNMP
2	IF OO	solarwinds	🔁 Page 🕅 📢 1 🕪 🕅	

Using the filter text box

To clear the filter, click on the 'Clear filter' button next to the text box.

Tip:

The list view filter can use a NOT (!) operator. This comes in handy when trying to exclude type mappings for a certain connector. For example, to exclude all mappings associated with the Native SNMP, you can type '!SNMP' in the filter.



Using the ! operator in filters

3.6.1.3 Adding new type mappings

To add a new mapping into the system, click on Settings->Type Mappings->New (or Ctrl-N). A type mapping needs to specify the name of the type used in the source and the corresponding (exact) name used for the same type in netTerrain. Finally select the device connector this mapping refers to.

id:	22		
Type Name in Source	1.3.6.1.4.1.9.1.485		
netTerrain Catalog Device	Cisco WS-C3550-24-SMI	▼ Fin	id
Data Source	<all></all>		

Using the type mapping dialog

In many cases the type mapping can be utilized for many different connectors, such as the case of the sysObjectId, which is a universal representation of a make and model. In those cases, you may want to assign the Data Source to all connectors. This not only comes in handy to assign a mapping to any existing connectors in the ITK (thus avoiding potential repeated work), but it will also apply to any future connectors that have a match with the source type.

To simplify the process of mapping a type, this dialog includes a 'Find...' button, which opens a type finder utility that can be used to search through different types in netTerrain without having to rely on the type drop down field.

burce	
Name in source: 1.3.6.1.4.1.9.1.	1045 Score 0 🔶
Probable sysOID matches:	
Cisco :: cisco2911 Cisco Systems :: 2911 Cisco :: C2900 Cisco Systems :: Cisco 2911	
et Terrain Catalog Names	
Suggestions: 2145	Filter
12 AC Plugs 12 AC Plugs_B 19in Blank 1RU 19in Blank 2RU 19in Blank 3RU 19in Blank 4RU 1RU Panel 24 port fiber panel	

Type Finder Tool matching for a sysOID

The type finder tool can be used in multiple ways. If the source type is an object identifier, netTerrain can suggest what type the OID corresponds to, using the embedded OID to type suggestions table. This feature works automatically when netTerrain finds a match between an OID and an entry in that table. It will then display a list of one or more values in the 'Probable sysOID matches' section. The support table contains one or more labels by which a given OID has been referenced by other systems or vendors in the industry (hence the reason why there can be multiple choices). With a set of possible matches available, the user can start typing a search string in the filter text box and the type finder tool will start narrowing down the options of types as the string gets more specific. Another option is to use the score counter, which starts narrowing down the options in the netTerrain catalog names section by increasing the matching score.

It is possible that a certain sysOID has no match in the suggestions table or that the name in the source is not an OID at all, but an actual human readable name. In those cases, the user can still use the filter option to search for a possible match. Just type in some relevant string that could match the type name in the source and the ITK will narrow down the options.

ource				
Name in source:	1.3.6.1.4.1.9	1.797	Score	0 🔤
Probable sysOID	matches:			
Cisco :: catalyst Cisco :: Cat 3560 Cisco Systems :: Cisco :: catalyst 3	8PC Catalyst 3560-	8PC-S		
tTerrain Catalog N	lames			_
Suggestions: 32	1	Filter 35	eol I	
Cisco WS-C3560 Cisco WS-C3560 Cisco WS-C3560 Cisco WS-C3560 Cisco WS-C3560 Cisco WS-C3560 Cisco WS-C3560	0-24PS-S 0-24TS-S 0-48PS-S 0-48PS-S 0-48TS-S 0-8PC-S			

Using the filter in the type finder tool

3.6.2 Preventing device imports without a mapped type

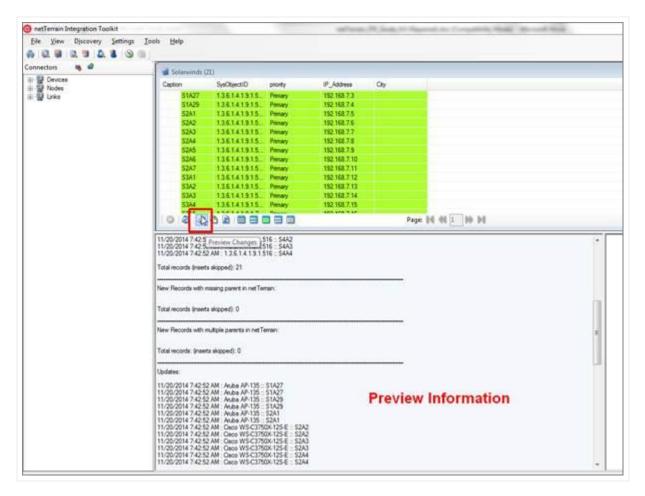
As mentioned above, by default the ITK will create a generic device type for any device that has no identifiable type (no mapped type). However, we can prevent the ITK from creating a device in netTerrain unless the type is mapped and force a 'device reconciliation'.

The Application settings dialog (ctrl-h) includes a tab where the user can uncheck the option 'Use generic devices for unmatched types', as displayed below. Unchecking this option will prevent the ITK from creating devices with unmatched types and will force the user to have to map a type for those unmatched types to import them into netTerrain.

Use generic devices fo	or unmatched types:
Records per Page:	25 💌
App server url:	http://localhost/vis
Silent mode:	
Output buffer:	2000000

3.6.3 Previewing a reconcilation process

Before importing and reconciling the data into netTerrain it is recommended to run a preview task. This will provide some insight into which devices will be inserted, updated or deleted. It will also provide a snapshot of devices that cannot be reconciled because no types have been mapped. The latter information can be used to add types to netTerrain or map existing netTerrain types with one of the device connector fields.



Previewing the reconciliation

The output window will display the expected operations and records affected by a reconciliation process.

The insert operations (the 'Insert New Nodes' option in the reconciliation section of the connector must be enabled) include:

- Records without a matching type in netTerrain: these are all the devices for which no source type information (make and model) has been matched with a type in netTerrain. In the event of a reconciliation, these records would create a generic device type in netTerrain (or skip the insert process if the 'Use generic devices for unmatched types' is unchecked.
- Records that are expected to be successfully inserted.
- Records with a missing parent in netTerrain: in case the connector uses a parent field to find the container diagram in netTerrain, any devices for which such parent cannot be matched with a diagram of the same name in netTerrain will also skip the insert process.
- Records with multiple parents in netTerrain: in case the connector uses a parent field to find the container diagram in netTerrain, any devices for which a parent value is matched with more than one diagram of the same name in netTerrain will skip the insert process. In other words, use unique names otherwise netTerrain doesn't know which parent to choose from.

The update operations (the 'Update Existing Nodes' option in the reconciliation section of the connector must be enabled) include:

• Records to be updated: any records for which one or more field values have changed will be updated in netTerrain once reconciled. Notice that the output will display one entry for each field that has a change. For example, if a certain device has three changes in three fields, then the output will display three entries.

The delete operations (the 'Delete Existing Nodes' option in the reconciliation section of the connector must be enabled) include:

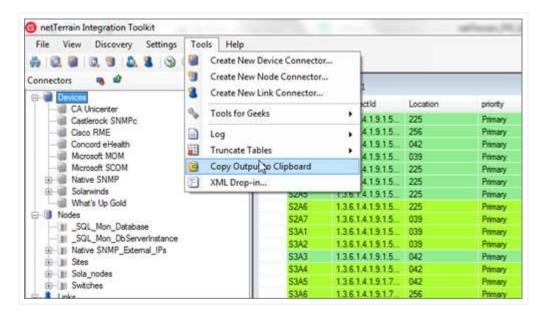
• Records to be deleted: any records that were inserted by that same connector in netTerrain in some previous operation, which are no longer in the source database will be deleted in the event of a reconciliation.

3.6.3.1 Copying the output window contents to the clipboard

If you need to work with the output window results in some other application, you can copy the contents:

- Right click on the output window
- Select all
- Hit Ctrl-C
- Paste the clipboard contents to the application

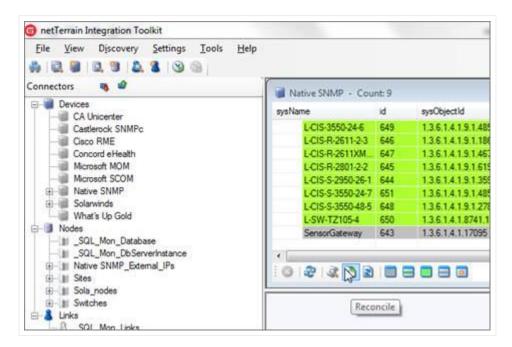
You can also copy the output window contents by clicking on Tools->Copy output to clipboard and then pasting the clipboard contents to the application.



Copying the output window contents to the clipboard

3.6.4 Reconciling data with netTerrain

Once you are ready to reconcile the data into netTerrain you can start the process by simply opening the list view for the connector and clicking on the 'reconcile' button.



A single button to discover and reconcile is also available (next to the reconcile button).

Reconciling data with netTerrain

Once the reconciliation starts, the ITK will display the same output displayed for the preview, with the actual devices being inserted, updated and /or deleted.

Note that for large bulk imports, this process may take several minutes or even hours as devices are properly imported, reconciled and indexed. For convenience, as the ITK is processing the reconciliation, a progress bar will be displayed on the bottom status bar of the application window.

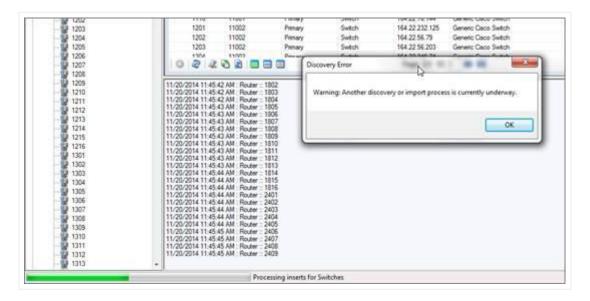
ITK progress bar

Once the reconciliation has finished, any devices that are 'type mapped' and have the proper container diagram information (either a default diagram or parent node that exists in netTerrain) will be created in netTerrain. If no rack units were mapped, each device will be placed sequentially on its corresponding diagram, starting from the top left corner of the netTerrain screen.

	20002488
G GRAFHEAL 🖛 🛋 🔄 🖬 🔮 🚳	- (1994) - (1995) -
Haranchy Top Level U D Top Lev	
0 62/4 0 62/2 0 62/4 0 7 10 10 10 10 10 10 10 10 10 10 10 10 10	tan C. mana panalari C. mana panalari
Nodes (Mill tree)	100
Cabinets Cab	Suid Company and and Company and and Company and And Company and And Company
Hidden Objects II Audi Thai 128	5

Attention!

When a discovery or a preview/reconciliation process is running (whether triggered manually or through the scheduler) you cannot start another process. Attempting to do so will yield an error as seen on the screenshot below.



Warning message for an attempt at concurrent discovery

3.6.5 Mapped fields missing in netTerrain

For device connectors, the ITK tries to match up mapped fields based on the mapping specifications, but it assumes that the field in netTerrain exists. This could present a difficulty for device connectors (not for node connectors since the mapping is against a particular type), because for device connector the reconciliation involves all types. A certain field may exist for certain device types in netTerrain but could be missing for others. For example, a field called IOS may exist for all Cisco types in the netTerrain catalog but not be available for Juniper types. As a consequence, you may find instances of reconciled devices in netTerrain that do not have a field that you expected to see, based on the mappings done in the ITK.

In some cases, this may not be a problem because the field wasn't needed for that type to begin with, but what can we do if it was indeed needed? You can obviously go to the netTerrain catalog and add the field for all the types that are missing it. This could present a headache if the field is missing for hundreds, let alone thousands of types.

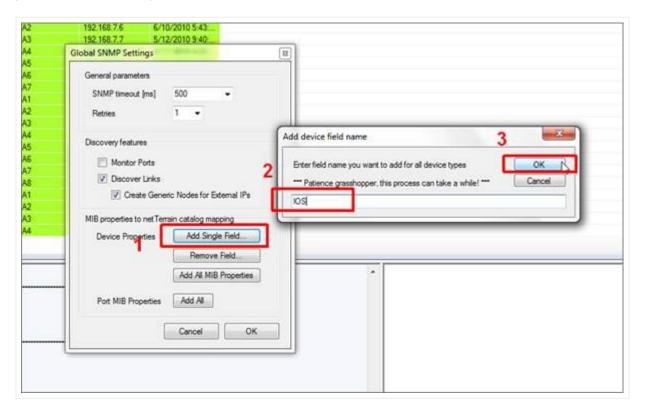
For such cases the ITK has a feature to add a certain field to every device type in netTerrain. This feature is mostly intended for usage with the SNMP discovery, so it is somewhat buried in the UI (a command is also available). Follow this 3-step process:

1) Go to Settings->Monitor->Configuration (or press Ctrl-G) and click on the 'Add single field' button

2) Type in the name of the field you want to add to all types in netTerrain

3) Click 'OK'

The ITK is smart enough to only add the field to the types that are missing it. And yes, be patient indeed, this process can take a couple of minutes.



Adding a field to all device types in netTerrain

You can also remove a field from all types in netTerrain, using the 'Remove Field' button. We will review the rest of the functions in this dialog in the chapter about Monitoring.

Attention!

Be careful with these functions as they affect all types and instances in netTerrain!

3.7 Automating the process

The entire process described in the previous sections can be automated so that it runs in the background, without a user having to manually start the discovery and reconciliation every time data needs to be synchronized between the sources and netTerrain.

3.7.1 Setting up the scheduler

The scheduler consists of two main attributes:

- Polling cycle: deals with the frequency of state information (status) update for devices that have already been imported into netTerrain and that exist in the original data source
- Discovery cycle: deals with the frequency of the insert/update/delete process that reconciles the data between the data source and netTerrain

To set up the scheduler go to Settings->Application and proceed to modify the Polling Cycle and Discovery cycle parameters based on how often the ITK needs to update the information in netTerrain.

Scheduler Other	
Polling Cycle [s]:	5
Discovery Cycle [h]:	0.25 👻
Run Discovery Upon Activation:	
Start day:	Sunday 👻
Start time:	12:00:00 AM

Setting up the scheduler

You can set the scheduler to run immediately upon activation, or to only start at a specified weekday and time. If you check the 'Run Discovery Upon Activation' option, the ITK will start immediately after you click on the 'Start Scheduler' button (see below). If this option is unchecked, after you click on the 'Start Scheduler' button the scheduler will start on the specified day and time and then fire up based on the frequency set in the 'Discovery Cycle' combo box. For example, a setting matching the screenshot below would mean that the scheduler will start on Tuesday at 3AM and then trigger every 24 hours (Wednesday 3AM, Thursday 3AM, etc.).

Scheduler Other	
Polling Cycle [s]:	5
Discovery Cycle [h]:	24 👻
Run Discovery Upon Activation;	
Start day:	Tuesday 🔻
Start time:	3:00:00 AM

Using the scheduler day and time settings

Tip:

It is recommended to set the discovery cycle to a value that is high (such as 24 hours) to avoid excessive SQL traffic. In general configuration data does not change often enough to require a refresh on the netTerrain inventory in real-time or near real-time. In many cases it is not even necessary to automate the discovery, since a manual process can be triggered once a day or even once a week.

3.7.2 Real-time status polling

As we saw above, one of the parameters in the scheduler is the polling cycle. This cycle essentially determines how often the ITK will update status (or state) values for any connectors that support it.

To enable status updating, the device connector itself needs to be able to pull state information from the source, which, of course, means that the source needs to be able to obtain real-time state information in the first place.

Note that the status polling we refer to here is status available from the original data source, not live status obtained from the actual devices. The latter is also possible using the ITK SNMP discovery tool (see the chapter on SNMP discovery).

3.7.2.1 Mapping the status field in the source

Assuming the source does indeed provide real-time status information for devices (such as Solarwinds, for instance) you need to map the field that pulls that information. To do this, follow these simple steps:

1) Make sure the status field in the source is already part of the mapped fields, so that netTerrain can import that data.

P 1005	CA Unicenter	SQL Server	location	TNG	2			6
P 1006	Castlerock SNM	MS Access		SNMFc.mdb	1			7
1007	Gece RME	MS Access		CecoRME mdb	1			8
1008	Morseoft SCOM	SQL Server	locahoat	SCOM	1.1			9
P 1009	What's Up Gold	SQL Server	locahost.	Wheelip	1			10
1010	Solawinda	SQL Server	.UAN_SQL_2014	Solarvinda	1	9/9/2015 6:04 1		11
				Mepped Field				
				Map New I				
				1.	enu source database			
					net Tensin	Assigned To		
								(AM
								1
				Felds Curre	ntly Mapped			
				nTid	50	urce Field	netTerrain Fiel	d
				meCort	act Co	rtect	eyeCortect	
				AveCes.		ectiption	sysDescr	
				One		6	Dee	
			-	1 A 100		August	U Possenie	
				2.0.4	3	Rus -	Satur	
			-	neupt	ine Sy	stemiloTime	eys Up Time	
/9/2015 6 04 12 Pt	M: Stating discovery	process for Solarve	nda. This process can la					Remove
13/2015 6:04 12 Pt	M. Finished process.							
								Occe
				-				
								D.

2) Right click on the device connector and select 'Status Mappings'

SCOM 1 WhatsUp 1 Struct Schemende 1 Suspend Activate Clone Edit Delete View Becords	9/9
2014 Suspend Suspend Activate Clone Edit Delete	9/9
Suspend Activate Clone Edit Delete	
Mapped Fields	
	-
Status Mappings	
Kefresh View	
	-
	Status Mappings

3) From the Status Mappings select the status field from the source in the drop down

Select Status Field		
Source Status Field	Status	
Add Status Values Value in source	Contact Description DNS IP_Address. Status SysName	L2
Flag color	SystemUpTime	-10
		Add
Flag color	Status value (source)	

4) As an optional feature, you can also set flag colors representing different status values for each record in the ITK list view. These colors do not have any effect on the representation of the devices in netTerrain. To actually change colors (or effects) for the visual representation of devices in netTerrain, you can create visual overrides in the netTerrain catalog (see Power User Guide).

Select Status Field		
Source Status Field	Status	-
Add Status Values		
Value in source	3	
Flag color	blue	
		Add Da
Flag color	Status value (source)	
₽ 1 ₽ 2	1	
Remove		
		Finish

Below is an example output using that shows records from the source along with the corresponding flag colors.

ili Device 3 Note 1 Line	Castor P 152 48.5 P 152 48.1 P 152 48.1 P 152 48.1 P 152 48.1 P 152 48.1 P 152 48.1	SyrOnyactiC	Coreat	Ceacitytion	DNS	#_Addmm 192.968.0.04	Date:	Syshiane	Notemily Time	profit, Preserv
	P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1					102,160.0.04	2		0	
	P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1 P 112 68.1									
	P 15 681 P 15 681 P 15 681 P 15 681 P 15 681 P 15 681 P 15 681					1921102112			0	Ponery
	P 152 48.1 P 152 48.1 P 152 48.1 P 152 48.1 P 152 48.1					152 168 1 36	1		8	Frenary
	7 15. 48.1 7 15. 48.1 7 15. 48.1 7 15. 48.1				WIN 828,2LU	192 198 1.46	1		0	Preserv
	9 15.0481 9 15.0683 9 15.0683					192 168 1 52			0	Finan
	P 15, 68.14				PHONE	152 168 1 56	1		0	Presary
	P 15, 451					132.168.1.6			10	Paran
						152 168 1.78	3		8	Prevents
	7 15 1811					192 168 1.8	1		8	Frenery
	971 mar PC				TTESTER-PC-	102.168.1.18	19		0	Frenze
	PET 1054		Sector .	Several ALL TZ		192 168 1.1	1	0.121054	4134710	Trenary
	PLC 385	136141514.		Care US Saltar		102.168.0.5	2	1.05355346	MINUT 7	Preserv
		136141911		Case Harration		192 198 0 3	3		507421.5	Frances
	71CH42	135141314	Sector	Deco KIS Softw.		192168.0.4	2	LOS#2010	507999.2	Frankry
	FLC #2	136141316	Stohan	Ceco IOS Safe		192.168.0.2	2	LC6428122	507433.A	Presare
	PLC #2	136141516	Stashan	Date XX5 Setter		192 168 0.8	2	LOS-R-2801-24	252.13	Frenary
	PLC 52	116141813	Stophan	Colo Marratan		152 168.5.5	1	LCIS-5-2965-24-3	1170-67	Preserv
		136141913		Date Hearten		192 165 5 7	11	LC552950261		Frenary
	PLC 51	135141314	Fed	Ceco IOS Safe		192 166 8 7	2	LCG-53885247	1107596	Finan
	FLC 51	136141812		Caso History		182.168.0.5	1	LCI5-5-350048-5		Dimary
	1 LO LEU	11614161	Station UPS	Del UPS Town		192,168.0.10	1	LOCILOPS-15	3699708	Prevary
	P 14 172	12814187811	Shaphan	Swelthau 12		182.162.0.50	T	LOW 121054	2079-45	Frenery
		136141110		100 Managed S.		152 198 5 11	2	L 7PLM 90321		Frenanc
	P NA.	1351418072		Linux Dekchates.	DISKSTATION	152 168 1.55	1	NAS	7312487	Pretary
	P Sterant C	136141201	Stephan-WokL	Hardware Intell	STEPHANPC	152.162.0.54	3	Sister/C	ANAMER	Tranary /
	PNA	1351418072	Jason.	Linux Dek Balls.		192 198 1 55	2	NAS	7312487	Pretary
	0.2 4				Page	14 44 E 10	H			

Status mappings associated with discovered records

3.7.3 Discovery order and passes

In some cases, you may want to specify the order by which the ITK will process the discovery and reconciliation of the connectors. This can be useful in cases where one connector may have a dependency with another. For example, if one connector discovers sites and another one discovers devices that will be placed under sites, which are discovered by the first connector, then you want to make sure the ITK first processes the sites and then the devices to avoid potential errors related to missing parent objects.

To specify the order of how connectors are to be processed by the ITK, follow these simple steps:

1) Go to the Settings menu -> Discovery Order

2) In the 'Discovery Order' dialog you will see a list of all the device and node connectors that currently exist in the ITK

3) Select the appropriate connectors and move them up and down in the order hierarchy using the green and blue arrows

d	Name	Sequence	Category
0006	Native SNMP_External_IPs	1	Node Connector
10007	Solarwinds to VMware View	2	Node Connector
8000	VMware Host Discovery	3	Node Connector
1001	Native SNMP	4	Device Connector
1004	SolarNewProduction	5	Device Connector
1005	CA Unicenter	6	Device Connector
1006	Castlerock SNMPc	7	Device Connector
1007	Cisco RME	8	Device Connector
1008	Microsoft SCOM	9	Device Connector
1009	What's Up Gold	10	Device Connector
1010	Solarwinds	11	Device Connector
			Gose

Attention!

Notice that link connectors (see chapter 5) are missing from the list. Link connectors are always processed last in the ITK. This ensures that any dependencies with nodes are always accounted for by discovering the nodes (or devices) first. Since links can have no cascading effect on other links or on nodes, specifying their discovery order would have no effect in the overall process.

In addition to the discovery order, you can also specify the number of times in a row a connector should be reconciled when the scheduler is running (also called "passes"). This can be useful when a specific connector has recurrent dependencies, such as for the parent ancestry. For example, if a site connector uses a parent locator field, which may expect other sites to exist and those sites may be imported from that same connector, then you may need to run the connector more than once. Since only nodes can server as parents of other objects, this feature is only applicable to node connectors.

As we would expect, the default number of passes is 1. To change that, go to the node connector list, select a connector, and then change the number of passes by using the '+' and '-' buttons, as depicted below.

Node Cor	metter List < Count: 3							
10006	alse Native SNMP_Exercisi, IPa	doEngne SQL Server	serverfilene 192.168.1.22	dbName ReaEncNadeE	status T	lastDiscovered 6/24/2015 10.4	lastReconciled 7/13/2015 12:0	decoveryOrder pesse 1
₩ 10008	Where Host Decovery	SQL Server	SQLEXPRESS SQLExpress	ScierWinde/liew	1	7/5/2015 4 44 0	7/9/2015 4 44 1	; C
	0 = 00							
-							1	

Changing the number of "passes" for a connector

3.7.4 Starting the scheduling process

After the scheduler has been configured, you can start the automated discovery and reconciliation process by simply clicking on the 'Start Scheduler' button, as shown below:

Eile View Discovery Settings Iools Help			
Connectors 🧠 🖉	📓 Native SNMP - Cou	nt 9	
CA Unicenter	sysName	id	
Castlerock SNMPc	L-CIS-3550-24-6	649	1
Gaco RME	L-CIS-R-2611-2-3	646	1
- Concord eHeath	L-CIS-R-2611XM	647	1
- Mcrosoft MOM	L-CIS-R-2801-2-2	645	1
- Microsoft SCOM	L-CIS-S-2950-26-1	644	1
Native SNMP	L-CIS-S-3550-24-7	651	- 1
⊕- Solarwinds	L-CIS-S-3550-48-5	648	1
What's Up Gold	L-SW-TZ105-4	650	1
E- Nodes	SensorGateway	643	1

Starting the scheduler

This automated process will cycle through any device connector that is set as active and run a discovery from the source and reconciliation process against netTerrain. The ITK will then insert, update and delete devices, depending on how device connector was configured in the reconciliation tab.

Attention!

If one or more connectors are not reconciling when the scheduler is running, make sure these connectors are set as 'Active' (see below).

3.7.5 Activating connectors

Sometimes you need to run a limited set of connectors without the rest being processed. For each connector in the ITK there is a flag that can be set to active (green) or suspended (gray). When using the scheduler, only connectors that are set as active will execute.

To set a device connector as active, click on the device connector list menu (Ctrl-A) and from there select the device connector and click on the 'Activate' button (or right click->Activate). To suspend it, use the 'Suspend' button, as shown below.

	nector List - Co					2.2.1		
d	alas	doEngine	server	database	status	lastDiscovered	lastReconciled	discoveryOrde
P 1001	Native SNMP SolarNewProc	SQL Server SQL Server	192 158 1 42 5	GNCORE Solar/WndsNew		2/10/0018 10 4	7/13/2015 4 44 7/9/2015 1 41 5	
P 1005	CA Unicenter	SQL Server	location	TNG	2	1010/2010 12 4.	1/3/2012 0413.	6
P 1006	Castlerock SN			SNMPc.mdb	1			7
P 1007	Cisco RME	MS Access	Company.	CacoRMEmdb	1			8
P 1008	Monat SCC	a lan our	وسطيب وا	1 62:04	12			19
F 1009	What Solan ands	Activate		prorps		3/9/2015 6.04 1		10
		a woment's						- 485
	11.00							
		3 Edt.						
		O Delete						
		View Records						
		Mapped Field	ts					
		Create New D	evice Connector	-				
		P Status Mappi		-				
				-				
		Refresh View						

Activating a connector

A command to activate and suspend all device, node and link connectors at once is also available (see the commands section at the end of the guide).

3.8 Analyzing the results

After the information has been discovered and reconciled into netTerrain we may need to do some discrepancy analysis or error checking, so it is important to know how to manipulate and analyze the results displayed in the ITK connector tables.

3.8.1 Device states and their corresponding color codes

As we mentioned earlier in the guide, the process of importing devices into netTerrain consists of two parts: the discovery process, where the connector reads the data from the source and dumps it into a raw table in the ITK and the reconciliation process, where the devices are inserted, updated or deleted in netTerrain. As such, a device can be in four possible states:

1) The same device (i.e. a device with the same name) also exists in netTerrain and it was discovered and reconciled into netTerrain by that same connector. Such devices have a lime fill color, as shown below.

2) The same device also exists in netTerrain, but it was created manually or it was discovered and reconciled into netTerrain by a different connector. Such devices have a green fill color, as shown below.

S3A1 1.3.6.1.4.1.9.1.516 Baltimore 192.168.7.12 Primary

3) The device in the connector table is currently not in netTerrain, but the type has been mapped in netTerrain so a reconciliation process (barring any parent issues) would create it in netTerrain. Such devices have a plain white fill color, as shown below.

100				241	
S3A2	1.3.6.1.4.1.9.1.516	Ellicott City	192.168.7.13	Primary	
	1.00.00.1.1.1.1.00.1.00.1.00	Children only	106.100.1.10	i tumany	

4) The device in the connector table is currently not in netTerrain and the type has not been mapped, so a reconciliation process would create a generic device type in netTerrain (or yield an import error if the 'Use generic devices for unmatched types' application setting is unchecked). Such devices have a gray fill color, as shown below. Note that after a reconciliation process, any grey devices that do indeed trigger the creation of a generic device would now exist in netTerrain, hence be displayed in lime.

	S3A7	1.3.6.1.4.1.9.1.797	Ellicott City	192.168.7.188	Primary
--	------	---------------------	---------------	---------------	---------

Below, we show an example of devices imported from a Solarwinds device connector, with different color codes based on the status of the discovered devices in netTerrain.

Caption	SysObjectID	City	IP_Address	priority
\$1A27	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.3	Primary
S1A29	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.4	Primary
52A1	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.5	Primary
\$2A2	1.3.6.1.4.1.9.1.516	Baltmore	192.168.7.6	Primary
S2A3	1.3.6.1.4.1.9.1.516	Towson	192.168.7.7	Primary
\$2A4	1.3.6.1.4.1.9.1.516	Baltimore	192.168.7.8	Primary
\$2A5	1.3.6.1.4.1.9.1.516	Washington, DC	192.168.7.9	Primary
\$2A6	1.3.6.1.4.1.9.1.516	Silver Spring	192.168.7.10	Primary
\$2A7	1.3.6.1.4.1.9.1.516	Silver Spring	192.168.7.11	Primary
\$3A1	1.3.6.1.4.1.9.1.516	Baltimore	192.168.7.12	Primary
\$3A2	1.3.6.1.4.1.9.1.516	Elicott City	192.168.7.13	Primary
S3A3	1.3.6.1.4.1.9.1.516	Elicott City	192,168,7,14	Primary
\$3A4	1.3.6.1.4.1.9.1.516	Columbia	192.168.7.15	Primary
\$3A5	1.3.6.1.4.1.9.1.797	Columbia	192.168.7.16	Primary
\$3A6	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.17	Primary
\$3A7	1.3.6.1.4.1.9.1.797	Elicott City	192.168.7.188	Primary
\$3A8	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.19	Primary
S4A1	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.20	Primary
\$4A2	1.3.6.1.4.1.9.1.516	Baltimore	192.168.7.21	Primary
\$4A3	1.3.6.1.4.1.9.1.516	Glen Burnie	192.168.7.22	Primary
\$4A4	1.3.6.1.4.1.9.1.516	Laurel	192.168.7.23	Primary

Attention!

Device color codes can be driven by changes in the source data, but also changes in netTerrain. For example, if a user changes the name of a device in netTerrain or deletes a device in netTerrain, this can trigger a change in the color code in the ITK. Make sure to refresh the page in the ITK to make sure you are reflecting any recent changes in netTerrain (see below).

3.8.2 Refreshing views

To make sure your ITK view is reflecting the latest data you can refresh a list by right clicking on it and clicking on the 'Refresh' option (or F5).

			THOVE	132.100.1.30	1.1
				192.168.1.6	1
				192.168.1.74	2
				192.168.1.8	1
			7TESTER-PC	192.168.1.18	1
4.1.8741.1	Stephan	SonicWALL TZ		192.168.1.1	1
4.1.9.1.4	Stephan	Cisco IOS		100 100 0.0.6	2
4.1.9.1.1	Stephan	Cisco Inte 2 D	elete Selected	.0.3	2
4.1.9.1.4	Stephan	Cisco IOS Co N	lap Type	.0.4	2
4.1.9.1.6	Stephan	Cisco IOS		.0.2	2
4.1.9.1.6	Stephan	Cisco IOS	runcate Table	1.0.8	2
4.1.9.1.3	Stephan	Cisco Inte	efresh View 🔓	1.0.9	2
4.1.9.1.3	Jan	Cisco Internetwo		102.100.0.1	1
4.1.9.1.4	Fred	Cisco IOS Softw		192.168.0.7	2
4.1.9.1.2	Stephan	Cisco Internetwo		192.168.0.5	2
4.1.674	Stephan-UPS	Dell UPS Tower		192.168.0.10	1
4187411	Stephan	SonicWALL TZ		192 168 0 50	1

Refreshing a view

3.8.3 Filtering devices based on color code

The ITK device connector views have a series of filter buttons that can be used to filter data based on the state of the devices in netTerrain. These filters include the following options:

- Only show devices not in netTerrain and without a mapped type (gray).
- Show all devices that have a mapped type in netTerrain (lime, green and white).
- Only show devices that exist in netTerrain (green and lime).
- Only show devices that do not exist in netTerrain (gray and white).

S1A27 1.3.6.1.4.1.9.1.565 Baltimore 192.168.7.3 Primary S1A29 1.3.6.1.4.1.9.1.565 Baltimore 192.168.7.4 Primary S2A1 1.3.6.1.4.1.9.1.565 Baltimore 192.168.7.4 Primary S3A5 1.3.6.1.4.1.9.1.565 Baltimore 192.168.7.5 Primary S3A5 1.3.6.1.4.1.9.1.797 Columbia 192.168.7.16 Primary S3A6 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.18 Primary S3A7 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.188 Primary S3A8 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.19 Primary S3A8 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.20 Primary S4A1 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.20 Primary	Caption	SysObjectID	City	IP_Address	priority
S2A1 1.3.6.1.4.1.9.1.565 Baltimore 192.168.7.5 Primary S3A5 1.3.6.1.4.1.9.1.797 Columbia 192.168.7.16 Primary S3A6 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.17 Primary S3A6 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.17 Primary S3A7 1.3.6.1.4.1.9.1.797 Elicott Cty 192.168.7.188 Primary S3A8 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.19 Primary	\$1A27	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.3	Primary
S3A5 1.3.6.1.4.1.9.1.797 Columbia 192.168.7.16 Primary S3A6 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.17 Primary S3A7 1.3.6.1.4.1.9.1.797 Bilcott Cty 192.168.7.188 Primary S3A8 1.3.6.1.4.1.9.1.797 Bilcott Cty 192.168.7.188 Primary	\$1A29	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.4	Primary
S3A6 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.17 Primary S3A7 1.3.6.1.4.1.9.1.797 Ellicott City 192.168.7.188 Primary S3A8 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.19 Primary	S2A1	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.5	Primary
S3A7 1.3.6.1.4.1.9.1.797 Elicott City 192.168.7.188 Primary S3A8 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.19 Primary	\$3A5	1.3.6.1.4.1.9.1.797	Columbia	192.168.7.16	Primary
S3A8 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.19 Primary	\$3A6	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.17	Primary
	\$3A7	1.3.6.1.4.1.9.1.797	Ellicott City	192.168.7.188	Primary
S4A1 1.3.6.1.4.1.9.1.797 Baltimore 192.168.7.20 Primary	\$3A8	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.19	Primary
	S4A1	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.20	Primary
0 2 2 0 10 = = 0 ktype_not_mapped> Fage: 14 41 1					Lage: 4 41 1 10

Using device color filters

Notice that when using a filter, the ITK automatically appends a value in brackets in the filter text box. In essence these filter buttons are simply applying a command to the filter text box and executing it.

To clear the filter, simply click on the 'Clear Filter' button next to the filter text box, as shown below.

Caption	SysObjectID	City	IP_Address	priority	
S1A27	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.3	Primary	
S1A29	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.4	Primary	
S2A1	1.3.6.1.4.1.9.1.565	Baltimore	192.168.7.5	Primary	
\$3A5	1.3.6.1.4.1.9.1.797	Columbia	192.168.7.16	Primary	
\$3A6	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.17	Primary	
\$3A7	1.3.6.1.4.1.9.1.797	Ellicott City	192.168.7.188	Primary	1
\$3A8	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.19	Primary	
S4A1	1.3.6.1.4.1.9.1.797	Baltimore	192.168.7.20	Primary	
		0			
2 2 3	22 = = =	type_not	_mapped>	Page:	88 1

Clearing a filter

Тір

An easy way to map types for any devices that are currently unmapped (gray) is to use the first color filter and then map the types directly from the view (see below).

3.8.4 Mapping types from the device view

Any unmapped device types in the ITK can be mapped directly from the device view by right clicking on the device (should be depicted with the gray fill color) and clicking on 'Map Type', as shown below.

					192.168.1.12	1
					192.168.1.36	2
		WI	N-B29	L2LJJ	192.168.1.46	1
					192.168.1.53	2
		PH	DVB		192.168.1.56	1
			0	Delete	Selected .	
			6	Map Ty	ype	
		7T		Trunca	te Table	
n	SonicWALL TZ			Turren	ite fubie	
r	Cisco IOS Softw			Refresh	n View	
n	Cisco Internetwo		-		192.168.0.3	Z
n	Cisco IOS Softw				192.168.0.4	2
n i	Cisco IOS Softw				192.168.0.2	2
n	Cisco IOS Softw				192.168.0.8	2
60 C	C 11 1				0.0.01.001	3

Mapping a type directly from the device view

3.9 Logs and data purging

The ITK generates a log for most processes that affect data, such as discoveries, reconciliation processes and commands, as well as all errors that can occur in the system. A separate log file is created for each day, to prevent the log file from growing too big.

To access the log, click on Tools->Log->Open (or Ctrl-L). This will open the most recent log file available. The log files are usually opened with a default text editor like notepad. To access older log files, you need to open them from the application server directly, usually in 'C:\ProgramData\Graphical Networks\netTerrain\ITK\Logs'.

Log files may also be purged. A command is available for that, but it is easier to just purge them by clicking on Tools->Log->Purge.

<u>File View Discovery Settings</u>	Tools	Help				
Connectors Orices	9	Create New <u>D</u> evice Connector Create New <u>N</u> ode Connector Create New Link Connector		:9		
CA Unicenter		Tools for Geeks	•	d	sysObjectId	sysUpTime
Castlerock SNMPc Gisco RME		_og		649	1.3.6.1.4.1.9.1.485 Open Ctrl+L	17094652 26378288
Concord eHealth	Iruncate Tables				Purge	26355791 26376900
Microsoft SCOM Microsoft SCOM Microsoft SCOM					1.3.6.1.4.1.9.1.359	17104103 17104434
Solarwinds What's Up Gold	-	L-SW-TZ105-4	PO	648	1.3.6.1.4.1.9.1.278	17104040 225251955
Nodes SQL Mon Database		SensorGateway		643	1.3.6.1.4.1.17095	251299213
SQL_Mon_DbServerinstance SQL_Mon_DbServerinstance Sola_notes Sola_notes Switches Links SQL_Mon_Links		6 8 8 0	Z			

Purging the ITK log

Attention!

When you purge the logs, all log files are removed from the log folder, not just the log for the current day.

The log file includes data such as an entry description, IP address, process description, start of process, thread number and timestamp.

And the second se	_			· · · ·	
4					
Entry Description Identifie	Process or Action Sta	rt of satch process)	threade		
Truncated table adabevices, Starting discours process Appended data in table adab Einiside process. I Proc. Truncated table adabevices, I convector insert i 11/ Solarwinds convector Insert	1002 Table fruncate for Solarwinds Startin evices_1002 Table appe ess completed 11/22/2014 1002 Yable fruncate 12/2014 9/15:44 am 0 11/22/2014 9:15:44 am 0	11/22/2014 9:15:52 44 g discovery 15/22/2 011/22/2014 9:15: 9115:14 44 0 11/22/2014 9:15:40 44	014 9135131 AM 0 34 AM 0 1 0		
	rrain: solarwinds bev	fee connector insert	11/22/2014 9:33144 AM 0	EI	
Total records: (inserts ski	pped): 0 Solarwinds co	resector insert 11/2	2/2014 9:15:44 AM 0		
nds Connector update (11/22/ dated) Solarwinds Connec	2014 9:15:44 AM 0 tor update 31/22/2014 9:3	5:44 am (¢)			
nds connector belete (11/22/ C15c0 w5-c1710-4895-c :: 52 C15c0 w5-c1710-4895-c :: 52 C15c0 w5-c1710-4895-c :: 52 C15c0 w5-c1730-4895-c :: 52 C15c0 w5-c1730-485-c :: 52 C15c0 w5-c1730-485-c :: 52 C15c0 w5-c1730-485-c :: 54 C15c0 w5-c1730-485-c :: 54 C15c0 w5-c1730-485-c :: 54	2014 9:13:44 JM 1 0 1 42 5242 501arwinds com 43 5244 501arwinds com 44 5244 501arwinds com 45 5245 501arwinds com 46 5246 501arwinds com 47 524 501arwinds com 42 5442 501arwinds com 43 5442 501arwinds com	ector Delete 11/22/ wettor Delete 11/22/ mettor Delete 11/22/ mettor Delete 11/22/ mettor Delete 11/22/ wettor Delete 11/22/ mettor	2014 0:11:45 Am 0 2014 0:15:45 Am 0		
Finished process. Proc Starting discovery process Appended data in table adab Finished process. Proc	eus completed 11/22/2014 for Solarwinds Startin evices_1002 Table appe eus completed 11/22/2014	9:15:46 AM 0 9 8 soovery 11/22/2 md 11/22/2014 9:15:	014 9:15:48 AM 0	winds connector be	fete 11/22/2014 9-15:45 we 0
C15C0 W5-C3750-4895-6 11 52 C15C0 W5-C3750-4895-6 11 52	42 Solarvinds Connecto Al Solarvinds Connecto Mi Solarvinds Connecto AS Solarvinds Connecto AS Solarvinds Connecto AS Solarvinds Connecto	r Insert 11/22/2014 r Insert 11/22/2014 r Insert 11/22/2014 r Insert 11/22/2014 r Insert 11/22/2014	9:16:00 AM 0 9:16:01 AM 0 9:16:01 AM 0 9:16:01 AM 0 9:16:02 AM 0		
	Intry Description Sourtifier Interception Sourtifier Interception (Source) Sourtifier Interception (Source) Source) Inter- Interpreted data in Table addae- introduction (Source) Interception Interception (Source) Inter- ation (Source) Interception (Source) Inter- ation (Source) Inter- Interception (Source) Inter- Inter- Inter- Interception (Source) Inter- Inter- Inter- Interception (Source) Inter-	<pre>intry Description Identifier Process or Action Sta Init complete Switchboard II/22/2014 9:13:10 ar Init complete Switchboard II/22/2014 9:13:10 ar Initial complete II/22/2014 9:13:10 ar Initial complete II/22/2014 9:13:10 ar Initial complete II/22/2014 9:13:10 ar Initial complete II/22/2014 9:13:14 ar 0 Initial complete II/22/2014 9:13:14 0 Initial complete II/22/2014 0 0 Initial complete II/22/2014 0 Initial complete II/22/2014 0 0 Initial complet</pre>	<pre>intry Description Identifier Process or Action Start of Banch Process] intercemptor [selfsthebard 11/22/2014 9:13:10.04 0] Throncated table addaevices.1000 Table function [11/22/2014 9:13:12.04 Paperedd data in Table addaevices.1000 Table function [11/22/2014 9:13:13:14 Paperedd data in Table addaevices.1000 Table function [11/22/2014 9:13:14 0:15] Throncated table addaevices.1000 Table function [11/22/2014 9:13:14 0:15] Throncated table addaevices.1000 Table function [11/22/2014 9:13:14 0:15] Interaction function [11/22/2014 9:13:14 0:15]] Datawinds Connector Insert 11/22/2014 9:13:14 0:16]] Datawinds Connector Insert 11/22/2014 9:13:14] Datawinds Connector Datawinds Conne</pre>	<pre>http://docs.jpiint/jpiint/states</pre>	<pre>http://docs.com/com/com/com/com/com/com/com/com/com/</pre>

Log file

3.9.1 Truncating (or purging) connector tables

Discovered data can also be purged from the ITK. This process will only truncate the intermediate ITK tables containing the discovered data. It will not delete data from the source or from netTerrain. You may want to purge connector data to start a process from scratch, or to remove data from netTerrain (see tip below).

To truncate connector data, go to Tools->Truncate Tables and select the appropriate connector you want to truncate.

Eile View Discovery Settings	Ico	ls <u>H</u> elp		-				
0 0 0 0 0 0 0 0 0		Create Ne	w Device Connector					
Connectors 🧠 🦉	8		w <u>N</u> ode Connector w Link Connector	9		and the Trans		in the second
CA Unicenter	\$	Tools for (Seeks 1		sysObjectId 1.3.6.1.4.1.9.1.485	sysUpTime 17094652	sysContact	sysDescr Caco IOS Soft
Castlerock SNMPc		Log		4	13614191186	26378288	Stephan	Caco Internety
Concord eHeath	1	Iruncate 1	lables		All Device Connectors	100	Stephan Stephan	Cisco IOS Soft
Microsoft SCOM		Copy Out;	put to Clipboard	T	Device Connector		CA Unicenter	Caco Internets
Native SNMP Solarwinds What's Up Gold	9	XML Drop	LCIS-9/0500484	-	All Node Connectors Node Connector		Castlerock SNMPc Cisco RME	Cisco IOS Soft Cisco Interneto
🕞 🕕 Nodes			L-SW-TZ105-4 SensorGateway		All Link Connectors		Concor	SonicWALL T Temperature &
SQL_Mon_Database SQL_Mon_DbServerInstance SQL_Mon_DbServerInstance SNMP_External_IPs Stes			0 0 0 0	9	Link Connector		Microsoft MOM Microsoft SCOM Native SNMP	4 44 1 10
Bola_nodes Bola_nodes Bola_nodes Bola_switches Bola_switches Bola_sol_Mon_Links Bola_SNMP_Links							Solarwinds What's Up Gold	

Truncating connector data

Another way to truncate a table is as follows:

- Go to the connector list view
- Right click on the view
- Click on 'Truncate table'

PLink-SG32' S phan-PC
S
S
S
S
PLink-SG321
W-TZ105-4
ELL-UPS-10
IS-S-3000-24
IS-S-2950-26 IS-S-3550-24
IS-S-2950-24
IS-R-2801-2-
IS-R-2801-2-
IS-R-2611X.

Truncating a table using the right click context menu

Tip:

A simple way to remove all records from netTerrain that were discovered by a given connector, is to first truncate the table in ITK and then reconcile the data. Be careful with this process, as you will not be able to recover the data in netTerrain unless you restore the database from its previous state or you reconcile the connector with the same discovered data that existed before the truncate process took place.

Also take into account that in order to delete records in netTerrain from the ITK, that connector needs to have the 'Delete devices without matches' option set to 'Yes'.

3.9.1.1 Truncating all device tables

In some cases, you may want to truncate all device tables, whether it is to recreate a process or to remove all devices from netTerrain. To truncate all devices for all connectors, go to Tools->Truncate Tables->All Device Connectors.

4 Creating custom device connectors

In addition to the list of built-in device connectors, netTerrain also allows you to create new device connectors for any third-party data source that uses a SQL Server, Oracle, PostgreSQL, MySQL or MS Access backend database.

If the data is stored in a different database engine or file format, an indirect method using a 'proxy database' is also possible. We discuss this method later in the guide.

Overall, the process for creating a new custom device connector is very similar to a tier-1 connector and the same features for discovery, reconciliation and data analysis apply.

4.1 Prerequisites

To create a new device connector, netTerrain must know certain aspects of the data source, such as connection properties, the table or query to import the data from and the fields that will be mapped to custom fields in netTerrain.

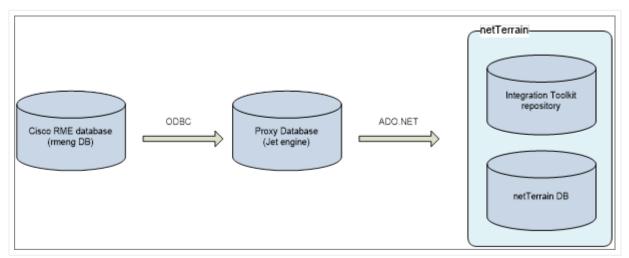
4.1.1 Proxy or source database?

The first step in creating a device connector requires understanding what the database engine for the source data will be.

The ITK can currently read from SQL Server, PostgreSQL, MySQL, Oracle and MS Access (jet) databases. If the source data resides in one of those three engines, then the connection string is easy to create by simply filling out the appropriate connection information in the device connector creator dialog.

In many cases though, the source information may be another database engine or a text file. In those cases, a device connector can still be created by means of a so called 'proxy database'.

Some of the built-in device connectors, such as the Cisco RME device connector, use this mechanism, which is depicted below.



Architecture of the Cisco RME device connector using a proxy database

In the example above, the intermediate database acts as a proxy for the source database, since the ITK does not have the capability to create a connection string directly into the Cisco RME database engine.

Other common examples of proxy settings include text files and comma separated values (csv) files that are exported as individual files by another system, to be imported automatically into the ITK. Countless such text or csv outputs have been used in netTerrain implementations where a non-database format output needs to be automatically synchronized with netTerrain node and link data.

4.1.1.1 Proxy set up use-case: OTDR readings

As an example of a text file input using a proxy, consider the following scenario common in netTerrain OSP applications: an Optical time-domain reflectometer (OTDR) that outputs a result to a text file. These text files are typically placed in a fixed drive location which, via a proxy connection, are linked to one or more ITK

connectors mapped to the corresponding netTerrain entities (for example, a fiber trunk or strand). The ITK then updates a property of choice (such as OTDR reading) on that fiber, which can be used to point the location of a possible fault.

The proxy database can be any of the engines the ITK supports natively, such as Microsoft SQL Server. It is up to the user to create the connection between the proxy and the source, and this method may depend on the computer configuration where the proxy will be set up. To not leave you hanging, we will provide two examples of proxy database settings using Microsoft SQL Server and Microsoft Access.

Below, we discuss specifically how to create a custom connector using a proxy database by means of a SQL Server proxy and an MS Access proxy.

4.1.1.2 Setting up the proxy database using SQL Server

In the following example we will set up a proxy database using SQL Server. We will assume the source is some csv data, as depicted below.

1	A	В	С	D	E	F	G	Н
1	Contact ID	;Site Nam	e;Latitude;	Longitude	;Address;t	oplevel;flag	g	
2	1;Albuque	rque;35.0	5;-106.60;1	24 Coal Str	eet;US Bac	kbone;0		
3	2;Atlanta;	33.65;-84.4	42;3453 Pea	chtree;US	Backbone	;0		
4	3;Augusta	;44.17;-69.	48;987 Mai	n St.;US Ba	ckbone;1			
5	101;Baltin	nore;39.18	;-76.67;100	0 Fell Stree	et;US Backl	bone;1		
6	4;Boise;43	NW;US Ba	ackbone;1					
7	5;Boston;4	42.37;-71.0	3;400 Nick	erson Road	;US Backb	one;1		
8	6;Buffalo;	42.56;-78.4	14;498 Niag	ra;US Back	bone;1			
9	7;Burlingt	on;44.28;-1	73.90;6409	Main St.;U	S Backbon	e;1		
10	8;Butte;45	.56;-112.3	0;54 Mount	tain View;	US Backbor	ne;1		
11	9;Charlest	on AFB;32	.54;-80.19;/	APO 30908	973;US Bac	kbone;1		
12	10;Cheyer	nne; <mark>41.90</mark> ;-	104.48;633	Jennifer F	Road.;US Ba	ackbone;1		
13	11;Chicago	o;41.90;-87	.66;54 Loo	Drive;Ala	ska;1			
14	12;Dallas;	32.51;-96.5	1;643 Long	horn;US Ba	ackbone;1			
15	13:Davton	:39.54:-84.	12:6209 10	th Ave.:US	Backbone	:1		

csv sample data to be imported via a proxy SQL Server database

There are a number of ways of setting up a proxy in SQL Server that will update the source data as tables or queries in SQL Server, including Linked Servers and DTS/SSIS packages. For our example we will use a more direct method, namely a stored procedure using a bulk insert. To ensure the data is up to date every time the ITK refreshes from the source, we will also automate the process of executing the stored procedure before the ITK discovers the data.

To set this up proceed as follows:

Step 1: Create (or using an existing) database that will serve as your proxy.

Ideally, we recommend this being an empty database that sits on the same engine as netTerrain. This database will just contain the stored procedures and the tables with the raw data imported from the source. Since netTerrain itself runs on SQL Server, sometimes that server (not the netTerrain database itself though!) is the most convenient place to set up a proxy, since the existence of that engine is guaranteed. Provided, of course, the DBA is nice enough to let you set up a proxy there, but that's a different story.

Step 2: Prepare the tables in your proxy database.

This usually just means creating the tables that will hold the raw data. Make sure the structure of the database is compatible with the source columns. This means using matching names and appropriate types. Continuing with our csv example shown above we could create a sites table using the following script:

```
USE [CsvProxy]
GO
/****** Object: Table [dbo].[sites] Script Date: 06/07/2016
16:28:35 ******/
SET ANSI_NULLS ON
GO
GO
CREATE TABLE [dbo].[sites](
       [Contact ID] [nvarchar](255) NULL,
       [Latitude] [nvarchar](255) NULL,
       [Latitude] [nvarchar](255) NULL,
       [Longitude] [nvarchar](255) NULL,
       [Ioplevel] [nvarchar](255) NULL,
       [flag] [int] NULL
) ON [PRIMARY]
GO
```

Proxy raw table script

As you can see, the structure of the table coincides with the columns defined in the csv file.

Step 3: Create the stored procedure.

The stored procedure will use a 'bulk insert' method to fill the raw tables we created in step 2.

For the stored procedure to work correctly, it must be able to fetch the csv data from the same place, every time it is executed. So, it is important to determine a specific location where the source files will be dumped, and not change the location after subsequent discoveries. We assume, of course, that the location of the csv is accessible for the stored procedure (both in terms of network connectivity and access permissions).

Also, the script will truncate the raw tables and fill them during every process. This is not mandatory (one could use a different method), but it is simple enough and usually not very taxing in terms of performance.

Finally, depending on the delimiters used in the csv file, the method used to successfully execute the stored procedure may vary. In our example we assume a line feed ('char(10)').

Here is a sample script that can be used for the stored procedure:

```
USE [CsvProxy]
GO
/****** Object: StoredProcedure [dbo].[FillCsvTables] Script Date:
06/07/2016 16:33:08 *****/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE PROCEDURE [dbo].[FillCsvTables]
AS
BEGIN
SET NOCOUNT ON;
DECLARE @Path NVARCHAR(255);
SET @Path = 'C:\Temp\CsvSamples\'
DECLARE @Rowterminator NVARCHAR(10);
SET @Rowterminator= CHAR(10);
```

```
-- sites table
TRUNCATE TABLE sites
EXEC('
BULK INSERT sites
FROM ''' + @Path + 'sites.csv''
WITH
(
FIRSTROW = 2,
FIELDTERMINATOR = '';'',
ROWTERMINATOR = ''' + @Rowterminator + '''
)')
END
GO
```

Step 4: Creating a dummy connector to set up the automation in the ITK

As opposed to Linked Servers (or linked tables in Access), where there is a dynamic link between the source and destination, a bulk import process pushes the data to the raw tables, which are not linked or connected to the source. This means that if the data changes in the source, the raw data in the proxy tables may be out of date. To prevent that, we make sure that right before the ITK runs a discovery, it first executes the stored procedure. This can be accomplished from the ITK itself.

We recommend making sure the ITK runs the stored procedure before anything else, so one way to ensure this is to create what we call a 'dummy' connector that does nothing except run that procedure and placing that connector first in the discovery order.

Create a dummy node connector by linking it to the table in the proxy database (see chapter 5 on how to create node connectors). You can use any netTerrain type, since it doesn't matter. the connector will not reconcile any data (in fact we can add a WHERE clause statement that ensures it doesn't even waste CPU cycles discovering anything).

Connection Mapping	Reconciliation
Connector name:	Dummy
Database engine:	SQL Server 🗸 🗸
Server:	
Windows authentica	tion: Yes 🔹
User:	
Password:	
Database:	CsvProxy 👻 📃
	Test Connection
	Cancel

Here is an example of the three connector tabs that show how to set it up:

Connection	Mapping	Reconcilliation		
Source tal	ble:	sites	-	
net Terrain type:		_SNMP_External_IPs 🔹		
Default dia	agram:	<null></null>	•	
Parent loc	ator field:	<null></null>		
Name/Id f	field:	Site Name	•	
X coordinate: Y coordinate: WHERE clause		<null></null>	•	
		<null></null>	•	
		WHERE 1=0		

n
No
No
No
execremote\EXEC FillCsv Tables

Notice two things: the 2nd tab includes a contradictory WHERE clause 1=0, which ensures no data is discovered (we don't need it) and the 3rd tab includes a 'pre import function', which is the process that executes the stored procedure remotely. The syntax for that is as follows (make sure the name after the EXEC statement matches the name of the stored procedure):

execremote\EXEC FillCsvTables

Also notice that the update, insert and delete options in the third tab are set to no. Again, we don't want any data going back and forth. The sole purpose of this connector is to execute the stored procedure.

Step 5: set the dummy connector discovery order

Finally, let's make sure this dummy connector is the first thing to run upon an ITK scheduled task, by setting the discovery order first (please see discovery order in chapter 3).

4.1.1.3 Setting up a proxy database using MS Access

In this example we will set up a proxy database like the one used for the CiscoWorks RME device connector, using an Access database as the proxy, which in turn is connected to another third – party database engine (the target database).

The first step in setting up the proxy database is to make sure that the machine where the proxy resides has the driver to the target database engine. Once that is verified, you proceed with the creation of a Machine DSN. A DSN is usually created from Control Panel->Administrative Tools->Data Sources ODBC.

Then, follow these steps to set up the proxy database:

1) Create an empty Access Database file that can be placed under

<ProgramData>\netTerrain\temp.

2) Go to the tables tab and from the external data tab create an ODBC connection by linking a table to the source (this process may differ between different versions of MS Access).

Read to a contract the second se	Definition Tests Sector Fails Sector Fails
Tables Seach.	Select the source and destination of the data
	Sportly have and where you want to other the data in the current database.
2	Const.

3) In the 'Data Source' dialog box, click on the 'Machine Data Source' tab and select the DSN database created before.

Data Source Name	Type	Description	
timEpm	System		
llmFh	System		
fminv xcel Files	System Uter		- 1
DM	System		
IS Access Database	User		
tieng	System		- 1
pm	System		
el.			
			New
'User'' data sources are s	pecific to a us	s machine, and cannot be a er on this machine. "System machine, or by a system-wi	n'' data

4) If needed, enter the credentials for this database.

5) From the Link tables dialog select the appropriate table or view that contains the devices that need to be imported into netTerrain.

Tables		
Tables		
dbo.sa_diagnostic_statement		OK
dbo.sa_diagnostic_statistics		
dbo.sa_diagnostic_tracing_level		Cancel
dbo.spt_collation_map dbo.spt_idatatype_info		
dbo.spt_idbc_conversion		Select All
dbo.spt_itext		
dbo.spt_mda		Deselect All
dbo.syscolumns		P.F. Control of
dbo.syscomments		
dbo.sysindexes		
dbo.syslogins		Saye password
dbo.sysobjects		
dbo.systypes		
dbo.sysusers Imsdatagrp.CHANGE_AUDIT_HISTORY		
Instatagrp.DEVICE_CONFIG_ARCHIVE_STATUS		
Imsdatagrp.DEVICE_CREDENTIAL_STATUS		
Imsdatagrp.DEVICE_ENERGYWISE		
Imsdatagrp.DEVICE_INVENTORY		
Imsdatagrp.DEVICE_INVENTORY_COLLECTION_STATUS		
Imsdatagrp.ENERGYWISE_DOMAIN		
Imsdatagrp.MEMORY_INVENTORY		
Imsdatagrp.MODULE_INVENTORY	_	
Insdatagrp.NETWORK_DEVICES	1.0	
Imsdatagrp.PORT_ENERGYWISE Imsdatagrp.PORT_INVENTORY	-	
Instatagrp.PORT_INVENTORY	1	

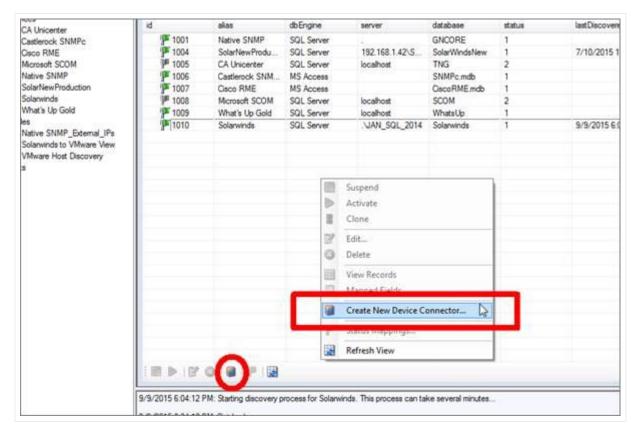
6) You may have to select a unique identifier for the view. It is not a mandatory step, since the query will not be updated.

7) Close the database.

4.2 Step 1: Creating the device connector

When creating the device connector, a 2-step wizard will guide you through the process. It is recommended to have certain mandatory and optional information beforehand, which will later have to be filled out when proceeding with the device connector creation.

To start the wizard, go to Tools-> Create new device connector. You can also start the wizard from the device connector list by using the 'Create new connector' button or right click context menu.



Creating a new connector

A 'Create new device connector' dialog window will appear, prompting you to fill out information to complete the first step in the device connector creation process. All the fields with a red label are mandatory.

	Device Con	nector List - Count:	9					
	id	alas	dbEngine	server	database	status	lastDiscovered	lastReci
	J# 1001	Native SNMP	SQL Server		GNCORE	2		11/5/20
	1003	Cisco RME	MS Access		GscoRME.m	do 1		
	P 1005	CA Unicenter	SQL Server	localhost	TNG	1		
	P 1007	Solarwinds	SQL Server	.Van	Solarwinda	1	11/24/2014 2:0	11/24/2
	P 1008	Concord eHealth		localhost		1		
	P 1009	Microsoft MOM	MS Access		Mom mdb	1		
	1010	Microsoft SCOM	and the second sec	localhost	SCOM	1		
	P 1011 P 1012	What's Up Gold Castlerock SNM		Step 1 of 2: Creat	e Device Connec	tor	1	
zance Ps				Connection Ma	pping Reconcilia	tion		
				Device Conne	001048500	I		
				Database eng	ne:			
				Server			•	
				Windows auth	entication:	*		
				User:	9			
	1.00 (5.10)	0.00.00.00		Password				-
	: III. IP. 107	0191919		Database			• (1)	
						Tes	t Connection	
				1		Cancel	Net	

Create new device connector wizard

4.2.1 Connection information

The database related information that the ITK needs will either be in an Oracle, PostgreSQL, MySQL, SQL Server or MS Access format. The source data either resides in one of those three engines or in a different database format that communicates through an Oracle, PostgreSQL, MySQL, SQL Server or an MS Access proxy.

Connection Mapping Rec	oncilliation		
Device Connector Name:	Solarwinds		
Database engine:	SQL Server 👻		
Server:	.Van 👻		
Windows authentication:	Yes 🔻		
User:			
Password:			
Database:	Solarwinds -		
	Test Connection		

Setting up the initial connection parameters

When using MS Access as the engine, the server is not required, as the path to the corresponding MS Access file will be used. In the case of using SQL Server, the server and database name must be specified.

Database credentials are only required for SQL Server, PostgreSQL, MySQL and Oracle based device connectors. It is important to note (and a relief for any DBA) that the ITK only makes 'SELECT' type statements against the target database. This means that (whenever applicable), a user with read-only access to the source will suffice. Any permission levels higher than read-only will have no additional effect on the process because the ITK never writes any data back to the source.

Both Trusted connections and SQL Server authentication are supported for SQL Server based device connectors.

Attention!

For Oracle connections you may need to have the Oracle ODBC client installed, so that a TNS name can be referenced. For PostgreSQL-based connectors you must first create a DSN from the machine hosting the ITK to the PostgreSQL database, so that the DSN can be referenced in the connector.

4.2.2 Mappings tab

The mappings tab for custom connectors is essentially the same as for any tier-1 device connectors (we'll spill the secret here and tell you that built-in connectors are in fact created using this exact same wizard). We'll repeat the instructions specified in the previous chapter on how to fill out the mapping tab

Attention!

It is important to understand the structure of the data source you want to import data from. For example, you need to know what table or view contains the devices to be imported as well as which fields contain the unique naming convention and device type information.

Also, if you change any fields in the mapping tab currently associated with an additional mapped field (see additional mapped fields section), then the mapped field will be removed from the mapped field list.

4.2.2.1 Source table

The source table represents the table or view where the records that need to be pulled from the data source are stored.

Tip:

If you need to modify some of the data being imported into netTerrain or need to correlate more information that is available in other tables, create a view that "massages" that data for you and point the source table field to that view.

4.2.2.2 Device type field

The device type field is the data field in the source table that holds the identifier for the type of device that will be mapped with the corresponding type in netTerrain. netTerrain uses a name field in the node catalog

table to identify a device type. In other words, netTerrain will try to map the type name from the source with the node type library name in netTerrain.

Tip:

The most accurate descriptor of a device type is the system object id (usually called sysObjectId or sysOID). This is the SNMP discovered unique make and model identifier for a device and can be nicely mapped to netTerrain's existing table of OID to device type information (more on that later)!

4.2.2.3 Default diagram

When importing devices from a third-party data source, netTerrain can assign a default diagram for the device. This is especially important when the source table has no fields that can provide information about the parent diagram containing each device. This default diagram in netTerrain will serve as the initial repository for newly imported devices. You can assign different diagrams for different device connectors instead of searching for devices from multiple device connectors in one generic diagram. To specify a default diagram, at least one diagram needs to exist in netTerrain beforehand.

4.2.2.4 Parent locator field

An alternative to using a default diagram is to automatically place devices under a specific parent object. This is possible if the source table contains a field that stores that parent ancestry data. This can be specified in the parent locator field.

Attention!

In order for the automatic placement to work, the parent diagrams must exist in netTerrain prior to importing the devices. We recommend creating a separate connector that pulls the parent objects in advance, which will then guarantee that the devices will be placed under the corresponding parent objects. This is yet another way to further automate your network documentation process.

4.2.2.5 Name field

The name field should contain the name or unique identifier for each device, and it will be mapped to the name field in netTerrain. Technically, it is not necessary for this field to pull values that are unique, but it is highly recommended. If the name field is mapped to a field in the source table that does contain repeated

values, then any devices with the same name field value will throw an error during the update process. Also, if devices do not have unique names in netTerrain, then if later on you decide to also import links using the ITK, any links that have any repeated devices as endpoints will not be imported.

4.2.2.6 Rack position field

Rack coordinates can be used to automatically place devices on a given rack and rack unit. In other words, this field can be used to import rack positioning information from the source data and avoid placing a device on a rack manually. Naturally, this requires the source data to contain the proper rack unit information for the imported devices. This field assumes that the parent for each device is a rack and is specified in the parent locator field. To summarize, the rack positioning in the ITK must comply with the following:

- The parent object type must be a rack and must exist.
- The source table must contain a field for the rack unit.
- The rack unit for each record in the source data must be consistent with the size and rack unit availability for the corresponding parent rack.

If no coordinate information is available, use the value from the drop-down box.

4.2.2.7 WHERE clause

The last field of the second tab contains a WHERE clause. This can be used as a mechanism to filter certain records from the source table. The syntax of the WHERE clause must correspond to the flavor of SQL that the source database uses and must start with the 'WHERE' keyword (see the screenshot for an example).

Attention!

If the syntax in a WHERE field is incorrect, the discovery process will fail. When writing the clause, you must start the filter with the 'WHERE' keyword itself (for example 'WHERE location=1'). Also, mind that SQL syntax as it may differ from different database engines. SQL Server uses T-SQL, Oracle uses PL/SQL and PostgreSQL, MySQL and MS Access have slightly different flavors of SQL as well, so there may be minor differences in the syntax. If you want to avoid all this hassle don't use the WHERE clause and instead connect to a custom view where the information is already pre-filtered.

Connection	Mapping	Reconcilliation	
Source table:		Nodes	•
Device Ty	vpe field:	SysObject1D	•
Default diagram:		<null></null>	•
Parent loc	ator field:	<null></null>	•
Name/Id field:		Caption	•
Rack Pos	ition	<null></null>	-
WHERE o	lause		

Mappings tab settings

4.2.3 Reconciliation settings

The last tab deals with the mechanism for device reconciliation into netTerrain.

4.2.3.1 Updates

If you want to update any field changes for devices that already exist in netTerrain, then set the 'update existing devices' combo box to 'Yes'.

4.2.3.2 Inserts

New devices that do not exist in netTerrain and were discovered by the device connector will be inserted into netTerrain, if the following criteria apply:

- The 'Use generic devices for unmatched types' application setting is checked or the device type can be mapped to a type in netTerrain (see type mapping)
- A default diagram has been assigned for the device connector (defined in the mappings tab) or a parent container field exists, and the proper parent object also exists in netTerrain
- The 'Insert new devices' combo box is set to 'Yes'

4.2.3.3 Deletes

Devices that exist in netTerrain but no longer exist in the source can be processed in two different ways:

- They can be deleted from netTerrain by setting the 'Delete devices without matches' combo box to 'Yes'
- The can be kept in netTerrain by setting the combo box to 'No'

Attention!

When the 'Delete devices without matches' combo box is set to 'Yes' only devices that were originally inserted by that same connector will be deleted from netTerrain. For instance, a router called '123' that no longer exists in the data source but still exists in netTerrain, will only be deleted if it was originally inserted by that same connector. Internally, any devices that are inserted in netTerrain by the ITK are tagged with the connector id. Then, when a delete process occurs, only devices with that connector id will be deleted (provided they no longer exist in the source).

Connection Mapping Reconcilliation	n
Update Existing Devices:	Yes 🔻
Insert New Devices:	Yes 🔹
Delete Devices without Matches:	Yes 🔹
Pre import function:	
Post import function:	

Reconciliation tab

4.2.3.4 Pre and post import functions

These fields are used to place advanced functions that are processed before and after an import occurs. An example of a pre-import function could be a call to execute a stored procedure in the source data, which massages the records to be imported. An example of a post import function could be a layout algorithm that is triggered after the import to automate node positioning.

Attention!

The Pre and Post import function fields are currently reserved for Graphical Networks consultants. If you think you need a function to perform a specific action, please enter a ticket in the support portal.

4.3 Step 2: Mapping additional fields

A list of additional fields that need to be imported from the table can be specified and mapped to the corresponding fields in netTerrain, just as we saw in the previous chapter for built-in device connectors. This is done in step 2 of the wizard.

Enter each field by specifying the name of the field in the source table or view and the field that it should be mapped to in netTerrain. For convenience, a button that maps all matching fields is included. This comes in handy when the source and netTerrain fields have the same name.

Attention!

The Create field options are not available for device connectors mainly because device connectors are not mapped to a type, so those fields would have to be created against all device types and the catalog. We prefer you to do this instead of assuming all fields need to exist for all device types.

ap New Field				
Field in source database:	IPAddress .			
	Create + Map All	Create + Map		
Field in netTerrain:	IP Address			
	Map Matched Fields	Map Selected Fields		

Field mapping dialog

Click on the 'Finish' button to register the connector.

Attention!

If the registration is successful, this does not necessarily mean that data will be imported successfully into netTerrain. Run a test a discovery process first to see if the records are being imported from the source as expected. If the connector creation process fails, please contact **support@graphicalnetworks.com** or enter a ticket in the support portal.

4.4 Tying it all together with an example

We'll review what we have learned so far this chapter by creating a device connector from scratch to a wellknown monitoring tool called Solarwinds NPM. Our assumptions are the following:

- The source resides on a SQL Server database (to keep it simple we have it on our local machine).
- We know that we can connect to the database via the Windows user.
- Also, we know that the device information sits in a table called 'Nodes'.
- The devices table has a field called 'caption' that uniquely identify devices in this database.
- The table also has a sysObjectId field that identifies the device types.
- Additional fields of interest include: IP_address, DNS and Last_Boot.

When building this device connector, we would like to mirror the information in netTerrain exactly how it resides in the source database. That is, all new devices discovered from the source should be inserted in netTerrain, and any other changes, such as updated fields, should be in synch with netTerrain. We would also like to remove devices in netTerrain that no longer have a match in the source database.

This is how we would set up the device connector in Step 1:

Connection Mapping Rec	oncilliation
Device Connector Name:	Solarwinds
Database engine:	SQL Server 🗸
Server:	.Van 👻
Windows authentication:	Yes
User:	
Password:	
Database:	Solarwinds
	Test Connection
	Cancel

Step 1, first tab

Step 1 of 2: Create Device	Connector
Connection Mapping F	Reconcilliation
Source table:	Nodes 👻
Device Type field:	SysObjectID 🗸
Default diagram:	<null></null>
Parent locator field:	<null></null>
Name/Id field:	Caption
X coord field:	<null></null>
Y coord field:	<null></null>
WHERE clause	
	Cancel

Step 1, second tab

Connection Mapping Reconcilliation	
Update Existing Devices:	Yes 🔻
Insert New Devices:	Yes 💌
Delete Devices without Matches:	Yes 🔹
Pre import function:	
Post import function:	

Step 1, third tab

Note that we chose a diagram called 'Baltimore', which is an existing diagram in the netTerrain project, to place all newly discovered devices, because the source database does not have a reliable data field that can tell us the parent location for each device.

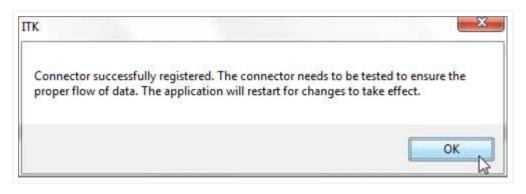
lap New Field	_				
Field in source database:		ssetTag			•
		Crea	ite + Map All	Create + Map	
Field in net Te	main: A	SSET_TA	G		•
		Map M	Natched Fields	Map Selected Ne	lds
ields Currently I	Mapped			Мар	sele
ntColumn	Source Field		netTerrain Field		
Dns IP Address sysUpTime	_		Dns IP Address sysUpTime		
Remove]				

In Step 2, we can add the following fields to our list of mapped fields.

Notice how the field in the source may not match exactly the name of the mapped field in netTerrain. Also notice that fields that were used in step 1 are not available in step 2.

4.5 Next steps

Once the 'Finish' button is clicked, the device connector should be registered in the ITK database and force an application restart:



At this point the user can verify the device connector entry by looking at the device connector list.

Device Conr	nector List - Count	g					
d	alas	dbEngine	server	database	status	lastDiscovered	lastReconciled
JF 1001	Native SNMP	SQL Server		GNCORE	2		11/5/2014 6:18
P 1003	Cisco RME	MS Access		OscoRME mdb	1		
1005	CA Unicenter	SQL Server	localhost	TNG	1		
P 1007	Solarwinda	SQL Server	.Van	Solarwinda	1	11/24/2014 2:0	11/24/2014 2.0
1008	Concord eHeath	Oracle	localhost		1		
P 1009	Mcrosoft MOM	MS Access		Mom.mdb	1		
P 1010	Moreart SCOM	SQL Server	localhost	SCOM	1		
P 1011	What's Up Gold	SQL Server	localhost	WhatsUp	1		
P 1012	Castlenck SNM	MS Access	and in contrast of	SNMFc mdb	17		

New device connector in list

As mentioned earlier, just because the device connector has been successfully registered does not mean that it will work correctly. Some factors that could affect the proper functioning of a device connector include:

- Incorrect type mapping field.
- NULL values in names or parent mapping fields.
- Syntax errors in a WHERE clause.

It is highly recommended that you test the device connector by first running a discovery and then a preview of the reconciliation process.

As a final note, once a device connector has been created, its management does not differ from built-in device connectors. All features that apply to built-in device connectors also apply to custom device connectors. You will also be required to create appropriate type mappings, in order to match types correctly in netTerrain.

4.6 Deleting and suspending a device connector

A device connector can easily be deleted completely from netTerrain by opening the device connector list (Ctrl-A), clicking on the device connector and then clicking on the delete button (or right-click->delete).

tion	1004 1005 1006	CA Unicenter Castlerock SNM Cisco RME	SQL Server SQL Server MS Access MS Access	localhost	TNG SNMPc.mdb CiscoRME.mdb	2	1/10/2010 12.4	773/2010 1.41
	1008 1009	Microsoft SCOM What's Up Gold	SQL Server	localhost localhost	SCOM Whatello	2		
ktemal_IPs fware View pcovery	1010	Solarwinds	SQL Server		Suspend Activate Clone Edit Delete View Records Mapped Fields Create New Device Cor Status Mappings Refresh View	nector	3/3/2015 6:04 1	
		🗿 🗿 🏴 🛃	rocess for Solarwi	nds. This proces	s can take several minutes			

Deleting a device connector

Just like with built-in connectors, this action cannot be undone. It will remove all traces of the device connector in the ITK, as well as any type mappings associated with it, but it won't remove any devices from netTerrain itself.

Tip:

Instead of deleting built-in connectors, it is recommended to simply change their status to suspended. That way, when an automatic scheduler is set up, any suspended device connectors will not trigger synchronization operations. Later, the connector may be reused.

4.7 Cloning a connector

A quick way to create a connector is to take an existing one and clone it. This is especially useful when the new connector has similar characteristics to the cloned one.

id	alas	doEngine	server	database	status	lastDiscovered	lastReconciled
1001 1004 1005 1005 1007 1007 1008 1008 1009	Native SNMP SolarNewProdu CA Unicenter Castlerock SNM Disco RME Microsoft SCOM What's Up Gold	SQL Server MS Access MS Access	localhost	GNCORE SolarWindsNew TNG SNMPc.mdb OiscoRME.mdb SCOM WhatsUb	1 2 1 1 2	7/10/2015 12:4	7/13/2015 4:44 7/9/2015 1:41:
		1	Mappe Create		tor	3	

To clone a connector simply right click on the base connector and click on the 'Clone connector' option.

Cloning a connector

After cloning the connector, the new connector will have the same name as the cloned one. Proceed to change the name and any other parameters by editing the connector as usual.

5 Node connectors

Node connectors are hooks into external databases or files to import records and map them with netTerrain generic node objects. Connectors are a very useful resource to automate the process of creating documentation in netTerrain by taking advantage of existing data from your environment.

You can create any number of node connectors and each connector will be tied to a predefined node type in the netTerrain catalog. To create a node connector, you can utilize a wizard to connect to the data source and map table columns to custom fields in netTerrain.

All node connectors in the ITK are user created and they can be found in the node connector list. From the connector list you can manage settings and schedule automated discovery processes.

Most of the functions and features for node connectors are very similar to the ones used for device connectors.

5.1 Viewing node connectors

To see which node connectors are currently included in the ITK, simply go to View-> Node connector list (Ctrl-O) and a list view of all the node connectors will be displayed.

File	View	Discovery Settings 1	Tools	Help			
0. 🛢		Device Connectors List Ctri	+A				
Connec	2	Node Connectors List 📐 Ctrl	+0				
	2	Link Connectors List Ct	rl+I	vice Adap	oter List - Count: 18		
- D	-				alias	dbEngine	versi
÷-9		Find Devices	•	1001	Native SNMP	SQL Server	5.4
		Find Nodes		1002	Orion NPM	SQL Server	
	8	Find Links		1003	What's Up Gold	SQL Server	12.4
L	-			1004	SNMPc	MS Access	7.1
				1005	Cisco Config Files	SQL Server	myG
				1006	CA Unicenter Trg	SQL Server	
				1007	Concord eHealth	MS Access	Rep
				1008	Microsoft MOM	MS Access	
				1009	V/MM/aca	MS Booos	

Node connector list view

5.2 Prerequisites for creating node connectors

To create a new node connector, netTerrain must know certain aspects of the data source, such as connection properties, the table or query to import the data from and the fields that will be mapped to custom fields in netTerrain.

5.2.1 Proxy or source database?

Just as with device connectors, the first step in creating a node connector requires knowing which database engine you will need to connect to.

The ITK can natively read data from SQL Server, Oracle, PostgreSQL, MySQL and MS Access (jet) databases. If the source data resides in one of those three engines, then the connection string is easy to create by simply filling out the appropriate login information in the node connector creator dialog.

In many cases though, the source information may be another database engine or a text file. In those situations, a node connector can still be created using a 'proxy database' (as explained earlier in this guide).

5.3 Step 1: creating the node connector

Similar to the device connector creation process, a 2-step wizard will guide you through the process of creating a node connector.

To start the node connector wizard, go to Tools-> Create New Node Connector. A similar button and a right click context menu are also available from the node connector list view.

	ector List - Count: 6			Second description	and a state of the	1 and a st
b	alas	dbEngine		serverName	dbName	statu
10002	Networks	MS Acce			C:\Temp\Netwo	
P 10003	Sweches	MS Acce		Sec	C:\Temp\Netwo	
P 10005	Sola_nodes	SQL Ser	1.	.Van	Solarwinds	2
P 10006	_SQL_Mon_DbServerinstance				GN	2
10007	_SQL_Mon_Database	SQL Ser			GN	2
P 10008	Native SNMP_Edemal_IPs	SQL Ser	ver		GN	1
			View Map	te Becords ped Eields		
		9	⊊rea	te New Node Cor	nnector	
		-	Refr	esh View	F5	24

Creating a new node connector

5.3.1 Connection information tab

This tab stores the name and connectivity information, so that the ITK can properly read the data from the source.

5.3.1.1 Database engine

As mentioned before, Oracle, PostgreSQL, MySQL, SQL Server or MS Access databases are natively supported for direct connections between the ITK and the data source. Otherwise, you can use a proxy database (as explained in the previous chapter). For example, if you want to bring in records from a MySQL database, you can create linked tables in MS Access (or a linked server in SQL Server), which then (via queries) connect to the ITK.

Connection Mapping Re	concilliation
Connector name:	Sites
Database engine:	-
Server:	MS Access SQL Server
Windows authentication:	Oracle PostgreSQL
User:	
Password:	
Database:	-
	Test Connection
	Cancel Next

Connectivity tab showing the database engine drop down box

When using MS Access, the server is not required, as the path to the corresponding MS Access file will be used. In the case of SQL Server, the server and database name must be specified in the appropriate fields. With Oracle, a TNS name will typically need to be set up on the ITK machine.

Connection Mapping Rec	concenduori	
Connector name:	Stes	
Database engine:	MS Access 🔹	- * *
Server:	- · · · · · · · · · · · · · · · · · · ·	
Windows authentication.	Yes +	
User:		
Password:		
Database:	C:\Proyectos\GraphicalNetwor +	Connector Connection t
	Test Connection	
	14°	Connection Successful!
	Cancel Next	
		ОК

Setting up the connection tab for a node connector

5.3.1.2 Database credentials

Database credentials are only required for SQL Server, PostgreSQL, MySQL and Oracle-based node connectors. In both cases a user with read-only access to the source will suffice. Both Trusted connections and SQL Server authentication are supported for SQL Server-based node connectors.

5.3.1.3 Source Database

If the database engine is SQL Server, then the database field does provide a drop-down box of all the databases available for that server. For MS Access-based connectors use the ellipsis '..' button to browse for the Access file (.accdb and .mdb extensions are supported). For Oracle-based connectors you must type in the TNS reference. For PostgreSQL-based connectors the Server field turns into a 'DSN' field. You must then make sure there is a DSN to the PostgreSQL database (from the machine hosting the ITK) and then reference that DSN in the DSN field.

5.3.2 Mapping tab

The mappings tab for custom connectors is essentially the same as for device connectors. The main difference is that device connectors need a device type mapping, whereas node connectors are explicitly mapped to one type. We'll repeat the instructions specified in the previous chapters on how to fill out the mapping tab

5.3.2.1 Source table

The source table represents the table or view where the records that need to be pulled from the data source are stored.

Tip:

If you need to modify some of the data being imported into netTerrain or need to correlate more information that is available in other tables, create a view that "massages" that data for you and point the source table field to that view.

5.3.2.2 netTerrain Type

The type field for nodes is used to specify which node type from the netTerrain catalog is mapped to our source table. What this means is that once the ITK starts importing records through this node connector,

every record will be an instance of the netTerrain type. Do not confuse this type field with the type field for device connectors (see chapters 3 and 4).

5.3.2.3 Default diagram

When importing nodes from a third-party data source, netTerrain can assign a default diagram for the node. This is especially important when the source table has no fields that can provide information about the parent diagram containing each node. This default diagram in netTerrain will serve as the initial repository for newly imported nodes. You can assign different diagrams for different node connectors instead of searching for nodes from multiple node connectors in one generic diagram. To specify a default diagram, at least one diagram needs to exist in netTerrain beforehand.

5.3.2.4 Parent locator field

An alternative to using a default diagram is to automatically place nodes under a specific parent object. This is possible if the source table contains a field that stores that parent ancestry data. This can be specified in the parent locator field.

Naturally, for the automatic placement to work, the parent diagrams must exist in netTerrain prior to importing nodes. It is possible to create a separate connector that pulls the parent objects in advance, which will then guarantee that the nodes will be placed under the corresponding parent objects.

5.3.2.5 Name field

The name field should contain the name or unique identifier for each node and it will be mapped to the name field in netTerrain. Technically, it is not necessary for this field to pull values that are unique, but it is highly recommended. If the name field is mapped to a field in the source table that does contain repeated values, then any nodes with the same name field value will throw an error during the update process. Also, if nodes names are not unique in netTerrain, then if you decide to also import links using the ITK, any links that have repeated endpoints will not be imported.

5.3.2.6 X and Y coordinate fields

Coordinates can be used to automatically place nodes on a given diagram. These fields can be used to import positioning information from the source data. Positioning information can refer to latitude and longitude information or any custom coordinate system, such as a grid. This requires the netTerrain parent

object to have a background with embedded coordinates. To configure coordinates in the ITK you must follow these steps:

- The parent object type must include a background image with embedded coordinates (see netTerrain User Guide).
- The source table must contain two coordinate fields (such as x and y or latitude and longitude).
- The coordinates for each record in the source data must fall within the boundaries defined for the background coordinate in netTerrain.

If no coordinate information is available, use the value from the drop-down box.

5.3.2.7 WHERE clause

The last field of the second tab contains a WHERE clause. This can be used as a mechanism to filter certain records from the source table. The syntax of the WHERE clause must correspond to the flavor of SQL that the source database uses and must start with the 'WHERE' keyword (see the screenshot for an example).

Attention!

If the syntax in a WHERE field is incorrect, the discovery process will fail. When writing the clause, you must start the filter with the 'WHERE' keyword itself (for example 'WHERE location=1'). Also, mind that SQL syntax as it may differ from different database engines. SQL Server uses T-SQL, Oracle uses PL/SQL and PostgreSQL, MySQL and MS Access also have slightly different flavors of SQL so there may be minor differences in the syntax. If you want to avoid all this hassle don't use the WHERE clause and instead connect to a custom view where the information is already pre-filtered.

Connection Mapping	Reconcilliation
Source table:	Sites 👻
netTerrain type:	Site 🔹
Default diagram:	<null> •</null>
Parent locator field:	<null> -</null>
Name/Id field:	Site Name 👻
X coord field:	Longitude 👻
Y coord field:	Latitude 👻
WHERE clause	
	Cancel Next

Configuring the mapping tab

5.3.3 Reconciliation

The last tab deals with the mechanism for node reconciliation into netTerrain.

5.3.3.1 Updating existing nodes in netTerrain

If you want to update any field changes for nodes that exist in the data source and have already been imported into netTerrain during a previous cycle, then the 'Update existing nodes' combo box needs to be set to 'Yes'.

5.3.3.2 Inserting new nodes into netTerrain

New nodes that do not exist in netTerrain and were discovered by the node connector will be inserted into netTerrain, if the following criteria apply:

- A default diagram or a parent locator field has been assigned for the node connector.
- The 'Insert new nodes' combo box is set to 'Yes'.

5.3.3.3 Deleting nodes without matches

Nodes that exist in netTerrain and were tagged as imported by the node connector during a previous cycle and do no longer exist may be:

- Deleted from netTerrain by setting the 'Delete nodes without matches' combo box to 'Yes'.
- Kept in netTerrain by setting the combo box to 'No'.

Update existing nodes: Insert new nodes: Delete nodes without matches: Pre import function: Post import function:	Connection Mapping Reconcilliation	
Delete nodes without matches: Yes Pre import function:	Update existing nodes:	Yes 🔻
Pre import function:	Insert new nodes:	Yes 🔹
	Delete nodes without matches:	Yes 🔹
Post import function:	Pre import function:	
	Post import function:	

Reconciliation tab

5.3.3.4 Pre and post import functions

These fields are used to place advanced functions that are processed before and after an import occurs. An example of a pre-import function could be a call to execute a stored procedure in the source data, which massages the records to be imported. An example of a post import function could be a layout algorithm that is triggered after the import to automate node positioning.

Attention!

The Pre and Post import function fields are currently reserved for Graphical Networks consultants. If you think you need a function to perform a specific action, please enter a ticket in the support portal.

5.4 Step 2: Mapping custom fields

Now that we have set the main parameters for the node connector, we can proceed to map fields from the source with custom fields in netTerrain. This is done in step 2 of our wizard. This step works pretty much the exact same way as we have seen before, but we'll review it again here.

5.4.1.1 Mapping fields when they already exist in netTerrain

When the destination fields in netTerrain already exist, you can simply map fields one by one or also use the option to map all fields with matching names.

To map a field from the source to an existing field in netTerrain, simply choose it from the source table and then select the corresponding destination field in netTerrain that you want the source field mapped to. Finally click on 'Map Selected Fields' and you are done.

Once added, the new mapping will show up in the 'Fields currently mapped' list view.

To remove a mapping, simply select it and hit 'Remove'.

Map New Field Field in source	database:	Contact ID Crea	ate + Map All	▼ Create + Map	
Field in net Ten		Administrato	r Natched Fields	Map Selected Fields	p se
ntColumn	Source Field		netTerrain Field		
28000000 28000000 28000000	Address Latitude		Address Latitude Longitude		
Remove					

Adding a new mapped field

When many of the fields in the source match the names of the fields in netTerrain, you can map them all in one simple process by clicking on the 'Map Matched Fields' button.

5.4.1.2 Mapping fields when they don't exist in netTerrain

As mentioned before, in case one or more of the source fields do not yet exist for the type in netTerrain, you can map and create them in the catalog, at once, straight from the ITK.

To map and create just one field from the source, select it first from the drop-down list, and then click on 'Create + Map' button. If you want to Create and map all the fields in the source, click on the 'Create + Map All' button.

Any mappings can be removed from this dialog by selecting the mapping from the list view and clicking on the remove button.

Attention!

When using x and y (or lat / long) coordinates you must also map the corresponding netTerrain fields in this step as well.

5.5 Next steps

Once the 'Finish' button is clicked, the node connector should be registered in the ITK database and force an application restart. The application restart is necessary so that the new connector can be registered in the ITK UI menus and list views.

K and a second sec	
Connector successfully registered. The connector nee proper flow of data. The application will restart for ch	
	ОК

After the restart, the new node connector will be available in the node connector list and any applicable menu options.

Even if a node connector is successfully registered, the actual import process may fail. Some factors that could affect the proper functioning of a node connector include:

- Certain key fields may have been deleted from type definition in netTerrain.
- NULL values in names or parent mapping fields.
- Syntax errors in a WHERE clause.

It is highly recommended to test the node connector by first running a discovery and then a preview of the reconciliation process.

Just as with device connectors, you can edit a node connector afterwards. Consider that editing a node connector may trigger a drop and create process of the node table, which will require a full discovery of the source data.

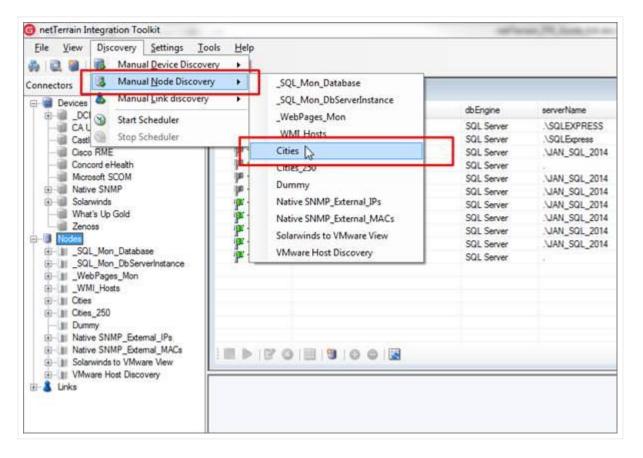
If later on you need to make changes to the mapped fields, these are also managed the same way as with device connectors.

5.6 Discovering and reconciling nodes

The discovery process for node connectors involves reading the source data and dumping it into a raw table in the ITK. This is the first (of two) steps to synchronize the source data with netTerrain (both processes can be automated when scheduling connectors).

These two processes are executed in the same order and fashion as with devices connectors (see previous chapter).

To run a discovery for the first time simply go to the 'Discovery' menu and click on the appropriate node connector to discover data from.



Tip:

You can also start a discovery by double clicking on the connector entry and then clicking on the 'Refresh List (Discover)' button, as displayed below.

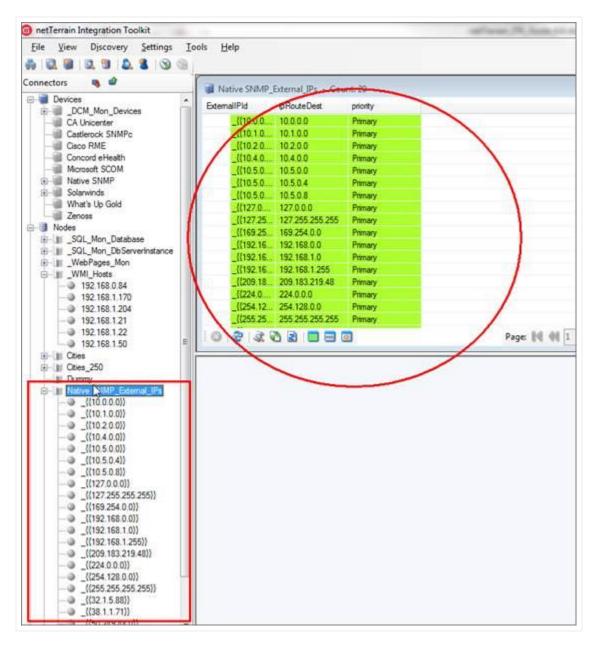
nectors 🧠 📽	Cities - Count 1564				
Devices	Id	Name	pronty	Lattude	Longtude
CM_Mon_Devices					
CA Unicenter	249850	Whetstone, AZ	Primary	31.9573	-110.342
Castlerock SNMPc	249860	Youngtown, AZ	Primary	33.5939	-112.303
Ceco RME	249870	Namo, CA	Primary	37.8502	-122.032
Concord eHealth	249880	Atadena, CA	Primary	34,1897	-118.131
Moreaoft SCOM	249890	Apple Valley, CA	Primary	34.5008	-117.186
Sciarwinds	249900	Ashland, CA	Primary	37.6947	-122.114
What's Up Gold	249910	Avla Beach, CA	Primary	35.18	-120.732
Zenoss	249920	Beaumont, CA	Primary	33.9295	-116.977
Nodes	249930	Bernuda Dunes	Primary	33.7428	-116.289
Gal SQL Mon Database	249940	Bishop, CA	Primary	37.3635	-118,395
SQL Mon DbServerInstance	249950	Boorwile, CA	Primary	39.0091	-123.366
WebPages_Mon	249960	Brea, CA	Primary	33.9167	-117.9
WMI_Hosts	249970	Burbank, CA	Primary	34,1808	-118.309
ii) al Cties	249980	Calpatra, CA	Primary	33.1256	-115.514
E (B Ctes 250	249990	Campbel, CA	Primary	37.2872	-121.95
III Dummy	250000	Carson, CA	Primary	33.8314	+118.282
- II Native SNMP Edemal IPs	250810	Century Day, CA	Premary	34.0556	-118.418
III Native SNMP_Edemal_MACs III Solarwinds to VMware Vew		3 0		Page: 14 41 1	80 88
William Host Discovery					

Running a discovery from the connector view

By clicking on this submenu, netTerrain will start the process of importing the raw data from the third-party data source and will display the results under the corresponding view menu. Note that the nodes are not yet imported into netTerrain. The latter involves the execution of the reconciliation process. The output window will also show the start and end times of the discovery process.

5.6.1 Viewing the results

Once nodes have been imported as raw data into netTerrain, you can view these nodes and associated columns by clicking on the 'View' menu and the corresponding node connector, or by double clicking on the connector in the connector list.



List of discovered nodes for a node connector

Each node will be represented by a row and will contain values for several columns that will depend on which fields were mapped during the node connector creation process.

Just like with devices, the list view uses specific color codes to identify the reconciliation status of the node in netTerrain.

Nodes can also be viewed from the tree view. In addition, if a user wants to view a node in more detail, by double-clicking on the row entry the ITK will display a dialog box with each attribute for the node.

Record not in net Terrain		-
Sysname: 192.168.1.204		E
priority: Primary		-
LogicalDrives: [1] Name=A: Caption [2] Name=C: Caption=C: Size=3754 [3] Name=D: Caption=D: Size=		
OS: [1] Name=Microsoft Windows S \Device\Harddisk0\Partition2 Versi Windows Server 2012 Standard Bui Corporation CodeSet=1252 Country SerialNumber=00183-80851-52914-	on=6.2.9200 Caption=Microsoft ildNumber=9200 Manufacturer=Mi Code=1 CurrentTimeZone=-240	
BIOS: [1] Manufacturer=Phoenix Te SerialNumber=VMware-56 4d a1 c4		9 ec
CPU: [1] Name=Intel(R) Xeon(R) CF Manufacturer=GenuineIntel Architec	PU E5-2430 0 @ 2.20GHz Family= sture=9 Caption=Intel64 Family 6 M	

Node details

5.7 Node reconciliation

So far, the discovery has simply pulled the data from the source into a raw table in the ITK, but it is not yet in netTerrain. To import nodes into netTerrain, we need to reconcile the discovered items with the netTerrain database. This reconciliation process includes the insert, update and/or delete of nodes from the data source into netTerrain, according to the rules specified in the node connector mapping settings.

5.8 Deleting and suspending node connectors

Node Connectors are deleted from the ITK by following these steps:

- Open the appropriate connector list (Ctrl-O).
- Click on the connector to be deleted.
- Click on the delete button (or right-click->delete connector).

Attention!

Note that this action cannot be undone. It will remove all traces of the connector from the ITK, but it will not remove objects in netTerrain.

Connectors can also be suspended, instead of deleted. That way, when an automatic scheduler is set up, any suspended connectors will not start the discovery and reconciliation process. To suspend a connector, right click on it from the list and click on the 'Suspend' option.

	-	id	alias			dbEngine	serverName	dbName
e		J# 10002	Network	5		MS Access		C:\Temp\Netw
erinstance		J# 10003	Switches	1		MS Access	10	C:\Temp\Netw
al_IPs	=	J# 10005	Sola_noo	des		SQL Server	.\Jan	Solarwinds
		J# 10006	_SQL_M	lon_D	bServerInstance	SQL Server		GN
		10007	_SQL_M	lon_D	atabase	SQL Server	* C	GN
	1.00	10008	Native S	NMP_	_External_IPs	SQL Server		GN
		10009	Stes		In the second second	MS Access		C:\Temp\Netw
					Suspend	R		
				D	Activate			
				3	Edit			
				0	Delete			
				-	Minu Basada		-	
			-	=	View <u>R</u> ecords			
					Mapped Fields			-
				1	Create New No	de Connector		
		Care and a sub-			Refresh View	F5		

Suspending a connector

6 Link Connectors

Link connectors are hooks into external databases or files to import records and map them with netTerrain link objects. Link connectors are a very useful resource to automate the process of creating documentation in netTerrain by taking advantage of existing data from your environment.

You can create any number of link connectors and each one will be tied to a predefined link type in the netTerrain catalog. To create a link connector, you can utilize a wizard to connect to the data source and map table columns to custom fields in netTerrain.

All link connectors in the ITK are user created and they can be found in the link connector list. From the connector list you can manage settings and schedule automated discovery processes.

6.1 Viewing link connectors

To see which link connectors are currently included in the ITK, simply go to View-> Link connector list (Ctrl-K) and a list view of all the link connectors will be displayed.

ile View Discovery Settings To	ols Help			
Device Connectors List Ctrl+	A			
nnge Node Connectors List Ctrl+				
🔒 💩 Link Connectors List🖕 Ctrl+	K nk Connec	tor List - Count: 5		
		alias	dbEngine	serverName
Find Devices	20002	VM Links	SQL Server	ASQLEXPR
Find Nodes	20003	LinksTest	MS Access	43
Find Links	20004	_SQL_Mon_Links	SQL Server	.VAN_SQL
Concolo eneaun	20005	Native SNMP_Links	SQL Server	JAN_SQL
- Microsoft SCOM	20006	Native SNMP_Links_Layer2	SQL Server	JAN_SQL
Native SNMP	12111111111			
🕀 🏢 Solarwinds				
- What's Up Gold				
Zenoss				
Nodes				
SQL_Mon_Database				
SQL_Mon_DbServerinstance				
⊕ WebPages_Mon				
- WMI_Hosts				

Link connector list view

6.2 Step 1: creating the link connector

Just like with device and node connectors, to create a new link connector, netTerrain must know certain aspects of the data source, such as connection properties, the table or query to import the data from and

the fields that will be mapped to custom fields in netTerrain. You also need to determine whether the data source is natively supported or not, in which case you may want to set up a proxy database (see previous chapters on setting up a proxy database).

Also, similar to the node connector creation process, a 2-step wizard will guide you through the process of creating a link connector.

To start the link connector wizard, go to Tools-> Create New Link Connector. A similar button and a right click context menu are also available from the link connector list view.

			of the local division of the local divisiono	the second second	10,1046	No. of Content of Cont
ools Help						
Link Connec	tor List - Count: 5					
el # 20002 # 20003 # 20004 # 20005 # 20005 # 20005	alas VM Links LinksTest _SQL_Mon_Links Native SNIMP_Links Native SNIMP_Links_Layer2	dbErgne SQL Server MS Access SQL Server SQL Server SQL Server	MAN_SQL_2014	ReesPerf ReesPerf	status 2 2 2 1 1	lastDacovered 7/9/2015 5.01 9/16/2015 10 5/11/2016 1 5/26/2016 3.5 5/26/2016 3.5
			Suspend Activate Clone Edit			
		3		Cactor		
		Link Connector List → Count: 5 d alea IP 20002 VM Links P 20003 Links Test IP 20004 _SQL_Mon_Links P 20005 Native SNMP_Links	Link Connector List - Count: 5 d alea deErgne # 20002 UM Links SQL Sover # 20004 _SQL_Mon_Links SQL Server # 20005 Netwe SNMP_Links SQL Server # 20006 Netwe SNMP_Links_Layer2 SQL Server # 20006 Netwe SNMP_Links_Layer2 SQL Server	Link Connector List - Count: 5 d alias dtErgine serverName # 20002 VM Links SQL Server VSQLEXPRESS # 20004 _SQL_Mon_Links SQL Server VAN_SQL_2014 # 20005 Native SNMP_Links SQL Server VAN_SQL_2014 # 20006 Native SNMP_Links_Layer2 SQL Server VAN_SQL_2014 # 20007 Base of the server SQL Server Verver # 20008 Base of the server SQL Server Verver <	Link Connector List - Count 5 d alse de Ergne serverName doName # 20002 UM Links SQL Server VSQLEDVPRESS SolarWindeNew # 20004 _SQL_Mon_Links SQL Server VAN_SQL_2014 ReesPerf # 20006 Native SNMP_Links_SQL Server VAN_SQL_2014 ReesPerf # 20006 Native SNMP_Links_Layer2 SQL Server VAN_SQL Server VAN_SQL_2014 ReesPerf # 20006 Native SNMP_Links_Layer2 SQL Server VAN_SQL	Link Connector List - Count: 5 d alse deErgne serverName doName status p 20002 VM Links SOL Server SOL Server SOLEXPRESS SolarWindsNew 2 VGN/PM/Sp. 2 VGN/PM/Sp. 2 VGN/PM/Sp. 2 VGN/SOL_2014 RecePer 1 VGN/SOL_2014 RecePer 1 Support SolarView SNMP_Links_Layer2 SOL Server VMN_SOL_2014 RecePer 1 Support Conce Conc

Creating a new link connector

6.2.1 Connection information tab

This tab stores the name and connectivity information, so that the ITK can properly read the data from the source.

6.2.1.1 Database engine

As mentioned before, Oracle, PostgreSQL, MySQL, SQL Server or MS Access databases are natively supported for direct connections between the ITK and the data source. Otherwise, you can use a proxy database (as explained in the previous chapter). For example, if you want to bring in records from a MySQL

database, you can create linked tables in MS Access (or a linked server in SQL Server), which then (via queries) connect to the ITK.

Connection Mapping Rec	oncilliation
Linker name:	MyLinks
Database engine:	N •
Server:	MS Access SQL Server
Windows authentication:	Oracle PostgreSQL
User	MySQL
Password	
Database	▼ [
	Test Connection
	Cancel Next

Connectivity tab showing the database engine drop down box

When using MS Access, the server is not required, as the path to the corresponding MS Access file will be used. In the case of SQL Server, the server and database name must be specified in the appropriate fields. With Oracle, a TNS name will typically need to be set up on the ITK machine.

Connection Mapping Re	conciliation	
Linker name:	MyLinks	
Database engine:	SQL Server •	
Server:	.VJAN_SQL_2014 +	
Windows authentication	Yes 👻	
User		
Paseword		
Database	WUG 🔹 💽	Linker Connection test
	Test Connection	Conector text of
		Connection Successful
	Cancel Next	Distance and the second second second
		OK

Setting up the connection tab for a link connector

6.2.1.2 Database credentials

Database credentials are only required for SQL Server, PostgreSQL, MySQL and Oracle-based link connectors. In both cases a user with read-only access to the source will suffice. Both Trusted connections and SQL Server authentication are supported for SQL Server-based link connectors.

6.2.1.3 Source Database

If the database engine is SQL Server, then the database field does provide a drop-down box of all the databases available for that server. For MS Access-based connectors use the ellipsis '..' button to browse for the Access file (.accdb and .mdb extensions are supported). For Oracle-based connectors you must type in the TNS reference. For PostgreSQL-based connectors the Server field turns into a 'DSN' field. You must then make sure there is a DSN to the PostgreSQL database (from the machine hosting the ITK) and then reference that DSN in the DSN field.

6.2.2 Mapping tab

The mappings tab for custom connectors is essentially the same as for node connectors. The main two differences between a node and a link connector are the following:

1) Link connectors do not require a default or parent network for proper placing of records in netTerrain. Instead, they require two fields that identify the endpoints of each link.

2) Link connectors are automatically rendered based on the location of the endpoints, which means that no x/y or other auto positioning methods apply to links.

6.2.2.1 Source table

The source table represents the table or view where the records that need to be pulled from the data source are stored.

Tip:

If you need to modify some of the data being imported into netTerrain or need to correlate more information that is available in other tables, create a view that "massages" that data for you and point the source table field to that view.

6.2.2.2 netTerrain Type

The type field for links is used to specify which link type from the netTerrain catalog is mapped to our source table. What this means is that once the ITK starts importing records through this link connector, every record will be an instance of the netTerrain type. Do not confuse this type field with the type field for device connectors (see chapters 3 and 4).

6.2.2.3 Name field

The name field should contain the name or unique identifier for each link and it will be mapped to the name field in netTerrain. Technically, it is not necessary for this field to pull values that are unique, but it is highly recommended. If the name field is mapped to a field in the source table that does contain repeated values, then any links with the same name field value will throw an error during the update process.

6.2.2.4 Endpoint locator fields

As mentioned above, link connectors require two endpoint identifiers. These endpoints can consist of nodes, devices, ports or any other category in netTerrain. Moreover, the endpoints can be a concatenation of several nodes. Your source database will need to contain a field that identifies the starting point for the link and another one for the ending point.

6.2.2.5 Endpoint separator (and how to create connections between ports)

Link connectors can use concatenated values to create links in netTerrain. This is very useful when the final endpoint nodes do not have unique names (such as ports, that are typically just numbered). For instance, your endpoint fields may consist of a concatenation of 'device::card::port', which uniquely identifies the endpoints. It is important to note that you still must have the endpoint values in one field. You cannot concatenate values from multiple fields. If your source data does not contain a single field with the concatenated values, then you can construct that field yourself as a concatenation of the original fields in some intermediate query or table.

In order to successfully use concatenated values, you must specify the character that is used as a separator. The ITK, upon reconciling the data, will then parse the endpoints, look for the separator and work its way down in the hierarchy. For instance, let's say a certain link has the a value of Cisco6009-primary::4::3

for endpoint 1, and we specify the string '::' as the endpoint separator, then netTerrain will parse this value as follows:

- The ITK will first look for a node in netTerrain called 'Cisco6009-primary'. This node needs to have a unique name
- If the ITK determines that the node is a device, and there is more than one part remaining, it will then look for a card (in this case called '4')
- When the ITK gets to the last part, it determines it must be a port (in this case '3') and creates the link

6.2.2.6 WHERE clause

The last field of the second tab contains a WHERE clause. This can be used as a mechanism to filter certain records from the source table. The syntax of the WHERE clause must correspond to the flavor of SQL that the source database uses and must start with the 'WHERE' keyword (see the screenshot for an example).

Attention!

If the syntax in a WHERE field is incorrect, the discovery process will fail. When writing the clause, you must start the filter with the 'WHERE' keyword itself (for example 'WHERE location=1'). Also, mind that SQL syntax as it may differ from different database engines. SQL Server uses T-SQL, Oracle uses PL/SQL and PostgreSQL, MySQL and MS Access also have slightly different flavors of SQL so there may be minor differences in the syntax. If you want to avoid all this hassle don't use the WHERE clause and instead connect to a custom view where the information is already pre-filtered.

Connection Mapping Re	econcilliation	
Source table:	Circuit	
net Terrain type:	LAN Copper	•
Name/Id field:	Linkld	÷
Endpoint 1 locator field:	Origination	
Endpoint 2 locator field:	Destination	•
Endpoint separator:		
WHERE clause:		
	Cancel	Next

Configuring the mapping tab for a link connector

6.2.3 Reconciliation

The last tab deals with the mechanism for link reconciliation into netTerrain.

6.2.3.1 Updating existing links in netTerrain

If you want to update any field changes for links that exist in the data source and have already been imported into netTerrain during a previous cycle, then the 'Update existing links' combo box needs to be set to 'Yes'.

6.2.3.2 Inserting new links into netTerrain

New links that do not exist in netTerrain and were discovered by the link connector will be inserted into netTerrain, if the following criteria apply:

- The endpoint fields have been assigned for the link connector.
- The 'Insert new links' combo box is set to 'Yes'.

6.2.3.3 Deleting links without matches

Links that exist in netTerrain and were tagged as imported by the link connector during a previous cycle and do no longer exist may be:

- Deleted from netTerrain by setting the 'Delete links without matches' combo box to 'Yes'.
- Kept in netTerrain by setting the combo box to 'No'.

ion
Yes 👻
Yes 💌
Yes 🔻

Reconciliation tab

6.2.3.4 Pre and post import functions

These fields are used to place advanced functions that are processed before and after an import occurs. An example of a pre-import function could be a call to execute a stored procedure in the source data, which massages the records to be imported.

Attention!

The Pre and Post import function fields are currently reserved for Graphical Networks consultants. If you think you need a function to perform a specific action, please enter a ticket in the support portal.

6.3 Step 2: Mapping custom fields

Now that we have set the main parameters for the link connector, we can proceed to map fields from the source with custom fields in netTerrain. This is done in step 2 of our wizard and is very similar to how you map custom fields for connectors or devices (as seen before).

6.3.1.1 Mapping fields when they already exist in netTerrain

When the destination fields in netTerrain already exist, you can simply map fields one by one or also use the option to map all fields with matching names.

To map a field from the source to an existing field in netTerrain, simply choose it from the source table and then select the corresponding destination field in netTerrain that you want the source field mapped to. Finally click on 'Map Selected Fields' and you are done.

Notice that the fields do not have to have the same names.

Once added, the new mapping will show up in the 'Fields currently mapped' list view.

To remove a mapping, simply select it and hit 'Remove'.

When many of the fields in the source match the names of the fields in netTerrain, you can map them all in one simple process by clicking on the 'Map Matched Fields' button.

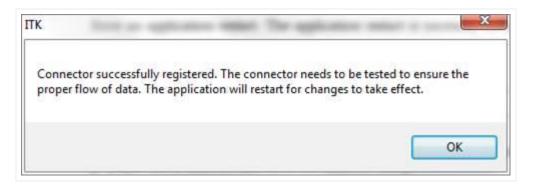
6.3.1.2 Mapping fields when they don't exist in netTerrain

As mentioned before, in case one or more of the source fields do not yet exist for the type in netTerrain, you can map and create them in the catalog, at once, straight from the ITK.

To map and create just one field from the source, select it first from the drop-down list, and then click on 'Create + Map' button. If you want to Create and map all the fields in the source, click on the 'Create + Map All' button.

6.4 Next steps

Once the 'Finish' button is clicked, the link connector should be registered in the ITK database and force an application restart. The application restart is necessary so that the new connector can be registered in the ITK UI menus and list views.



After the restart, the new link connector will be available in the link connector list and any applicable menu options.

Even if a link connector is successfully registered, the actual import process may fail. Some factors that could affect the proper functioning of a link connector include:

- Certain key fields may have been deleted from type definition in netTerrain.
- NULL values in names or endpoint mapping fields.
- Syntax errors in a WHERE clause.

It is highly recommended to test the link connector by first running a discovery and then a preview of the reconciliation process.

Just as with node connectors, you can edit a link connector afterwards. Consider that editing a link connector may trigger a drop and create process of the link table, which will require a full discovery of the source data.

If later you need to make changes to the mapped fields, these are also managed the same way as with node connectors.

6.5 Discovering and reconciling links

The discovery process for link connectors involves reading the source data and dumping it into a raw table in the ITK. This is the first (of two) steps to synchronize the source data with netTerrain (both processes can be automated when scheduling connectors).

These two processes are executed in the same order and fashion as with devices connectors (see chapter 4).

The ITK automatically takes care of properly connecting a link with its endpoints. The following important rules for links apply:

- Links must have two endpoints and these endpoints need to exist prior to the reconciliation process for a link record to be created.
- Any link that has one or more endpoints that appear to be repeated in netTerrain (i.e. the endpoint name is not unique) will not be imported and an error will be logged.
- If both endpoints of a given link exist on different diagrams, netTerrain automatically creates an inter diagram link and takes care of the creation of reference nodes.



Example of nodes and links discovered from the ITK

6.6 Deleting and suspending link connectors

Link Connectors are deleted from the ITK by following these steps:

- Open the appropriate connector list (Ctrl-L).
- Click on the connector to be deleted.
- Click on the delete button (or right-click->delete connector).

Attention!

Note that this action cannot be undone. It will remove all traces of the connector from the ITK, but it will not remove objects in netTerrain.

Connectors can also be suspended, instead of deleted. That way, when an automatic scheduler is set up, any suspended connectors will not start the discovery and reconciliation process. To suspend a connector, right click on it from the list and click on the 'Suspend' option.

File View Discovery Settings	and the second				
Connectors 🧠 🖉	Link Connecto	or List - Count: 6			
Devices Nodes	id	alas	dbEngine	serverName	dbName
E Links	₩ 20002 ₩ 20003 ₩ 20004 ₩ 20005 ₩ 20006	VM Links LinksTest _SQL_Mon_Links Native SNMP_Links Native SNMP_Links	SQL Server MS Access SQL Server SQL Server SQL Server	VAN_SQL_2014 VAN_SQL_2014 VAN_SQL_2014 VAN_SQL_2014	ReesPe
	20007	Sul send	83.		C:\Tem
		 Clone Edit Delete 			
		View Records Mapped Fields	_		
		Create New Link Conno Refresh View	ector		

Suspending a link connector

7 Monitoring

In the previous chapters we saw powerful features for importing data from external data sources using device, node and link connectors. In addition to the discovery of data from external databases, the ITK also has several native monitoring tools:

- An SNMP auto-discovery engine
- A WMI discovery engine
- An AWS discovery utility
- An environmental monitoring module supporting IPMI, SNMP, SSH, WS-MAN, HTTPS and Inband Protocol (separate license required, please consult the Environmental Monitoring module guide for details)
- A simple website monitoring tool
- A SQL Server monitor

7.1 General parameters

The monitoring engine for the ITK includes a series of configuration settings that help you tune the process to your liking. The configuration options include some general parameters that, such as threads, fields and more which you can access by clicking on Settings->Monitoring->Configuration (or ctrl-g).

Monitoring Configur	ation				×
General Parameters	SNMP	WMI	DCM	AWS	
General parameters	3				_
Timeout [ms]	Ę	5000	•		
Threads	·	1 .	•		
Global Device Prop	oerties				
System MIBs		Map to	o all Devi	ices	
Single Property			Add		
		R	emove		
Port Object					
Port Table Prop	erties (Add All			
	(Cano	:el	0	к

Configuration options for monitoring

The general parameters for SNMP discovery include the timeout and multithreading settings, MIB properties (which let you add properties to devices in netTerrain besides just SNMP), and settings for the port object.

7.1.1 Timeout and threads

The timeout setting controls the time for a background worker process to wait for a device to respond to an SNMP get command. The multithreading combo box option provides a few values for the number of threads that the engine uses for all discovery purposes. The default number of threads is 2. For any value greater than 1, the engine issues multiple parallel threads to discover the network faster. We do not recommend using more than 5 threads, other than for testing purposes.

In general, we recommend using the default values for these general parameters, as they should suit most needs.

7.1.2 Device properties

The discovered properties won't be very useful if the corresponding fields are not created in the netTerrain catalog for each corresponding type. For example, the ITK may be able to discover ifSpeed for ports, but if the port object in the netTerrain catalog doesn't include that field, then it won't be reflected in the project either. The same applies for devices: if, say, the sysDescription field does not exist in the netTerrain catalog, then the discovered sysDescription values for any devices that the ITK scans will not be reflected in the netTerrain diagrams.

For convenience, the ITK includes buttons that create these fields automatically, without having to go to the netTerrain catalog. This is particularly useful for devices, since a given system MIB value (the MIBs mapped to devices) would have to be created for any possible type that we expect to be discovered via SNMP. This could be a tedious task involving dozens or hundreds (maybe thousands) of types.

The process for creating new values for all device types in the catalog was explained in chapter 3 (Mapped fields missing in netTerrain), but we'll repeat it here for convenience.

To set up a specific netTerrain property for devices, click on the 'Add...' button in the Global Device Properties group. This will prompt you to enter the name of the property you want created in the catalog for devices.

The ITK is smart enough to only add the field to the types that are missing it. And yes, be patient indeed, this process can take a couple of minutes.

[1] Name=A: Ca. [1] Name=A: Ca.							
	Monitoring Settings						
	General Parameters SNMP WMI DCM General parameters Timeout [ms] 5000 • Threads 5 • Global Device Properties						
= =	Device Types System MIB Map to all Devices Add device field name Enter field name you want to add for all device types Remove Remove						
	Port Object Port Table Properties Add Al						
	Cancel OK						

Adding a field to all device types in netTerrain

You can also remove a field for all device types using the 'Remove...' button.

You can also add all System MIB properties at once, by clicking on the 'Map to all Devices' button and have patience, as this process can take several minutes to execute.

For ports, there is a button that simply adds to the port object type every interface group MIB property described at the beginning of this chapter.

Attention!

Be careful with these functions as they affect all types and instances in netTerrain! Also remember that the properties will be created for every single device type in netTerrain!

7.2 SNMP auto-discovery

The Native SNMP auto-discovery module can discover devices from the network, by polling the device management IP addresses. It will then discover properties from those devices using a predefined list of so-

called 'MIB' (Management Information Base) variables. This component currently supports versions SNMPv1, SNMPv2c and SNMPv3.

Via SNMP, the ITK can discover the following device related information:

- Standard System MIB properties
- Any custom (public or private) MIB, which can be mapped to any custom field in netTerrain
- Interface information, including status, reading from the MIB interface table
- Layer 3 links (via IP address and routing tables)
- Layer 2 links (via interface and bridge tables)
- Up/down status for devices (this also uses Ping as a primary method, along with SNMP System get as a backup method)

Once devices are discovered, this module behaves much like a device connector in the sense that it maps the discovered elements with devices in netTerrain. Moreover, the ITK also uses a pre-defined device connector specifically for native SNMP. This predefined connector is part of the device connector list and is called 'Native SNMP' (with the id 1001). This connector can also be scheduled for automatic discovery and reconciliation, just like any other connector.

	ANT - C	- 1 m										- 1 40
			selbedu	data Tere	auCrisit	where .	axiome .	automat.	fileter	a Addee	asDecovered.	-
an DANA	1418-255-244	144	1381418148		Barrat	Date Of Schware CON Sel	Dioha-Ud			10210254	TU25/2014 1.5	-
tel	LOSADENIAS		1161418118		Barris	Cale Instantion Operating Str.		-		192,148,0.3	VI.(25/2014 118.	
(artiseth	LOG-R DETEND	547	13614191467	26206791	Sector	Cars DS Selvan C200 Sel	SNONieLNE			110.163.04	11/25/2014 1.5	arbna
ANCH	LOS#280122	645	1361415189	26178300	Stepheni .	Cecu IOS Suffrage 2001 Suffrag.	DNORM-LAB			102108.02	11/23/2014 115	URNER
DM .	105539634		33814181398	17104103	-Jan	One transmith Garating Sys.		1	24	102108-01	11/25/2014 115	interest
	1.05.5388.24		13111111111	17104434	Ped	Cash US Saferes C200 Soft			28	102.168.5.7	1103-2014-115	
	05538048		13414181278		Station .	City Hendrick Commy Se.		2	52	102.148.0.5	11/05/0014 1-5	
	1.04-12105-4		336141890.1		Septer		SNON#	178.00		112 148.0.50	95/25/2014 htt	
	Darwor Cateriore	BAS C	1111111111111	20296213	They if your party	Temperature & Service Galaxies	DADRIE (AB	CONTRACT.	1.1	192 198 5 77	11/18/2014 1.5	LANGED
	0 2 2 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2											
Teng Janes 15 ppg Janes 16 ppg	2014 3.17 11 FW 2014 3.17 11 FW 2014 3.17 14 FW 2014 3.17 14 FW 1016 3.17 14 FW 1016 3.17 14 FW 1016 3.17 14 FW 2014 3	IE Values A Autorempt I Autorempt I Autorempt I P address of of Inee. In Hillor Val Stable gat Stable gat Stable gat Stable gat Stable gat Stable gat Stable gat Stable gat Stable gat	r established connects ar for IF address 152 152 165 5.5 veturned ar r established connects at for IF address 152	14 potential 14 potential (C1 A 201 Investo (C1 A	M341 M341 Xisode: A convector at worker Your has failed in 1110 1000 A convector at worker Your has failed in 1110 x000A, T2 101 weeks A 4.0 (2011) X0007 Am	hengi faled because the connected p in segment in Song/Paqueal hengi faled because the connected p in segment in Song/Paqueal en it (proced) domarced \$3335.3p						

Native SNMP discovery list view

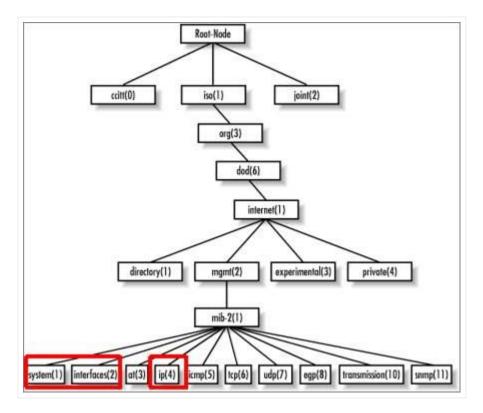
The Native SNMP discovery configuration for SNMP parameters as well as for the connector itself can be accessed from the Settings->Monitoring-> SNMP menu. We'll review each submenu in a bit.

File View Discovery	Set	tings Tools Help	1							
Connectors S Connectors	11	Device Connectors Node Connectors Link Connectors	ink C	onnectorList - Count:6	_		doEngne	serverNat		doName
 I Nodes Links 	0	Monitoring	· =	SNMP		50	IP Address Ranges	Ctrl+I	RESS	SolarWindsNew
B.ANative_SNMP_Lin B.ANative_SNMP_Lin B.ANative_SNMP_Lin B.ASQL_Mon_Links	1.0	Discovery Order	. @	WMI Power / Temp Web Pages	•		Device Discovery Sett	ttings		D.'GN\PM\Funx C.\Temp\Netwo Jan
							SNMP Config sation.		014	
⊕ A Crouts	۹					yer2	SQL Server	_Van_sd	2014	Jan
⊕-∄ LinksTest ⊕-₿ VM Links			3	AWS SQL Server Monitor		-	SQL Server	.\jan_ed_	2014	Jan
			a.	Configuration Ctrl+G						

Native SNMP configuration menus and settings

7.2.1 Built-in MIBs

The foundation of an SNMP-based management system is a database containing information about the objects in the network to be queried. This database is referred to as the Management Information Base (MIB) and each resource to be managed in that database is an object. The MIB then is a structured collection of objects in the form of a tree. Associated with each object in the tree is an object identifier (OID) which follows a notation (Abstract Syntax Notation 1 or ASN.1) consisting of a set of integers separated by dots. The figure below illustrates part of the MIB-2 structure.



MIB-2 structure

The Native SNMP discovery uses the following OID prefixes (leafs depicted in red above):

- System group (OID 1.3.6.1.2.1.1): they obtain basic device information.
- Interface group (OID 1.3.6.1.2.1.2): they obtain basic interface (port) information. This data can be automatically mapped to the ports defined for a given type in the netTerrain catalog.
- IP address group (OID 1.3.6.1.2.1.4): they comprise the IP address and routing table MIBs to obtain layer 3 link information between devices.

7.2.1.1 System MIBs

The system MIBs that are currently supported include the list below (we also include the ASN.1 definition for each):

- sysName: "An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name".
- ipAddress
- sysObjectId: "The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed".
- sysUpTime: "The time (in hundredths of a second) since the network management portion of the system was last re-initialized".
- sysContact: "The textual identification of the contact person for this managed node, together with information on how to contact this person".
- sysDescr: "A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters".
- sysLocation: "The physical location of this node".
- sysServices: "The value which indicates the set of services that this entity primarily offers. The value is a sum. This sum initially takes the value zero, Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L 1) is added to the sum. For example, a node which performs primarily routing functions would have a value of 4 ($2^{(3-1)}$). In contrast, a node which is a host offering application services would have a value of 72 ($2^{(4-1)} + 2^{(7-1)}$)".
- if Number: "The number of network interfaces (regardless of their current state) present on this system".

In addition, devices will have a lastDiscovered timestamp appended to them, which is determined by the ITK itself.

7.2.1.2 Interface MIBs

When port monitoring is enabled, the ITK can discover interface properties for devices using the interfaces group MIB (not yet supported with SNMPv3). The properties that can be monitored include:

- ifDescr: "Textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface".
- ifType: "The type of interface, distinguished according to the physical/link protocol(s) immediately `below' the network layer in the protocol stack".
- ifSpeed: "An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth".
- ifPhysAddress: "The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
- ifAdminStatus: "The desired state of the interface".
- ifOperStatus: "The current operational state of the interface".
- ifLastChange: "The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value".

Of special interest are the ifAdminStatus and ifOperStatus, which can be used to represent status values in netTerrain and be used as a visual override to change the port colors. Possible values for these parameters are:

- up (1)
- down (2)
- testing (3)

7.2.1.3 IP address table and routing table MIBs

When link monitoring is enabled, the ITK can discover layer-3 topology for routers or devices that store routing table information in the IP group MIBs (not yet supported with SNMPv3).

Discovered links will include the following properties:

- ipRouteDest: "The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use".
- ipRouteAge: "The number of seconds since this route was last updated or otherwise determined to be correct".
- ipRouteMask: "Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field".
- ipRoutelfIndex: "Index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex".
- ipRouteMetric1: "Primary routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1".
- ipRouteNextHop: "IP address of the next hop of this route".
- ipRouteType: "Type of route".
- ipRouteProto: "Routing mechanism via which this route was learned".

The ipRouteType is an integer value with the following translation table:

- 1: other
- 2: invalid
- 3: direct
- 4: indirect

The ITK will store the actual integer value for each route and append the string value when it reconciles the routes as links in netTerrain.

The ipRouteProto is an integer value with the following translation table:

- 1: other
- 2: local
- 3: netmgmt
- 4: icmp
- 5: egp
- 6: ggp
- 7: hello
- 8: rip
- 9: is-is
- 10: es-is
- 11: ciscolgrp
- 12: bbnSpflgp
- 13: ospf
- 14: bgp

The ITK will store the actual integer value for each route ipRouteProto and append the string value when it reconciles the routes as links in netTerrain.

7.2.2 Configuring SNMP parameters

The first step in configuring the Native SNMP discovery engine is to set up some basic parameters. To access the SNMP configuration, go to Settings->Monitoring-> SNMP-> Configuration (or ctrl-G -> SNMP tab).

Monitoring Configuration
General Parameters SNMP WMI DCM AWS
Discovery features
☑ Discover Ports
Layer 3 Links
☑ Discover Links
Create Generic Nodes for External IPs
Layer 2 Links
Discover Links
Create Generic Nodes for External MACs
Status
☑ Up/Down Status
✓ 1: Ping ✓ 2: SysName Get
Cancel

SNMP configuration

The SNMP discovery features control the granularity of the information you will be retrieving from the network.

When the 'Discover Ports' option is checked, the ITK will scan all interfaces associated with a discovered device. In the next section we will review how we can control which properties can be scanned for a specific IP address or range.

When the 'Discover Links' for Layer 3 option is checked, the ITK will scan IP address tables and routing tables for the managed device to determine what routes were configured for that particular device. netTerrain will then display these routes as links between that device and the endpoints.

In addition, when this option is checked, the 'Create generic nodes for external IPs' will be enabled. If this is also checked, netTerrain will automatically create generic nodes for any IP addresses that exist in the routing tables, which are not part of the registered IP address (i.e. not directly discoverable via SNMP).

When the 'Discover Links' for Layer 2 option is checked, the ITK will scan the MAC address tables and bridging tables for the managed device to determine what layer 2 links were configured for that particular device. netTerrain will then display these links as lines between that device and the endpoints.

In addition, when this option is checked, the 'Create generic nodes for external MACs' will be enabled. If this is also checked, netTerrain will automatically create generic nodes for any MAC addresses that exist in the bridging tables, which are not part of the registered MAC address tables of any discovered device (i.e. not directly discoverable via SNMP).

Finally, the status group lets you set up the real time status monitoring option for devices. When the 'Up/ down status' option is checked, the ITK will update the status of an existing device using two methods:

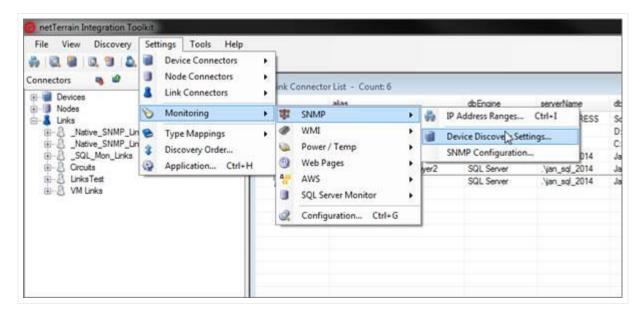
- Ping
- SNMP device name get

We will review the live status options later in this chapter.

7.2.3 SNMP device connector settings

In many ways, the Native SNMP discovery behaves like any other device connector, with the difference being that the source is the SNMP discovery process itself and the connector has been built in advance.

Most of the parameters in the Native SNMP connector settings are not editable, but still, you can edit some of the connector settings to better suit your discovery needs. To open the SNMP connector settings, go to Settings->Monitoring->SNMP->Device Discovery Settings...



SNMP Connector settings

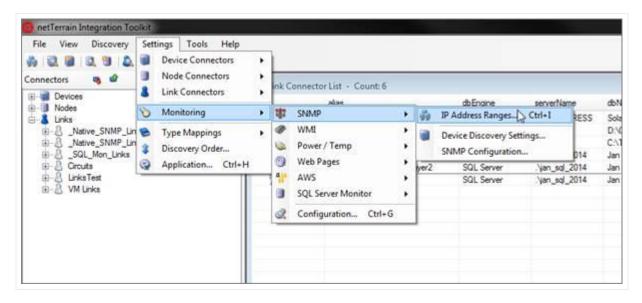
The editable parameters include:

- Default diagram to place newly discovered objects.
- Parent locator field (only sysLocation and sysContact can be used here).
- All reconciliation tab parameters.

7.2.4 Configuring SNMP: IP address manager

To discover network devices using the Native SNMP we need to specify which individual IP addresses should be scanned and the parameters and discovery settings associated with each. This is done through the IP address manager tool.

Start by clicking on Settings->Monitoring-> SNMP->IP Address Ranges (or Ctrl-I) to open the IP address manager dialog.



Setting up IP address ranges

The IP address ranges window will provide the user with an entry form for adding any number of Class-C IP address ranges or individual IP addresses (essentially with a range of 1 address).

IP Address List 10.1.0.1 - 1 10.1.0.2 - 2 10.5.0.5 - 5 10.5.0.6 - 6 10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.1 - 1 192.168.0.2 - 2 192.168.0.3 - 3 192.168.0.50 - 50 192.168.0.57 - 77	IP Addresses Configuration Settings Community UDP Port 161 Version v2c v Enabled v Custom MiBS	Edit IP Address Range From To Class: C • Load IP Addresses from txt File
192.168.0.222 - 222 192.168.0.224 - 224 192.168.0.228 - 228 192.168.1.1 - 1 192.168.1.12 - 12 192.168.1.14 - 14 192.168.1.16 - 16 192.168.1.21 - 21 192.168.1.21 - 21 192.168.1.48 - 48	Pot Monitoring Enabled if Descr if PhysAddress if AdminStatus if Type if Speed if LastChange if OperStatus	Submit List
To csv		Apply

IP address manager dialog

IP addresses can be entered manually from the top right section of the dialog or they can be uploaded from a text file using the 'Upload' button.

7.2.4.1 Manual IP address entry

When you enter an IP address range manually, the manager will enable or disable each octet based on the entered values. The manager also checks for addressing consistency, thus avoiding malformed addresses. Once each octet in the 'From' and 'To' row has been entered you can click on the 'Submit' button to save the

address. The settings and port monitoring that apply to the address are controlled in the middle sections of the dialog. These settings include:

- Community string: the default value is public and with the 'T' / '*' button you can view the string in clear text or with password characters.
- Port: the UDP port number the SNMP agent listens to (the default is 161).
- SNMP version, which can be v1, v2c or v3.
- Enabled status: determines whether that address or range is enabled for discovery.
- Port monitoring enabled status: determines whether port monitoring is enabled for that address or range.
- Port monitoring MIBs: determines which MIBs should be discovered for that IP address or range.

Attention!

All IP addresses in the same range will share the same community string and port. If for a given range two or more IP addresses must use different settings, you must create two or more ranges.

7.2.4.2 Setting devices with SNMPv3

For devices that need to be discovered with SNMPv3, follow these simple steps:

- 1) First select that version from the drop-down box
- 2) Notice a key button appearing next to the version box

3) After clicking on that key button, fill out the SNMPv3 security credentials for that particular IP address range

IP Addresses Configuration Settings Community UDP Pot 161 Version v3 V	Edit IP Address Pange From 152 168 0 8 T_n 152 158 0 8 SNMPv3 Credentials 23
Enabled Custom MIBS. Pot Montoring Enabled Control Montoring Finabled Filemar Filemar	Main Settings Flags Auth OFF / Encrypt OFF V3 User Auth-Intraston Auth Nethod O: MD5 @ SHA. Painword Encryption Enccyption Enccyption Encryption Encryption Encrypti

SNMPv3 security credentials form

SNMP version 3 provides additional security features compared to SNMPv1 and v2s, which only provide a community string parameter:

- A user identifier
- Authentication of the user who sent the PDU. The authentication protocols include SHA and MD5.
- Encryption of protocol data units (PDUs) to prevent unauthorized users from viewing the contents. SNMPv3 supports AES and DES for encryption.
- A context string parameter

As with SNMPv1 and v2c, each IP address or range can have its own SNMPv3 parameters.

Depending on the security settings for the range in question, you can set the flags that define which security features are needed.

7.2.4.3 Uploading IP addresses from a text file

The IP address manager tool has a utility to upload IP addresses straight from a text file. First, check the text file to make sure that there is one IP address per line. If any IP address is malformed or falls outside the range of a valid IP address it will not be loaded. Do not append or prepend any characters to the IP addresses, otherwise they will be discarded.

File	Edit	Format	View	Help	
192. 192. 192. 192. 192. 192.		0.2 0.3 0.4 0.5 0.6			*
4					

Sample IP address txt file

After you uploaded the IP addresses, the preview window will show which IP addresses were parsed correctly, as shown below:

P Address List	IP Addresses Configuration	
10.1.0.1 - 1 10.1.0.2 - 2	Settings Community	Edit IP Address Range From 192 168 0 1
10.5.0.5 - 5 10.5.0.6 - 6 10.5.0.9 - 9	UDP Port 161	To 192 168 0 1
10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.1 - 1	Version 🔽 🔹	Class: C 💌
192.168.0.2 - 2 192.168.0.3 - 3 192.168.0.50 - 50	Enabled Custom MIBS	Load IP Addresses from bit File
192.168.0.77 - 77 192.168.0.222 - 222	Port Monitoring	Upload
192.168.0.224 - 224 192.168.0.228 - 228 192.168.1.1 - 1	Enabled	192.168.0.1
192 168 1 12 - 12 192 168 1 14 - 14 192 168 1 14 - 14 192 168 1 16 - 16 192 168 1 18 - 18 192 168 1 21 - 21 192 168 1 48 - 48	 ✓ fDescr ✓ fPhysAddress ✓ fAdminStatus ✓ fType ✓ fSpeed ✓ fLastChange 	192.168.0.3 192.168.0.4 192.168.0.5 192.168.0.7 192.168.0.7 192.168.0.77 192.168.0.77 10.0.0.100 10.0.0.101
X I I I	IfOperStatus	Submit List
To csv		Apply

Parsed IP addresses from txt upload (bottom right)

Once you hit 'Submit list', the addresses will be loaded in the system using the IP address configuration settings in the middle section and displayed in the leftmost IP address list.

Attention!

All IP addresses in the parsed list (bottom right) will share the same community string and port defined in the settings. If for a given list two or more IP address should use different settings, you must add them in two or more upload steps, changing the settings in between.

Also, you cannot have two identical IP address ranges in the system, but it is possible to configure lists with overlapping IP addresses, which will cause redundant network scans.

7.2.4.4 Editing the settings of an IP address

To edit an IP address (or range) simply click on the entry on the IP address list and edit the settings in the middle section (community, UDP port, port settings, etc.). Note that to submit changes, you must then press on the 'Apply' button. As part of the editing process you can also change the address range itself.

10.1.0.1 - 1 10.1.0.2 - 2 10.5.0.5 - 5 10.5.0.6 - 6 10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.1 - 1 192.168.0.2 - 2 192.168.0.50 - 50 192.168.0.222 - 222 192.168.0.222 - 222 192.168.0.222 - 222 192.168.0.228 - 228 192.168.0.228 - 228 192.168.1.12 - 12 192.168.1.16 - 16 192.168.1.21 - 21 192.168.1.21 - 21 192.168.1.48 - 48	Settings Community	Edit IP Address Range From 192 168 1 12 To 192 168 1 12 Class: C • Load IP Addresses from bt File Upload Submit List
---	-----------------------	--

Editing an IP address (from left to right): select it, change the settings, and apply

7.2.4.5 Adding and removing addresses

To add a new IP address range, simply click on the 'New' button and this will clear the last octet values and port settings so that you can enter a new range. Of course, you can also add new IP addresses from a text file with the 'Upload' functionality.

Address List	IP Addresses Configuration	
Address List 10.1.0.1 - 1 10.1.0.2 - 2 10.5.0.5 - 5 10.5.0.6 - 6 10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.2 - 2 192.168.0.3 - 3 192.168.0.22 - 222 192.168.0.224 - 224 192.168.0.228 - 228 192.168.0.228 - 228 192.168.1.1 - 1 192.168.1.12 - 12 192.168.1.14 - 14 192.168.1.18 - 16 192.168.1.21 - 21 192.168.1.21 - 21 192.168.1.48 - 48	IP Addresses Configuration Settings Community UDP Port 161 Version V3 • ♠ Enabled Custom MIBS Port Monitoring V Enabled V Enabled V fDescr V fAdminStatus V fAdminStatus V fSpeed	Edit IP Address Range From 192 , 168 , 0 , 224 To 192 , 168 , 0 , 224 Class: C Load IP Addresses from bt File Upload
To csv	 ✓ ifLastChange ✓ ifOperStatus I new IP address entry 	Submit List

Adding a new IP address entry

To remove IP addresses simply select a range and click on the 'Remove' button. You can also remove all the IP addresses from the list, but be careful, as you cannot undo the removal process.

	IP Addresses Configuration	
10.1.0.1 - 1 10.1.0.2 - 2 10.5.0.5 - 5 10.5.0.6 - 6 10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.1 - 1 192.168.0.2 - 2 192.168.0.50 - 50 192.168.0.50 - 50 192.168.0.224 - 224 192.168.0.228 - 228 192.168.1.1 - 1 192.168.1.1 - 1 192.168.1.2 - 21 192.168.1.4 - 48	IP Addresses Configuration Settings Community UDP Poit 161 Version V3 • • Enabled Custom MIBS Port Monitoring V Enabled V Enabled V FinysAddress V fAdminStatus V fSpeed V fSpeed V fSpeed V fOperStatus	Edt IP Address Range From 192 168 0 221 To 192 168 0 224 Class: C • Load IP Addresses from bt File Upload Submit List

Deleting IP address entries

7.2.4.6 Enabling and disabling addresses

The IP address manager can enable or disable individual IP addresses or ranges. This comes in handy when you want to run a discovery against a smaller set of IP addresses without having to remove the remaining addresses from the list.

P Address List	IP Addresses Configuration	
10.1.0.1 - 1	Settings	Edit IP Address Range
10.1.0.2 - 2 10.5.0.5 - 5 10.5.0.6 - 6	Community T	From 192 168 0 224
10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.1 - 1	Version v3 👻 👟	Class: C •
192.168.0.2 - 2 192.168.0.3 - 3 192.168.0.50 - 50	Enabled Custom MIBS	Load IP Addresses from bit File
132.168.0.77 - 77 192.168.0.72 - 77 192.168.0.222 - 222 192.168.0.224 - 224 192.168.1.1 - 1 192.168.1.1 - 12 192.168.1.1 - 12 192.168.1.1 - 14 192.168.1.1 - 14 192.168.1.1 - 16 192.168.1.18 - 18 192.168.1.21 - 21 192.168.1.48 - 48	Port Monitoring Finabled Fibescr Fib	Upload
	ddresses for discovery	Apply

Enabling and disabling IP addresses from the discovery

7.2.4.7 Outputting a csv report of your IP addresses

The IP address manager has a very useful button to output a report of all the IP addresses. To launch the report, simply click on the 'To csv' button.

Address List	IP Addresses Configuration					
10.1.0.1 - 1	Settings	Edit IP A	ddress	Range		
10.1.0.2 - 2 10.5.0.5 - 5	Community T	From	192	168].[0	. 224
10.5.0.6 - 6 10.5.0.9 - 9	UDP Port 161	То	192	168	0	224
10.5.0.10 - 10	Version 🔽 🔻 🔌	Class:	C •	l.		
192,168.0.2 - 2 192,168.0.3 - 3 192,168.0.50 - 50	Enabled Custom MIBS	Load IP	Addres	ses from	bd File	
192.168.0.77 - 77 192.168.0.222 - 222 192.168.0.224 - 224 192.168.0.228 - 228	Port Monitoring	29			Upi	oad
192.168.1.1 - 1 192.168.1.12 - 12 192.168.1.14 - 14 192.168.1.16 - 16	 Interior filter Interior filter Interior filter 					
192, 168, 1, 18 - 18 192, 168, 1, 21 - 21 192, 168, 1, 48 - 48	 fAdminStatus fType 					
	I fSpeed					
	 ✓ ifLastChange ✓ ifOperStatus 				Subr	mit List
To cay						Apply

Output to csv

This report has a few interesting features:

- It shows every single IP address that was added to the list, not just the ranges themselves.
- It provides a column that shows the last time the ITK discovered a device with that IP address via Native SNMP. This can be useful when trying to determine IP addresses that do not exist on the network or cannot be reached via SNMP.
- It provides a summary of all IP addresses and unreachable IP addresses

Below is a sample csv report opened in Excel:

-	WOIKDOOK VIEWS			311010		
	A249 🔻 (*	f _x	10.0.0.93			
A	A		В	С	D	E
1	IPaddress .	LastDiscov	vered			
2	10.0.0.1	2/	1/2015 21:00			
249	10.0.0.93	2/	1/2015 21:43			
250	10.0.0.94	2/	1/2015 21:44			
251	10.0.0.95	2/	1/2015 21:41			
252	10.0.0.96	2/	1/2015 21:43			
253	10.0.0.99	2/	1/2015 21:46			
256	10.20.1.0					
257	10.20.1.1					
258	10.20.1.2					
259	10.20.1.3					
260	192.168.0.1	2/	1/2015 21:45			
261	192.168.0.2	2/	1/2015 21:47			
262	192.168.0.3	2/	1/2015 21:47			
263	192.168.0.4	2/	1/2015 21:48			
264	192.168.0.5	2/	1/2015 21:43			
265	192.168.0.50	2/	1/2015 21:43			
266	192.168.0.6	2/	1/2015 21:45			
267	192.168.0.7	2/	1/2015 21:47			
268	192.168.0.77	2/	1/2015 21:47			
269	192.168.1.14	2/	1/2015 21:48			
270	192.168.1.16	2/	1/2015 21:45			
271	192.168.1.18	2/	1/2015 21:47			
272	192.168.1.22	2/	1/2015 21:47			
273	192.168.1.24	2/	1/2015 21:48			
274	192.168.1.49	2/	1/2015 21:48			
275	192.168.1.73	2/	1/2015 21:47			
276						
277	Total Ip addresses: 274	Not Disco	vered: 4			
278						

Sample csv IP address report

7.2.4.8 Running a ping sweep for an IP address range

One convenient way of finding out which devices could possibly exist on the network is to configure one or more IP address ranges and then running a 'ping sweep' for each range.

P Address List	IP Addresses Configuration					
10.1.0.1 - 1	Settings	Edit IP A	ddress	Range		
10.1.0.2 - 2 10.5.0.5 - 5	Community I	From	192	168	. 0	. 0
10.5.0.6 - 6 10.5.0.9 - 9	UDP Port 161	То	192	. 168	. 0	. 50
10.5.0.10 - 10 192.168.0.1 - 1	Version v2c •	Class:	C 🕶	ļ.		
192.168.0.1 - 50 192.168.0.2 - 2	Enabled V Custom MIBS	Load IP	Address	ses from	bt File	
192.168.0.3 - 3 192.168.0.50 - 50 192.168.0.77 - 77 192.168.0.222 - 222	Port Monitoring				Upk	ad
192.168.0.224 - 224 192.168.0.228 - 228 192.168.1.1 - 1	Enabled					
192.168.1.12 - 12 192.168.1.14 - 14 192.168.1.16 - 16 192.168.1.18 - 18	#PhysAddress #AdminStatus					
192.168.1.21 - 21 192.168.1.48 - 48	/ #Type					
	fLastChange				Subr	nit List
						Apply
	Ping sweep selected Ip Address / Range				-	

Running a ping sweep for an IP address range

A ping sweep basically executes a couple of pings against each IP address in that range and then stores the response in memory.

IP Address List	IP Addresses Configuration Settings	Edit IP Address Range
10.1.0.1 - 1 10.1.0.2 - 2 10.5.0.5 - 5 10.5.0.6 - 6 10.5.0.9 - 9 10.5.0.10 - 10 192.168.0.1 - 1 192.168.0.1 - 50	Community T UDP Port 161 Version V2C V Enabled V	From 192 168 0 1 To 192 168 0 50 Class: C •
192.168.0.50 - 50	Ping Sweep Progress	Upload
192.168.0.224 - 224 192.168.0.228 - 228 192.168.1.1 - 1 192.168.1.12 - 12 192.168.1.14 - 14	12.168.0.3 Reached!	Stop
192 168.0.224 - 224 192.168.0.228 - 228 192.168.1.1 - 1 192.168.1.12 - 12	☐ #Type ☐ #Speed ☐ #LastOhange ☐ #OperStatus	Stop

Ping sweep progress

Any address that can be pinged is labeled green; otherwise it is labeled in red.

After the range has been scanned, a csv report with the responses is generated by the ITK.

-	Clippoard	FC	ont	tai.		Alig
	B1 ★ (*	fx	PingStat	us		
4	A		В	С	D	E
1	IPaddress	PingSta	atus			
2	192.168.0.1	TF	IUE			
3	192.168.0.2	TF	UE			
4	192.168.0.3	TF	UE			
5	192.168.0.4	FA	LSE			
6	192.168.0.5	FA	LSE			
7	192.168.0.6	FA	LSE			
8	192.168.0.7	FA	LSE			
9	192.168.0.8	FA	LSE			
10	192.168.0.9	FA	LSE			
11	192.168.0.10	FA	LSE			
12	192.168.0.11	FA	LSE			
13	192.168.0.12	FA	LSE			
14	192.168.0.13	FA	LSE			
15	192.168.0.14	FA	LSE			
16	192.168.0.15	FA	LSE			
17						
18	Total Ip addresses tried: 15	Respon	nsive: 3			
19						
20						
21						
22						

Ping sweep response

7.2.5 Mapping device types for native SNMP

As with other device connectors, the ITK uses a type field to match the source device type with the netTerrain catalog type. The native SNMP discovery connector uses the sysOID MIB for that purpose.

The ITK already has a wide list of supported sysOIDs in its database, but most of them are not mapped to a specific type in netTerrain. To filter the mappings for a specific OID, simply type it in the filter box and press 'Enter'.

and the second second second	ppings [filtered by '1.3.6.1.4.1.9.1.104']		1142 10 x 220/W.N	
b	Type Name in Source	Type Name in netTerrain	Data Source	
21878	1.3.6.1.4.1.9.1.104	NO_NAME	Native SNMP	
21134	1.3.6.1.4.1.9.1.1040	NO_NAME	Native SNMP	
19375	1.3.6.1.4.1.9.1.1041	Cieco CISCO3945/K9	Native SNMP	
19376	1.3.6.1.4.1.9.1.1042	Casco CISCO3925/K9	Native SNMP	
19380	1.3.6.1.4.1.9.1.1043	Caco CISCO2951/K9	Native SNMP	
19381	1.3.6.1.4.1.9.1.1044	Caco CISCO2921/K9	Native SNMP	
19382	1.3.6.1.4.1.9.1.1045	Casco CISCO2911/K9	Native SNMP	
20976	1.3.6.1.4.1.9.1.1046	NO_NAME	Native SNMP	
20990	1.3.6 1.4.1.9.1.1047	NO_NAME	Native SNMP	
21220	1.3.6.1.4.1.9.1.1048	NO_NAME	Native SNMP	
21196	1.3.6.1.4.1.9.1.1049	NO_NAME	Native SNMP	
1 20 0	13.61.4.1.9.1.104 I	Page: 84 48 1 1 1 1		

Using the filter text box to find a specific set of OIDs

To clear the filter, click on the 'Clear filter' button next to the text box.

To add a new mapping into the system, click on Settings->Type Mappings->New (or Ctrl-N). A type mapping needs to specify the Name of the type used in the source and the corresponding (exact) name used for the same type in netTerrain.

Attention!

Before adding a new mapping, make sure the OID does not already exist, by running it through the filter. If it exists and it is mapped to 'NO NAME', select the proper netTerrain model this OID should be mapped to (double click on the entry in the list view). In the mapping dialog, make sure the Data Source is 'Native SNMP'.

	Type Mapp	ings [filtered by '1.3.6.1.4.1.9.1.104'] - Count 11			
Devices	d	Type Name in Source		Type Name in netTerrain	Data Source	
Trg	21878	13614191104		NO_NAME	Native SNMP	
Files	21134	1.3 6 1.4 1 9 1 1040		NO_NAME	Native SNMP	
	19375	136141911041		Cieco CI5C03945/K9	Native SNMP	
ħ	19376	1.3.6.1.4.1.9.1.1042		Caco CISCO3925/K9	Native SNMP	
	19380	136141911043		Daco CISC02951/K9	Native SNMP	
	19381	1.36.1.4.1.9.1.1044		Cieco CI5C02921/K9	Native SNMP	
	19382	1.3.6.1.4.1.9.1.1045		Dace CI5C02911/K9	Native SNMP	
4	20070	130141311040		HOJHAND	name 314MP	
	20990	1.3.6.1.4.1.9.1.1047		NO_NAME	Native SNMP	
	21220	1361/19110/8		NO_MAME	Native Child	
te	21196	1.3.6.1.4.1.9.1.1049		NO_NAME	Native SNMP	
			84			-
			(🔅 Type Mapping	12	83
			1	Main		
				52-2		
				id: 20990		
		TTRUE & State of the state of		Name in Source 1.3.6.1.4.1.9.1.1047		
	800	13614191104				
				Name in netTerrain X007W0506150523		
				Data Source Native SNMP		
				AutoAutoAuto		
				()) ()		
				Subm	Cancel	
				Surger State	Carce	
				0.67. 5		
						and the second second

Native SNMP device mapping

Tip:

Before parsing over thousands of OIDs to see which ones are mapped, we recommend running a discovery first, and then configuring any unmapped types directly from the list of gray devices.

7.2.6 Starting the SNMP device discovery

To start the Native SNMP discovery, use the same procedure as with any other connector, by using the Discovery menu or directly from the Native SNMP list, using the discovery button.

File View Discovery Settings Tools Hel	P CA Unicenter				
Connectors Manual Node Discovery Manual Link discovery CAU Cast Cast Cast Cast Cast Cast Cast Cast	Castlerock SNMPc Cisco RME Concord eHealth Microsoft MOM Microsoft SCOM	sysObjectid 1.3.6.1.4.1.9.1.485 1.3.6.1.4.1.9.1.186 1.3.6.1.4.1.9.1.467	sysUpTime 26632316 35915756 35893004	sysContact Stephan Stephan Stephan	sysDescr Cisco IOS Cisco Inte Cisco IOS
Microsoft MOM Microsoft SCOM Visitive SNMP CICS-3550-24-6 LICIS-R-2611/2-3 LICIS-R-2611/XM-24 LICIS-R-2611/XM-24 LICIS-R-2601-2-2 LICIS-S-3550-28-5 LICIS-S-3550-28-5 LICIS-S-3550-28-5 LICIS-S-3550-28-5 SensorGateway	Native SNMP Solarwinds What's Up Gold L-SW-TZ105-4 669 SensorGateway 643	13.6.1.4.1.9.1.619 13.6.1.4.1.9.1.359 13.6.1.4.1.9.1.278 13.6.1.4.1.9.1.278 13.6.1.4.1.9.1.278 13.6.1.4.1.8741.1 13.6.1.4.1.17095	25641230 26641230 26642184 26641175 234790325 251299213	Stephan Jan Fred Stephan Stephan http://www.serve	Cisco IOS Cisco IOS Cisco Inter Disco IOS Cisco Inter SonicWAL Temperatu
B Solarwinds What's Up Gold B - 3 Nodes B - 3 Links	() () () () () () () () () () (Page:	4 44 1

Starting the native SNMP discovery

Once started, the ITK will scan all the IP address ranges that were set up earlier. Note that as opposed to other discovery methods, this connector triggers a communication process with the actual devices and generates SNMP traffic on the network.

The performance of the scanning process depends on which parameters were set up for each IP address. Enabling the port discovery may increase the time spent on each device by an order of magnitude. Errors, such as non-responding hosts or OID problems due to mismatched SNMP versions will be shown in the output window. All SNMP activity is also logged.

den a d	Category and a											Party and the
Devices	uil 160-y 2009 (2)				Statistics of	Search 1						1111.141
Tables	systems		avched at	ayata/Teve	epiContact	esDeud	No. Conception	ant factors	flater	8,A68mm	intGeorged	88.4
LPAS	LIDE-3650-24.8		1341419140		Deter	Geor IOS Safware, C3010 Sall	ONORMAL/AR	1		10.10.28	11/25/2014 12	-
	LOSE2012		1341419140		Sector:	Case International Operating Sea Case KVS Software, C2000 Set.	GNORMUNE GNORMUNE	-		1021003	11/25/2014 12	-
						Case Kit Salvare 2811 Salvas				102108-02	11/25/2014 12	uninces.
		Carpo Manadacon Operating San	Girofortat			10210001	11/25/2014 12	united and				
	10553000		1251410140		14	Case Of Subway, Clifford Sale	ON OTHER LAS			10210027	11/25/2018 U	-
	100500000		1361419127		Sector.	Case International Coversing Sun	ON OTHER LAS			10210605	11/25/2014 12	
	1.081721054		1351412311		Sector	Sincles 17 105 seales hit	Onotice			192 146 0 50	11/28-2014 12	and the second
	Second annual		1351411206		Into Channe Amon	Tangentury & Server Galerow		1000		182 182 0 77	T1/16/2014 3.2	
	* Instantion in the											2
	0 2 4 3	1 1 1			Page 1	4 46 5 10 14						
						7. TT. C						
	11.29/2014 12:00:42 PM 11.09/2014 12:00:42 PM 11.09/2014 12:00:42 PM 11.09/2014 12:00:42 PM 11.09/2014 12:00:42 PM 11.09/2014 12:00:42 PM 11.09/2014 12:00:42 PM	1000 100 100 100 100 100 100 100 100 10	for IP address TIC 14 for IP address TIC 10 for avjaten L C/5 S 20 for IP address TIC 10 for IP address TIC 10 for IP address TIC 10	20.7 retrieved the 10-24-7 and post 26 25.7 esterwed the 0.3.7 esterwed the 0.3.7 esterwed the	408 Antonit Nati 42MINT298							
	11 (0)(2014) 47 (0) 42 (0)(4) 11 (0)(2014) 47 (0)(4) (0)(4) 11 (0)(1)(1)(1)(1)(1)(1)(1)(1)(DADP of Shall out Shall out Sh	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	2017 retenued the Color Part and Sector 2018 2017 retenued the 2017 retenued the 2018 ret of 2018 retenued the 2018 retenued the	4038 %400 %40 403406/0288 1 1 1 1 1 1 1 1 1 1 1 1 1	allemat halo bacasaan hel soviensite megand hi Simaj Magaandi	d under det met					

Running the Native SNMP discovery

Just like with other device connectors, the discovery has so far just pulled the data from the network into a raw table in the ITK, but it is not yet in netTerrain. From here on, the Native SNMP behaves pretty much like any other device connector. For convenience we will review the process in the upcoming sections.

To import devices into netTerrain, we need to reconcile the discovered items with the netTerrain database. This reconciliation process includes the insert, update and/or delete of devices from the discovered devices into netTerrain (depending on the rules specified in the Native SNMP connector mapping settings).

7.2.7 Viewing discovered device details

After the device discovery is completed, the Native SNMP list is populated with all the devices that were found on the network. The same color coding used for device connectors is utilized for the Native SNMP connector. Hence, each device can be in four possible states:

1) The same device also exists in netTerrain and it was discovered and reconciled into netTerrain by the Native SNMP connector. Such devices have a lime fill color, as shown below.

				-
S2A7	1.3.6.1.4.1.9.1.516	Silver Spring	192.168.7.11	Primary

2) The same device also exists in netTerrain, but it was created manually or it was discovered and reconciled with netTerrain by a different connector. Such devices have a green fill color, as shown below.

		S3A1	1.3.6.1.4.1.9.1.516	Baltimore	192.168.7.12	Primary
--	--	------	---------------------	-----------	--------------	---------

3) The device in the connector table is currently not in netTerrain but the type has been mapped so that a reconciliation process (barring any parent issues) would create it in netTerrain. Such devices have a plain white fill color, as shown below.

S3A2	12014101510	Ellisatt Cha	103 100 7 13	Defense	
33MZ	1.3.6.1.4.1.9.1.516	Ellicott City	192.168.7.13	Primary	

4) The device in the connector table is currently not in netTerrain and the type has not been mapped, so a reconciliation process would create a generic device type in netTerrain (or yield an import error if the 'Use generic devices for unmatched types' application setting is unchecked). Such devices have a gray fill color, as shown below. Note that after a reconciliation process, any grey devices that do indeed trigger the creation of a generic device would now exist in netTerrain and displayed in lime.

S3A7	1.3.6.1.4.1.9.1.797	Ellicott City	192.168.7.188	Primary	
------	---------------------	---------------	---------------	---------	--

Also, like the device connector cousins, the Native SNMP discovery provides a detailed view of each device when you double click on a specific entry in the Native SNMP device list.

7.2.8 Previewing a reconcilation process

Just like with regular device connectors, before importing and reconciling the data into netTerrain you should run a preview task. This will provide some insight into which devices will be inserted, updated or deleted. It will also provide a snapshot of devices that cannot be reconciled because no types have been mapped. The latter information can be used to add types to netTerrain or map existing netTerrain types with the device sysOID.

Eile View Discovery Settings Iools Help						
Connectors 🧠 🦉	Native SNMP (9)					
Devices CA Unicenter	sysName	id	sysObjectId	sysUpTime	sysContact	sysDes
Castlerock SNMPc	L-CIS-3550-24-6	688	13614191485	34400028	Stephan	Cisco I
- Geco RME	L-CIS-R-2611-2-3	684	1.3.6.1.4.1.9.1.186	43683556	Stephan	Cisco I
Concord eHealth	L-CIS-R-2611XM	685	1.3.6.1.4.1.9.1.467	43660696	Stephan	Cisco
- Microsoft MOM	L-CIS-R-2801-2-2	683	1.3.6.1.4.1.9.1.619	43683850	Stephan	Caco I
- Microsoft SCOM	L-CIS-S-2950-26-1	682	1.3.6.1.4.1.9.1.359	34408984	Jan	Cisco I
Native SNMP	L-CIS-S-3550-24-7	689	1.3.6.1.4.1.9.1.485	34409854	Fred	Caco I
🔅 🛄 Solarwinds	L-CIS-S-3550-48-5	686	1.3.6.1.4.1.9.1.278	34408898	Stephan	Cisco I
- What's Up Gold	L-SW-TZ105-4	687	1.3.6.1.4.1.8741.1	242557810	Stephan	Sonic
Inces Inces	SensorGateway	690	1.3.6.1.4.1.17095	13957	http://www.serve	Tempe
	i - 200 2		3 🖬 🖶 🚳		Page:	4 44
	1/25/2014 2:02 1 Preview 1/25/2014 2:02 15 Preview 1/25/2014 2:02 15 PM S 1/25/2014 2:02 15 PM S 1/25/2014 2:02 15 PM S 1/25/2014 2:02 15 PM S	NMP get NMP get NMP get	for IP address 192.168. for IP address 192.168. for IP address 192.168. for IP address 192.168.	0.7 retrieved this: 4 0.7 retrieved this: 0.7 retrieved this: 1 0.7 retrieved this: 1	294967295	

Previewing the reconciliation

The output window will display the expected operations and records affected by a reconciliation process.

The insert operations (the 'Insert New Nodes' option in the reconciliation section of the SNMP connector must be enabled) include:

- Records without a matching type in netTerrain: these are all the devices for which no source type information (make and model) has been matched with a type in netTerrain. In the event of a reconciliation, these records would skip the insert process.
- Records that are expected to be successfully inserted.
- Records with a missing parent in netTerrain: in case the SNMP connector uses a parent field to find the container diagram in netTerrain, any devices for which such parent cannot be matched with a diagram of the same name in netTerrain will also skip the insert process.
- Records with multiple parents in netTerrain: in case the SNMP connector uses a parent field to find the container diagram in netTerrain, any devices for which a parent value is matched with more than one diagram of the same name in netTerrain will skip the insert process. In other words, use unique names otherwise netTerrain doesn't know which parent to choose from.

The update operations (the 'Update Existing Nodes' option in the reconciliation section of the SNMP connector must be enabled) include:

• Records to be updated: any records for which one or more field values have changed will be updated in netTerrain once reconciled. Notice that the output will display one entry for each field that has a change. For example, if a certain device has three changes in three fields, then the output will display three entries.

The delete operations (the 'Delete Existing Nodes' option in the reconciliation section of the SNMP connector must be enabled) include:

• Records to be deleted: any records that were inserted by that same connector in netTerrain in some previous operation, which are no longer in the source database will be deleted in the event of a reconciliation.

7.2.9 Reconciling SNMP devices with netTerrain

Once you are ready to reconcile the data into netTerrain you can start the process by simply opening the list view for the Native SNMP connector and clicking on the 'reconcile' button.

A button for triggering a discovery immediately followed by a reconciliation is also available (next to the reconcile button).

Connectors 🧠 🖉	Native SNMP (9)			
E- Bevices	sysName	id	sysObjectId	sysUpTime
Castlerock SNMPc	L-CIS-3550-24-6	688	1.3.6.1.4.1.9.1.485	34400028
- Gaco RME	L-CIS-R-2611-2-3	684	1.3.6.1.4.1.9.1.186	43683556
Concord eHealth	L-CIS-R-2611XM	685	1.3.6.1.4.1.9.1.467	43660696
- Mcrosoft MOM	L-CIS-R-2801-2-2	683	1.3.6.1.4.1.9.1.619	43683850
- Mcrosoft SCOM	L-CIS-S-2950-26-1	682	1.3.6.1.4.1.9.1.359	34408984
Native SNMP	L-CIS-S-3550-24-7	689	1.3.6.1.4.1.9.1.485	34409854
Solarwinds	L-CIS-S-3550-48-5	686	1.3.6.1.4.1.9.1.278	34408898
- What's Up Gold	L-SW-TZ105-4	687	1.3.6.1.4.1.8741.1	242557810
R-13 Nodes	SensorGateway	690	1.3.6.1.4.1.17095	13957
	11/25/2014 2:02:14 P Recco 11/25/2014 2:02:15 Premi	1		0.7 metrievend this: 1

Reconciling data with netTerrain

Once the reconciliation starts, the ITK will display the same output displayed for the preview, with the actual devices being inserted, updated and /or deleted.

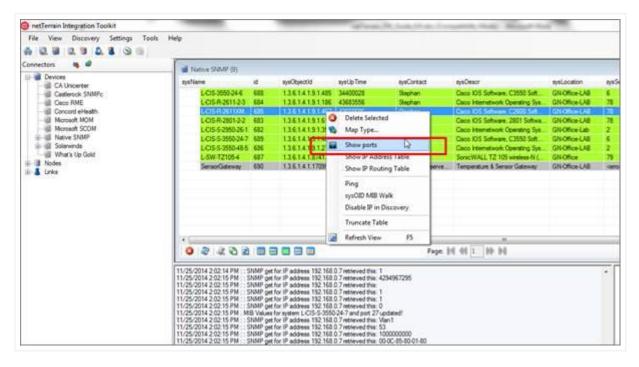
If port monitoring is enabled, then the ITK will also try to reconcile the ports discovered via SNMP with the port definitions that exist for the parent device type in the netTerrain catalog. For this to work correctly, port mappings need to exist for each device type. We will review this later in this chapter.

Attention!

Before adding a new mapping, make sure the OID does not exist, by running it through the filter. If it exists and it is mapped to 'NO NAME', select the proper netTerrain model this OID should be mapped to (double click on the entry in the list view). From the mapping dialog make sure the Data Source is set to 'Native SNMP'.

7.2.10 Viewing ports

If the port discovery is enabled, a 'Show ports' context menu is available for any devices with discovered interfaces.



Show ports option

Any devices that have no discovered interfaces will have the 'Show ports' option disabled. When you click on the 'Show ports' menu a new list view will display all the ports associated with that particular device.

A C B C P C B C C	ools Help										
onnectori 🖷 📽	Lan	of List - Court B									
E Ch Univerter			frides	perchane	(Descr	17,04	Figured	#Phys.Address	Advertises	Kipeline.	f.arCarpt
all Catterock ShMPo		223-83012212	1.0	106430533	Fairfrang/0/5	and a fundamental of	100 50000000	SCALST-MATCH.	and the second second	1.00	340940
III Ceco RIFE		LOS-R-38013-2-2	2	LOSR38122		stand and		ICAA6186-TOCT	direct.	down;	4528
Concord #Health		LOS#380132-3	(0)	LCIS-R2801-22		jacaPointToPoint.	128.000000 Vbps			down .	5171
III Microeft MOM		LOS-H380132:4	4	14054930192	Serat0/1/1	amphone lufum.	128.00000 4bys		dowi	down:	4003
III III Native Story		CONTRACTOR N		105428122	CONTRACTOR OF	100	4214 36125500		100	-	100
What's Le Cold					A PERSON		ACK #1700				
Links		1-CE-R-2801-2-2		Page 24 -01 1	PP 24						
	11/25/2 11/25/2 11/25/2	Charfibe Startering Start Startering Start Startering Start Startering Start Startering Start Startering Start Startering Start	es for avitars L.C.	192 142 3 7 estenved the 192 142 3 7 estenved the 192 142 5 7 estenved the 192 142 5 7 estenves the 193 142 5 7 estenves the	and and			-			

Port list

Ports displayed in green have an ifOperStatus value 'up', whereas the pink ones have a status value 'down'.

Notice that the port list is really a filtered list, with the filter value being the parent device. You can clear the filter, which would then reload the view with all the interfaces for all devices discovered in the system. We recommend working with the filters, because you may have thousands of ports in the system, which would clutter the view. Now if you happen to be looking at an unfiltered view, you can see only ports belonging to a specific parent by right clicking on any port belonging to that parent device and selecting the 'Filter by parent' option.

l id		findex	parentName	fDescr
14		THORK		
	L-CIS-R-2801-2-2 1		L-CIS-R-2801-2-2	FastEthemet
	L-CIS-R-2611XM-2-4 = 1	4.	L-CIS-R-2611X	FastEthemet
	L-SW-TZ105-4 :: 1	a	L-SW-TZ105-4	X0 (LAN)
	L-CIS-S-3550-48-5 = 1	- A	L-CIS-S-3550-48-5	VLAN1
	L-CIS-S-3550-24-7 :: 1	1	L-CIS-S-3550-24-7	FastEthemet
	L-CIS-S-2950-26-1 :: 1	1	L-CIS-S-2950-26-1	FastEthemeti
	L-CIS-R-2611-2-3 :: 1	1	L-CIS-R-2611-2-3	Ethemet0/0
	L-CIS-3550-24-6 = 1	1	L-CIS-3550-24-6	FastEthemet
	L-CIS-R-2611XM-24-2	2	L-CIS-R-2611X	FastBhemet
	L-CIS-S-2950-26-	Map Ports	L-CIS-S-2950-26-1	FastEthemet
	L-CIS-R-2611-2-3	Filter By Parent	L-CIS-R-2611-2-3	Senal0/0
	L-CIS-S-3550-24-7	Enter by Laterit B	L-CIS-S-3550-24-7	FastEthemet(
	L-CIS-R-2801-2-2 :: 2	2	L-CIS-R-2801-2-2	FastEthernet
	L-CIS-S-3550-48-5 2	2	L-CIS-S-3550-48-5	FastEthemet
	L-SW-TZ105-4 2	2	L.SW-T2105-4	X1 (WAN)

Filtering ports by parent

If you double click on a port, a detailed pop-up window with all port attributes will be displayed.

Attention!

The discovery process for ports may bring in a lot of undesired objects, such as NULL interfaces or VLANs. These objects may clutter the ITK interface but will not be imported into netTerrain unless they are somehow mapped with actual ports from the netTerrain catalog (see below).

7.2.11 Mapping port types

As mentioned before, if port monitoring is enabled, then every time a device reconciliation process occurs the ITK will also try to reconcile the ports discovered via SNMP with the port definitions that exist for the parent device type in the netTerrain catalog. For this to work correctly, port mappings need to exist for each device type.

Let's try to understand this with an example. Imagine we discover a router with 4 ports on the motherboard. Usually the interface indexes (ifIndex) for ports are 1-based sequential integers. In our example, each port would be numbered from 1 through 4. But that same router may have its ports named eth1, eth2, eth3 and eth4 in the netTerrain catalog model. To correctly match each discovered port with its corresponding graphical representation in netTerrain we need to first set the "port mapping" for that device type.

The port mapping process is typically done before discovering anything, but it can be easier to first run a discovery and reconciliation process and then compare the MIB interface numbering with the device model generated in netTerrain. Once the mapping is done, we can rerun the reconciliation again. Just like with any other modeling or mapping process, this is a one-time task.

The port mapping can be accessed from a couple of different places. We can map the ports from the type mapping dialog, as displayed below:

id:	22		
Name in Source	1.3.6.1.4.1.9.1.485		
Name in netTerrain	Cisco WS-C3550-24-SMI		Find
Data Source	Native SNMP	•	

Accessing port mappings from the type mapping dialog

We can also access the port mapping by right clicking on any port that belongs to a certain device type.

 Port List - Count S				
d	findex	parentName	fDescr	fTy
LCIS-R-2611-2-3 :: 1	1	L-CIS-R-2611-2-3	Ethernet0/0	ethe
L-CIS-R-2611-2-3 :: 2	2	L-CIS-R-2611-2-3	Serial0/0	prog
L-CIS-R-2611-2-3 ::: 3		L-CIS-R-2611-2-3	Ehemet0/1	10070
L-CIS-R-2611-2-3 :: 4	4	L-CIS-R-2611-2-3	Serial0/1	prog
LCIS-R2611/23=5		ep Ports	Nul0	oth
(m) L-CIS-R-2611-2-3		Page 14 44 1		

Accessing port mappings from the port view

The port mapping dialog displays a column with the ifIndex values per their MIB definition, another column with the port names in the mapped netTerrain device type and a list with the current mappings.

evice Model				
In Source		In netTerrain		
1.3.6.1.4.1.9.	1.485	Cisco WS-C355	0-24-SMI	View Model
ort Mapping				
ifIndex (Src)	Port # in net Terrain (Catalog	Mapping	
1 • 1 2 · E 4 · 5 6 · 7 8 · 9 10 · 11 12 · 13 14 · 15 16 · 17 18 · 19 20 · 21 22 · 23 24 · ·	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24			
P	P 🕑 📀			

Port mapping dialog

The port mapping dialog has many ways to speed up the mapping process, but at its simplest:

- Select one or more ports from the left column.
- Select the same amount of ports from the right column.
- Click on the single arrow button and you are done.

As you map ports, the utilized ones are removed from the left and right columns, to avoid repeated mapped ports.

At this point it may become clear that the selected ports on the left and on the right are mapped in ascending order. The order that is used for the columns on the left or on the right can be reverted to

descending. That way, the first selected port on the left is mapped to the last one on the right and so on. The right column has the following sorting features:

- Sort ports in ascending order.
- Sort ports in descending order.
- Sort ports by horizontal position on backplane (as visually modeled in the netTerrain catalog).
- Sort ports by vertical position on backplane (as visually modeled in the netTerrain catalog).
- reverse sort order.

With all these combinations of sorting, you may be able to order the ports on the left and on the right in such a way that the sequence in both columns only requires one mapping step. If you want to map all the ports from the left and/or the right column (and the sequence is correct) you can also use the double arrow. This will create n mappings, where n is the number of ports on the left column or the right column (whichever is lower).

evice Model				
In Source		In netTerrain		-
1.3.6.1.4.1.9.1	.485	Cisco WS-C3	550-24-SMI	View Mode
nt Mapping				
findex (Src)	Port # in net Terrai	in Catalog	Mapping	
28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 445 446 47 48 95 51 *			$1 \Rightarrow 1$ $2 \Rightarrow 2$ $3 \Rightarrow 3$ $4 \Rightarrow 4$ $5 \Rightarrow 5$ $6 \Rightarrow 6$ $7 \Rightarrow 7$ $8 \Rightarrow 8$ $9 \Rightarrow 9$ $10 \Rightarrow 10$ $11 \Rightarrow 11$ $12 \Rightarrow 12$ $13 \Rightarrow 13$ $14 \Rightarrow 14$ $15 \Rightarrow 15$ $16 \Rightarrow 16$ $17 \Rightarrow 17$ $18 \Rightarrow 18$ $19 \Rightarrow 19$ $20 \Rightarrow 20$ $21 \Rightarrow 21$ $22 \Rightarrow 22$ $23 \Rightarrow 23$ $24 \Rightarrow 24$	E
\$	P 🐉 🔮	2 🚱] 🔳 🙆

Port mapping using the double arrow button

To remove a mapping from the list, simply select the desired mapping and hit the 'Delete selected mapping' button on the lower right corner of the dialog. The two buttons on the left of the delete button can be used to deselect, or select all mappings, in case you need to operate on the whole set without having to click on each mapping.

Attention!

The counts on the left and right column are most likely not going to match. For example, the SNMP discovery may bring in VLANs, which most likely will not match a netTerrain port (unless these are also modeled for the device type). Don't worry; during the mapping process the ITK will only map as many ports as the lesser of the two counts.

7.2.12 Viewing ports in netTerrain

Ports in netTerrain are never inserted or deleted, as they are part of the device (or card) definition. As such, the reconciliation process for ports in the ITK is automatic: the user does not have to reconcile ports specifically; it is done in conjunction with the reconciliation of the parent devices if port monitoring is enabled. Also, the reconciliation process for ports only involves updates (again, ports cannot be inserted or deleted). If the port monitoring is disabled, the actual physical ports for each device will still exist in netTerrain! They will just not contain any updated values coming from an SNMP discovery.

As we know, ports only reside in the backplane of an equipment or card. Once reconciled, ports in netTerrain will contain the latest SNMP discovered values as part of their properties, assuming the catalog port object includes the MIB properties.

The screenshot of the device backplane below shows ports with status colors. We are taking advantage of the ifOperStatus MIB values and configured a visual override so that when the status value is up, the port is green, and when it is down, the port is red.

		ISISISIE	12000 7.930		Catalyst 2950 1 Vitimet 1 4 Catalyst 2050 Catalyst 2950 Catalyst 2950 Cataly	
•	Automa 166-1274s 8 dia 200 automa 80 Automa 10 Automa 10 Automa	Manual Active Ac	•		LIGE NOG	٠

Device backplane view after a device reconciliation with port discovery enabled

In sum: to bring in port information via SNMP, you need the following:

- Port monitoring enabled in Global Settings.
- Port monitoring parameters enabled for the device IP address range.
- Port numbers mapped for the parent device type.

7.2.13 SNMP link discovery

The ITK Native SNMP engine can discover IP address tables and routing tables, which can be used to represent layer 3 links in netTerrain. For every device that has n routes to n destination IP addresses the ITK will create n links.

The ITK can also discover layer 2 links by discovering MAC address tables and bridging tables, which can be used to represent layer 2 links in netTerrain.

For the link discovery to work, we first need to enable our configuration options in the appropriate configuration section (ctrl-g->SNMP). You can have layer 3 enabled and layer 2 disabled or vice versa if you prefer.

Monitoring Configuration
General Parameters SNMP WMI DCM AWS
Discovery features
✓ Discover Ports
Layer 3 Links
✓ Discover Links
Create Generic Nodes for External IPs
Layer 2 Links
Discover Links
Create Generic Nodes for External MACs
Status
Up/Down Status
✓ 1: Ping ✓ 2: SysName Get
Cancel OK

SNMP link discovery configuration

Just like with any other method for automatically bringing in links into netTerrain from an external source, the layer 2 and layer 3 link discovery processes require active link connectors to import data into netTerrain. The good news is that you don't need to know how to create them since the ITK creates these connectors automatically when you enable the layer 2 or layer 3 link discovery options.

Monitoring Configuration	<u>a</u>
General Parameters SNMP WMI DCM	AWS
Discovery features	
Discover Ports	
Laver 3 Links	
C Discover Links	
Create Generic Nodes for Edemal	IPs .
Layer 2 Links	
Discover Links	
Create Generic Nodes for Ex	
Status	
Vp/Down Status	Wh-oh, we couldn't find the _Native_SNMP_Links connector. By default, we use this link connector to map the discovered links to
	netTerrain.
V 1: Ping V 2: SysName	Not to worry, my friend, we can create it for you! Is that OK?
	OK Cancel
Cancel	

Automatic SNMP layer 3 link connector creation dialog

Click on the 'OK' button if you haven't already created the connector beforehand.

If you choose to have the ITK create the SNMP link connectors for you, the application restarts, the link connectors are registered and displayed in the link connectors view using the default name ('Native_SNMP_Links' for layer 3 and 'Native_SNMP_Links_Layer2' for layer 2).

lastReconciled 7/9/2015 5:02:
7/9/2015 5:02
9/16/2015 11.0
AND COMPANY

ITK generated SNMP link connector

7.2.13.1 Discovering Layer 3 link data

From a networking perspective layer 3 links are usually routes between routers and layer 2 links are links between switches. In the SNMP configuration section, when the 'Layer 3 links' option is checked, the 'Create generic nodes for external IPs' will also be enabled. If you check this option for the first time, then the ITK will show you the following message:

General Parameters SNMP WMI DCM AWS Discovery features	
Discover Ports	
LEVEL 3 LEVES	
V Discover Links	
Croce Generic Nodes for External IPs	
Layer 2 Links	
Discover Links	
Create Generic Nodes for Eder	<u> </u>
Status	
Up/Down Status Hmm, apparently the connector to map External IP devices wasn't creat	ted.
V 1: Ping Z 2: SysName Ge No worries, we'll create it for you (app will restart).	
(Mar. 17.1.172) Mar. (19.172) 17.17	
	ок

Enabling the Native SNMP_External_IPs connector

What's happening here? Very simple, external IPs are reconciled in netTerrain using a bread and butter node connector, but instead of you having to figure out how to create it, the ITK can do it automatically. A new connector called 'Native SNMP_External_IPs' is created and mapped to the node type 'Node' in netTerrain.

Later, when you discover layer 3 links, netTerrain will also automatically create generic nodes for any IP addresses that exist in the routing tables, which are not part of the registered IP address (i.e. not directly discoverable via SNMP).

7.2.13.2 Running the layer 3 link discovery and reconciliation

With the layer 3 link discovery enabled and the layer 3 link connector created we can now discover and reconcile these links in netTerrain. The link discovery is triggered automatically as soon as you start the SNMP discovery, so there are no extra steps involved, but if during the configuration process you checked

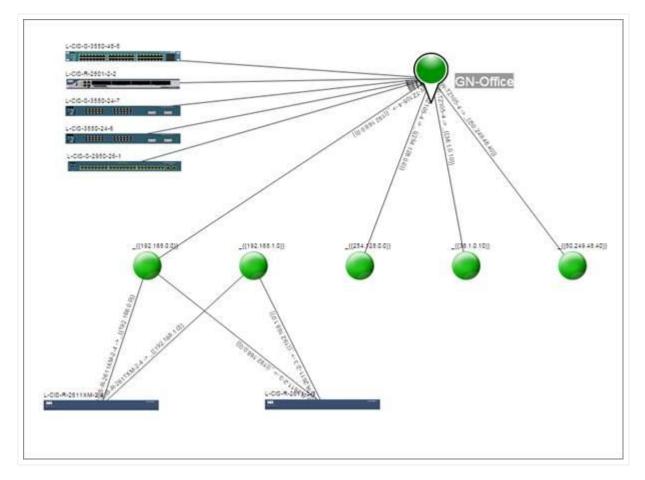
the 'Create Generic Nodes for External IPs' option, then you must also discover these external IP addresses by doing a discovery of the 'Native SNMP_External_IPs' connector.

Reconciling the links in netTerrain requires three connectors to be reconciled:

- The SNMP connector.
- The 'Native SNMP_External_IPs' (if you want to display external IP address).
- The Native_SNMP_Links connector.

Sounds too complicated? It's not remember you can simply enable all these connectors and run the scheduler and forget about all these details.

After the reconciliation process is complete you can now view the devices, nodes and links created in netTerrain, such as the example below.

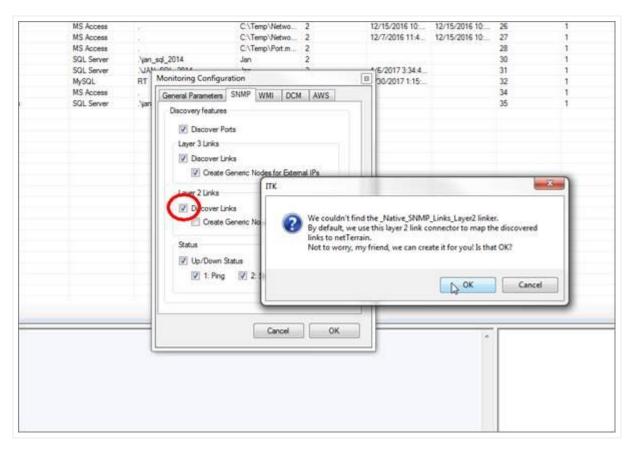


Snapshot of Graphical Networks_' very own lab discovered with netTerrain

7.2.13.3 Discovering Layer 2 link data

The process for discovering layer 3 link data is very similar to the steps involved for layer 3 links.

Just as with layer 3, in the SNMP configuration section, you may be prompted with a message to automatically create the layer 2 link connector upon checking it from the settings.



Enabling the layer 2 link connector

When the 'Layer 2 links' option is checked, the 'Create generic nodes for external MACs' will also be enabled. If you check this option for the first time, then the ITK will show you the following message:

0	MS Access		C:\Temp\Netwo	1	12/15/2016 10	12/15/2016 10	26
	MS Access		C:\Temp\Netwo	2	12/7/2016 11.4	12/15/2016 10	27
	MS Access		C:\Temp\Port.m	2			28
	SQL Server		Jan	2			30
1	SQL Server	11411-001-0014	-lee	-	4/6/2017 3 34 4		31
	MySQL	Monitoring Configuration		8	4/30/2017 1:15:		32
	MS Access	Contract and the second s	VMI DCM AWS				34
External_IPs	SQL Server	Discovery features					35
	CONTRACTOR AND A CALL						
		Discover Ports					
		Layer 3 Links					
		V Discover Links					
		Create Generic Nod	les for External IPs				
		Layer 2 Links					
		Discover Links	пк			- 23	D
		Creare Generic No					
		Status			map External MACs w	isn't created.	
		Up/Down Status	No worries, we'll cre	eate it for you (a	pp will restart).		
		21 22 23 23 24 10 10 10 24 24 24 24 24 24 24 24 24 24 24 24 24					
		V 1: Ping V 2:				-	
						ОК	
				_	_		
			Cancel OK				
C							N

Enabling the Native SNMP_External_MACs connector

Again, as with layer 3, a new connector called 'Native SNMP_External_MACs' is created and mapped to the node type 'Node' in netTerrain.

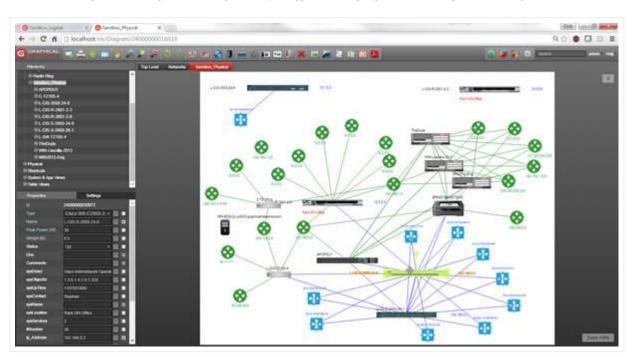
Later, when you discover layer 2 links, netTerrain will also automatically create generic nodes for any MAC addresses that exist in the bridging tables of your discovered switches, which are not part of any discovered MAC address tables.

7.2.13.4 Running the layer 2 link discovery and reconciliation

With the layer 2 link discovery enabled and the layer 2 link connector created we can now discover and reconcile these links in netTerrain. The link discovery is triggered automatically as soon as you start the SNMP discovery, so there are no extra steps involved, but if during the configuration process you checked the 'Create Generic Nodes for External MACs' option, then you must also discover these external MAC addresses by doing a discovery of the 'Native SNMP_External_MACs' connector.

Reconciling the links in netTerrain requires three connectors to be reconciled:

- The SNMP connector.
- The 'Native SNMP_External_MACs' (if you want to display external MAC addresses).
- The Native_SNMP_Links_Layer2 connector.



Below is a diagram of a layer 2 and layer 3 topology, showing layer 3 links in green and layer 2 links in blue.

Snapshot of Graphical Networks_' very own lab with layer 2 and layer 3 links

7.2.14 Using custom MIBs

In addition to the standard MIB OIDs that are embedded in the ITK, users can also use any other MIB OIDs to be discovered via SNMP.

Custom MIBs can be assigned to any particular IP address or range of IP addresses. This is especially useful when you want to discover specific properties for certain device types, such as MIBs that are part of the private enterprise branch.

When you create a new MIB OID field for an IP address, you are in essence instructing the SNMP engine to issue a get request for that particular MIB OID and that particular IP address range. This custom MIB must be mapped to a specific field in netTerrain, so that upon a reconciliation, the engine can populate that field in netTerrain with the discovered values for that MIB.

To add a new custom MIB OID, follow these steps:

- Open the IP address manager (Ctrl-I).
- Choose the IP address for which you want to apply the custom MIBs.

0.0.0.1 · 1 0.0.02 · 2 0.0.03 · 3 0.0.04 · 4 0.0.05 · 5	Settings Community	Edit IP A From	ddress 10			
0.0.2-2 0.0.03-3 0.0.04-4 0.0.05-5		From	10			
0.0.4 - 4 0.0.5 - 5			144	0	0	
	UDP Port 161	То	10	0	0	12
0.0.0.6 - 6	Version v2c 💌			10-	Su	bmt
0.0.0.7 - 7 0.0.0.8 - 8 0.0.0.9 - 9	Enabled V	Load IP	Adda	eas from	tot Elle	
0.0.0.10 - 10	Custom MIBS	LUGUIF	Aurea	969 11041		
0.0 0 12 - 12	Port Monitoring				Upic	
0.0.0.14 - 14	Enabled					
0.0.0.15 - 15 0.0.0.16 - 16	Ø #Descr					
0.0.0.17 - 17 0.0.0.18 - 18	[☑] #PhysAddress					
0.0.0.19 - 19 0.0.0.20 - 20	V fAdminStatus					
0.0.0.21 - 21 *	V fType					
	I fSpeed					
	fLastChange fOperStatus				C. c.	bmit
To csv	V ropersidius				30	EXTING

- Click on the Custom MIBS button (as shown above).
- In the custom MIBs dialog type the MIB OID string and map it to the field in netTerrain, such as the example below, where we are creating a new MIB OID that maps external temperature values for a sensor with a field in netTerrain called 'Ext. Temperature'.

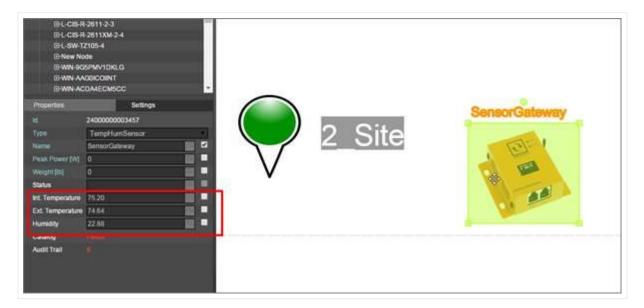
Map New OID OID:		etTerrain Field:	
1.3.6.1.4.1.17095		ot. Temperature	•
	82/25/		Add
IP Address / Range	OID	netTerrain Field	ITK Field
192.168.0.77 - 77			customOid103
192.168.0.77 - 77	1.3.6.1.4.1.17095.3.2.0	Int, Temperature	CustomOid 101

• You can remove custom fields, by highlighting them and clicking on the 'Remove' button.

• Once you are done, click on the Finish button.

Upon a discovery and reconciliation, the SNMP engine will try to discover the values of custom MIB OIDs for any IP addresses that have said MIBs associated.

The example screenshot below, shows our sensor with three custom MIB OID fields mapped to the corresponding netTerrain fields.



Example of custom MIB OID values mapped to netTerrain

7.3 WMI Discovery

According to Microsoft's MSDN page, 'Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems.

Also 'WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. CIM is developed and maintained by the Distributed Management Task Force (DMTF)'.

The ITK comes equipped with a WMI monitoring tool that discovers WMI instance data for any computers and servers that have the protocol enabled.

Via the WMI protocol, the ITK can discover the following computer related information:

- Computer System data
- Operating System
- CPU characteristics
- Memory characteristics
- Logical drives
- BIOS characteristics
- Running processes
- System enclosure data
- List of installed applications
- List of web sites configured in IIS (when applicable)
- List of network adapter configuration parameters

The WMI connector discovers registered computers, their parameters and associated lists, which can then be reconciled in netTerrain.

This module behaves much like a node connector in the sense that it maps the discovered elements with nodes in netTerrain. Moreover, the ITK also has a WMI connector initializer that uses a pre-defined node connector specifically for WMI. This predefined connector is part of the node connector list and is called '_WMI_Hosts'. This connector can also be scheduled for automatic discovery and reconciliation, just like any other connector.

nelTensin Integration Toolkit	New York Contractor									
File View Discovery Set	ttings Tools Help									
	9.0									
Connectors 🍓 🖉	WML Holts + Court 1 -									
	192 168 0.84 192 168 1.21	ptorty Precary Precary Precary	may [1] Name-C Ca. [1] Name-Nom. [1] Manufacturer. [1] Namer-Nom. [1] Manufacturer. [1] Namer-Nom. [1] Manufacturer. [1] Namer-Nom.		[1] Nane-Intel [1] Nane-Intel	Memory [1] Name-Phys. [1] Name-Phys. [1] Name-Phys.	Processes (1) Name-Syste (1) Name-Syste (1) Name-Syste	SystemEnclosure [1] SMEKOSAese [1] SMEKOSAese [1] SMEKOSAese	ConputerSystem [1] Manufacturer [1] Manufacturer [1] Manufacturer	
		Record C	letails	0						
	Calified and the second	System protey Logics (2) Na (2) Na (2	Inst in nell'area ar. 152: 152: 152 Timay Bhree (1) Harn-A, Caga are-C Capton-A. San-J are-O Capton-O. San-J are-O Capton-O. San-J are-O Capton-O. San-J are-O Capton-O. San-J are-O Capton-O. San-J (Nano-Al-Monadr Mindus) are-O Capton-O. San-J (Nano-Al-Monadr Mindus) (Nano-Al-Monadr	5429486376 n Server 2012 Stand mon-4, 2 5500 Capit Build Auster - 5200 M House - 5200 M H	on-Alexand Ian Jackson-Alexand Ian Jackson-Alexand Ian Jackson - Alexand Ian Jackson - Alexandro 20019; Family-2 tell-K Family-2 tell-K Family-5; Micdael	-				

WMI discovery list view

The WMI discovery configuration can be accessed from the Settings->Monitoring-> WMI menu.

View Discovery	Sett	ings Tools Help							
actors 🍋 🖉	1	Node Connectors Link Connectors		priority I	onicalDrives		05	BIOS	CPU
SQL_Mon_Databa	0	Monitoring	• =	SNMP		ła	[1] Name+Micro	[1] Manufacturer	[1] Name
SQL_Mon_DbSen		Type Mappings	. @	WMI			Register Hosts		[1] Name-
WebPages_Mon WMI_Hosts UDD Cties	Discovery Order Application Ctrl+H					WMI Configuration		[1] Name	
Cties_250 Dummy Native SNMP_Exter	nai		0	Web Pages Configuration C	trl=G	Γ			
Native SNMP_Eder Solarwinds to VMwa Wware Host Disco Links	nal, re \								

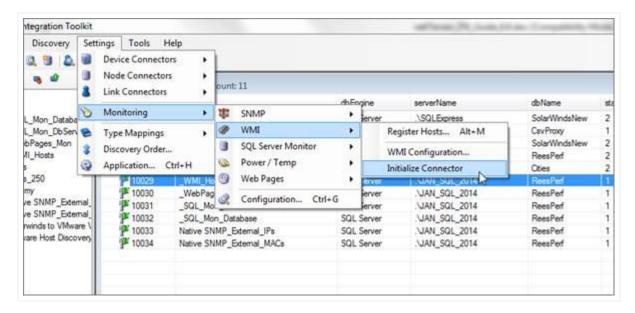
WMI configuration menus and settings

7.3.1 Initializing the WMI connector

As mentioned above, netTerrain utilizes a standard connector to reconcile WMI information from the ITK to netTerrain. This connector is called '_WMI_Hosts' and generated automatically upon initialization.

This connector is also mapped to a node type in netTerrain of the same name, which has predefined fields and an icon automatically created for you upon WMI initialization.

By default, the WMI monitoring function is not enabled and the connector and netTerrain type do not exist. You could create everything yourself, but then you would need to know a thing or two about where the source data resides, what fields to pull and how to map them. Thankfully there is a simple process to automatically create the connector, the netTerrain type and enable the monitoring in one click. Simply go to Settings-> Monitoring->WMI->Initialize connector.



Initializing the WMI monitor

7.3.2 Registering WMI hosts

WMI hosts will not just happily hand over the data to the ITK. You need to register the instances in the ITK first, providing valid credentials that can read the WMI data.

To register a WMI instance go to Settings-> Monitoring->WMI->Register Hosts... and fill out the proper credentials in the dialog that pops up.

@ WMI Host Regis	tration	fagter 1	×
Registered WMI H	osts		
192.168.0.84 192.168.1.21 192.168.1.22			
Enable	Disable		Remove
Register New WM	l Host		
Host Name / IP	10.10.10.1		
User	admin		
Pwd			
DNS			
		Test Connection	Add
			ОК

WMI host registration process

If the proper credentials have been passed the host instance should be reachable. You can test this by clicking on the 'Test connection' button.

1.0141.1	120007(010	otoprior			19
1.9.1.619	379001948	Seoban	Osco IOS Software 2801	Rack GN-Office	78
1.9.1.619	WMI Host Registration	-		Rack GN-Office	78
1.9.1.619				Rack GN-Office	78
1.9.1.324	Registered WMI Hosts			Rack GN-Office	2
1.9.1.359	192.168.0.84			Rack GN-Office	2
1.8741.1	192 168 1 21			Rack GN-Office	79
1.17095			1 100	Rack GN-Office	noSuchO
1,311,1,1				Colo Colo	79 77
	Enable Du Register New WMI Host Host Name / IP 192.16 User admini Pwd		WMI Host Connection T.		
	DNS	Test Connec	tion Add		

Reachable host

After testing the WMI connectivity, register the host by clicking on 'Add'. You can edit the credentials for an existing host as well, by clicking on it, editing the values and then clicking on the 'Update' button.

To remove a host from the list, simply click on it and press 'remove'.

You can enable or disable individual hosts for discovery by clicking on the host and pressing the 'enable' / 'disable' button.

WMI Host Regist	ration	×
Registered WMI H	osts	
192.168.0.84 192.168.1.21 192.168.1.22 :: [Disabled	
Enable	Disable	Remove
Register New WM	Host	
Host Name / IP	192.168.1.22	
User	administrator	
Pwd		
DNS		
	Test Connection	Update
		ОК

Enabling and disabling hosts for discovery

You can select multiple hosts at once for enabling or disabling.

7.3.3 Setting WMI discovery parameters

The WMI discovery engine has a series of parameters (or templates) and each parameter can collect several data points. You can control which parameters are enabled during the WMI discovery process. To do that, open the monitoring configuration dialog and click on the WMI tab or go to

in Integration Too	olkit					1007	sease, 70, Surger 11	des Competition, 10	10000
w Djscovery	Settings Iools	Help							
	Qevice Conne Node Connect Link Connects	tors +	MP - Count 1	3	eve(Obv				
16	> Monitoring	,	THE SNMP				sysUpTime	sysContact	\$75
• <u>2</u>	S Type Mapping	μ.,	Ø ₩MI		,	1 311 1 1 3 1 1 Register Ho	62956095 sts Alt+M	Modeler Jason Sherman	Ha
	3 Discovery Ord	er	SQL Serv	er Monitor	•	WMI Config	guration Ď	Jason Stephan	Bro
	Application	Ctrl+H	Power/	Temp	*	Initialize Co		Stephan	Co
		LCIS	🕘 🛛 Web Pag	jes		1.1.9.1.619	378965891	Stephan	Ce
		F LCIS	Continue	ration C	trl+G	191619	378967577 1157190497	Stephan Stephan	Ca Ca
		LCIS	5-2950-26-1	4524	1.3.6.1	4.1.9.1.359	378973350	Jan	Cis
		P L-SW	-TZ105-4	4523	1.3.6.1	4.1.8741.1	1285128846	IT.	Sor
		P Senso	Gateway	4528	1.3.6.1	4.1.17095	409100370	http://www.serv	Ter
		TheD		4531		4.1.311.1.1.3.1.2	1252372370	Testdive	Ha
		WIN2	012-Eng	4530	1.3.6.1	4.1.311.1.1.3.1.2	14968461	GN Staff ENG	Ha

Changing WMI configuration data

In the configuration dialog you can check or uncheck the different templates based on your needs. The only mandatory parameter that the connector always collects is the computer system data.

Monitoring Configuration
General Parameters SNMP WMI DCM
WMI discovery parameters
Computer System
▼ OS
CPU
Memory
✓ Logical Drives
✓ BIOS
Processes
System Enclosure
Applications <list></list>
✓ IIS <list></list>
Network Adapter Configuration <list></list>
Cancel OK

WMI parameters

The following data is collected for WMI host instances:

1) Computer system data:

- a. Manufacturer
- b. Roles
- 2) Operating system:
- a. Name
- b. Version
- c. Caption
- d. Build number
- e. Manufacturer
- f. Code set
- g. Country code
- h. Current time zone
- i. Serial number
- 3) CPU characteristics (processor):
- a. Name
- b. Family
- c. Manufacturer
- d. Architecture
- e. Caption
- f. Device ID
- 4) Memory characteristics (physical memory):
- a. Name
- b. Manufacturer
- c. Capacity
- d. Speed

e. Version

- f. Caption
- g. Install date
- 5) Logical drives (logical disk):
- a. Name
- b. Caption
- c. Size
- 6) BIOS characteristics:
- a. Manufacturer
- b. Serial number
- 7) Running processes:
- a. Name
- 8) System enclosure data:
- a. SMBIOS asset tag
- b. Manufacturer
- c. Model
- d. Name
- e. Part Number
- f. Serial number
- 9) List of installed applications:
- a. Name
- b. Description
- c. Install date
- d. Install location
- e. Identifying number

f. SKU number

g. Vendor

h. Version

- 10) List of web sites configured in IIS (when applicable):
- a. Path
- b. Site name
- c. Application pool
- d. Enabled protocols
- 11) List of network adapter configuration parameters:
- a. Caption
- b. Default IP gateway
- c. DHCP server
- d. DNS domain
- e. DNS host name
- f. IP address
- g. MAC address

Templates 9, 10 and 11 actually generate separate tables that can be accessed from the ITK interface, as discussed below.

7.3.4 Discovering WMI host data

To discover WMI host data, simply run a discovery and reconciliation process for the WMI connector, just like you would with any other connector (see chapter 4).

Systeme	priority	LogicalDrives	05	BIOS	CPU	Memory	Processes	SystemEnclosure	ComputerSystem
192 168 0.84 192 168 1.21 192 168 1.22	Penary Penary Penary	(1) Name-C Captori-C Sze-S120 (1) Name-A Captori-A Sze-(2) N (1) Name-A Captori-A Sze-(2) N.	[1] Name+Micro	(1) Manufacturer (1) Manufacturer (1) Manufacturer	[1] Nane-Intel [1] Nane-Intel [1] Nane-Intel	[1] Mane-Phys. [1] Mane-Phys. [1] Mane-Phys.	(1) Name-Syste . (1) Name-Syste . (1) Name-Syste .	[1] SMEIOSAsse [1] SMEIOSAsse [1] SMEIOSAsse	[1] Marufacturer [1] Marufacturer [1] Marufacturer

Discovered WMI hosts

WMI hosts, as mentioned before, can show the applications that are installed, network configuration data as well as configured IIS websites (when applicable).

sname	priority	Logical	Drives	OS		BIOS
192 168 0.84	Primary	[1] Nam	e=C: Caption=C: Size=5120	[1] Name=N	licro	[1] M
192.168.1.21 192.168.1.22	Primary	[1 3	Delete Selected	[PT Monocali	pro	[1] M
			Show Applications	D		1.1.
			Network Adapter Configu Show Websites			
			Truncate Table			
			Refresh View			
		- Longer			ť.,	

To view this information in the ITK, right click on the host and select the appropriate parameter:

Application, network and website data

8	Host	Name	Description	InstalDate	Installupcation	klentfyingNumber	SKUNeber	Vendor	Version	
192.168.1	192.168.1.21	Carec Stel	Oansic Shell	20131203		(36885224-805		iveSalt	4.0.2	
192.168.1	192,168,1,21	ItS URL Reverse Module 2	15 URL Revete	20140224		IEB67500A-3C9		Moteoft Copor .	722	
192,168,1	192,168,1,21	Intel/F0 Datacenter Manager	Intel(R) Detacen	20150522	C:\Program Files.	(F9E7798F-C0F_		Intel Corporation	1.0.4.1	
192.168.1	192,168,1,21	Morosoft, NET Framework 4 Multi-Targeting Pack	Morearch NET	20131203	The second s	CFEF48A88F8		Moteoft Corpor	4.0.30319	
192,168.1	192,168,1,21	Morosoft Application Error Reporting	Morearet Applic	20150718		(95120000-008		Moteoft Corpor	12.0.6015 5000	
192,168.1	192,168,1,21	Moroach Baseline Security Analyzer 2.3	Mcrosoft Basel	20150105		(D6005854-07F		Moteoft Corpor	23,2208	
192.168.1	192,168,1,21	Morosoft Help Viewer 1.1	Morosoft Help V.	20131203		(E5748030-7E6		Moreast Corpor	1.1.40219	
192.168.1	192,168,1,21	Morosoft Report Vewer 2012 Runtime	Mcrosoft Report	20131203		BCCE40CE-AB		Moreaet Corpor	11.0.2100.60	
192.168.1	192,168,1,21	Microsoft SQL Server 2008 R2 Management Objects	Moroart SQL 5	20131203		(30F2B8F4-5CF		Moreast Corpor	10.51.2500.0	
152.168.1	192,168,1,21	Moroach SQL Server 2008 R2 Netive Clent	Moreart SQL 5	20150718		(471AAD2C-907		Moreast Corpor	10.51.2500.0	
192 168 1	192,168,1,21	Moroacit SQL Server 2008 R2 Refx Driver	Moreault SQL 5	20150718		(D8C2380E-47)		Moreaet Corpor	10 51 2500 0	
152 168 1	192,168,1,21	Moroach SQL Server 2008 R2 Setup (English)	Moroauth SQL 5	20150718		(21078888-298		Moreaet Corpor	10 51 2500 0	
192 168 1	192,168,1,21	Microsoft SQL Server 2008 Setup Support Files	Moroant SQL 5	20131203		(B40EE888-400		Moreast Corpor	10127310	
192.168.1	192,168,1,21	Moroach SQL Server 2012 Data-Tier App Framework	Moroacth SQL 5	20131203		0F3A8164.84F		Morenoft Corpor	111.2816.0	
192.168.1	192,168,1,21	Microsoft SQL Server 2012 Management Objects	Morearth SQL 5	20131203		EDA1C1761-574.		Motest Coper	11.0.2100.60	
192.168.1	192.168.1.21	Microsoft SQL Server 2012 Management Objects (x54)	Moroactt SQL 5	20131203		(FADA244E-FXC		Motest Coper	11.0.2100.60	
192.168.1	192.168.1.21	Moroach SQL Server 2012 Native Clent	Moroactt SQL 5	20131203		(D411E9C9-CE6		Monast Corpor	111.3005.0	
192.168.1	192.168.1.21	Moroach SQL Server 2012 Policies	Mcrosoft SQL 5	20131203		EDC487E40-048		Moreast Corpor	11.0.2100.60	
192.168.1	192.168.1.21	Moroach SQL Server 2012 Polis Driver	Mcrosoft SQL 5	20131203		(\$1537ADE-FEE		Motest Corpor	11130000	
192.168.1	192.168.1.21	Moroach SQL Server 2012 Setup (English)	Mcrosoft SQL 5	20131203		BC80713F-CFE.		Notest Corpor	11.1.3128.0	
192.168.1	192.168.1.21	Microsoft SQL Server 2012 Transact-SQL Complex 5	Mcrosoft SQL 5	20131203		(BRCB5DFD-6C		Moteoft Corpor	1113128.0	
192.168.1	192.168.1.21	Microsoft SQL Server 2012 Transact-SQL ScriptDon-	Moroauth SQL 5	20131203		(54C50418-0E9		Moteoft Corpor.	11130000	
192 168.1	192.168.1.21	Morosoft SQL Server 2012 T-SQL Language Service	Moreart SQL 5	20131203		ICC88009A-98C		Norosoft Corpor	11.0.2100.60	
192.168.1.21		Page 84 48 1 00 04								
						<u>-</u>				-
						ê				

Application list

	Host	Caption	Default/PGateway	DHCPServer	DNSDoman	DNSHoetName	IPAddress	MACAddress	
192.168.1	192.168.1.21	(00000000) WAN Minpot (L2TP)							1
192 168.1	192 168 1 21	[00000001] WAN Minport (SSTP)							
192.168.1	192 168 1.21	[00000002] WAN Mrippet (IKEx2)							
192.168.1	192 168 1 21	(00000003) WAN Mexport (PPTP)							
192.168.1	192,168 1 21	(0000004) WAN Minpot (PPPOE)							
192,158.1	192.168.1.21	(00000005) WAN Mrippet (IP)							
192.168.1	192,168,1,21	[00000006] WAN Minport (IPv6)							
192.168.1	192.168.1.21	(00000007) WAN Minpot (Network Monitor)							
192.168.1	192 168 1.21	(0000008) Morosoft Kernel Debug Network Adapter							
192,168.1	192.168.1.21	[0000009] RAS Arynic Adapter							
192 168.1	192.168.1.21	[00000010] Heel(R) \$2574L Gigabit Network Connection	192.168.1.1,			TheDude	192.168.1.21/e	00-0C-29-F1:80	
152.168.1	192.168.1.21	(00000011) Microsoft ISATAP Adapter							
192.168.1	192.168.1.21	(0000012) Morosoft Teredo Tunneling Adapter							
192 168 1	192.168.1.21	[00000013] Microsoft ISATAP Adapter							

Network adapter list

	host	Path	SteName	application Pool	EnabledProtocols	status	last Response Time
7544	192.168.0.84	/Oppenheimer	Default Web Ste	Oppenheimer	http	Up	688
7545	192.168.0.84	/Opptrain	Default Web Ste	OppenheimerTra	http	Up	802
7546	192.168.0.84	/jacksonlab	Default Web Ste	jacksonlab	http	Up	740
7547	192,168.0.84	/Tulva	Default Web Ste	Distech	http	Up	659
7548	192.168.0.84	/ASA	Default Web Ste	ASA	http	Up	816
7549	192 168 0 84	Andelsbanken	Default Web Ste	Classic NET Ap	http	Down	- 14 · · · · · · · · · · · · · · · · · ·
7550	192.168.0.84	/Benjamin	Default Web Ste	65Demo	http	Up	982
7551	192,168,0.84	/Woodgroup	Default Web Ste	DemoPool	http	Up	190
7552	192.168.0.84	/PavlovMedia	Default Web Ste	DemoPool	http	Up	824
7553	192.168.0.84	/Test	Default Web Ste	DemoPool	http	Down	
7554	192.168.0.84	/TECO	Default Web Ste	DemoPool	http	Up	21
7555	192.168.0.84	/Demo65	Default Web Site	DemoPool	http	Down	
7556	192.168.0.84	/TEC0	Default Web Ste	DemoPool	http	Up	795
7557	192.168.0.84	/DataYard	Default Web Ste	DemoPool	http	Up	565
7558	192.168.0.84	/ENOOMED	Default Web Ste	DemoPool	http	Up	7
7559	192,168.0.84	/#	Default Web Ste	DemoPool	http	Up	743
7560	192.168.0.84	/BSI	Default Web Ste	DemoPool	http	Up	807
7561	192.168.0.84	/BIS	Default Web Ste	DemoPool	http	Up	980
7562	192.168.0.84	/Nextel	Default Web Ste	DemoPool	http	Up	806
7563	192.168.0.84	/videotron	Default Web Ste	DemoPool	http	Up	1
7564	192.168.0.84	/martin	Default Web Ste	DemoPool	http	Up	925
7565	192.168.0.84	/leivas	Default Web Ste	DemoPool	http	Up	694
7566	192 168 0 84	/Manacor	Default Web Ste	DemoPool	http	Up	21

Website list

7.3.5 Setting up and troubleshooting WMI in your environment

The setup process for WMI discovery does come with its kinks: hosts need to have the WMI service enabled, proper permissions need to need to be set up and more. As such, WMI issues may occur during configuration.

RPC errors may occur, which usually mean your settings are not correct and you cannot even get to the server for authentication. This can be a firewall issue or simply a bad DNS or IP address information.

Authentication errors usually mean it's your user and/or password that are incorrect. It may also mean you need to add a different user to the WMI namespace.

7.3.5.1 Adding a user to the WMI namespace

Typically, the default administrator account will work for WMI monitoring. However, if you are using a different administrator account or you want to add an AD user account to use when monitoring WMI then you need to add the user and apply the appropriate permissions for this user account. For troubleshooting purposes, you can use a WMI management tool (WmiMgmt).

To modify the permissions, do the following:

1) Start the WmiMgmt tool

Programs (1)
🚟 WmiMgmt
Search the Internet
wmimgmt × Log off +

2) Right click the WMI control and select properties

• · · · ·	WimiMgmt - (Console Root)/W	fi Control (Local)]	= 0 X
	n View Favorites Window Help		_ # 1
Console Roo (d) WMA Cor		Actions	
and the case	Connect to another computer	and a second second second	
	View + the Windows Management	More Actions	,
	New Window from Here Horice.		
	New Taskpod View		
	Properties		
	Help		
	The current selection.		

- 3) Select the appropriate namespace -
- a. The default name space is CIMV2

b. If you want to monitor IIS then you would look for the WebAdminstration namespace and apply the security settings to this namespace a well

c. After selecting the namespace press the Security button

WMI Control (Local) Properties
General Backup/Restore Security Advanced
Namespace navigation allows you to set namespace specific security.
Security
OK Cancel Apply

4) Add the user and select the remote enable permissions for the user

ecunty		
Group or user names:		
& Authenticated Users		
👗 john smith (john.smith@grap	hicalnetworks.com)	
8 LOCAL SERVICE		
RETWORK SERVICE		
Administrators (INSTALLTE:	STONE vadministrato	rs)
		0
	Add	Remove
Permissions for john smith	Allow	Deny
Enable Account	v	<u> </u>
Remote Enable	•	
Read Security		
Edit Security		
Special permissions		
For special permissions or advance click Advanced.	ced settings.	Advanced
Learn about access control and p	oemissions	

7.3.5.2 DCOM permissions

As part of the WMI set up process on the monitored host, you may also need to add the user to the DCOM settings for the machine. To add the user, you need to go into the properties for the computer following these steps:

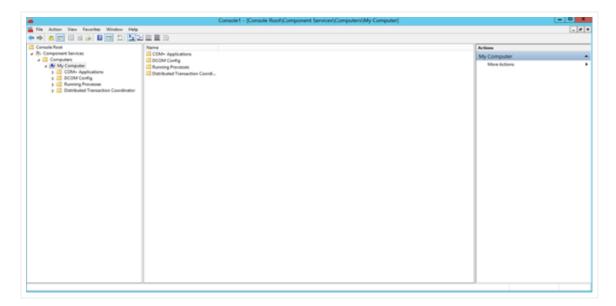
1) To get to the DCOM settings start the MMC application

Programs (1)
mmc
a mmc
Search the Internet
mmd X Log off >

2) Press the Add/Remove snap in option

			Canade? - (Canade Root)			
a Adam New Parallel	Window No.					6.04
Sec.	Calula					
Spar.	04-0	Name .			Artiste	
See.	Oaks		These are in them in door in the or	-	Connector Name	
See No.					Must Arturn	
And Renner Step In-	Can-M					
Options.						
1 March Speet						
1 and 1						
1.00						
ter.						
					1	
					1	
					1	
An english constitu						

3) Add the snap in called component services, then right click the My Computer icon



4) Press the COM Security settings and then press the "Edit Limits" for the Launch and Activation Permissions

My	Computer Pro	perties	? X
General	Options	Default	Properties
Default Protocols	COM Sec	unity	MSDTC
Access Permissions			
You may edit who is a also set limits on appl			
	dfying access perm ns to start, connect		
	Edt Limits	Edit	Default
Launch and Activation	Permissions		
You may edit who is a activate objects. You determine their own p	may also set limits		
	difying launch and a sity of applications recurely.		
	Edit Limits	Edit	Default
Leam more about setting	these properties.		
	ОК	Cancel	Apply

5) Add the user and select the Remote Launch and Remote Activation permissions

Launch and Activation	on Permission	? X
Security Limits		
Group or user names:		
& Administrators (INSTALLT		
Performance Log Users (I B Distributed COM Users (IN)		
A john smith (ohn smith@gr		
		~
		,
	Add	Remove
Permissions for john smith	Allow	Deny
Local Launch	•	
Remote Launch Local Activation	2	
Remote Activation		H
	induction of the second	_
Learn about access control an	d permissions	
	OK	Cancel
	UK	Cancel

7.3.5.3 Testing a WMI connection

If you are having problems using WMI you may test connectivity issues by using the WBEMTest.exe tool. This is built into most Windows machines and can be used as follows:

1) Start the WBEMtest application by simply typing WBEMTest into your local search engine

Programs (1)
i wberntest
Search the Internet
wberntest × Log off +

2) Press the connection button

Windows Ma	nagement Instru	imentation Teste	er 🗕 🗆 🗙
Namespace:			Connect Exit
IWbemServices			
Enum Classes	Enum Instances	Open Namespace	Edit Context
Create Class	Create Instance	Query	Create Refresher
Open Class	Open Instance	Notification Query	
Delete Class	Delete Instance	Execute Method	Ī
Method Invocation (C Asynchronous C Synchronous C Semisynchronous Use NextA			-
10 Batch	Count (enum. only)	5000 Timeout	t (msec., -1 for infinite)

3) Enter the credentials

C	Connect
Namespace	Connect
Connection:	
Using: IWbemLocator (Nam	espaces) 💌
Returning: IWbemServices	Completion: Synchronous
Password:	
Locale	- How to interpret empty password
	NULL C Blank
Impersonation level	Authentication level
C Identify	C None Packet
Impersonate	Connection C Packet integrity
O Delegate	C Call C Packet privacy

4) If you have a successful connection the services will be active and can be selected

Windows Ma	nagement Instru	imentation Teste	r 🗕 🗆 🗙
Namespace: \\192.168.1.204\roo	t\cimv2		Connect Exit
- IWbemServices			
Enum Classes	Enum Instances	Open Namespace	Edit Context
Create Class	Create Instance	Query	Create Refresher
Open Class	Open Instance	Notification Query	
Delete Class	Delete Instance	Execute Method	
Method Invocation C	otions		
C Asynchronous		Enable All Privi	leges
C Synchronous		Use Amended	Qualifiers
Semisynchrono	us	Direct Access	on Read Operations
Use NextA	tync (enum. only)		
10 Batch	Count (enum. only)	5000 Timeout	(msec., -1 for infinite)

7.4 AWS Discovery

The ITK comes equipped with an AWS monitoring tool that discovers a number of objects related to your AWS environment.

Using the AWS API, the ITK can discover the following AWS related entities:

- Instances
- Security groups
- Security group rules
- Buckets
- Health checks
- Volumes
- Volume attachments

Just like other utilities (like the WMI, SNMP or SQL), this module behaves much like a node connector in the sense that it maps the discovered elements with nodes in netTerrain. Moreover, the ITK also has an AWS connector initializer that uses a pre-defined node connector specifically for AWS. This predefined connector is part of the node connector list and is called '_AWS_instances'. This connector can also be scheduled for automatic discovery and reconciliation, just like any other connector.

This predefined connector will only reconcile AWS instances in netTerrain using a predefined AWS instances type in the catalog. For the other objects that the AWS utility discovers (buckets, health checks, etc.) you would have to create a connector for them manually. To do that, please check the tables that start with adaAws in your GNCORE database. These include:

- adaAwsBuckets
- adaAwsHealthChecks
- adaAwsSecurityGroups
- adaAwsSecurityGroupsRules
- adaAwsVolumeAttachments
- adaAwsVolumes

7.4.1 Initializing the AWS connector

As mentioned above, netTerrain utilizes a standard connector to reconcile AWS instance information from the ITK to netTerrain. This connector is called '_AWS_Instances' and generated automatically upon initialization.

This connector is also mapped to a node type in netTerrain of the same name, which has predefined fields and an icon automatically created for you upon AWS initialization.

By default, the AWS monitoring function is not enabled and the connector and netTerrain type do not exist. You could create everything yourself, but then you would need to know a thing or two about where the source data resides, what fields to pull and how to map them. Thankfully there is a simple process to automatically create the connector, the netTerrain type and enable the monitoring in one click. Simply go to Settings-> Monitoring->AWS->Initialize connector.

File View Discovery	Settings	Tools Help							
Connectors S &	 Device Connectors Node Connectors Link Connectors 		, , ,	e Coi	nnector List - Count: 16	_		doEngine	serverName
⊕-∰ Nodes ⊛-& Links	TypeDisc	ittoring • Mappings overy Order lication Ctrl+H	•	4	SNMP WMI Power / Temp Web Pages	* * * *		SQL Server SQL Server SQL Server SQL Server SQL Server	\SQLEXP \SQLExpre \JAN_SQL
					AWS SQL Server Monitor Configuration Ctrl+G	•	AWS	unt Settings Configuration lize Confectors	Van_sql_2 Van_sql_2
				10030 10033 10034 10035 10036	Ports _WMI_Hosts _AWS_Instances			MS Access SQL Server SQL Server MySQL MS Access	.Van_sql_2 .VJAN_SQL RT

Initializing the AWS monitor

7.4.2 Configuring AWS for first time use

To configure the AWS connector, you need to provide the ITK your AWS account settings and set up some configuration parameters.

7.4.2.1 Storing the AWS account settings

AWS will not just happily hand over the data to the ITK. You need to first provide the AWS account settings in order for the ITK to access the data through the AWS API.

The read AWS data through its API, the ITK needs the AWS Access Key Id as well as the secret key. This is an AWS requirement. The secret key is never shown in clear text and is also encrypted in the backend.

To set up the AWS account go to Settings-> Monitoring->AWS->Register Hosts... and fill out the proper credentials in the dialog that pops up.

Eile View Discovery	Settings	Iools H	elp						
த 🔯 🕲 🔍 🕲 💩 Connectors 🧠 🖉	■ No	vice Connector de Connectors k Connectors			e Connector List - Co	ount 16	_		
Devices Nodes	-	K CONNECTORS		1	alas		_	dbEngine	serverName
E-IJ Nodes E-▲ Links	Yo Mo	onitoring		•	SNMP		• 🗖	SQL Server	SQLEXPRE
	E Tvi	pe Mappings			WMI		• 🗆	SQL Server	.\SQLExpress
				34 L	Power / Temp			SQL Server	.VAN_SQL_2
	3 Discovery Order			170				SQL Server	1.
	Ap	plication C	trl+H		Web Pages		- 10	SQL Server	Van_sql_201
1				1	AWS		•	Account Settings	Nan_sql_201
				8	SQL Server Mor	nitor	•	AWS Configuration	Van_sql_201
				ju -	Configuration Ctrl+C			Initialize Connectors	
				10 10	0030 Ports		_	MS Access	
		- pr pr			10033 _WMI_Hosts 10034 _AWS_Instances			SQL Server	.\jan_sql_201
								SQL Server	.VAN_SQL_2
				P 10	0035 Mysql			MySQL	RT
				1 10	0036 Sites			MS Access	8

AWS account setup

After the proper credentials have been passed you can proceed to configure the parameters you want discovered from AWS.

7.4.2.2 Configuring AWS parameters

The AWS discovery process discovers the parameters that you enable from the AWS configuration settings section.

File View Discovery	Settings	Tools Help								
Connectors	Nod	ice Connectors le Connectors Connectors	* * *	tor List - Count: 1	7					
- Nodes	S Mor	nitoring		SNMP		• 1	dbEngine	serverNa		
🕀 👗 Links		ł	WMI Power / Temp	:	SQL Server SQL Server SQL Server SQL Server SQL Server	\SQLEprin \SQLEprin \JAN_SQL	QL_2014			
		10019	3	AWS			Account Settin		2014	
		1002	8	8	SQL Server	Monitor	•	AWS Configur	ation	2014
		P 10025					Configurat	on Ctrl+	5	Initialize Conn
		₩ 10030 ₩ 10033	RTAR			MS Access SQL Server	.\Jan_S	d_2014		
		10034 10035		_AWS_Instances Mysql			SQL Server MySQL	.VAN_S	QL_2014	

AWS configuration

First make sure AWS discovery is enabled.

Monitoring Configura	tion			-		x
General Parameters	SNMP	WMI	DCM	AWS	1	
Enabled AWS discovery pa Regions Instances Securit				•		
Securit Securit Volume Buckets Health Check	s					
		Can	cel	0	К	

Enabling AWS discovery

You can then choose several parameters to discover and monitor. Notice how Regions, Instances and Security Roles are always discovered

To find out if AWS has been properly set up, you basically need to run a discovery process. This will soon reveal if there were any problems during the set-up process.

7.4.3 Discovering from AWS

To run a discovery, you can simply click on the discovery button on the AWS list or find the newly registered AWS connector located in Discovery->Manual Node Discovery->_AWS_Instances. This discovery process will discover any parameters enabled during the setup but will only display a view of the instances. The rest is available in tables as described above.

File View Discovery Settings To	ools Help						
Connectors	AWS Instance						
ar-tal Devices ar-13 Nodes ar-15 Linka	id +0110858 +018696- +03621e +035045 +036750- +036750- +0367757 +005452 +0337757 +005452 +0632196	Primary Primary Primary Primary Primary Primary Primary	RegionName us-exet-1 us-exet-1 eu-central-1 us-exet-1 us-exet-1 us-exet-1 us-exet-1 us-exet-1 us-exet-1 us-exet-1	PublicDnsName ec234-154-151-13 ec22322-138-174 ec254-174-224-24 ec252-44-58-22 e ec2-34-138-21-58 ec2-34-139-21-58	p-172-31-26-44 p-172-31-11-26 p-172-31-25-49 p-172-31-25-49 p-172-31-12-23 p-172-31-12-23 p-172-31-12-23 p-172-31-17-15 p-172-31-30-39	23 22 198 174 54 174 224 24 52 44 58 22 34 198 21 98	Priva 172 172 172 172 172 172 172 172 172
	5/2/2017 4:01:21 PM	E Starting discov	ery process for _	AWS_Instances. This p	rocess can take seve		

Discovering AWS data

7.5 SQL Server Monitoring

The ITK comes equipped with a simple SQL Server monitoring tool that discovers SQL Server instance data and all the underlying databases along with some of their key parameters.

7.5.1 Initializing the SQL monitoring connector

netTerrain utilizes three standard connectors to pass SQL information from the ITK to netTerrain:

- •_SQL_Mon_DbServerInstance node connector: stores information about the SQL Server instances.
- _SQL_Mon_Database node connector: stores information about each SQL Server database on registered instances.
- _SQL_Mon_Links: enables visual links in netTerrain to show which database is associated with which SQL Server.

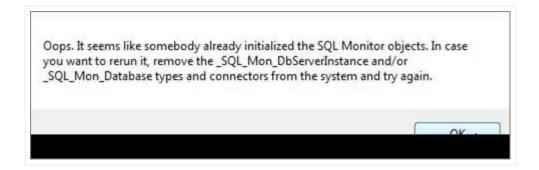
Each of these three connectors should be mapped to the corresponding type in netTerrain. The netTerrain catalog will require similar types with the appropriate fields for you to take advantage of this monitoring functionality.

By default, the SQL monitoring function is not enabled, and these connectors and types are not created in netTerrain. You could create everything yourself, but then you would need to know a thing or two about where the source data resides, what fields to pull and how to map them. Thankfully there is a simple process to automatically create the connectors and enable the monitoring. Simply go to Settings-> Monitor->SQL Server Monitor->Initialize to create all three connectors in one click.

ain Integration Too	olkit	100	man, 76 States 14 Aurolan 7 mage					
ew Discovery	Settings Tools Help							
2, 9 2, 8	Device Connectors •							
: 1	Node Connectors	ttor List - Count: 2						
vices _DCM_Mon_Device CA Unicenter Trig Cisco Config Files CiscoRME	Link Connectors	alas di Focioe serverName	dbName status					
	📎 Monitor 🔸	SQL Server Monitor Register Server In						
	Application	Native SNMP Initialize	stwo 1					
Concord eHealth Microsoft MOM Microsoft SCOM Native SNMP Orion NPM RHN		La ^c						

Initializing the SQL Server monitor

This process not only creates the connectors, but also creates the necessary types in netTerrain. Note that if any of the three connector names already exist in the ITK or in the netTerrain catalog, the process will fail with the following message:



7.5.2 Registering SQL Servers

SQL Server databases will not just happily hand over the data to the ITK. You need to register the instances in the ITK first, providing valid credentials that can read the master databases (many a DBA would cringe at the mere reading of this paragraph, but since the ITK will read statistics for each database from the master database, a user with permissions to read from there must be created in the SQL Server instance).

To register a SQL Server instance, go to Settings-> Monitoring->SQL Server Monitor->Register Server Instances and fill out the proper credentials in the dialog that pops up.

Database Monitoring	and the second	23 other	2489504
Concentration (NS	and the second s	other	408029
Servers List		other	500806
		other	2489504
Jan SQLEXPRESS			
ELGORDO JAN_SOL_2	14		
h		1	
	Remove		
Register New Server			
Database services	SQL Server		
Database engine:	CTREATOR .		
DB Server instance:	ELGORDO JAN_SQL_2014	Database server o	onnection
Windows authentication:	No •	-	
	ITK	Database Server	and the balant
User	IIK	Database Server	reachable:
Password	an and the second se		
	Test Connection Submit		OK
	Tea contractory	-	UN
		L	-
	OK		

SQL Server registration process

If the proper credentials have been passed (i.e. the server is reachable), the SQL Server instance can be registered. Note that this will not guarantee proper reading of the data, as permissions may not be enough to access the master database.

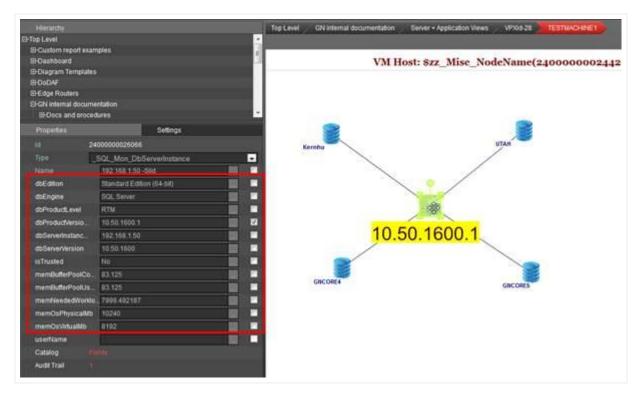
You can register as many instances as needed, and once this process is completed you can click on the 'Enable Monitor' button on the bottom left corner of the dialog and then 'OK'.

7.5.3 Discovering SQL Server data

To now discover SQL Server data, simply run a discovery and reconciliation process for all three SQL monitoring connectors.

The following data is collected for SQL Server instances:

- Database edition
- Database engine
- Database product level
- Database product version
- Database server instance
- Database server version
- Is trusted flag
- Memory buffer pool committed [Mb]
- Memory buffer pool used [Mb]
- Memory needed workload [Mb]
- Memory OS physical [Mb]
- Memory OS virtual [Mb]



SQL Server database view

Databases for each instance will be discovered automatically and linked to the parent instance, as the image above shows. The following data is collected for SQL Server databases:

- Create date
- Database_id
- Database name
- Data file name
- Data file size
- Database engine
- Database server instance
- Log file name
- Log file size

8 Other settings and commands

8.1 Commands

The ITK can issue commands from the input window (bottom right window of the switchboard).

A U U U U U A I	TT 2004 344 8								DATATI
a di Denote 3 Voies 3 Line 3 Line	HLAN Descat Descat Descat Descat Descat mint LOBARI, LOBARDIAI TSINILLE Margin TSINILLE Margin LOBARI, LOBARDIAI TSINILLE Margin TSINILLE Margin LOBARI, LOBARDIAI TSINILLE Margin TSINILLE Margin LOBARI, LOBARDIAI LOBARDIAI TSINILLE Margin TSINILLE Margin LOBARIZ, LOBARDIAI LOBARDIAI TSINILLE Margin Margin Margin LOBARDIAI LOBARDIAI TSINILLE Margin Margin Margin Margin Margin LOBARDIAI Margin LOBARDIAI	2 (100)	9763946530 14034653 14034658 14034658 4514659 6550 6550 6550 6550	pfloatfyre Bed Ndred Ared Ared Bed Bed Bed Ared	eficatives lost lost lost lost lost lost lost los	effectinge E S S S S S S S S S S S S S S S S S S	pTourities 255.255.255 8 255.255 9 255.255 255 9 255.255 255 9 255.255 255 8 255.255 255 8 255.255 255 8 255.255 255 9 255.255 255 5		
	11/26/2014 10:19:54 PMDWAY_June - L.006 12/1014 = _2012464 Total words: 8	- 0	1						
	Team Processities with respect year of provents in real Terminia	1							
	Tean Faculti with reasong and porter in real Tearset Tean Faculti statement aligned; 0 Tean Faculti with redgets and porter in real Tearset Tean Faculti Streets aligned; 0				Comm	and int	out window	v	
	Tend wordt (ream alsgewit) 5 Tene Planste wit vedigte er djaste is val Tenes Teld wordt (ream dignet) 8 Teldam Teldam			a 1	Comm	nand inj	out window	v	
	Tend worked; South Hagent; S Fore Flocates with reduce end parts in red Tensor Tend worker, South Hagent; S Tenders				Comm	nand inp	out window	v	

Command input window

These commands can trigger events that affect data in the ITK or in netTerrain.

The command input window is mainly used for development and consulting purposes, but the following commands have been made available for end users:

- addFieldToAllCards\<fieldName> adds given field to all card types in catalog
- addFieldToAllDevices\<fieldName> adds given field to all device types in catalog
- addFieldToAllLinkTypes\<fieldName> adds given field to all link types in catalog
- addFieldToAllNodeTypes\<fieldName> adds given field to all node types in catalog
- addporttomodel\<decimal typeid>?<string portname> adds a port to the model (and all instances) of the given type using the given name
- addFieldToAllRacks\<fieldName> adds given field to all rack types in catalog
- addSnmpPortFields adds all missing port properties that are discovered via snmp to port object in netTerrain
- setDefaultForAllCardTypes\<fieldName>?<defaultValue> sets a default value to a
 given field for all card types in catalog
- setDefaultForAllDeviceTypes\<fieldName>?<defaultValue> sets a default value to a
 given field for all device types in catalog
- setDefaultForAllLinkTypes\<fieldName>?<defaultValue> sets a default value to a
 given field for all link types in catalog
- setDefaultForAllNodeTypes\<fieldName>?<defaultValue> sets a default value to a
 given field for all node types in catalog
- setDefaultForAllRackTypes\<fieldName>?<defaultValue> sets a default value to a
 given field for all rack types in catalog
- applyDefaultToCardInstancesOfType\<string typeName>?<fieldName> applies the default value of a given field to all instances of that specific card type
- applyDefaultToDeviceInstancesOfType\<string typeName>?<fieldName> applies the default value of a given field to all instances of that specific device type
- applyDefaultToLinkInstancesOfType\<string typeName>?<fieldName> applies the default value of a given field to all instances of that specific link type
- applyDefaultToNodeInstancesOfType\<string typeName>?<fieldName> applies the default value of a given field to all instances of that specific node type
- applyDefaultToRackInstancesOfType\<string typeName>?<fieldName> applies the default value of a given field to all instances of that specific rack type
- applyDefaultToCardInstancesAllTypes\<fieldName> applies the default value of a given field to all instances of all card types
- applyDefaultToDeviceInstancesAllTypes\<fieldName> applies the default value of a given field to all instances of all device types
- applyDefaultToLinkInstancesAllTypes\<fieldName> applies the default value of a given field to all instances of all link types
- applyDefaultToNodeInstancesAllTypes\<fieldName> applies the default value of a given field to all instances of all node types
- applyDefaultToRackInstancesAllTypes\<fieldName> applies the default value of a given field to all instances of all rack types
- <ARROW DOWN> displays last command in buffer

- <ARROW UP> displays first command in buffer
- clearSnmpAddressTable deletes contents from the SNMP IP address table
- clearSnmpRouteTable deletes contents from the SNMP routing table
- cls clears output screen
- deleteDefaultFromAllCardTypes\<fieldName>?<defaultValue> sets the default value to given field for all card types in catalog to NULL
- deleteDefaultFromAllDeviceTypes\<fieldName>?<defaultValue> sets the default value to given field for all device types in catalog to NULL
- deleteDefaultFromAllLinkTypes\<fieldName>?<defaultValue> sets the default value to given field for all link types in catalog to NULL
- deleteDefaultFromAllNodeTypes\<fieldName>?<defaultValue> sets the default value to given field for all node types in catalog to NULL
- deleteDefaultFromAllRackTypes\<fieldName>?<defaultValue> sets the default value to given field for all rack types in catalog to NULL
- deleteFieldForAllCards\<fieldName>
- deleteFieldForAllDevices\<fieldName>
- deleteFieldForAllLinkTypes\<fieldName>
- deleteFieldForAllNodeTypes\<fieldName>
- deleteFieldForAllRacks\<fieldName>
- deleteUnusedNonSystemLinks
- deleteUnusedNonSystemNodes
- disabledc disables all device connectors
- disablelc disables all link connectors
- disablenc disables all node connectors
- enabledc enables all device connectors
- enablelc enables all link connectors
- enablenc enables all node connectors
- <ESC> clears input
- <F5> clears buffer
- mibget\ip:<ip address>oid:<mib oid>comm:<community string> -gets MIB value for given IP address and OID.
- oid\<oid> finds matching model to oid
- ping \< ip address> pings the given ip address or name
- pl purges log
- portmonoff disables SNMP port monitoring for all ip addresses
- portmonon enables SNMP port monitoring for all ip addresses
- resequenceConnectors reindexes all connector sequences
- s0 disables silent mode

- s1 runs discovery in silent mode (no output of individual records)
- walk\ip:<ip address>oid:<mib oid> walks a MIB stubtree for a given IP address and root OID. Example: walk\ip:192.168.1.1oid:1.3.6.1.2
- unfavoriteAllCategories
- unfavoriteAllDeviceTypes

8.2 Other application settings

From the Settings->Application menu you can open the application settings dialog to configure certain global parameters in the ITK.

Besides the scheduler settings (explained above), from here we can also set the following parameters:

- records per page on list views
- app server URL (to access netTerrain directly from the ITK)
- silent mode
- size of the output buffer

App Settings	x
Scheduler Other	
Use generic devices for	unmatched types:
Records per Page:	25 🔹
App server url:	http://localhost/vis
Silent mode:	
Output buffer:	2000000
Set Discovery Order	Submit Cancel

Other application settings