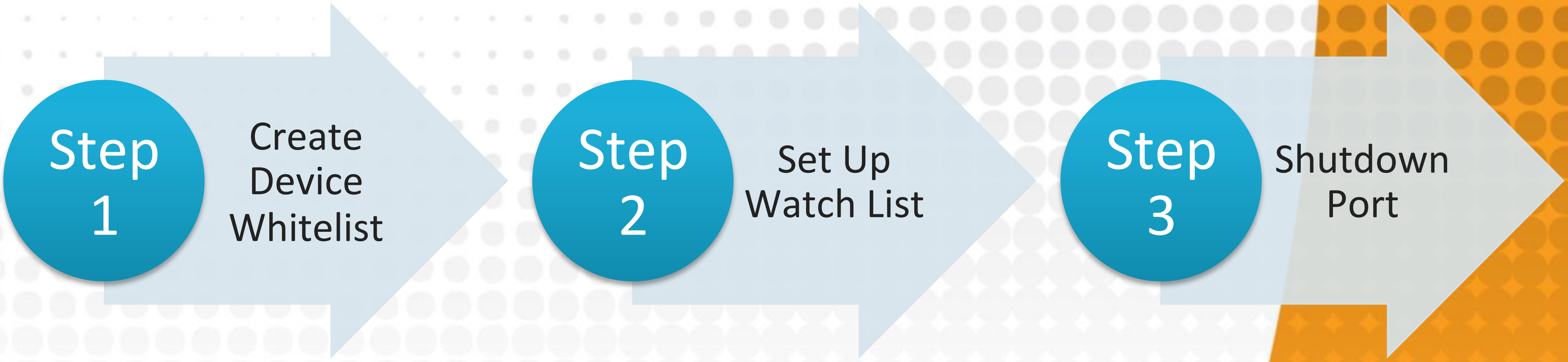
solarwinds

3 Simple Steps to Take Charge of Your Network Access Security



Step 1 Create Device Whitelist

Step 2 Set Up Watch List

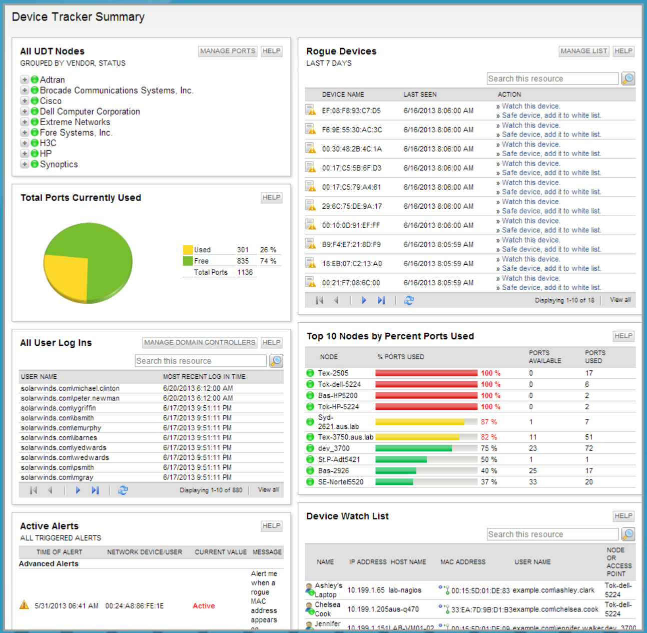
Step 3 Shutdown Port

Are you feeling the pain of an increasingly dynamic and growing network?

Are you in control of who and what is connected to your network?

Are you frustrated with tracing cables to track down a problem device?

Why not use a tool that can do all the hard work for you?



Device Tracker Summary

All UDT Nodes
GROUPED BY VENDOR, STATUS

- Adtran
- Brocade Communications Systems, Inc.
- Cisco
- Dell Computer Corporation
- Extreme Networks
- Fore Systems, Inc.
- H3C
- HP
- Synoptics

Total Ports Currently Used

🟨 Used	301	26 %
🟩 Free	835	74 %
Total Ports	1136	

All User Log Ins

USER NAME	MOST RECENT LOG IN TIME
solarwinds.com\michael.clinton	6/20/2013 6:12:00 AM
solarwinds.com\peter.newman	6/20/2013 6:12:00 AM
solarwinds.com\ygriffin	6/17/2013 9:51:11 PM
solarwinds.com\bsmith	6/17/2013 9:51:11 PM
solarwinds.com\emurphy	6/17/2013 9:51:11 PM
solarwinds.com\ibarnes	6/17/2013 9:51:11 PM
solarwinds.com\yedwards	6/17/2013 9:51:11 PM
solarwinds.com\wedwards	6/17/2013 9:51:11 PM
solarwinds.com\psmith	6/17/2013 9:51:11 PM
solarwinds.com\mgray	6/17/2013 9:51:11 PM

Displaying 1-10 of 880

Active Alerts
ALL TRIGGERED ALERTS

TIME OF ALERT	NETWORK DEVICE/USER	CURRENT VALUE	MESSAGE
Advanced Alerts			
5/31/2013 06:41 AM	00:24:A8:86:FE:1E	Active	Alert me when a rogue MAC address appears on

Rogue Devices
LAST 7 DAYS

DEVICE NAME	LAST SEEN	ACTION
EF:08:F8:93:C7:D5	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
F6:9E:55:30:AC:3C	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
00:30:48:2B:4C:1A	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
00:17:C5:5B:6F:D3	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
00:17:C5:79:A4:61	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
29:6C:75:DE:9A:17	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
00:10:0D:91:EF:FF	6/16/2013 8:06:00 AM	» Watch this device. » Safe device, add it to white list.
B9:F4:E7:21:8D:F9	6/16/2013 8:05:59 AM	» Watch this device. » Safe device, add it to white list.
18:EB:07:C2:13:A0	6/16/2013 8:05:59 AM	» Watch this device. » Safe device, add it to white list.
00:21:F7:08:6C:00	6/16/2013 8:05:59 AM	» Watch this device. » Safe device, add it to white list.

Displaying 1-10 of 18

Top 10 Nodes by Percent Ports Used

NODE	% PORTS USED	PORTS AVAILABLE	PORTS USED
Tex-2505	100 %	0	17
Tok-dell-5224	100 %	0	6
Bas-HP5200	100 %	0	2
Tok-HP-5224	100 %	0	2
Syd-2621.aus.lab	87 %	1	7
Tex-3750.aus.lab	82 %	11	51
dev_3700	75 %	23	72
St.P-Adt5421	50 %	1	1
Bas-2926	40 %	25	17
SE-Nortel5520	37 %	33	20

Device Watch List

NAME	IP ADDRESS	HOST NAME	MAC ADDRESS	USER NAME	NODE OR ACCESS POINT
Ashley's Laptop	10.199.1.65	lab-nagios	00:15:5D:01:DE:83	example.com\ashley.clark	Tok-dell-5224
Chelsea Cook	10.199.1.205	aus-q470	33:EA:7D:9B:D1:B3	example.com\chelsea.cook	Tok-dell-5224
Jennifer	10.199.1.151	LAB-VM01-02	00:15:5D:01:DE:09	example.com\jennifer.walker	dev_3700

To help protect and safely resolve high-risk situations on the network, organizations need to take a proactive stance in controlling who and what is allowed on the network.

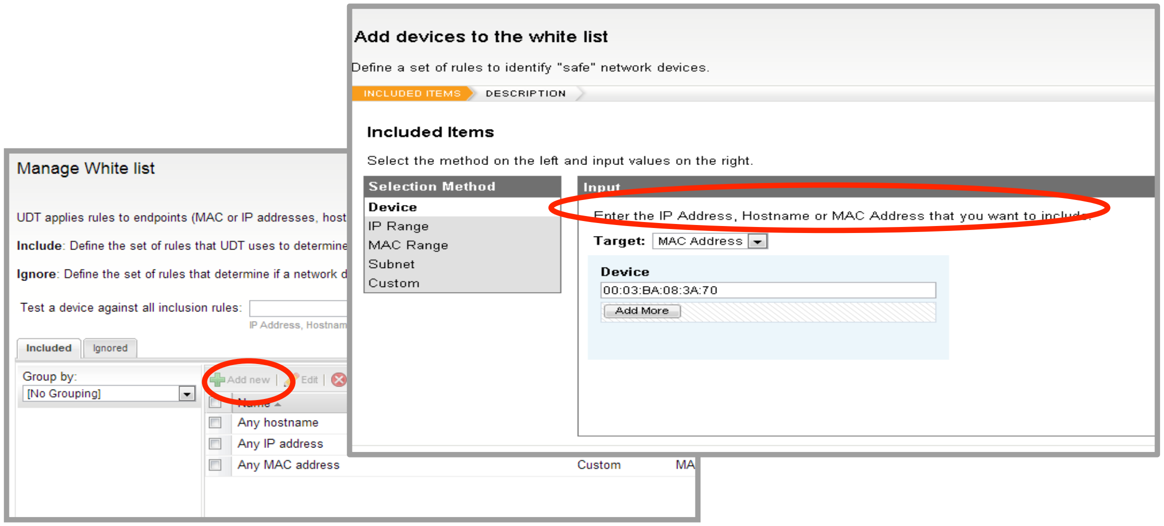
SolarWinds User Device Tracker (UDT)

can be tactically deployed to help you manage the onslaught of mobile devices and keep rogue devices from wreaking havoc on your network.

UDT can help you set up and take charge of your network access security in **3 simple steps**! Here's how…

Step 1

Create Device Whitelist



Add devices to the white list

Define a set of rules to identify "safe" network devices.

Included Items

Select the method on the left and input values on the right.

Selection Method	Input
Device	Enter the IP Address, Hostname or MAC Address that you want to include.
IP Range	Target: MAC Address
MAC Range	Device: 00:03:BA:08:3A:70
Subnet	
Custom	

Manage White list

UDT applies rules to endpoints (MAC or IP addresses, host

Include: Define the set of rules that UDT uses to determine

Ignore: Define the set of rules that determine if a network d

Test a device against all inclusion rules:

IP Address, Hostnam

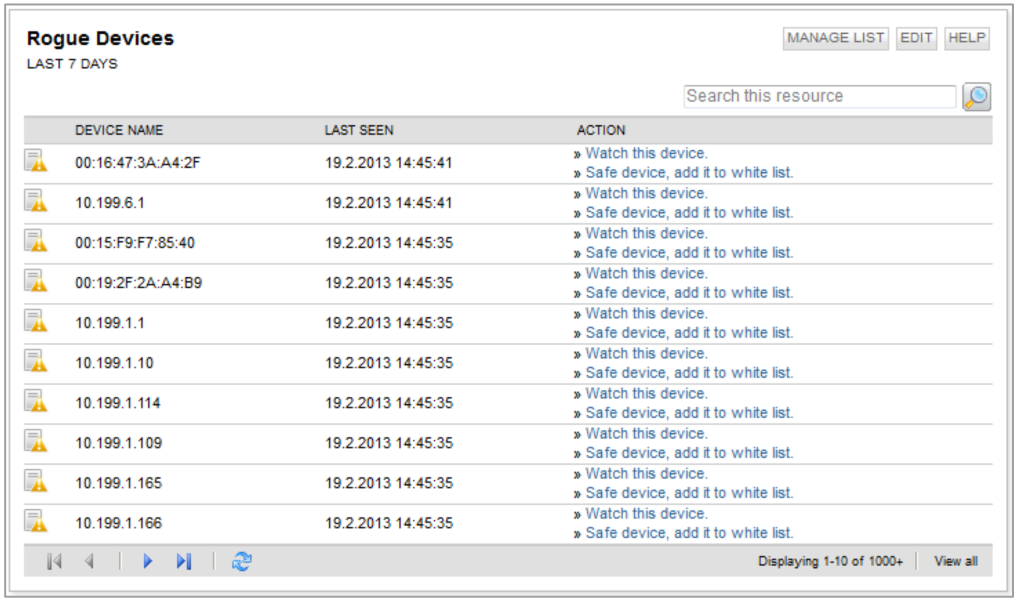
☐	Name		
☐	Any hostname		
☐	Any IP address		
☐	Any MAC address	Custom	MA

- From the UDT web console, specify what devices are allowed to access the network. You can add devices by:
  - Individual IP, MAC address, or hostname
  - IP address ranges
  - MAC address ranges
  - Subnets
  - Custom patterns

Step 1
Create Device Whitelist
Step 2
Set Up Watch List
Step 3
Shutdown Port

Step 1

Create Device Whitelist cont.



Rogue Devices

LAST 7 DAYS

DEVICE NAME	LAST SEEN	ACTION
00:16:47:3A:A4:2F	19.2.2013 14:45:41	» Watch this device. » Safe device, add it to white list.
10.199.6.1	19.2.2013 14:45:41	» Watch this device. » Safe device, add it to white list.
00:15:F9:F7:85:40	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
00:19:2F:2A:A4:B9	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
10.199.1.1	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
10.199.1.10	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
10.199.1.114	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
10.199.1.109	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
10.199.1.165	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.
10.199.1.166	19.2.2013 14:45:35	» Watch this device. » Safe device, add it to white list.

Displaying 1-10 of 1000+ | View all

- Devices are categorized as ‘**Included**’ *(whitelisted)* and ‘**Ignored**’. Those not in the list are marked as ‘**Rogue**’ and an immediate alert will be generated.

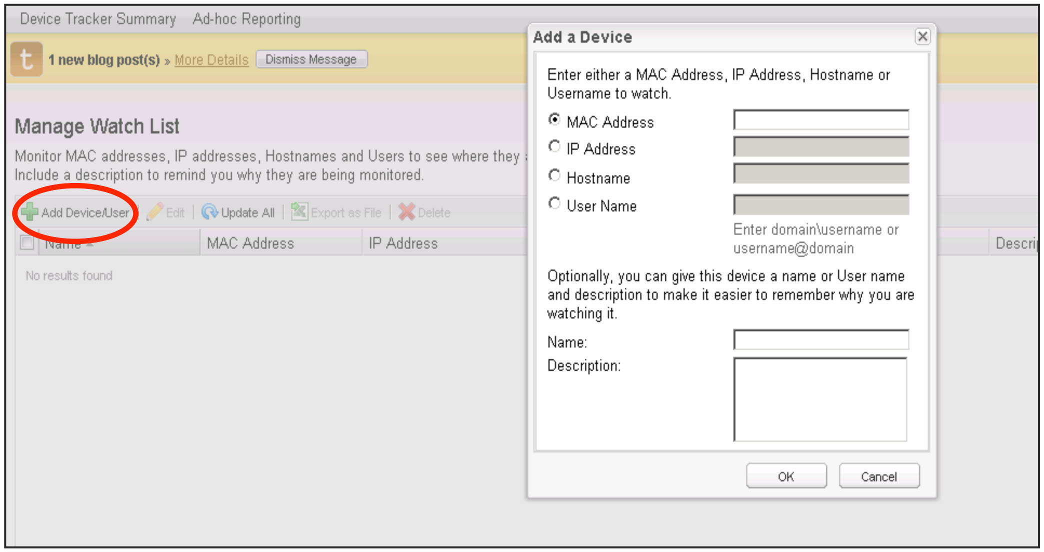
Step 1 Create Device Whitelist

Step 2 Set Up Watch List

Step 3 Shutdown Port

Step 2

Set Up Watch List



Manage Watch List

Monitor MAC addresses, IP addresses, Hostnames and Users to see where they
Include a description to remind you why they are being monitored.

No results found

Add a Device

Enter either a MAC Address, IP Address, Hostname or Username to watch.

● MAC Address

○ IP Address

○ Hostname

○ User Name

Enter domain\username or username@domain

Optionally, you can give this device a name or User name and description to make it easier to remember why you are watching it.

Name:

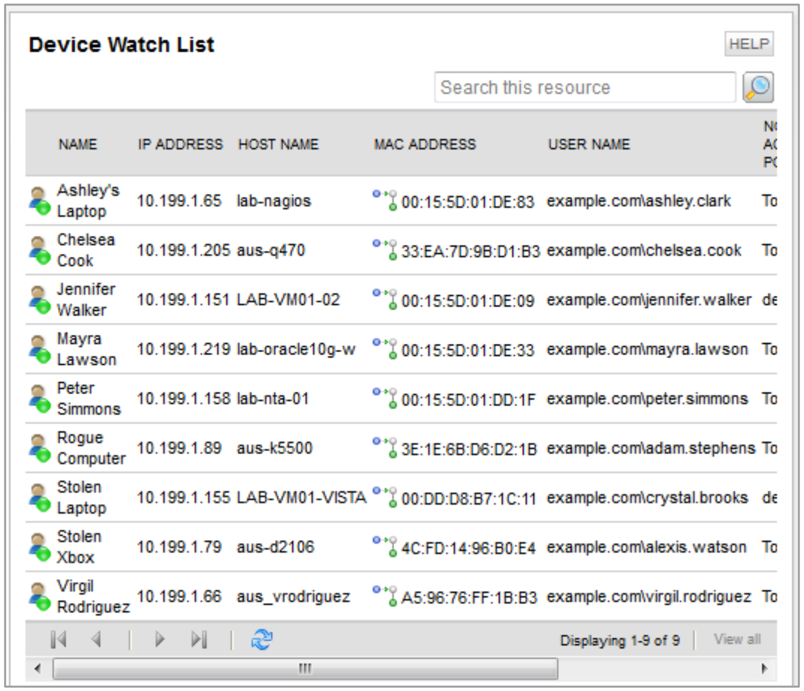
Description:

- To watch for a specific user or device, simply specify a MAC address, IP address, hostname or user name to monitor *(you can even add an optional description to indicate why you are watching it).*

Step 1
Create Device Whitelist
Step 2
Set Up Watch List
Step 3
Shutdown Port

Step 2

Set Up Watch List cont.



Device Watch List

	NAME	IP ADDRESS	HOST NAME	MAC ADDRESS	USER NAME	N A P
	Ashley's Laptop	10.199.1.65	lab-nagios	00:15:5D:01:DE:83	example.com\ashley.clark	To
	Chelsea Cook	10.199.1.205	aus-q470	33:EA:7D:9B:D1:B3	example.com\chelsea.cook	To
	Jennifer Walker	10.199.1.151	LAB-VM01-02	00:15:5D:01:DE:09	example.com\jennifer.walker	de
	Mayra Lawson	10.199.1.219	lab-oracle10g-w	00:15:5D:01:DE:33	example.com\mayra.lawson	To
	Peter Simmons	10.199.1.158	lab-nta-01	00:15:5D:01:DD:1F	example.com\peter.simmons	To
	Rogue Computer	10.199.1.89	aus-k5500	3E:1E:6B:D6:D2:1B	example.com\adam.stephens	To
	Stolen Laptop	10.199.1.155	LAB-VM01-VISTA	00:DD:D8:B7:1C:11	example.com\crystal.brooks	de
	Stolen Xbox	10.199.1.79	aus-d2106	4C:FD:14:96:B0:E4	example.com\alexis.watson	To
	Virgil Rodriguez	10.199.1.66	aus_vrodriguez	A5:96:76:FF:1B:B3	example.com\virgil.rodriguez	To

Displaying 1-9 of 9

- When that user or device on the watch list connects, you will be automatically notified.
- You can then view the node or access point, port or SSID, and VLAN of the device or user being tracked.

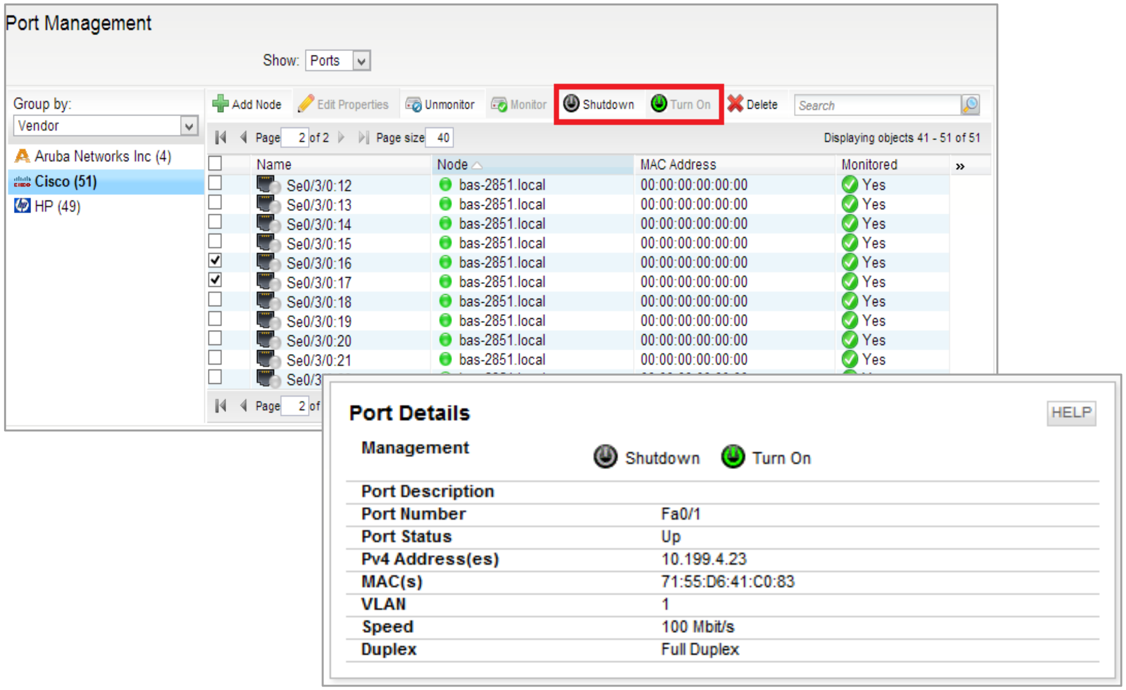
Step 1 Create Device Whitelist

Step 2 Set Up Watch List

Step 3 Shutdown Port

Step 3

Shutdown Port



Displaying objects 41 - 51 of 51

□	Name	Node	MAC Address	Monitored
□	Se0/3/0:12	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:13	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:14	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:15	bas-2851.local	00:00:00:00:00:00	✓ Yes
☑	Se0/3/0:16	bas-2851.local	00:00:00:00:00:00	✓ Yes
☑	Se0/3/0:17	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:18	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:19	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:20	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3/0:21	bas-2851.local	00:00:00:00:00:00	✓ Yes
□	Se0/3			

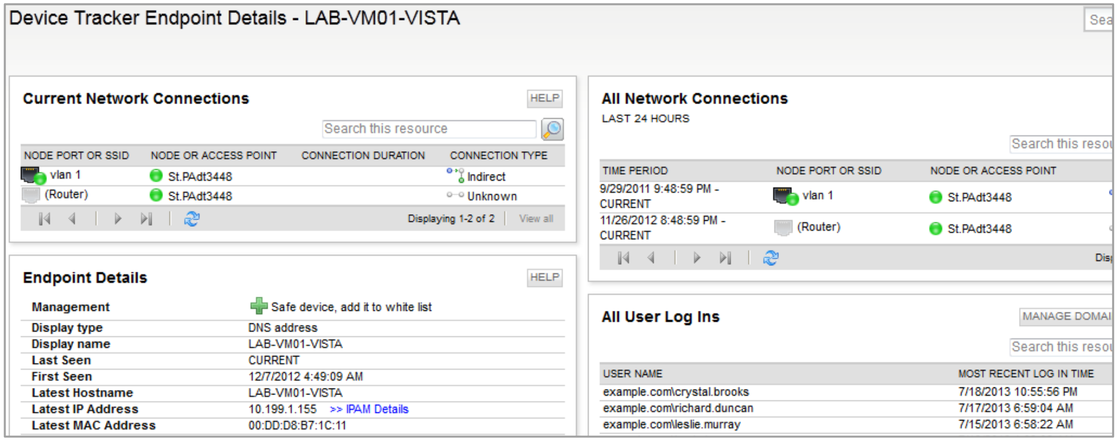
Management	Shutdown Turn On
Port Description	
Port Number	Fa0/1
Port Status	Up
Pv4 Address(es)	10.199.4.23
MAC(s)	71:55:D6:41:C0:83
VLAN	1
Speed	100 Mbit/s
Duplex	Full Duplex

- If you suspect a malicious user or believe a port has been compromised, simply shut down the port directly from the UDT console with the ***click-of-a-button***.

Step 1
Create Device Whitelist
Step 2
Set Up Watch List
Step 3
Shutdown Port

Step 3

Shutdown Port cont.



Device Tracker Endpoint Details - LAB-VM01-VISTA

Current Network Connections

NODE PORT OR SSID	NODE OR ACCESS POINT	CONNECTION DURATION	CONNECTION TYPE
vlan 1	St.PAdt3448		Indirect
(Router)	St.PAdt3448		Unknown

Displaying 1-2 of 2

Endpoint Details

Management	Safe device, add it to white list
Display type	DNS address
Display name	LAB-VM01-VISTA
Last Seen	CURRENT
First Seen	12/7/2012 4:49:09 AM
Latest Hostname	LAB-VM01-VISTA
Latest IP Address	10.199.1.155 >> IPAM Details
Latest MAC Address	00:DD:D8:B7:1C:11

All Network Connections

LAST 24 HOURS

TIME PERIOD	NODE PORT OR SSID	NODE OR ACCESS POINT
9/29/2011 9:48:59 PM - CURRENT	vlan 1	St.PAdt3448
11/26/2012 8:48:59 PM - CURRENT	(Router)	St.PAdt3448

All User Log Ins

USER NAME	MOST RECENT LOG IN TIME
example.com\crystal.brooks	7/18/2013 10:55:56 PM
example.com\richard.duncan	7/17/2013 6:59:04 AM
example.com\leslie.murray	7/15/2013 6:58:22 AM

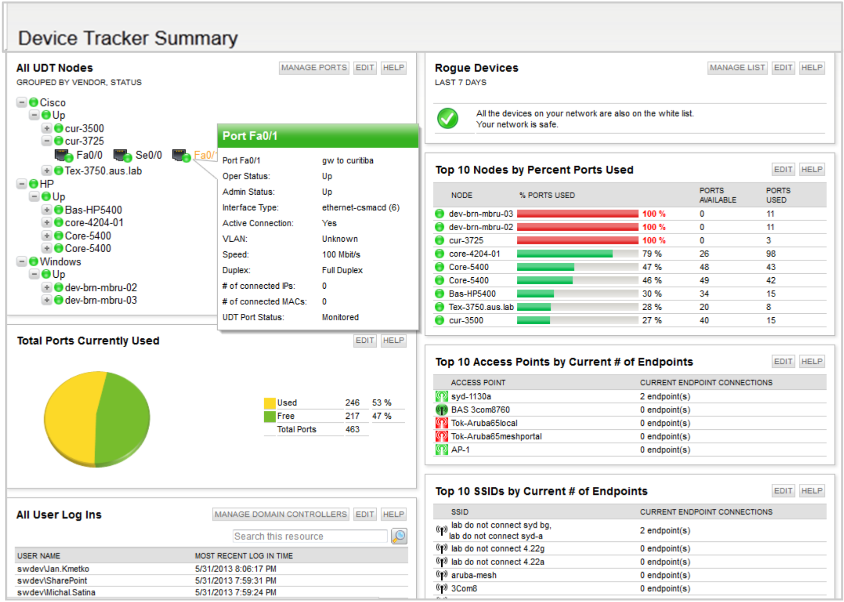
- Plus, you can view device port details, user logins, and connection history to easily investigate and troubleshoot a network problem.

Step 1 Create Device Whitelist

Step 2 Set Up Watch List

Step 3 Shutdown Port

Done!



Device Tracker Summary

All UDT Nodes
GROUPED BY VENDOR, STATUS

- Cisco
  - Up
    - cur-3500
    - cur-3725
      - Fa0/0 Se0/0 Fa0/1
    - Tex-3750.aus.lab
- HP
  - Up
    - Bas-HP5400
    - core-4204-01
    - Core-5400
    - Core-5400
- Windows
  - Up
    - dev-brn-mbru-02
    - dev-brn-mbru-03

Port Fa0/1

Port Fa0/1	gw to curitiba
Oper Status:	Up
Admin Status:	Up
Interface Type:	ethernet-csmacd (6)
Active Connection:	Yes
VLAN:	Unknown
Speed:	100 Mbit/s
Duplex:	Full Duplex
# of connected IPs:	0
# of connected MACs:	0
UDT Port Status:	Monitored

Total Ports Currently Used

🟨	Used	246	53 %
🟩	Free	217	47 %
	Total Ports	463	

All User Log Ins

USER NAME	MOST RECENT LOG IN TIME
swdev\Jan.Kmetko	5/31/2013 8:06:17 PM
swdev\SharePoint	5/31/2013 7:59:31 PM
swdev\Michal.Satina	5/31/2013 7:59:24 PM

Rogue Devices
LAST 7 DAYS

✓ All the devices on your network are also on the white list.
Your network is safe.

Top 10 Nodes by Percent Ports Used

NODE	% PORTS USED	PORTS AVAILABLE	PORTS USED
dev-brn-mbru-03	100 %	0	11
dev-brn-mbru-02	100 %	0	11
cur-3725	100 %	0	3
core-4204-01	79 %	26	98
Core-5400	47 %	48	43
Core-5400	46 %	49	42
Bas-HP5400	30 %	34	15
Tex-3750.aus.lab	28 %	20	8
cur-3500	27 %	40	15

Top 10 Access Points by Current # of Endpoints

ACCESS POINT	CURRENT ENDPOINT CONNECTIONS
syd-1130a	2 endpoint(s)
BAS 3com8760	0 endpoint(s)
Tok-Aruba65local	0 endpoint(s)
Tok-Aruba65meshportal	0 endpoint(s)
AP-1	0 endpoint(s)

Top 10 SSIDs by Current # of Endpoints

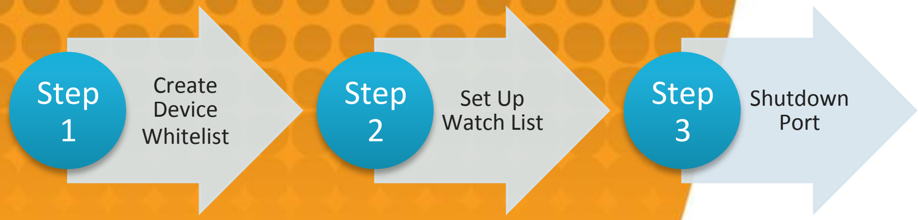
SSID	CURRENT ENDPOINT CONNECTIONS
lab do not connect syd bg, lab do not connect syd-a	2 endpoint(s)
lab do not connect 4.22g	0 endpoint(s)
lab do not connect 4.22a	0 endpoint(s)
aruba-mesh	0 endpoint(s)
3Com8	0 endpoint(s)

You are now set up for Active Network Access Security. Keep all unwanted Devices and Users out!

Take control of who and what accesses your network!

SolarWinds User Device Tracker(UDT)

Active Network Access Security



Step 1 Create Device Whitelist

Step 2 Set Up Watch List

Step 3 Shutdown Port

UDT

Key Features and Benefits of SolarWinds UDT

- Automatically discover, map, and monitor switches, ports, and network devices—wired or wireless
- Quickly find devices and retrieve the user name, switch port details, connection history and more
- Track current or past location of users and devices
- Create a whitelist to identify safe vs. rogue devices
- Get an automatic alert when a rogue endpoint or watched user/device connects
- Remotely shut down a compromised port with the click-of-a-button
- Get detailed switch port usage data, capacity analysis, and built-in reporting.

UDT

SolarWinds User Device Tracker

Active Network Access Security

Learn More