



KASEYA INTERNATIONAL LIMITED



Our Automation. Your Liberation.™

RELEASE ANNOUNCEMENT
Kaseya Network Discovery and Network
Monitoring
Version 1.0

ANNOUNCEMENT DATE: DECEMBER 2010

TARGET AVAILABILITY: DECEMBER 2010

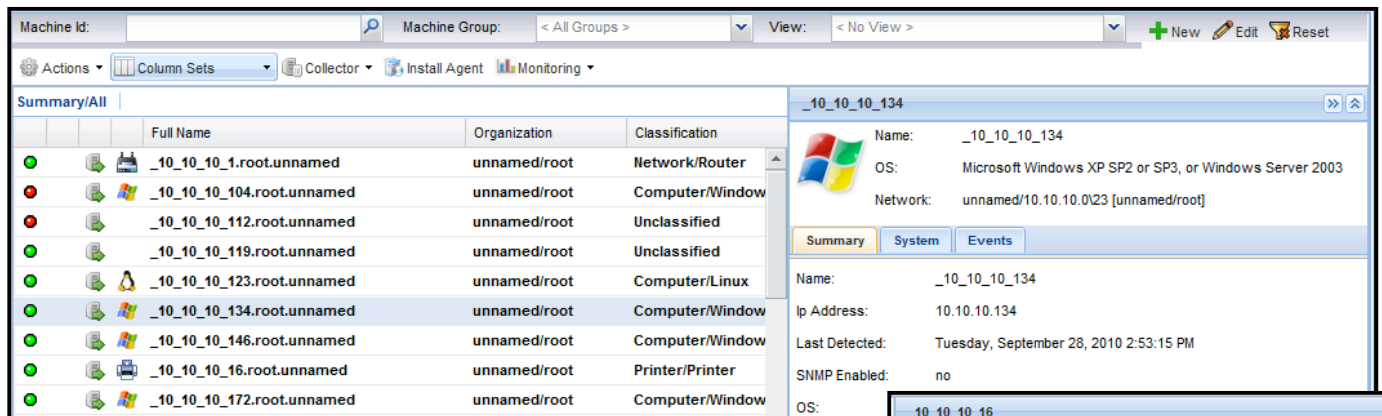
TABLE OF CONTENTS

OVERVIEW	1
NETWORK DISCOVERY	2
DISCOVER DEVICES	2
<i>Collector</i>	2
MULTIPLE SCAN METHODS.....	2
VIEW DISCOVERED DEVICES.....	2
<i>Device Types</i>	2
<i>Column Sets</i>	2
<i>Property Sheet</i>	2
<i>Device Navigator</i>	2
DEPLOY AGENTS AUTOMATICALLY	2
NETWORK MONITORING.....	2
RELEASE LOGISTICS.....	3
UPDATE BEST PRACTICES	3
AVAILABILITY	3
WEB CASTS AND TRAINING	3

KASEYA NETWORK DISCOVERY AND NETWORK MONITORING

OVERVIEW

Simply said, if you cannot find everything connected to the network, you cannot manage it. The role of Kaseya Network Discovery is to find all IP based devices connected and interconnected to a network or networks. Once these devices are discovered, they will be cataloged within the system. The Network Discovery process will run periodically to discover new devices or devices that are no longer visible within the network and provide for automated agent deployment for instant management of Windows, Mac and Linux devices. Network Monitoring utilizes SNMP to provide a graphical view of CPU, RAM, Disk and Network Interface data. As is the case with all Kaseya functionality, the Network Discovery and Network Monitoring is completely integrated within the Kaseya framework to ensure a Single Pane of Glass web-based interface for network administrators.



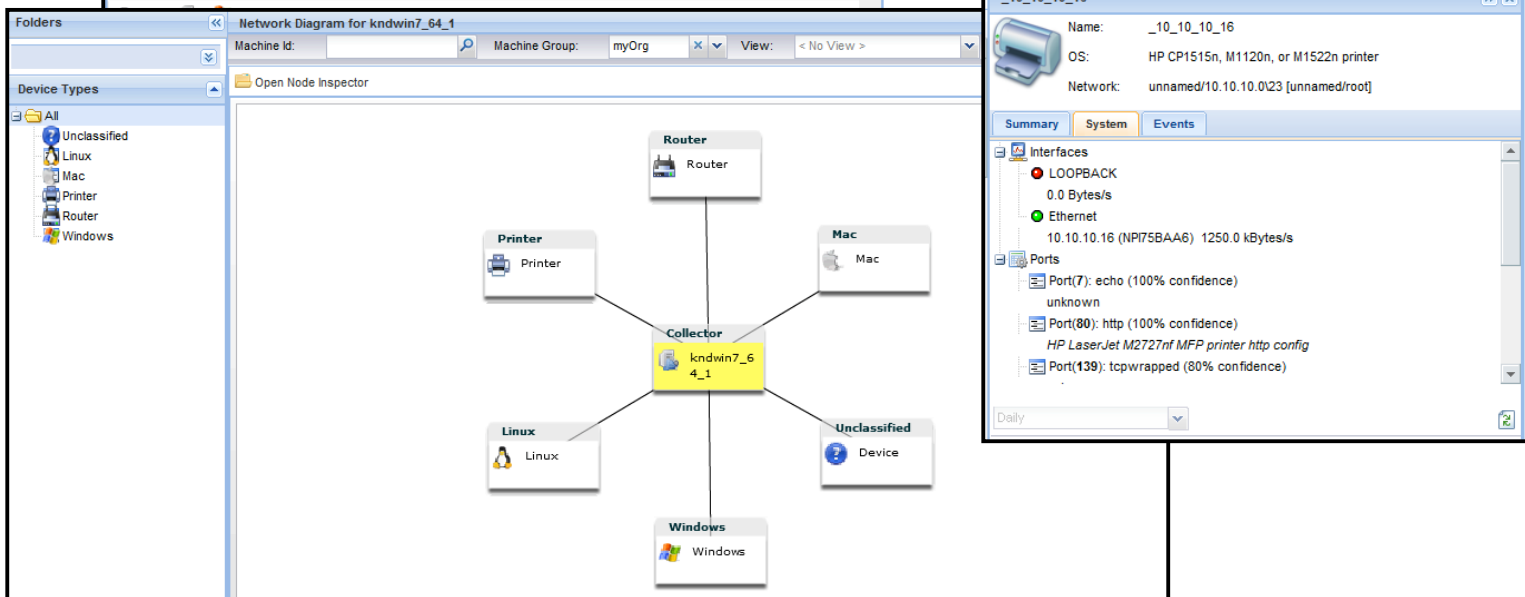
Full Name	Organization	Classification
_10_10_10_1.root.unnamed	unnamed/root	Network/Router
_10_10_10_104.root.unnamed	unnamed/root	Computer/Window
_10_10_10_112.root.unnamed	unnamed/root	Unclassified
_10_10_10_119.root.unnamed	unnamed/root	Unclassified
_10_10_10_123.root.unnamed	unnamed/root	Computer/Linux
_10_10_10_134.root.unnamed	unnamed/root	Computer/Window
_10_10_10_146.root.unnamed	unnamed/root	Computer/Window
_10_10_10_16.root.unnamed	unnamed/root	Printer/Printer
_10_10_10_172.root.unnamed	unnamed/root	Computer/Window

Machine Details: _10_10_10_134

Name: _10_10_10_134
 OS: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
 Network: unnamed/10.10.10.0/23 [unnamed/root]

Summary | System | Events

Name: _10_10_10_134
 Ip Address: 10.10.10.134
 Last Detected: Tuesday, September 28, 2010 2:53:15 PM
 SNMP Enabled: no
 OS:



Network Diagram for kndwin7_64_1

Machine Id: Machine Group: myOrg View: < No View >

Open Node Inspector

```

graph TD
    Router[Router] --- Collector[kndwin7_64_1]
    Printer[Printer] --- Collector
    Mac[Mac] --- Collector
    Linux[Linux] --- Collector
    Unclassified[Unclassified Device] --- Collector
    Windows[Windows] --- Collector
            
```

Machine Details: _10_10_10_16

Name: _10_10_10_16
 OS: HP CP1515n, M1120n, or M1522n printer
 Network: unnamed/10.10.10.0/23 [unnamed/root]

Summary | System | Events

Interfaces

- LOOPBACK: 0.0 Bytes/s
- Ethernet: 10.10.10.16 (NP175BAA6) 1250.0 kBytes/s

Ports

- Port(7): echo (100% confidence) unknown
- Port(80): http (100% confidence) HP LaserJet M2727nF MFP printer http config
- Port(139): tcpwrapped (80% confidence)



NETWORK DISCOVERY

Discover Devices

Collector

Network Discovery is collector based and can be installed on any Windows based system that has a Kaseya agent installed. This system should be one with high availability and access to the local network. The availability information is displayed within the Collector installation function.

Multiple collectors can be deployed within a given network.

Multiple Scan Methods

Network Discovery includes multiple scanning methods to ensure all devices across a network can be scanned and catalogued with immediate knowledge of the device type. Each method will scan by Network Mask or 23 bit network by default and will process based on pre-defined intervals.

The scan methods include:

- Ping Scan– Mac Address
- Port Scan – OS and Device Type
- SNMP Scan – System Attributes, Interfaces, Drives, CPU, RAM

View Discovered Devices

Device Types

A new device type option has been introduced to help administrators quickly filter out specific devices from the lists being displayed. The Device Types are displayed in a tree folder structure with viewable counts for each device type. Selecting the folder will dynamically filter the list and also provide sub-filtering options.

Column Sets

Pre-defined and customizable column sets retrieve filtered device information based on catalogued data.

Filter criteria includes:

- Hardware
- Network Address
- Collector Installed
- Managed Agents
- Discovered Devices
- Summary
- Categories of Devices

Property Sheet

A docked tabbed property sheet displays key device status information for the highlighted device.

- Device Type including OS Type
- Version
- IP Address
- RAM, DISK, CPU
- Interfaces
- Ports

Device Navigator

A visual navigator provides a snapshot view of devices found by the collector. By selecting device types including Windows, Mac, Linux, Printer and Router, the view can be filtered to allow for different navigational views.

Deploy Agents Automatically

Begin managing systems immediately. Network Discovery provides automatic agent deployment for Windows, Mac or Linux agents. Customized agent installation packages can be assigned to a single device or group of Windows, Mac or Linux operating systems.

NETWORK MONITORING

Network Monitoring provides a view into SNMP data from enabled devices. In this release, the monitoring is limited to a graphical view of the information collected.

Simply turn on the SNMP option for the device and the system will collect and allow for viewing current and historical device information in a graphical format. This functionality does not require a Kaseya agent to be installed on the device being monitored.



The following information is displayed for computers:

- CPU
- RAM
- Disk
- Network Interfaces

The following information is displayed for non-computer SNMP devices such as routers, printers and switches:

- Network Interfaces

RELEASE LOGISTICS

Update Best Practices

We know that Kaseya is a mission critical application within your organization. As such, proper planning and process is necessary for upgrades or changes to these systems. Failure to plan properly and follow a change management process will yield less than desirable results.

Availability

General Availability – December 15, 2010

Available to all Kaseya 2 version 6.01 or higher Master IT Service Edition (MITSE) or Enterprise Edition (EE) on-premises customers current on maintenance.

Web Casts and Training

December 14, 2011 thru Q1 2011 – Overview, Upgrade and Training



Kaseya Corporation makes no representations or warranties with respect to the contents of this publication and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice.

©Copyright 2010 by Kaseya Corporation. All Rights Reserved.
No part of this publication may be reproduced in any form without the prior written consent of Kaseya Corporation.

Trademark Acknowledgments:
All other trademarks are the property of their respective owners.