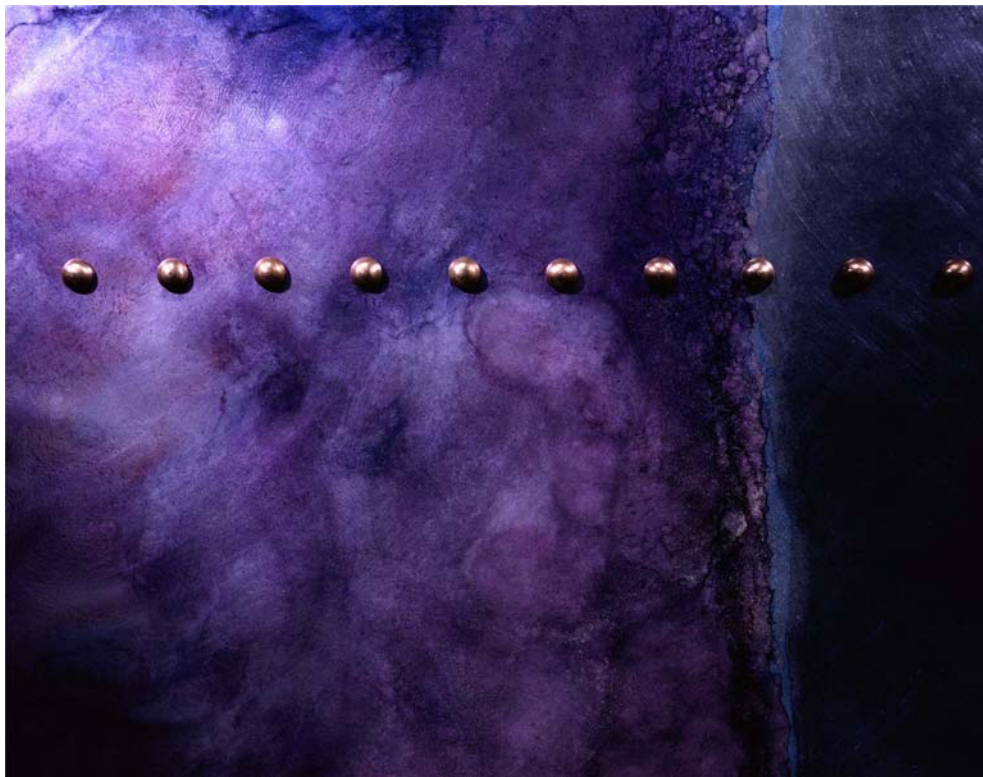


Alloy Discovery Express 8

Comprehensive Network Inventory Solution for Network Administrators and IT Service Providers



Product Version: 8.0

Document Date: June 27, 2019

Alloy Software Incorporated
400 Broadacres Dr, Suite 100, Bloomfield,
NJ 07003, USA

phone: +1 (973) 661-9700
fax: +1 (973) 661-9777
e-mail: sales@alloysoftware.com
web: www.alloysoftware.com



Copyright © 2020 Alloy Software, Inc. All rights reserved. Alloy Software, Alloy Navigator, Alloy Navigator Express, Alloy Discovery, and Alloy Discovery Express logos are registered trademarks owned by Alloy Software, Inc. All other trademarks and brand names are the property of their respective owners. This manual, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Alloy Software, Inc. Alloy Software, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this book. This manual is protected by United States and foreign copyright. This manual shall not be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior permission of Alloy Software, Inc.

Portions of the software described in this manual may utilize or include third party software and other copyrighted material. For details, see the `acknowledgments.txt` files located in the `Documentation` folders under your Alloy Discovery Express installation folder (typically, `C:\Program Files\Alloy Software\Alloy Discovery Express 8\Documentation\`).

Table of Contents

PREFACE	1
About This Document	1
Document Audience	1
Product Documentation Available for Alloy Discovery Express 8	1
Document Conventions	2
About Screenshots	3
CHAPTER 1. Introducing Alloy Discovery Express	4
Alloy Discovery Express at a Glance	4
Basic Architecture	4
Overview of Audit Methods	5
On-Demand Audit	5
On-Demand Audit on Schedule	6
Scriptable Audit	6
Audit via E-mail	6
Portable Audit	6
Alloy Control Panel	6
CHAPTER 2. Installing Alloy Discovery Express	8
Planning Your Installation	8
Supported Platforms and System Requirements	8
Additional Software Requirements and Related Links	12
Licensing Alloy Discovery Express	14
Installing Alloy Discovery Express	14
Running Setup	14
Updating Alloy Discovery Express License	15
Next Steps	15
CHAPTER 3. Upgrade to the Latest Version	17
Upgrade from Alloy Discovery Express 7	17
CHAPTER 4. Quick Start with Alloy Discovery Express	20
Running the Application	20
Instant Audit with the Quick Start Wizard	20
Next Steps	23
CHAPTER 5. Configuring Alloy Discovery Express	24
Configuring the Audit	24
Configuring the Capture of Registry Keys	26
Configuring Event Log Options	31
Configuring File Scan Options	34
Configuring the SMBIOS Filter	38
Configuring the Progress Indicator	41
Configuring Available Controls	42
Configuring Custom Input Fields	44
Configuring the Exclusion Rules	47
Setting the Bypass Rules	48
Next Steps	50

CHAPTER 6. Auditing Computers with Alloy Discovery Express	51
On-Demand Audit	51
Managing Audit Credentials	51
Enabling SNMP Discovery	53
Auditing Groups of Computers and Devices	55
Auditing Standalone Computers or Devices	68
Scheduling an On-Demand Audit	69
Scriptable Audit	70
Deploying the Inventory Analyzer onto a Shared Folder	70
Automating the Scriptable Audit	72
Next Steps	79
Audit via E-mail	79
Creating E-mail Audit Groups	80
Building Inventory Analyzer packages for the Audit via E-mail	84
Running the Audit via E-mail on the Target Network	86
Checking E-mail Audit Groups for New Snapshots	87
Next Steps	88
Portable Audit	89
Building Inventory Analyzer Packages for the Portable Audit	90
Running the Portable Audit on Client Machines	92
Transporting Audit Snapshots to the Inventory Repository	92
Next Steps	92
Auditing Linux and Mac Computers	93
Specifying Connection Parameters for VMware ESX / ESXi Hypervisors	93
CHAPTER 7. Analyzing Audit Snapshots	95
Viewing Software and Hardware Inventory	95
Analyzing Inventory Data using Groups	95
Viewing File Scan Results	97
Searching For Files	98
Viewing File Statistics	99
Viewing Individual Audit Snapshots	100
Previewing Computer Data	100
Viewing SNMP Data	101
Viewing Audit Snapshots	103
Viewing Network Device Details	108
Working with Audit Properties	110
Reclassifying Unrecognized Computers or Network Devices	111
Specifying Individual SNMP Credentials	113
Specifying Individual Audit Credentials	114
Working with Static and Dynamic Computer Groups	115
Configuring Dynamic Computer Groups	116
CHAPTER 8. Advanced Options	119
Understanding Audit Snapshots	119
Comparing Audit Snapshots	120
Understanding the Audit Snapshot Viewer	122
Configuring Computer List	123
External Tools	125
Configuring External Tools	127
User-Defined Fields	129
Working with User-Defined Fields	129
Storing Data in User-Defined Fields	130

Batch Updating User-Defined Fields	130
Associating Virtual Machines with Host Machines	131
Automatic Association of Virtual Machines to their Hypervisor Hosts	131
Manual Association of Virtual Machines to their Hypervisor Hosts	131
Inventory Analyzer Command-Line Options	132
Output Options	132
User ID Options	132
Mode Options	133
Inventory Options	133
Interactive Mode Options	133
E-mail Options	133
Linux Inventory Analyzer Command-Line options	134
Mac Inventory Analyzer Command-Line options	136
Report Designer	138
CHAPTER 9. Troubleshooting	139
Troubleshooting the On-Demand Audit	139
Windows On-Demand Audit	139
Linux and Mac On-Demand Audit	150
Hypervisor On-Demand Audit	154
Troubleshooting Agent-Based Audit	156
Windows Audit	156
Linux Audit	158
Mac Audit	159
CHAPTER 10. Contact Information	161
About Alloy Software	161
Follow Us	161
Obtain Technical Support	161
Contact Us	162
Online	162
E-Mail	162
Phone	162
Fax	162
Mailing Address	162
CHAPTER 11. Glossary	163
Audit	164
Audit Agent	164
Audit Configuration	164
Audit Snapshot	164
Audit Snapshot Viewer	164
Audit Group	164
Audit via E-mail	164
Built-in Mode	164
Client Machine	164
Computer Group	165
Default On-Demand Audit Credentials	165
Dynamic Group	165
E-mail Audit Group	165
External Audit Snapshot Source Group	165
Group for the On-Demand Audit of an IP Address Range	165
Group for the On-Demand Audit on a Windows Domain	165

Hardware and Software Inventory165
Host Machine165
Hypervisor165
Interactive Mode165
Interactive Once Mode165
Intermediary Repository166
Inventory Analyzer166
Inventory Analyzer Package166
Inventory Repository166
Minimally Necessary Permissions166
On-Demand Audit166
On-Demand Audit Credentials167
On-Demand Audit Group167
Portable Audit167
Scriptable Audit167
Scriptable Audit Group167
Shared Folder Machine167
Sidebar167
Silent Mode167
SMBIOS Filter167
SNMP167
Standalone Mode167
Static Group168
Style168
UNC168

List of Figures

Figure 1:	Audit Methods Diagram	5
Figure 2:	Alloy Control Panel	7
Figure 3:	Specifying an IP address range.	21
Figure 4:	Providing Credentials for On-Demand Audit Account.	22
Figure 5:	Audit Settings Dialog	24
Figure 6:	Registry Keys	26
Figure 7:	Edit Registry Key dialog box.	27
Figure 8:	Microsoft Registry Editor	28
Figure 9:	Adding Registry Key	29
Figure 10:	Event Log Options.	31
Figure 11:	Adding a filtering condition	33
Figure 12:	Filtering criteria for capturing Event Log events	34
Figure 13:	File Scan Options	34
Figure 14:	Adding drive E to the file scan	36
Figure 15:	SMBIOS Filter	40
Figure 16:	Display Options.	41
Figure 17:	Available Controls	42
Figure 18:	Inventory Analyzer Splash Screen with All Controls Enabled	43
Figure 19:	Custom Input Fields	44
Figure 20:	Editing Custom Field	45
Figure 21:	Exclusion Rules	47
Figure 22:	Bypass Rules	49
Figure 23:	Default On-Demand Audit Credentials	52
Figure 24:	Default SNMP Settings.	55
Figure 25:	Specifying an IP address range.	58
Figure 26:	Specifying Custom On-Demand Audit Account	59
Figure 27:	Specifying group SNMP settings	60
Figure 28:	Finishing the New Group Wizard.	62
Figure 29:	On-Demand Audit Group Created	62
Figure 30:	Status of the Discovering Process	63
Figure 31:	Computers Discovered.	64
Figure 32:	On-Demand Audit Status pane	65
Figure 33:	On-Demand Audit Status dialog box	66
Figure 34:	Audited On-Demand Audit Group	67

Figure 35:	Auditing a Single Computer	68
Figure 36:	Scheduled On-Demand Audit Status shown in the System Tray	69
Figure 37:	Creating Network Share on the Alloy Discovery Express Host Machine	72
Figure 38:	Auditing Computers on a Windows Domain	73
Figure 39:	Registry Editor	76
Figure 40:	Startup Menu Items	77
Figure 41:	Inventory Analyzer as a Scheduled Task	78
Figure 42:	Auditing Computers via E-mail	80
Figure 43:	Configuring Incoming Mail Server Settings.	82
Figure 44:	Configuring Outgoing Mail Server Settings (New Group Wizard).	83
Figure 45:	Configuring Outgoing Mail Server Settings (Portable Audit Wizard).	85
Figure 46:	Processing E-mail Messages	88
Figure 47:	Auditing Non-Networked Computers	89
Figure 48:	Specifying Destination Folder	91
Figure 49:	Computer List tab Being Filtered by Operating System	97
Figure 50:	Searching for files within the results of the Detailed File Scan	98
Figure 51:	Viewing file statistics gathered by the Summary File Scan	99
Figure 52:	Preview Pane	101
Figure 53:	Previewing SNMP Data from a Network Device.	102
Figure 54:	Computer Snapshot, System Overview	103
Figure 55:	Computer Snapshot, Windows Device Drivers	107
Figure 56:	Network Device Details dialog box	109
Figure 57:	Specifying the type of unrecognized network device.	111
Figure 58:	Specifying the OS type of unrecognized computer	112
Figure 59:	Specifying individual SNMP credentials	114
Figure 60:	Specifying individual audit credentials	115
Figure 61:	An inclusion rule for a single attribute	117
Figure 62:	An inclusion rule for a multiple attribute	118
Figure 63:	Viewing Snapshot File Name	120
Figure 64:	The Compare With dialog box	121
Figure 65:	Comparing Audit Snapshot Files	122
Figure 66:	Viewing File Scan results in Audit Snapshot Viewer.	123
Figure 67:	Configuring the Computer List	124
Figure 68:	External Tools (Preview Pane)	125
Figure 69:	The External Tools dialog.	127
Figure 70:	"Ping" Properties.	128

Figure 71:	Configuring user-defined fields129
Figure 72:	Accessing the default domain policy143
Figure 73:	Accessing the domain profile144
Figure 74:	Selecting the profile item144
Figure 75:	Enabling the File and Printer Sharing Exception145
Figure 76:	Viewing the File and Printer Sharing firewall exception on a Windows 7 computer .	.146
Figure 77:	Creating a Windows Inventory Analyzer debug package157

PREFACE

Welcome to the *Alloy Discovery Express 8 Administration Guide*.

About This Document

Document Audience

The *Alloy Discovery Express 8 Administration Guide* (the *Administration Guide*) targets system administrators who install, configure, manage, and work with Alloy Discovery Express 8 (ADX8). This guide provides a complete overview of the installation and configuration steps to help you get started with *Alloy Discovery Express*.

It is expected that the reader has a good knowledge and the skills necessary for system administration.






Product Documentation Available for Alloy Discovery Express 8



Alloy Software offers a collection of product documentation to help you get the most out of our products.

Document	Description
Help System	<p>The Help System can be accessed by pressing the F1 key, and contains specific information about your current location (context-sensitive help). There may be tips about using the current dialog box or details about the functions and buttons in that box.</p> <p>You may also access the Help System by clicking Help > Help Contents from within the application's main menu.</p>

Document Conventions

The following table summarizes stylistic conventions used throughout the document.

Typeface	Usage
Bold	Bold type indicates interface items: buttons, check boxes, menu items, dialog box captions, etc. <i>Example:</i> Choose Audit > Audit Settings from the main menu.
<i>Italic</i>	Italic type is used for new terms and the titles of other resources. <i>Example:</i>  For details, see the <i>Help System: Displaying Computer Details</i> .
>	The right-pointing arrow indicates a series of menu or navigation selections. <i>Example:</i> Choose Tools > External Tools from the main menu and click the tool name.
Fixed-width font	Fixed-width font indicates a filename, path, or a code example. It also indicates placeholders for different parameters to provide. <i>Example:</i> By default, the installer extracts its installation package to the following directory: <code>C:\AlloyDiscoveryExpress.cd\</code>
	The warning icon indicates a warning or caution. <i>Example:</i>  If your network is a domain network managed by a network administrator, you might not be able to change the network location.
	The bulb icon indicates a note or tip. <i>Example:</i>  When the Audit Configuration is changed or the audit agents are updated, you need to re-create the Inventory Analyzer packages and re-deploy them.

Typeface	Usage
	<p>The information icon indicates a reference to another related material.</p> <p><i>Example:</i></p> <p> For details, see "Obtain Technical Support" on page 161.</p>

About Screenshots

The screenshots in this guide have been optimized for printing. If you are reading this PDF on your computer screen, we recommend increasing magnification level to 120% or above to see a legible image.

CHAPTER 1. Introducing Alloy Discovery Express

Alloy Discovery Express is a budget-friendly, easy-to-deploy solution for automated discovery and audit of networked and standalone computers, collecting and analyzing their hardware and software configurations.

Alloy Discovery Express at a Glance

Alloy Discovery Express provides offers the following features:

- Automated discovery, identification, and analysis of computers, network devices, and installed software assets throughout your organization.
- Audit of networked and non-networked physical and virtual computers running Windows, Linux, and macOS.
- Automated discovery and identification of networked computers and SNMP devices.
- Accurate inventory of installed software products.
- Web reporting for publishing audit results on your intranet.
- Reporting and charting.
- Automatic grouping of audited computers based on custom criteria.

Basic Architecture

Alloy Discovery Express includes the following modules:

- **Main Console** — The Main Console is a user interface for IT personnel to *Alloy Discovery Express* functions. The console provides you with all the tools you need to configure, deploy, and run the audit. It also provides analytical and reporting tools to analyze and interpret audit results.
- **Inventory Analyzer** — The Inventory Analyzer is an audit agent that captures the information about hardware configurations and installed software, and produces audit snapshots. There are three platform-dependant versions of the Inventory Analyzer: Windows Inventory Analyzer, Linux Inventory Analyzer, and macOS Inventory Analyzer.
- **Audit Snapshot Viewer** — The Audit Snapshot Viewer is a tool included in *Alloy Discovery Express* for viewing audit snapshots. *Alloy Discovery Express* uses the Audit Snapshot Viewer to display the content of audit snapshots in the Main Console. The Audit Snapshot Viewer can also be used as a standalone tool for viewing audit snapshots from the command line.
- **ADT to XML conversion utility** — This is a command-line utility for converting audit snapshots to XML format.
- **Web Reporting module** — The Web Report Module is a command-line utility for generating HTML reports.

Overview of Audit Methods

The following diagram introduces the methods that you can use to audit computers with *Alloy Discovery Express* and helps you to understand which methods suit your environment.

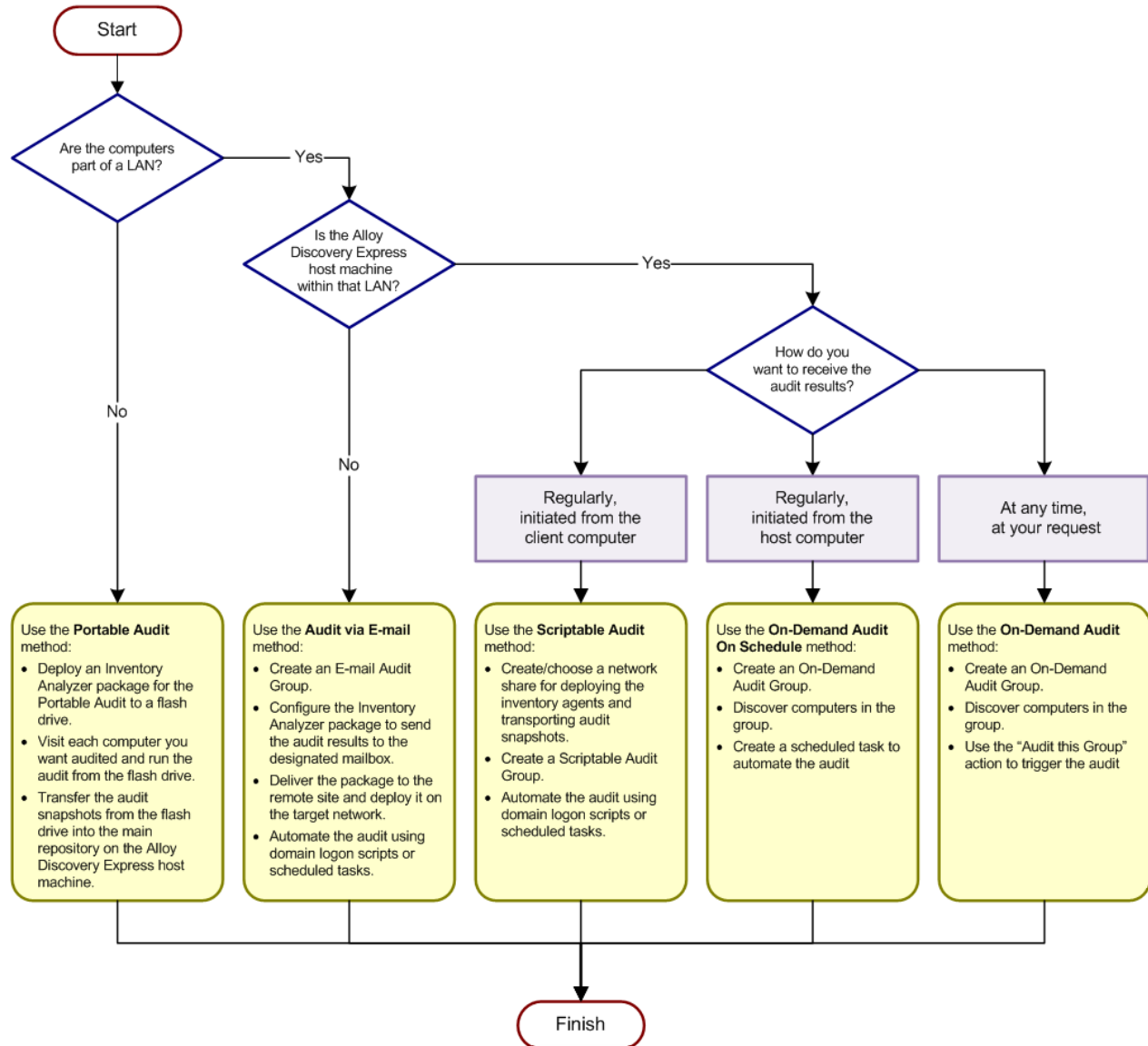


Figure 1: Audit Methods Diagram

On-Demand Audit

The On-Demand Audit is a method of auditing LAN computers and discovering network devices at your request, without the need to deploy standalone audit agents. Built-in audit agents audit multiple networked computers running Windows, Linux, or Mac OS X simultaneously for up-to-the-minute audit snapshots.

On-Demand Audit on Schedule

The On-Demand Audit on Schedule is an agentless method of auditing LAN computers and discovering network devices. With this feature, you can schedule the silent agentless On-Demand Audit method to audit the specified computers on a regular basis. For example, you may create a Windows Scheduled Task that runs a batch file at your desired interval.

Scriptable Audit

The Scriptable Audit is a method of LAN audit, based on using standalone audit agents. With this method you can audit networked computers on a regular basis. It involves two steps: the deployment of the Inventory Analyzer package to a centralized location, accessible by all networked computers (i.e. a network shared folder), and the automation of the Inventory Analyzer using domain logon scripts or scheduled tasks. Audit snapshots are stored in an intermediary repository on the same network share until they are loaded by *Alloy Discovery Express* into the main Inventory Repository. *Alloy Discovery Express* automatically reflects changes in the audit configuration on the host machine in the configuration of the deployed audit agents.

Audit via E-mail

The Audit via E-mail is a method of WAN audit, based on using standalone audit agents. This audit method is similar to the Scriptable Audit method, however the network share where the Inventory Analyzer package is being deployed is accessible only by computers on the external (remote) network, with no direct connection from the local network.


This method involves two steps: the deployment of the Inventory Analyzer Package to the target network and the automation the Inventory Analyzer on that network using domain logon scripts or scheduled tasks. The audit snapshots are delivered to the main Inventory Repository via e-mail. When using this audit method, there is no direct link between the host machine and the deployed audit agents; this is why any configuration changes or updated versions of the audit agents have to be manually re-deployed.

Portable Audit

The Portable Audit is a method of auditing computers on locked-down networks and non-networked computers using standalone audit agents. Typically, the audit agent is deployed to a flash drive, which is used to audit individual computers manually. Audit snapshots are stored on the same flash drive and then uploaded into the main Inventory Repository when you bring the flash drive back to the *Alloy Discovery Express* host machine.

Alloy Control Panel

The Alloy Control Panel provides easy central access to all locally installed components and administrative tools of Alloy Software products including *Alloy Discovery Express*, as illustrated in [Figure 2 below](#).

To launch the Alloy Control Panel, double-click its icon  from the desktop or choose **Start > Alloy Software > Alloy Control Panel** from the Windows Start menu.

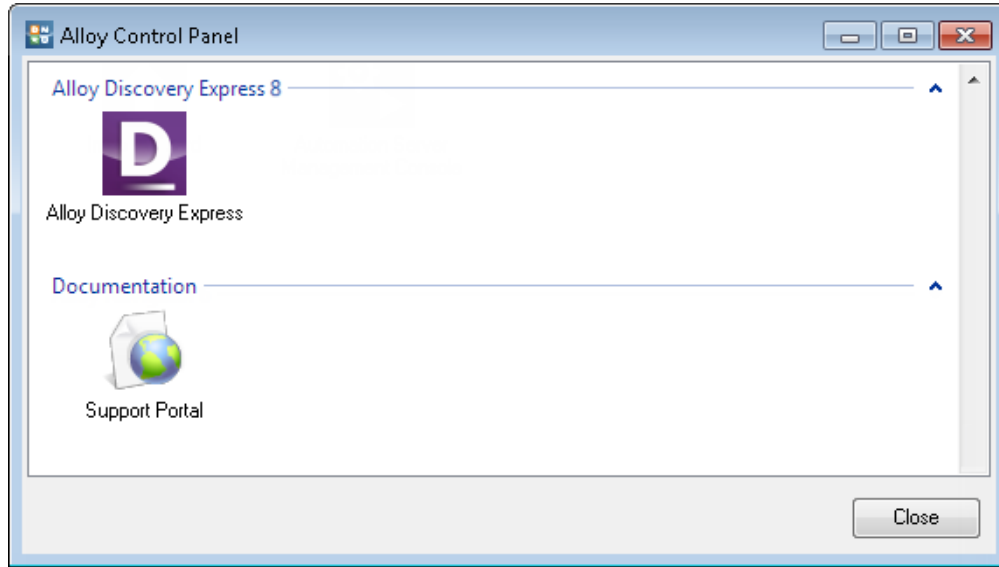


Figure 2: Alloy Control Panel

CHAPTER 2. Installing Alloy Discovery Express

This chapter helps you plan your installation and explains the installation procedure in detail.



For details on upgrading Alloy Discovery Express, see ["Upgrade to the Latest Version" on page 17.](#)

Planning Your Installation

Please read "[Supported Platforms and System Requirements](#)" and "[Licensing Alloy Discovery Express](#)" sections, before installing *Alloy Discovery Express*.

Supported Platforms and System Requirements



Alloy Discovery Express Host Machine




Alloy Discovery Express is usually run from the network administrator's workstation or from a workstation dedicated to the task. The *minimum* requirements for the computer hosting Alloy Discovery Express are as follows:



Component	Minimum Requirement
<i>CPU</i>	1 GHz
<i>RAM</i>	512 MB plus approximately 330 KB RAM for each audit snapshot file (or 560 KB, if the File Scan is enabled). For example, viewing 500 audit files will require 160 MB (or 275 MB) of additional RAM.
<i>Free Hard Disk Space</i>	130 MB of free hard disk space for the installation plus approximately 400 KB for each audit snapshot file. For example, processing 500 audit files will require 200 MB of additional free disk space.
<i>OS</i>	Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016. Both 32-bit and 64-bit versions of Windows are supported. <div data-bbox="516 1633 583 1696" style="display: inline-block; vertical-align: middle;"> </div> <div data-bbox="646 1608 1427 1703" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>If you are planning to audit computers running VMware ESX/ESXi hypervisors, Microsoft.NET Framework 4.6.1 or later must be installed.¹</p> </div>

Audit Clients

Audit clients are computers and network devices (audit nodes) to be audited. The following operation systems are supported:


Platform	Version
Operating System	
<i>Windows</i>	<p>Windows XP Professional, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016.</p> <p>Both 32-bit and 64-bit versions of Windows are supported.</p>
<i>Linux</i>	<p>A wide variety of popular Linux distributions including Debian/Ubuntu, Red Hat/Fedora, and Slackware/SUSE families.</p> <div style="display: flex; align-items: center;">  <div style="border-left: 2px solid blue; padding-left: 10px;"> <p>The On-Demand Audit feature requires that the SSH server service is running on each client computer.</p> </div> </div> <p>Alloy Discovery Express has been tested on the following Linux distributions: Linux Mint 18.2 "Sonya," Fedora release 26, CentOS 7.4, Ubuntu Server 17.04 (Zesty Zapus), Ubuntu Desktop 16.04 (Xenial Xerus), OpenSUSE Leap 42.3, Gentoo 2017 (release 2.2), Calculate Linux 17.6, Debian 9.2, OpenMandriva Lx 3.0 (Einsteinium).</p> <p>Alloy Discovery Express successfully audits computers running other Linux distributions because there are no special requirements for Linux audit clients.²</p>
<i>macOS (previously OS X and Mac OS X)</i>	<p>10.5 or later</p> <div style="display: flex; align-items: center;">  <div style="border-left: 2px solid blue; padding-left: 10px;"> <p>The On-Demand Audit feature requires that the SSH server service is running on each client computer.</p> </div> </div>

Platform	Version
Virtualization Platform (Hypervisor)	
<i>Microsoft Hyper-V</i>	<p>Alloy Discovery Express has been tested on the following versions: Microsoft Hyper-V Server 2008 (standalone version), Microsoft Hyper-V Server 2008 R2 (standalone version), Microsoft Hyper-V Server 2012 (standalone version), Microsoft Hyper-V Server 2016 (standalone version), the Hyper-V role in Microsoft Windows Server 2008, the Hyper-V role in Microsoft Windows Server 2008 R2, the Hyper-V role in Microsoft Windows Server 2012, the Hyper-V role in Microsoft Windows Server 2012 R2, the Hyper-V role in Microsoft Windows Server 2016.</p> <p>Alloy Discovery Express successfully audits computers running other versions because there are no special requirements for Microsoft Hyper-V audit clients.</p>
<i>VMware ESX</i>	<p>Alloy Discovery Express has been tested on the following versions: VMware ESX Server 3.5 Update 5, VMware vSphere ESX 4.0 Update 4, VMware vSphere ESX 4.1 Update 2.</p> <p>Alloy Discovery Express successfully audits computers running other versions because there are no special requirements for VMware ESX audit clients.²</p> <div style="display: flex; align-items: center;">  <div style="border-left: 2px solid #0070C0; padding-left: 10px;"> <p>For the On-Demand Audit feature we recommend that the SSH server service is running on each VMware ESX client computer. Otherwise, make sure that the computer hosting Alloy Discovery Express has Microsoft.NET Framework 4.6.1 installed.¹ However, the On-Demand Audit via SSH will collect more audit data.</p> </div> </div>
<i>VMware ESXi</i>	<p>Alloy Discovery Express has been tested on the following versions: VMware ESXi 3.5 Update 5, VMware ESXi 4.0 Update 4, VMware ESXi 4.1 Update 2, VMware ESXi 5.0 Update 1, ESXi 6.0 Update 3, ESXi 6.5 Update 1.</p> <p>Alloy Discovery Express successfully audits computers running other versions because there are no special requirements for VMware ESXi audit clients.²</p> <div style="display: flex; align-items: center;">  <div style="border-left: 2px solid #0070C0; padding-left: 10px;"> <p>Only the On-Demand Audit method is supported. For details on audit methods, see "Overview of Audit Methods" on page 5.</p> </div> </div> <div style="display: flex; align-items: center; margin-top: 10px;">  <div style="border-left: 2px solid #0070C0; padding-left: 10px;"> <p>The Alloy Discovery Express host machine must have Microsoft.NET Framework 4.6.1 or later installed.¹</p> </div> </div>
<i>Xen</i>	<p>Alloy Discovery Express has been tested on the following versions: Xen 3.1, Xen 4.0, Xen 4.1.</p> <p>Alloy Discovery Express successfully audits computers running other versions because there are no special requirements for Xen audit clients.²</p>

Platform	Version
	 <p>The On-Demand Audit feature requires that the SSH server service is running on each client computer.</p>
<i>Citrix XenServer</i>	<p>Alloy Discovery Express has been tested on the following versions: Citrix XenServer 5.6.1 SP2, Citrix XenServer 6.0.201, Citrix XenServer 7.2. Alloy Discovery Express successfully audits computers running other versions because there are no special requirements for Citrix XenServer audit clients.²</p>  <p>The On-Demand Audit feature requires that the SSH server service is running on each client computer.</p>
Networked Devices	
<i>SNMP version</i>	SNMPv1, SNMPv2c, SNMPv3

Shared Folder Machine

If you plan to use the Scriptable Audit feature, which allows you to audit networked computers on a regular basis, you need to dedicate a server to host a shared folder for the Inventory Analyzer and an intermediate inventory repository, where audit snapshots will be created. The following configuration is recommended for the machine hosting the network share:

Component	Minimum Requirement
<i>Free Hard Disk Space</i>	Each audit snapshot requires about 100 KB on the hard disk. If the File Scan is enabled, it will require an additional 100 to 500 KB per audit snapshot
<i>OS</i>	<p>Windows</p> <p>Windows Server 2003 SP2, Windows Server 2003 R2 SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016.</p> <p>Both 32-bit and 64-bit versions of Windows are supported.</p>  <p>We recommend that you use a server edition of Windows to host the shared folder for audit snapshots.</p> <p>Using non-server OSes (Windows XP Professional SP3, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10) is not recommended due to the limit on concurrent network connections they have.</p>

Component	Minimum Requirement
	<p>Linux</p> <p>A Linux OS with Samba 3 or higher installed and configured to support high availability and seamless integration into the Windows network environment (for details, see the Official Samba HOWTO at https://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/).</p>

Additional Software Requirements and Related Links

1. Microsoft .NET Framework 4.6.1

If you are planning to audit computers running VMware ESX/ESXi hypervisors, the Alloy Discovery Express host machine must have Microsoft .NET Framework 4.6.1 or later installed.



Windows 10 and Windows Server 2016 include .NET Framework 4.6.1 or later. Therefore, you do not have to install Microsoft .NET Framework 4.6.1 if you have one of these operating systems.

2. Linux Audit Requirements

Alloy Discovery Express successfully audits Linux distributions that allow running the following standard Linux commands:

- `which`
- `whoami`
- `uname`
- `ifconfig`
- `finger`
- `df`
- `smbclient`
- `chkconfig`

For collecting software information:

- `dpkg`
- `rpm`
- `equery`
- `ls /var/log/packages`
- `locale`

Additional commands for the On-Demand Audit:

- `pwd`

- date
- cat
- find
- od

For VMware ESX audit:

- vmware
- vmware-cmd

For Xen audit:

- virsh
- xe

For Citrix XenServer audit:

- xapi
- xe
- xm

For sending e-mail (if the E-mail Audit method is used):

- A sendmail-compatible Mail Transfer Agent (MTA) must be configured and started, and the PATH environment variable should contain the sendmail directory, or you must have access to an SMTP server.

Licensing Alloy Discovery Express

The Alloy Discovery Express' licensing concept is based on the number of computers (audit nodes) tracked with the product. A license identifies the number of nodes that Alloy Discovery Express can audit.

In order to use Alloy Discovery Express, you must activate it over the internet.



For details on activating Alloy Discovery Express, see ["Installing Alloy Discovery Express"](#) below.

Installing Alloy Discovery Express

Before starting, be sure you review all of the system requirements carefully. The administrator's computer where you install Alloy Discovery Express must meet the Host Machine requirements (for details, see ["Alloy Discovery Express Host Machine" on page 8](#)). Any computers on the network that you want to audit must meet the Client Machines requirements (for details, see ["Audit Clients" on page 9](#)).



If you are upgrading to *Alloy Discovery Express 8*, please see ["Upgrade to the Latest Version" on page 17](#).

Running Setup

To install *Alloy Discovery Express*, follow the instructions below:

1. Run the *Alloy Discovery Express 8* installer.
2. Click **Next** on the **Welcome...** page. The **End-User License Agreement** page opens.
3. Review and accept the terms of the license agreement, then click **Next**. The **Installation Folder** page opens.
4. Click **Next** to install *Alloy Discovery Express 8* to the default installation folder.



If you want to install *Alloy Discovery Express 8* to a different folder, click **Change**, choose the installation folder, then click **Next**.

The **Product Activation** window opens.

5. In the **Product Activation** window, provide your registered e-mail address and your serial number.



If you have not registered yet, click **Register** and follow the on-screen instructions. If have any questions or concerns, please contact us at <https://www.alloysoftware.com/company/contact-us/> for assistance.

6. Click **Activate** to complete the activation process.

Updating Alloy Discovery Express License

To use *Alloy Discovery Express*, you must activate it over the internet. There are two activation scenarios:

- Activate *Alloy Discovery Express* after the installation or upgrade, as described in ["Running Setup"](#) above. This also includes moving your *Alloy Discovery Express* from one computer to another.
- Update your license after your license has been changed (for example, after increasing the number of audit nodes).

The activation requires your registered e-mail address and the serial number received after obtaining the new license.



If have any questions or concerns, please contact us at <https://www.alloysoftware.com/company/contact-us/> for assistance.

To update your *Alloy Discovery Express* license:

1. Select **Help > Activate** to bring up the **Product Activation** window.
2. Provide your registered e-mail address and your new serial number, then click **Activate**.
3. Review the **License Update** details and click **Apply** to apply your changes.



The **License Update** window displays only differences.

Next Steps

Now that you have installed and activated *Alloy Discovery Express*, run the application and complete the Quick Start Wizard. The wizard will start automatically and guide you through the steps required to initially configure the system and audit computers on your network. For details, see ["Quick Start with Alloy Discovery Express" on page 20](#).

You can also quickly audit your computer and try out the product's features before performing a full-featured audit deployment of the network. To audit your computer, select **Audit > Audit My Computer** from the main menu. For details, see ["Audit Your Computer" on page 69](#).

CHAPTER 3. Upgrade to the Latest Version

Once a new version of *Alloy Discovery Express* has been released, you can upgrade your installation to the latest version.



Please note that the earliest supported version of Windows is Windows Server 2008 R2 for server editions and Windows 7 for non-server editions of Windows. If your existing installation is running on an earlier version, you will not be able to upgrade to version 8. However, Alloy Discovery Express 8 still successfully audits computers running earlier version of Windows.

For the list of supported operating systems and other system requirements, see ["Supported Platforms and System Requirements" on page 8](#).



For details on installing Alloy Discovery Express 8, see ["Installing Alloy Discovery Express" on page 8](#).

Upgrade from Alloy Discovery Express 7

Perform the following steps to upgrade:

1. [Install Alloy Discovery Express 8](#)
2. [Activation of Alloy Discovery Express 8](#)
3. [Optional: Re-deploy the Inventory Analyzer Packages](#)

1. Install Alloy Discovery Express 8

Run the Alloy Discovery Express 8 Installer on the computer hosting Alloy Discovery Express 7 (i.e. on the Alloy Discovery Express host machine):

1. Run the Alloy Discovery Express 8 Installer. The Setup Wizard starts and the **Welcome** page appears.
2. When prompted to upgrade your Alloy Discovery Express 7, click **Next**. The **Ready to install Alloy Discovery Express 8** page appears.
3. Click **Install** to start the installation. Click **Back** if you need to review or change any of your settings.
4. When the installation is complete, the **Completed** page appears. Keep the **Run Alloy Discovery Express 8** check box selected if you want to launch it immediately and proceed with the activation. If you want to launch Alloy Discovery Express later, clear the check box.

Click **Finish** to complete the installation.

2. Activation of Alloy Discovery Express 8

To use Alloy Discovery Express 8, you need to activate it over the internet. In the **Product Activation** window, provide your registered e-mail address and your serial number.



If you have not registered yet, click **Register** and follow the on-screen instructions. If you have any questions or concerns, please contact us at <https://www.alloysoftware.com/company/contact-us/> for assistance.

3. Optional: Re-deploy the Inventory Analyzer Packages

If you have already updated your Alloy Audit Tools to the latest version using the Alloy Audit Tools Update, skip this section.

Re-deploy the E-mail Audit Package

If you have configured E-mail Audit Groups, re-deploy the Inventory Analyzer package for each of such groups individually, as follows:

1. In the Sidebar, right-click the E-mail Audit Group and choose **Properties** from the pop-up menu.
2. On the **General** tab of the group's properties window, click **Create**.
3. Complete the Portable Audit Wizard in order to build a new Inventory Analyzer package for the operating system you want to audit.

Depending on the way you use the Audit via E-mail method, do one of the following:

- If the Inventory Analyzer package has been deployed on your network, re-deploy the new package. If you have multiple networks, deploy the new package to each one.
- If you have used the Audit via E-mail method to audit standalone computers, prepare and distribute the new Inventory Analyzer package (for example, using a USB flash drive).



For instructions, see ["Audit via E-mail" on page 79](#).

Rebuild the Portable Audit Package

If you use the Portable Audit, re-create each of the Inventory Analyzer packages that you use for this audit method as follows:

1. Choose **Audit > Create Portable Audit Package** from the main menu. The Portable Audit Wizard starts.
2. Complete the Portable Audit Wizard in order to create a new Inventory Analyzer package.

3. Deliver the new Inventory Analyzer Package to each individual client computer (for example, using a USB flash drive) and run the audit.



For instructions, see ["Portable Audit" on page 89](#).

CHAPTER 4. Quick Start with Alloy Discovery Express

This chapter gives you step-to-step instructions on how to quickly configure *Alloy Discovery Express* and begin auditing computers on your network.

Running the Application

After *Alloy Discovery Express* has been installed, you can run the application. There are many ways to access *Alloy Discovery Express*:

- On the desktop, double-click the Alloy Discovery Express shortcut;
- In the Alloy Control Panel, click the Alloy Discovery Express icon (see [Figure 2 on page 7](#));
- From the Windows Start menu, choose **All Programs > Alloy Software > Alloy Discovery Express 8 > Alloy Discovery Express 8**.

Instant Audit with the Quick Start Wizard

When you run *Alloy Discovery Express* for the first time, you are greeted by the Quick Start Wizard. This wizard guides you through a simple process of configuring *Alloy Discovery Express* and allows you to audit computers on your network immediately.



You can also start the Quick Start Wizard by selecting **Tools > Quick Start Wizard** from the main menu, if you would like to use the wizard at a later time.

A successful completion of the Quick Start Wizard results in the following:

- Networked computers are discovered and organized into an Audit Group,
- Default On-Demand Audit Credentials are specified.
- Optionally (if you chose to do so), *Alloy Discovery Express* initiates the On-Demand Audit of the computers in the newly-created Audit Group.

To complete the Quick Start Wizard:

1. On the **Welcome** page, click **Start**. The **Discovery Method** page appears.
2. Choose the method of discovering computers in the group that best suits your network:
 - To discover computers in a Windows domain or workgroup, click **In a Windows domain** and click **Next**. The **On-Demand Audit on a Windows Domain** page opens. Proceed to [Step 3](#).
 - To discover computers within an IP address range, click **Within an IP address range** and click **Next**. The **IP Address Range** page opens. Proceed to [Step 4](#).
3. Specify your Windows domain or workgroup using either of the following methods:

- Type the domain or workgroup name in the **Domain** field and click **Next**. The **On-Demand Audit Account** page appears. Proceed to [Step 6](#).
 - Click **Browse** and choose a domain or workgroup in one of the two search areas:
 - To search through the list of all domains and workgroups currently available on your network, select **Network Browser** in the **Search in** list. Then double-click the desired domain or workgroup and click **Next**. The **On-Demand Audit Account** page appears. Proceed to [Step 6](#).
 - To search through the list of domains specified in your Active Directory, select **Active Directory** in the **Search in** list. Then double-click the desired domain or workgroup and click **Next**. The **On-Demand Audit Account** page appears. Proceed to [Step 6](#).
4. Click **Add** and specify an IP address range to discover computers on your network in either of the following ways:
- If you want to specify the IP address range manually, enter the **Start IP Address** and **End IP Address** of the range and click **OK**.
 - If you want to determine the IP address range of your network automatically, click **My Network** and click **OK**.

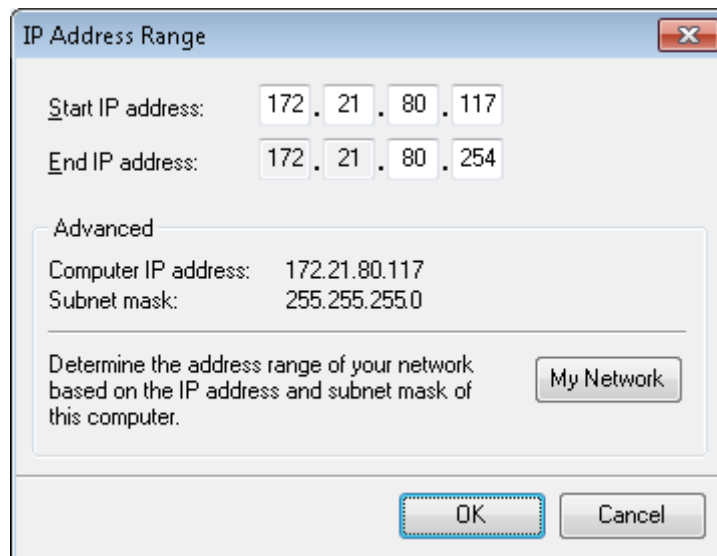


Figure 3: Specifying an IP address range

5. Repeat the previous step to add as many ranges as you need and click **Next**. The **On-Demand Audit Account for Windows computers** page appears.

6. Specify the account for running the On-Demand Audit on Windows computers in either of the following ways:

Quick Start Wizard

On-Demand Audit Account for Windows computers

Provide credentials for the account which will be used to run the audit on Windows computers. A domain Administrator's account is recommended. If you prefer using a local account, it must belong to the local Administrators group on every computer.

Currently logged in user
 This account

Name:
 (e.g. Domain\Administrator)

Password:

These credentials will be used as the default credentials for the On-Demand Audit of Windows computers. If you are going to audit Linux or Mac computers on demand, specify the default credentials for Linux and Mac after you have completed this wizard (select Audit | Audit Settings from the main menu and click the On-Demand Audit Credentials tab). On the same tab, you can also modify the default audit credentials for Windows computers, if needed.

< Back Next > Cancel

Figure 4: Providing Credentials for On-Demand Audit Account

- If you are logged on as a Domain Administrator and you want to use your current account, click **Currently logged in user**. Click **Next**. The **Discovery** page appears.



If you expect to encounter Linux or Mac computers within the specified Windows domain or IP address range, you must specify their On-Demand Audit Credentials after you completed this wizard in order to audit these computers. This can be accomplished by right-clicking the group in the Sidebar, selecting **Properties**, and then selecting the **Audit Credentials** tab.

For details on setting the global default credentials used for all Mac and Linux computers, see ["Managing Audit Credentials" on page 51](#).

- Enter the name and password of the account that is a member of the local Administrators group on each Windows computer you want audited as long as this account exists on every computer you want audited as well as on the host machine. We recommend that you use a domain administrator's account. Click **Next**. The **Discovery** page appears.

7. Review the list of discovered computers and click **Next**. The **Group Name and Description** page appears.
8. Review the group name and edit it, if necessary. Optionally, enter a description for the group. Then click **Next**. The **Ready to Create New Group** page appears.
9. Review your settings. When you are ready to proceed with creating the group, click **Next**. If you want to modify any settings, click **Back** and make the necessary changes. After the wizard finishes creating the audit group, it will display the **Group Created** page.
10. Choose what to do after finishing the wizard:
 - If you want to audit the discovered computers immediately after finishing the wizard, keep the **Audit computers in this group now** check box selected and click **Finish**. The **On-Demand Audit** dialog box appears, where you can monitor the progress of the audit.
 - To run the audit later, clear the **Audit computers in this group now** check box and click **Finish**. You can audit the computers in that group when you are ready to do so. For details, see ["Auditing Groups of Computers and Devices" on page 55](#).

Next Steps

Now that you have completed the Quick Start Wizard, you can do the following:

- View the audit results by locating and selecting the group you created on the Sidebar. Then you can view the associated audit results in the right pane. For details, see ["Analyzing Inventory Data using Groups" on page 95](#).
- Use other audit methods and deployment options. For details, see ["Configuring Alloy Discovery Express" on page 24](#).

CHAPTER 5. Configuring Alloy Discovery Express

This chapter explains the audit methods available in *Alloy Discovery Express* and outlines how to configure the audit.

Configuring the Audit

The audit configuration defines how the data is collected during the audit process. You specify the audit configuration options on the **Audit Configuration** tab of the **Audit Settings** dialog box. To access the **Audit Settings** dialog box, select **Audit > Audit Settings** from the main menu.

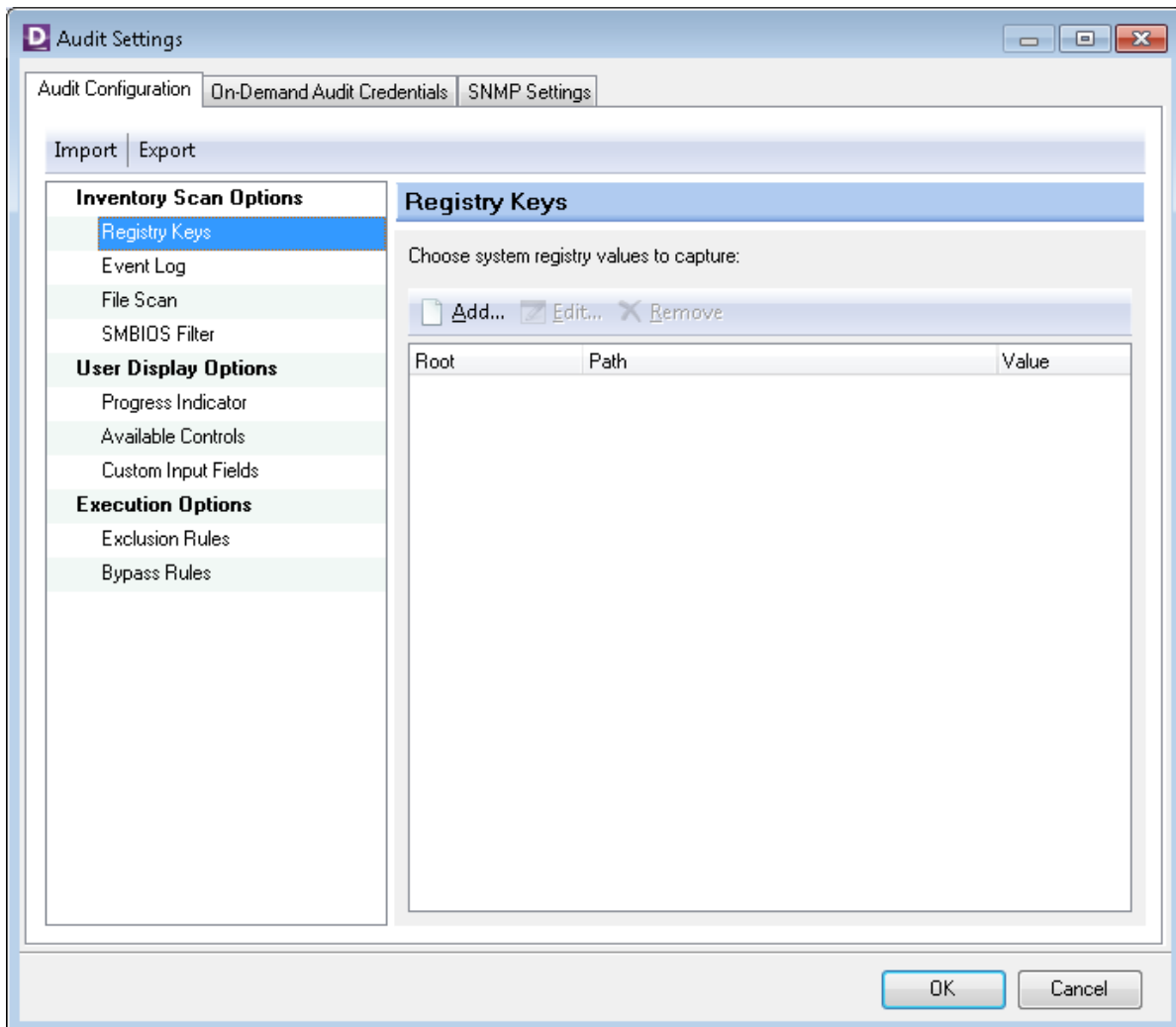


Figure 5: Audit Settings Dialog

Using the **Import** and **Export** buttons, you can save or restore your audit settings from an external configuration file (.cfg).



The **On-Demand Audit Credentials** tab provides various options that ensure successful on-demand audits for Microsoft Windows, Linux and Mac operating systems. For detailed information on setting credentials for each of these OS types, see ["Managing Audit Credentials" on page 51](#).

On the **SNMP Settings** tab you can enable the SNMP discovery to discover and identify network devices such as routers and network printers. For details, see ["Enabling SNMP Discovery" on page 53](#).

To modify the default audit configuration, click each node you want to reconfigure and follow the instructions below. The following screens are available:

- **Inventory Scan Options** section, where you specify whether to detect installed software and how to perform this discovery. The section includes the following screens:
 - **Registry Keys** screen, where you can configure the list of registry keys to capture (for details, see ["Configuring the Capture of Registry Keys" on page 26](#)).
 - **Event Log** screen, where you can choose the entries of Windows Event Log to capture (for details, see ["Configuring Event Log Options" on page 31](#)).
 - **File Scan** screen, where you configure the file scan process (for details, see ["Configuring File Scan Options" on page 34](#)).
 - **SMBIOS Filter** screen, where you can customize the filter for dummy values from the System BIOS (for details, see ["Configuring the SMBIOS Filter" on page 38](#)).
- **User Display Options** section, where you specify the appearance of the audit progress indicator and the Windows Inventory Analyzer start screen displayed to the user while his or her computer is being audited. The section includes the following screens:
 - **Progress Indicator** screen, where you specify whether the progress indicator appears on the screens of client machines during the audit (for details, see ["Configuring the Progress Indicator" on page 41](#)).
 - **Available Controls** screen, where you can add various interactive options for the user (for details, see ["Configuring Available Controls" on page 42](#)).
 - **Custom Input Fields** screen, where you can specify a number of additional input fields that should be presented to the user before starting the audit (for details, see ["Configuring Custom Input Fields" on page 44](#)).
- **Execution Options** section, where you specify exclusions from the audit. The section provides the following screens:
 - **Exclusion Rules** screen, where you can exclude some computers from the audit (for details, see ["Configuring the Exclusion Rules" on page 47](#)).

- **Bypass Rules** screen, where you can exclude some user accounts from the audit (for details, see [“Setting the Bypass Rules” on page 48](#)).

Configuring the Capture of Registry Keys

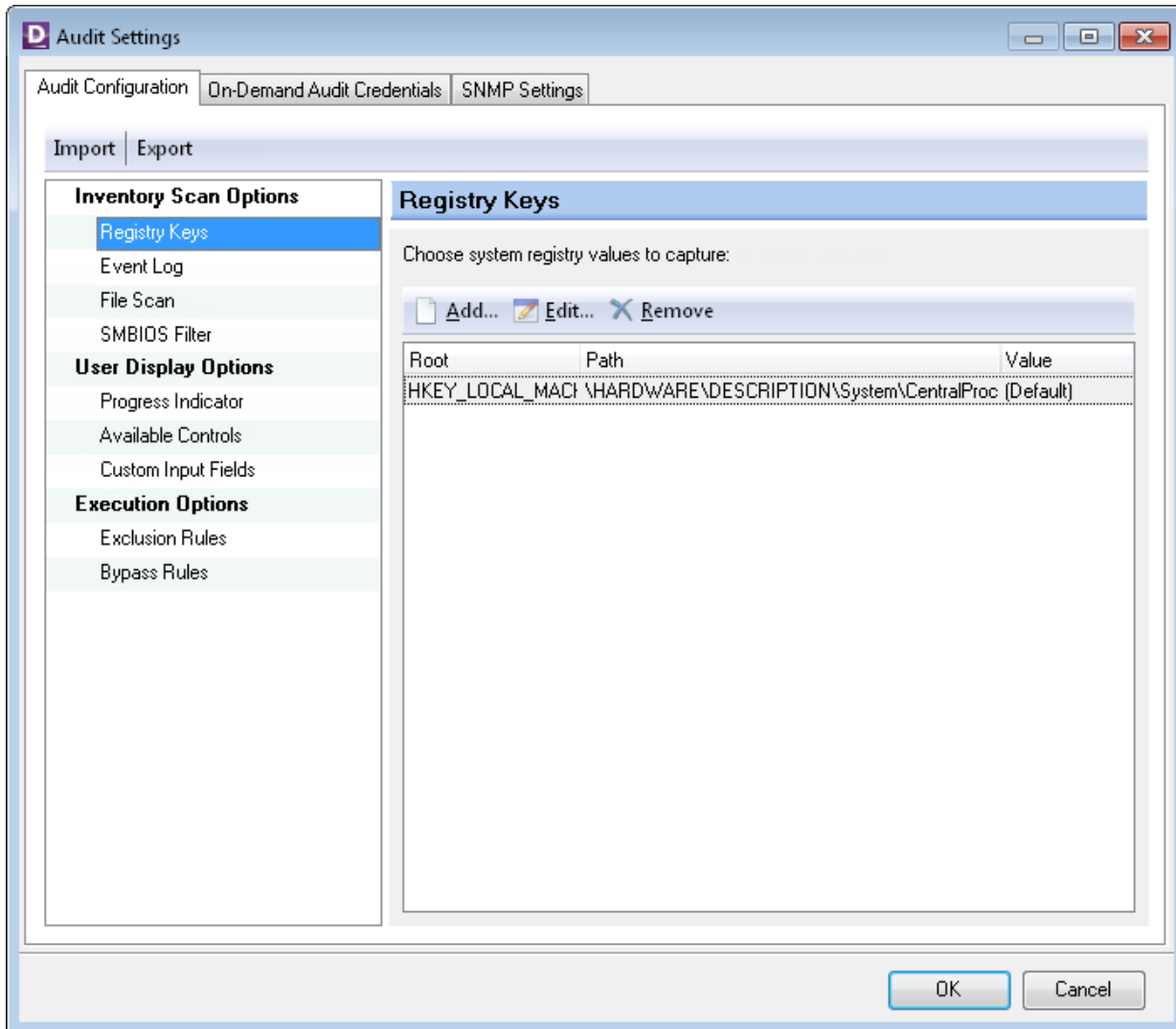


Figure 6: Registry Keys

The **Registry Keys** screen lets you enable the Inventory Analyzer to scan the Windows registry for specific keys and report their values in audit snapshots. To do so, just add a number of registry key fields for Computer records using the Main Console. Registry key fields are special database fields for computers where *Alloy Discovery Express* stores captured registry key values. As soon as you add such a field, *Alloy Discovery Express* automatically enables the capture of the target registry key for all your computer groups and reports its values after the first audit.

Adding Registry Keys

To add a new registry key:

1. Click **Add**. The **Edit Registry Key** dialog box appears.

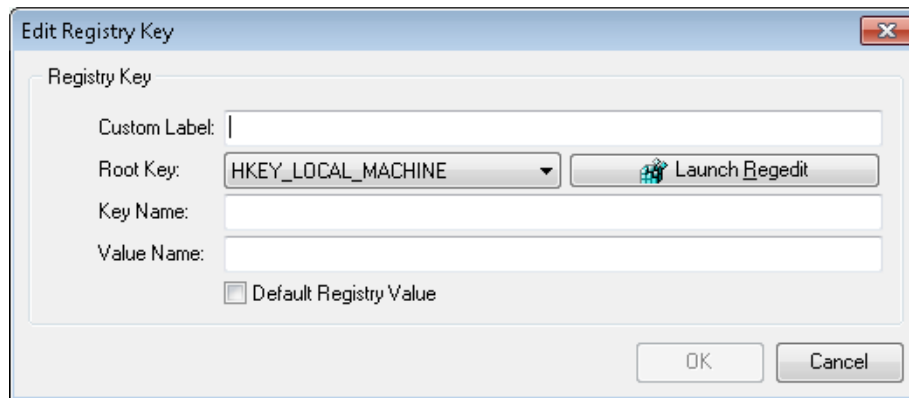


Figure 7: Edit Registry Key dialog box

2. In the **Custom Label** field, type in a label for the registry key field where *Alloy Discovery Express* will store captured registry key values.
3. Specify the exact path to the registry key that you want to capture on Windows computers:
 - If the registry on your local computer contains the target key, you can just paste it from your Microsoft Registry Editor as follows:
 - 1) Open the Registry Editor. For example, you can just click **Launch Regedit** in the **Edit Registry Key** dialog box.

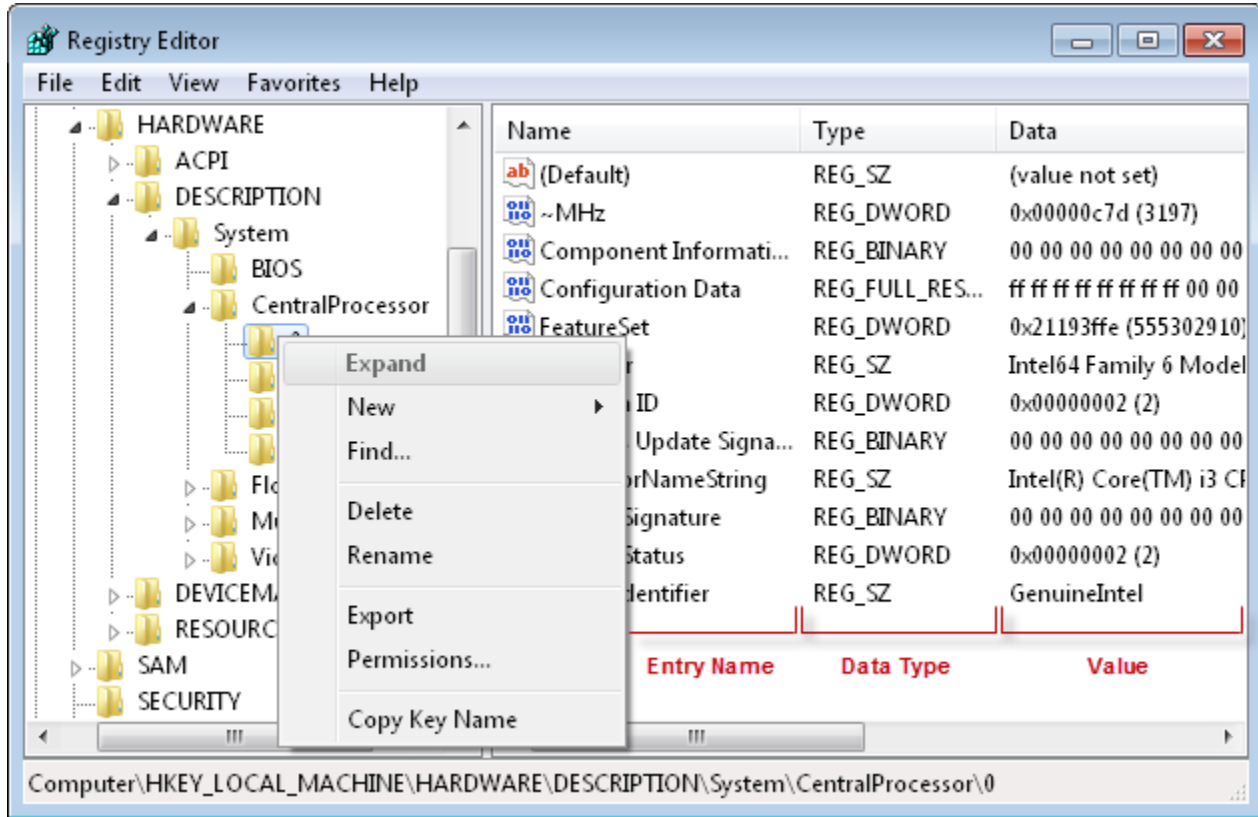


Figure 8: Microsoft Registry Editor

- 2) In the navigation area of the Registry Editor, locate the key to query during the audit, right-click it, and choose **Copy Key Name** from the context menu.
- 3) Switch to the **Edit Registry Key** dialog box in *Alloy Discovery Express* and paste the copied value into the **Key Name** field. The value of the **Root Key** field will be set automatically to match the selected registry hive.
 - If your local registry does not contain the target key, just enter the exact path to the key in the **Key Name** field. The best way is to copy and paste it from a reliable source. The value of the **Root Key** field will be set automatically to match the selected registry hive.



Make sure that you enter the exact path to the registry key.

4. Specify the entry to capture:
 - To query the default key value, select the **Default Registry Value** check box.
 - To specify a non-default key value, enter it in the **Value Name** field. The most reliable way is to copy and paste it from the Registry Editor. For example, to copy a value to the clipboard, right-click its name

in the Registry Editor, choose **Rename** from the pop-up menu, press CTRL+C, and then press ESC to exit the replace mode.



Make sure that you enter the exact path to the registry key.

The following data types are currently supported:

REG_SZ
 REG_DWORD
 REG_MULTI_SZ
 REG_EXPAND_SZ
 REG_DWORD_LITTLE_ENDIAN

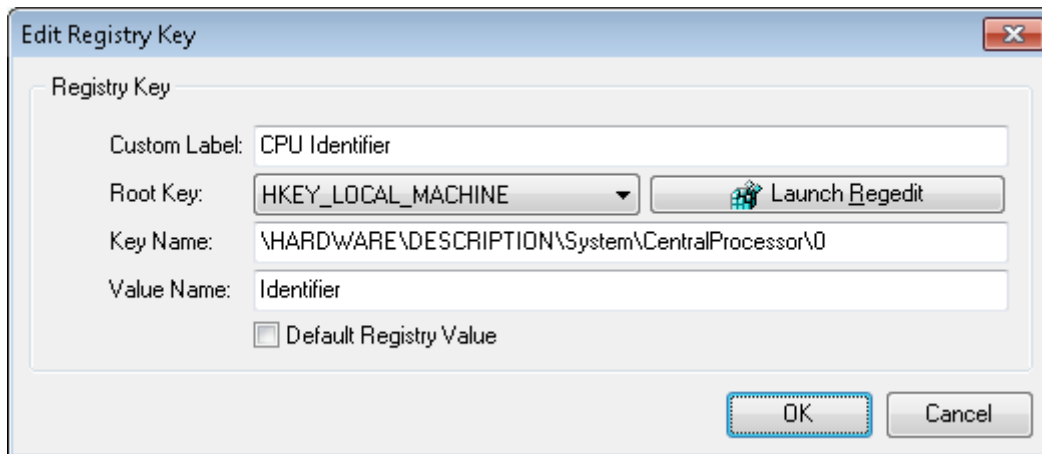


Figure 9: Adding Registry Key



On 64-bit Windows, registry entries for 32-bit applications are stored under a special registry node **Wow6432Node**:

HKEY_LOCAL_MACHINE\Software\WOW6432Node

If you want to retrieve a 32-bit registry key value from the HKEY_LOCAL_MACHINE\SOFTWARE section on 64-bit versions of Windows, make sure to include the **Wow6432Node** node in your registry path. For example:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Adobe\Adobe Bridge CS6\Installer\InstallPath

If there are both 32-bit and 64-bit versions of Windows in your audit scope, you can use this solution to capture 32-bit application data on both 32-bit and 64-bit versions using the same registry path, because Alloy Discovery Express automatically removes the **Wow6432Node** node from the path when running on 32-bit Windows.

5. Click **OK**.

Modifying Parameters of Registry Key Capture

To modify the parameters of a registry key capture, follow these steps:

1. On the list of Registry Keys, double-click a key. The **Edit Registry Key** dialog box appears.
2. Modify the capture parameters as needed.
3. Click **OK**.

Removing Registry Keys

- To remove a registry key from the list of captured keys, select the key and click **Remove**.

Displaying the Captured Values

After configuring the registry keys, configure *Alloy Discovery Express* to display the captured values in the Computer List:

1. Select **Tools > Configure Computer List** from the main menu.
2. Expand the **Registry Fields** node and double-click each field you want to be displayed.
3. Click **OK**.

Configuring Event Log Options

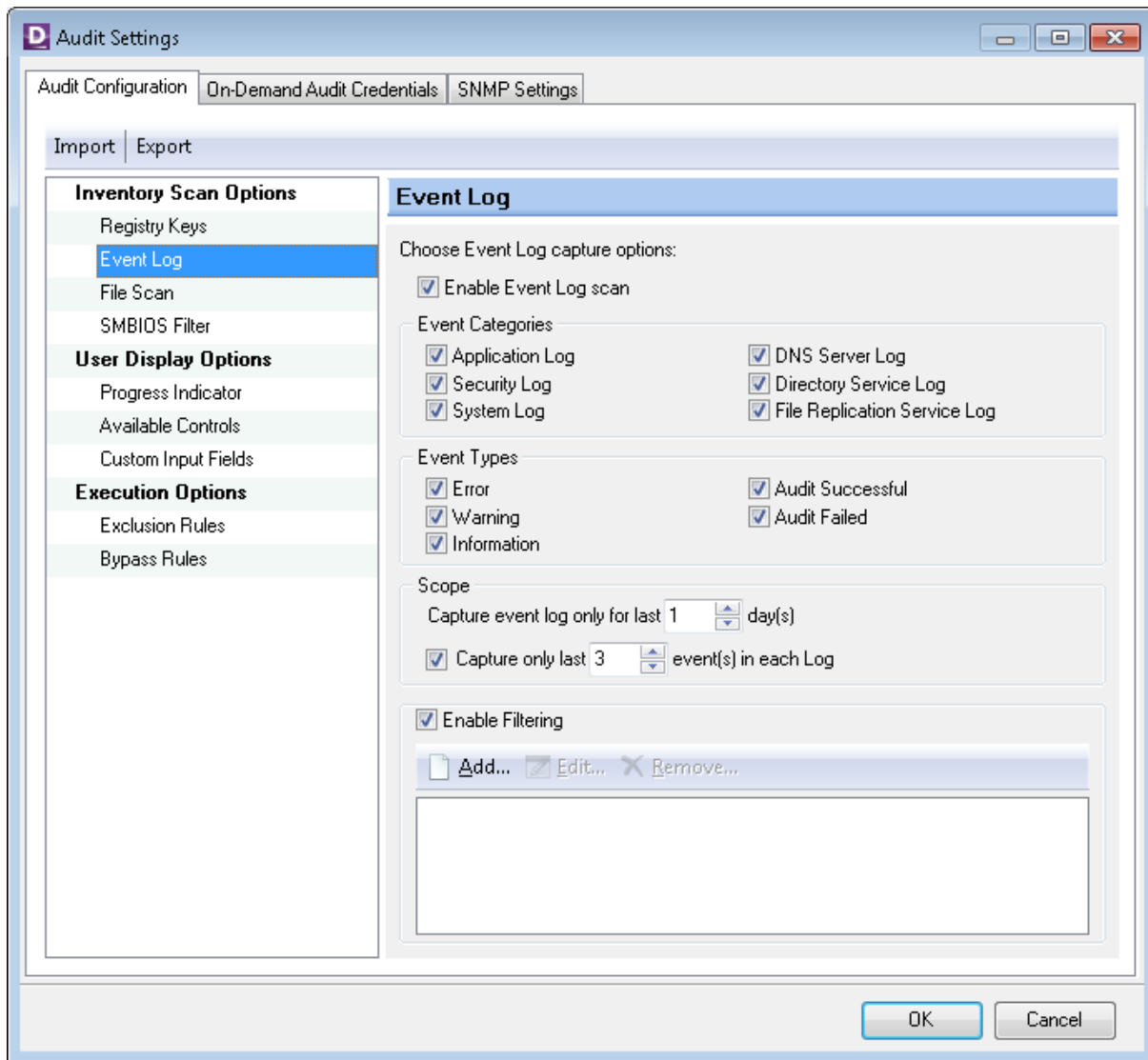


Figure 10: Event Log Options

On the **Event Log** screen you can enable the capture of the system Event Log records and specify the types of events you are interested in.

Using the **Event Log** screen you can specify the options for capturing the system Event Log entries as follows:

1. Keep the **Enable Event Log scan** check box selected. If you clear the check box, you temporarily disable capturing of the Event Log records.



The Event Log scan is applicable only for Windows computers. When auditing Linux and Mac computers, the Event Log options are ignored.

2. Under **Event Categories**, select appropriate check boxes to capture records from the following event logs:
 - **Application Log** – This log contains events logged by Windows applications or programs.
 - **Security Log** – This log records all security-related events: logons and logoffs, file-access failures and successes, startups and shutdowns, etc.
 - **System Log** – This log contains events logged by Windows system components.
 - **DNS Server Log** – This log contains events logged by Windows DNS service, which are associated with resolving DNS names to Internet Protocol (IP) addresses.



Available only on computers configured as DNS servers.

- **Directory Service Log** – This log contains events logged by Windows directory service.



Available on Windows 2000, Windows Server 2003, or Windows Server 2008, and Windows Server 2008 R2 domain controllers.

- **File Replication Service Log** – This log contains events logged by Windows File Replication service during the replication process between domain controllers.



Available on Windows 2000, Windows Server 2003, or Windows Server 2008, and Windows Server 2008 R2 domain controllers.

3. Under **Event Types**, select check boxes corresponding to the types of events you want captured: **Error**, **Warning**, **Information**, **Audit successful**, or **Audit failed**.
4. Under **Scope**, enter the period (up to 30 days) for which you want the specified Windows Event Logs captured.



Entering a long period can significantly increase the size of audit snapshots and the time required to process audit snapshots.

5. If you want to capture only a limited number of most recent events, select the **Capture only last** check box and enter the number of events to capture.
6. If you want to capture only events that satisfy certain criteria, select the **Enable Filtering** check box and create a number of filtering conditions as follows:
 - 1) Click **Add** to bring up the **Edit Log Event Filter** dialog box.

- 2) Define the parameter, operator, and the value of the filtering condition. Events can be filtered by the following parameters:
- **Source** – the source of the event, i.e. the name of a program, a system component, or an individual component of a large program;
 - **Category** – the classification of the event, as defined by the event source;
 - **Event ID** – the event ID, as defined by the event source;
 - **User** – the user name if the event is attributed to a specific user;
 - **Computer** – the name of the computer where the logged event occurred.

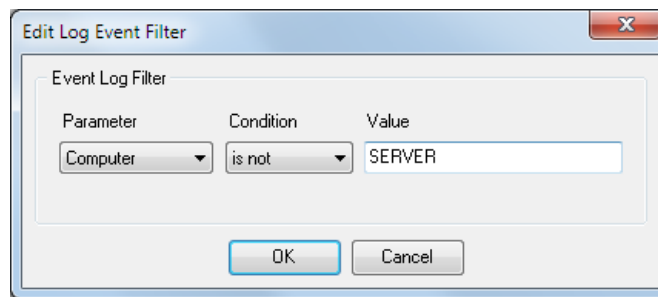


Figure 11: Adding a filtering condition

7. Click **OK**.

Repeat these steps to create other conditions as needed. All conditions are connected with AND logic, meaning that every condition must be satisfied in order for the filtering criteria to result in a match.

You can assign several conditions to a single parameter as follows:

- When you add a new condition with the "is" operator, the resulting logical expression for those two conditions becomes connected with OR logic, which means a positive match is detected if any of the specified conditions is satisfied.
- When you add a new condition with the "is not" operator, AND logic is used.

For an example of filtering criteria, see [Figure 12 below](#). The screenshot illustrates the following sample filter:

Source IS Windows Update Agent AND (Category IS Installation OR Category IS Software Synch)

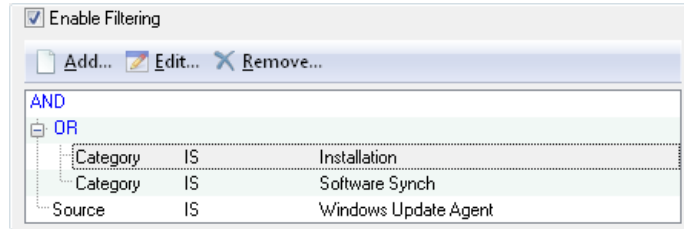


Figure 12: Filtering criteria for capturing Event Log events

Configuring File Scan Options

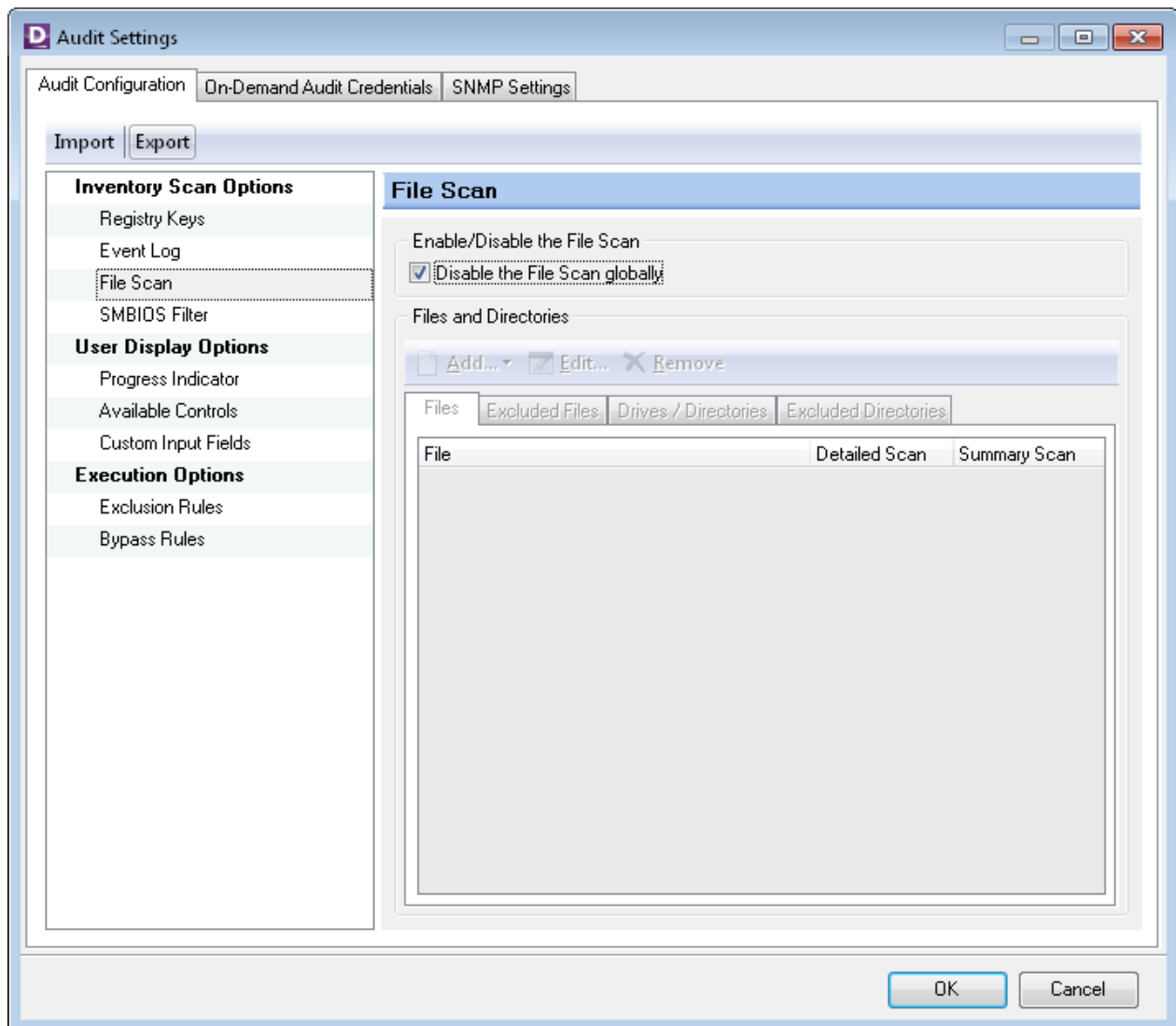


Figure 13: File Scan Options

If you want to search computers' hard drives for individual files or collect volume statistic on certain file types, click **File Scan** in the navigation bar, clear the **Disable file scan globally** check box, and follow the instructions below.



Since the hard disk scan may take a significant time to run, the file scan is disabled by default.

1. On the **Files** tab, specify the file types to scan and the level of detail you want.

The following options of the file scan can be configured independently:

- The **Detailed Scan** collects physical characteristics as well as the file version properties of individual files that match the search mask:
 - **Computer Name** — the name of the computer where the file was detected
 - **User** — the name of the user
 - **File Name** — the file name
 - **Publisher** — the name of the company that produced the file
 - **Product Name** — the name of the product with which the file is distributed
 - **Product Version** — the version number of the product with which the file is distributed
 - **Path** — the full path to the file on the hard drive
 - **Size** — the size of the file in bytes
 - **File Version** — the version number of the file
 - **Description** — the file description
 - **Date** — the date and time when the file was last modified
- The **Summary Scan** produces volume statistics for all files that match the search mask, broken down by folder location.



We recommend that you use the Detailed Scan only for executable files, such as .exe, .dll, .sys, or .com. The Detailed Scan of other file types typically produces no useful information. It will also dramatically increase the size of audit snapshot files. Ultimately, this may adversely affect the performance of Alloy Discovery Express.

- 1) To add a common file type (executable, graphic, multimedia, or archive files), click **Add > [File Group]** and then either select **All [File Group]** to add all file types from the group or select an individual file mask.

By default, a newly-added file mask has the Detailed Scan option enabled. To change it, double-click the mask, select the option as needed, and click **OK**. The default Audit Profile also includes pre-configured Detailed Scan for *.EXE file mask. To delete it, select the file mask and click the **Remove** button.

- 2) To add a custom file mask or a specific file name, click **Add > New**, type in the file name in the **File Mask** field. Next, specify the scan detail level you want by selecting the **Summary Scan** and/or **Detailed Scan** check boxes, and click **OK**.



You can use wildcard symbols to define a file mask: the asterisk (*) substitutes for any number of characters, the question mark (?) substitutes for any single character.

2. If you want to exclude certain file groups or files from the file scan, click the **Excluded Files** tab. The same file mask can be added to both lists — Files and Excluded Files — however, the latter takes precedence over the Files list, which allows you to temporarily exclude certain masks from the scan without modifying the contents of the Files list.

Configure the list of excluded items as follows:

- 1) To exclude files of one of the four predefined groups (executable, graphic, multimedia, or archive files), click **Add > [File Group]** and then choose either all files of the selected group or a particular file format.
- 2) To exclude a file mask or a certain file from the audit, click **Add > New**, type a file mask or a file name in the **File Mask** field, and click **OK**.



You can use wildcard symbols to define a file mask: the asterisk (*) substitutes for any number of characters, the question mark (?) substitutes for any single character.

3. If you want to limit the scope of the file scan to particular hard drives or directories, click the **Drives/ Directories** tab, clear the **Scan all hard drives** check box, and specify the desired scope as follows:
 - To add a particular directory or drive, click **New**, type the full name of a directory or hard drive in the **Directory/Drive Name** field, and click **OK**.

You can use environment variables (such as %WinDir% or %CommonProgramFiles%) to specify predefined system directories, or you can enter a full path (such as C:\Program Files\Common Files\). However, the latter method requires that the directory has the same location on all computers you want audited. If the specified directory does not exist on an audited computer, it will be skipped during the audit.

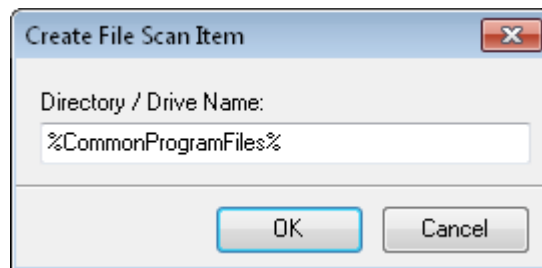


Figure 14: Adding drive E to the file scan

Repeat this step to add other directories or drives as needed.

4. If you want to exclude certain drives or directories from the file scan, click the **Excluded Directories** tab and add such drives and directories to the exclusion list. A single directory can be added to both lists — Drives/Directories and Excluded Directories — however, the latter takes precedence over the Drives/Directories list, which allows you to temporarily exclude certain locations from the scan.

There are four predefined locations that are excluded from the file scan by default:

- *Windows Directory* — The Windows system directory stores system files that are not usually changed and may be excluded from auditing. Depending on the OS you're running, the system's root directory can be `C:\Windows` or `C:\WINNT`.

If you want to include the Windows system directory in the audit, clear the **Skip the Windows folder** check box.

- *Browser Cache Directory* — The Internet browser cache directory stores the contents of many Web pages, graphic files, etc. loaded from browsed sites and usually is of little interest. The supported Internet browsers are: Internet Explorer 6 and later, Mozilla Firefox 2 and later, and Opera 9 and later.

If you want to include the Internet browser cache directory in the audit, clear the **Skip the browser cache directory** check box.

- *Recycle Bin* — The Windows Recycle Bin temporarily stores deleted files and folders before they are permanently deleted from a storage device. Each physical disk has a hidden folder where those deleted items are stored. Depending on the OS you're running, the Recycle Bin folder can be `Drive:\RECYCLER` or `Drive:\$RECYCLE.BIN`.

By default, the Recycle Bin is excluded from the audit. We recommend that you keep the defaults.

- *System Volume* — The System Volume Information directory is a hidden Windows system folder used by the System Restore tool to store its information and restore points. There is a hidden System Volume Information folder on every partition of the computer.

This data is protected by the system and is excluded from the audit by default. If you want to include the System Volume Information directory in the audit, clear the **Skip the System Volume** check box.

- To exclude a specific directory from the file scan, click **New**, type in the full name of the directory or the disk name in the **Directory/Drive Name** field and click **OK**.

You can use environment variables (such as `%WinDir%` or `%CommonProgramFiles%`) to specify predefined system directories, or you can enter the full path. However, the latter method requires that the excluded directory has the same location on all computers you want audited.

Repeat this step to exclude other directories as needed.

Configuring the SMBIOS Filter

Sometimes, system identification values obtained from the BIOS may report dummy text, such as "To be filled by O.E.M." or "No asset information." Some BIOS manufacturers use these placeholders instead of empty fields to indicate that no meaningful value was specified and expecting original equipment manufacturers to update them. However, not all original equipment manufacturers do that, and you certainly don't want these dummy values reported as this may affect the accuracy of your inventory.

The SMBIOS filter makes the Inventory Analyzer to replace placeholder values obtained from the BIOS with empty values during the audit.



The SMBIOS filter is applicable only for Windows and Linux computers; when auditing Mac computers, this filter is ignored.

The Inventory Analyzer has a built-in SMBIOS Filter with standard placeholder values to ignore during the audit:

- 1111TEST1111*123456789*
- *987654321*
- *AssetTag*
- Base Board*
- Chassis Manufacture
- Chassis Serial Number
- Chassis Version
- Default String
- [Empty]
- Eval
- *Manufacturer*
- MKF_PROCESSOR_SERIAL_NO_*
- MKF_PROCESSOR_SOCKET_DESIGNATION_*
- ModulePartNumber*
- N/A
- No Asset Information
- No Asset Tag
- NO DIMM
- No Enclosure
- None
- Not Applicable
- Not Available
- *PartNum*

- *SerialNumber
- *SerNum*
- System Manufacturer
- System Name
- System Product Name
- System Serial Number
- System Version
- To Be Filled By O.E.M.

If your inventory contains other dummy values, you can supplement the built-in SMBIOS Filter with those values in the **SMBIOS Filter** section of your Audit Configuration, and they will no longer be reported.



Both the built-in and user-defined SMBIOS filters are applicable only for Windows and Linux computers.

When auditing Mac computers, the SMBIOS Filter is ignored because the Mac Inventory Analyzer does not collect hardware information from the BIOS but uses the System Profiler tool instead.

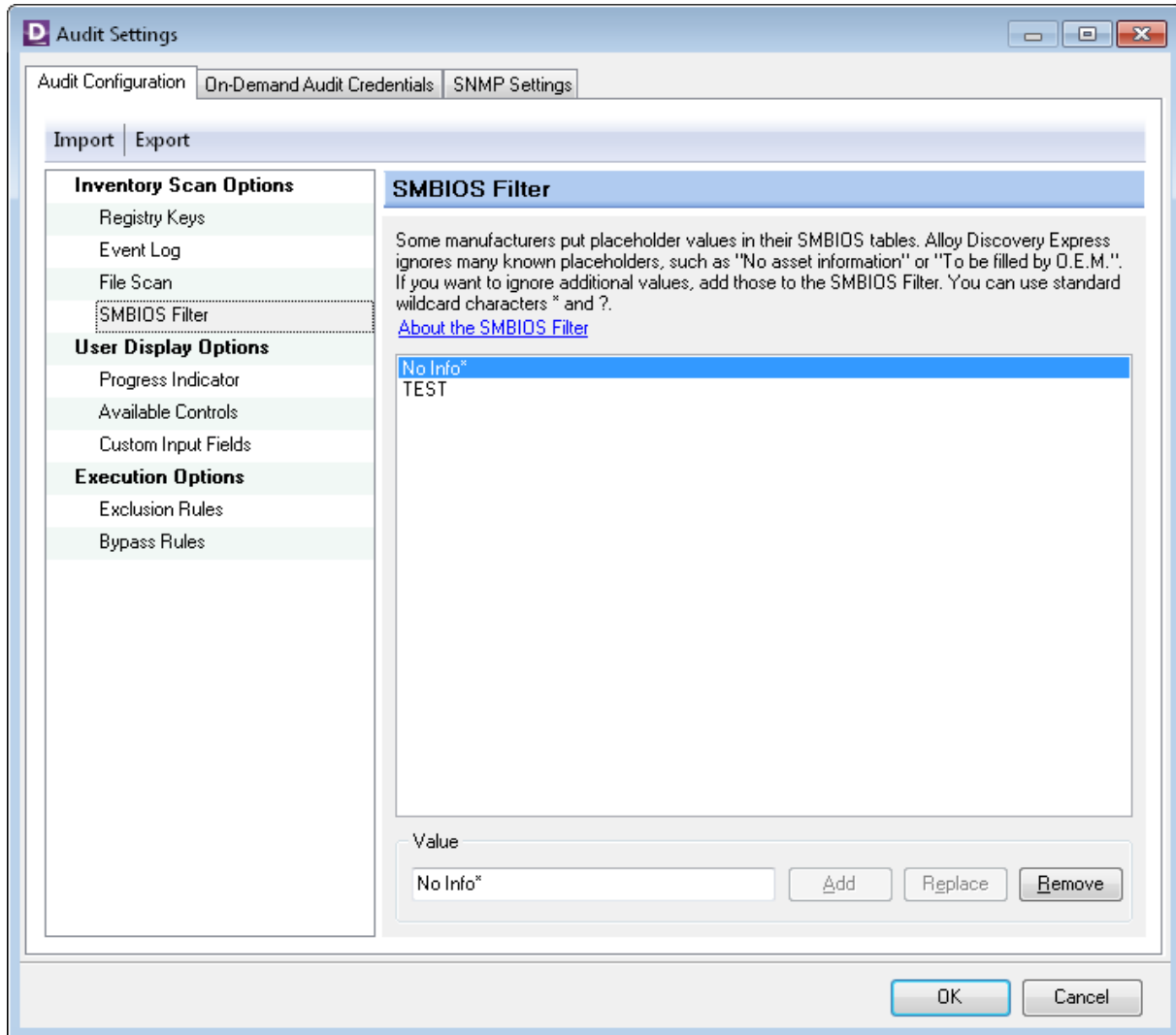


Figure 15: SMBIOS Filter

If you want to supplement the built-in SMBIOS Filter with your custom values, click **SMBIOS Filter** and follow the instructions below.

- To add a new custom value to the SMBIOS Filter, under **Add/Replace/Remove Value**, type in the value in the text field and click **Add**.



You can use the standard wildcards: an asterisk (*) to represent any number of characters, including zero, and the question mark (?) to represent any single character. For example, to filter out both "No Information" and "No Info" values, you can use a single filter rule for "No Info*".

- To modify a custom value, select it, edit the value in the text field below, and then click **Replace**.
- To delete a custom value from the SMBIOS Filter, select it and click **Remove**.

Configuring the Progress Indicator

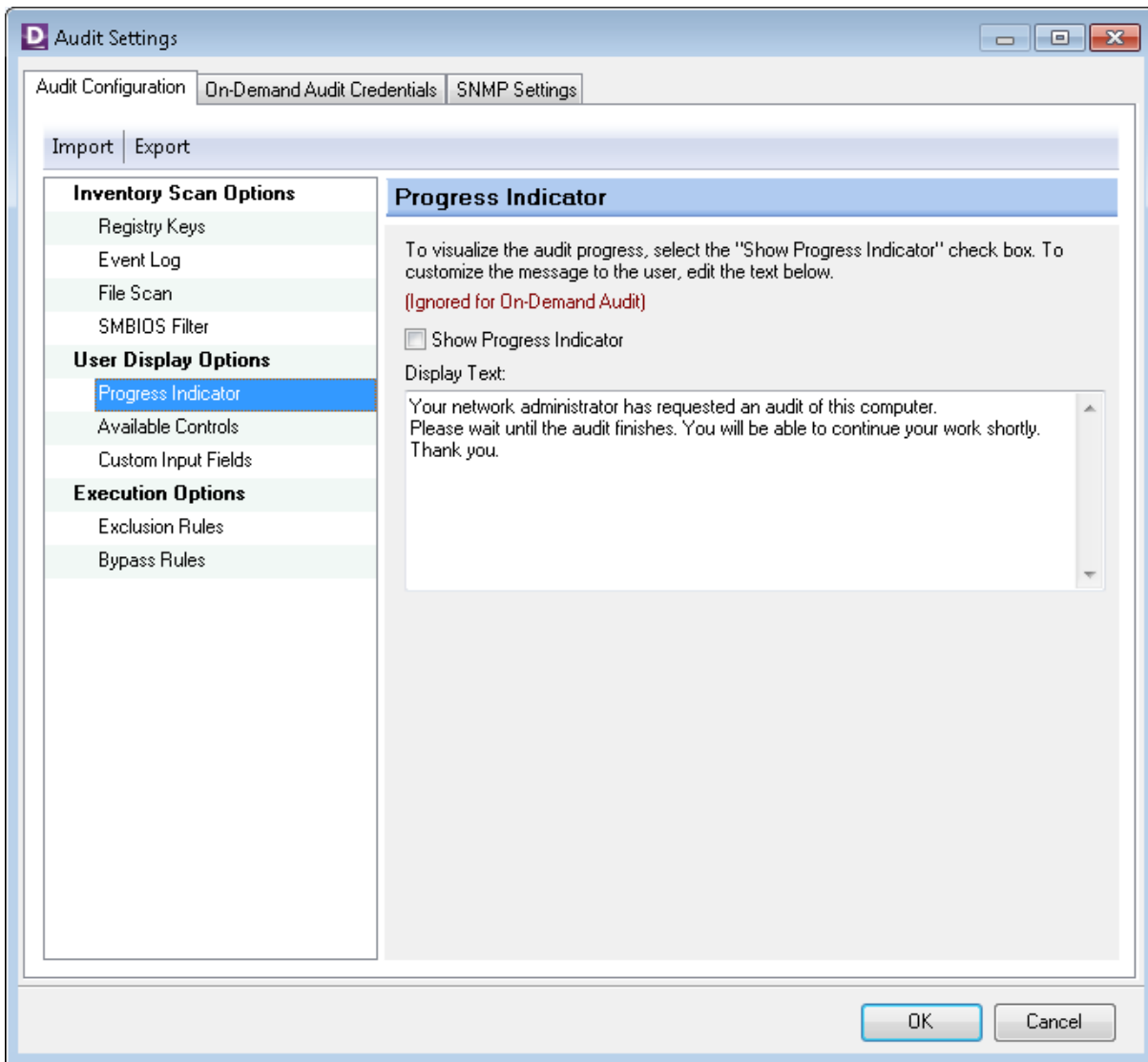


Figure 16: Display Options

The **Display Options** screen lets you choose whether the progress indicator appears on the screens of client machines during the audit and customize the message shown to the users when the audit starts.

To show the indicator, select the **Show Progress Indicator** check box. To modify the message, edit the text in the **Display Text** field.

Configuring Available Controls

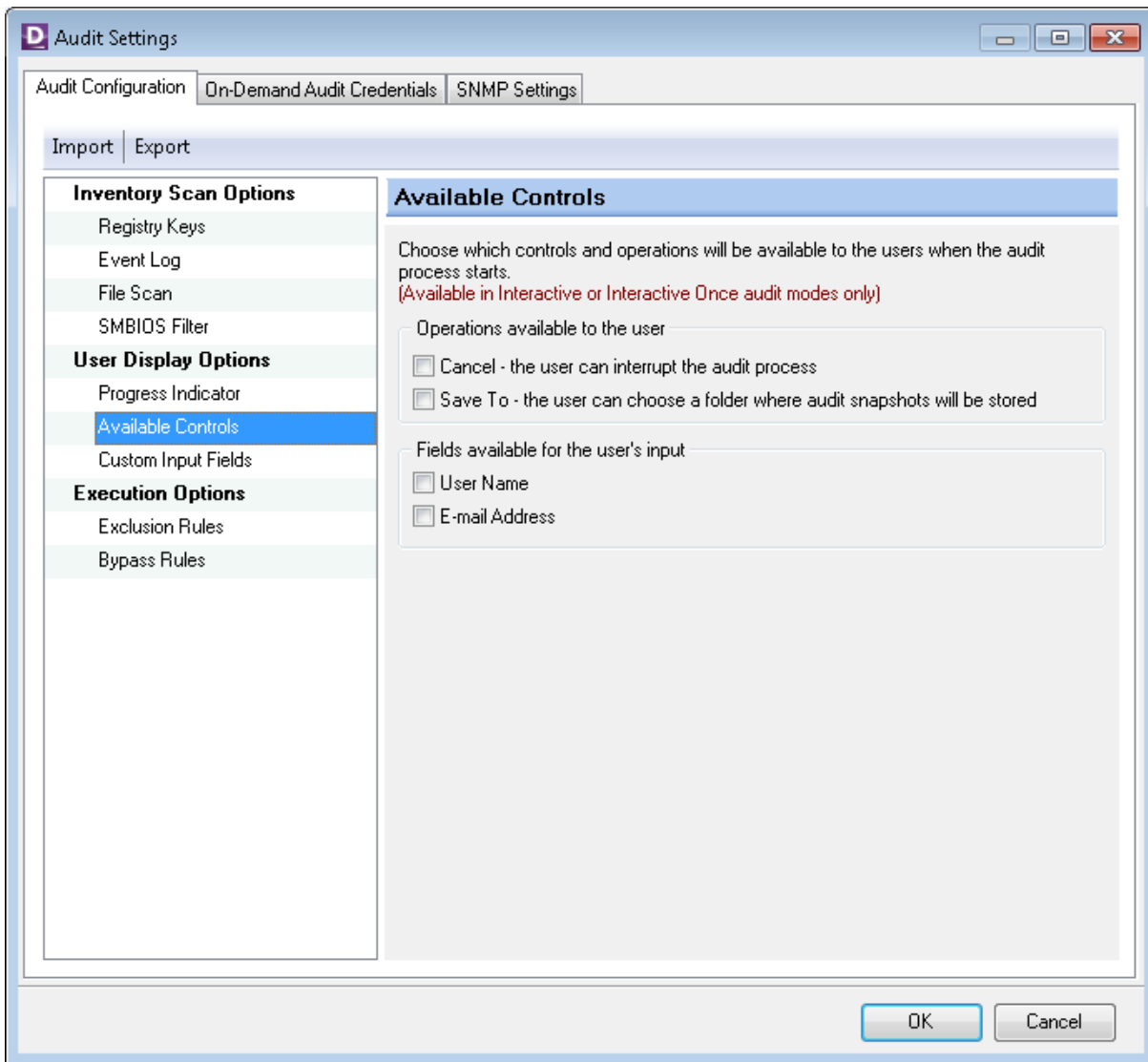


Figure 17: Available Controls

The **Available Controls** screen lets you choose a number of interactive options for the user. These options may be needed only when the audit is performed by trained technicians, and typically should remain disabled in all other audit scenarios.



These options are only available in Interactive or Interactive Once audit modes.

- To let users cancel the audit session, select the **Cancel** check box. The **Cancel** button will appear on the Inventory Analyzer splash screen.

- To let users redirect the output to another folder, select the **Save To** check box. The **Save Audit to** option will appear on the Inventory Analyzer splash screen.
- To prompt users for their first and last name, select the **User Name** check box. The **First Name** and **Last Name** mandatory fields will appear on the Inventory Analyzer splash screen. However, if the Inventory Analyzer is able to obtain the name of the logged on user from the Active Directory, these fields will appear pre-populated and read-only.
- To prompt users for their e-mail address, select the **E-mail Address** check box. The **E-mail** mandatory field will appear on the *Inventory Analyzer splash screen*. However, if the *Inventory Analyzer* is able to obtain the name of the logged on user from the Active Directory, this field will appear pre-populated and read-only.

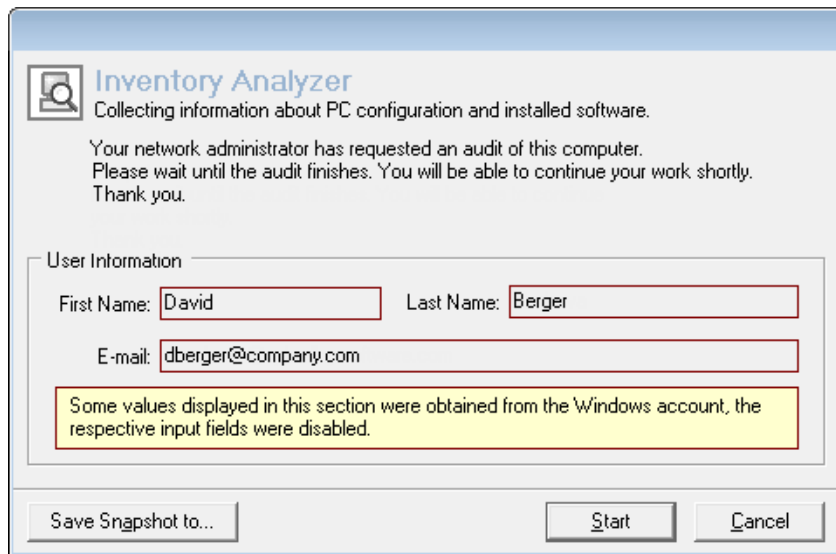


Figure 18: Inventory Analyzer Splash Screen with All Controls Enabled

Configuring Custom Input Fields

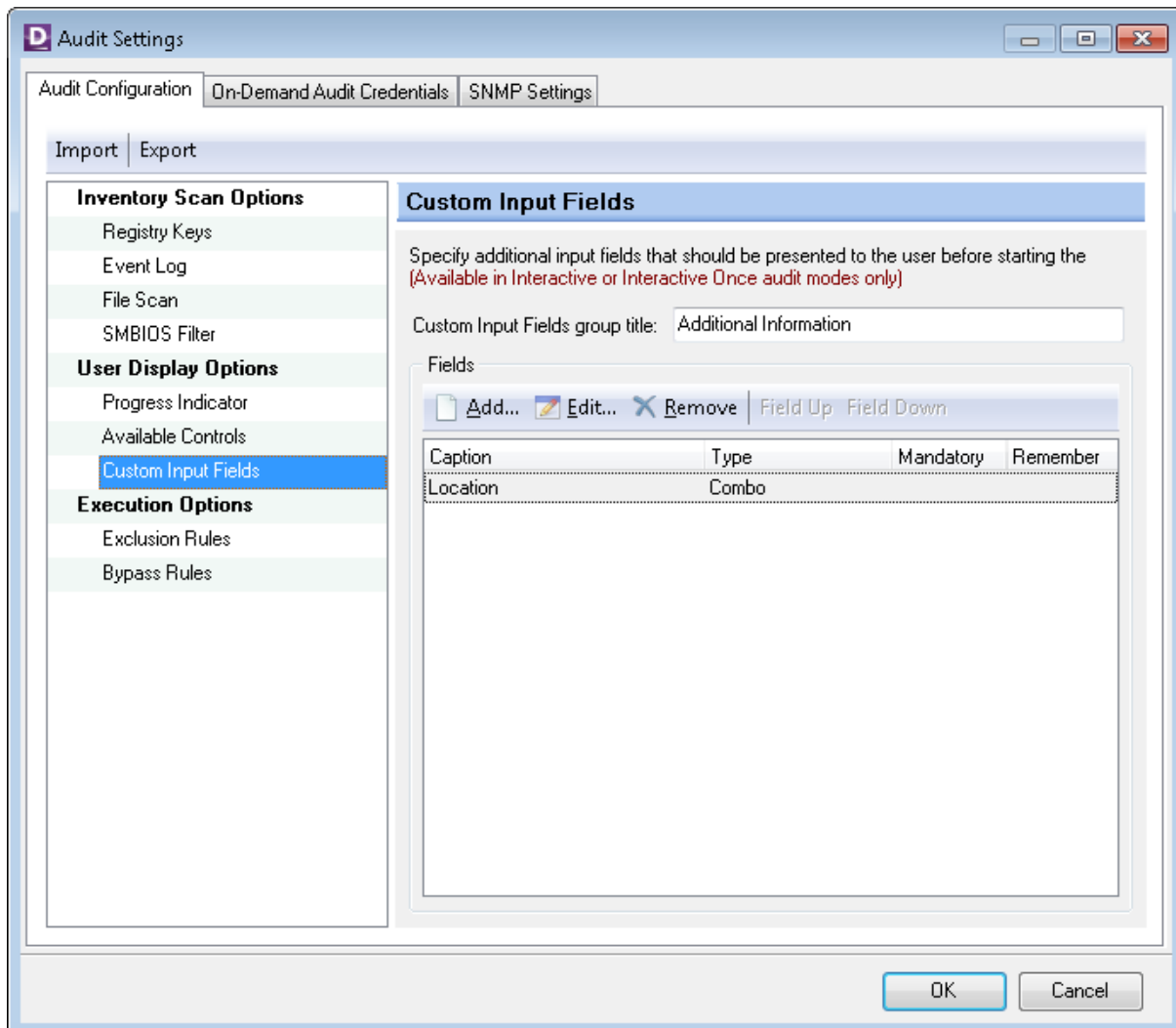


Figure 19: Custom Input Fields

The **Custom Input Fields** screen enables you to define additional input fields that should be presented to the user before starting the interactive audit.



These custom fields are only available in Interactive and Interactive Once audit modes.

The custom fields will appear on the Inventory Analyzer splash screen in a separate group box. By default, the caption of this group box is **Additional Information**, but you can modify it in the **Custom Input Fields group title** field.

Adding Custom Fields

To add a custom field:

1. Click **Add**. The **Edit Field Definition** dialog box appears.

Figure 20: Editing Custom Field

2. In the **Field Caption** field, type in a caption that describes the field.
3. Optional: Type in the default value for the field in the **Default Value** field.
4. Under **Field Type**, choose one of the following:
 - To let users enter text, click **Input**. Then proceed to [Step 6](#).
 - To let users select a value from the list, click **Select** and proceed to the next step.
 - To let users select a value from the list or enter text, click **Combo** and proceed to the next step.

5. For a **Select** or **Combo** field, specify the list of available values as follows:
 - To add a value, type it in the text field at the bottom and then click **Add**.
 - To edit a value, select it, enter a new value in the text field at the bottom, and then click **Replace**.
 - To remove a value from the list, select it and click **Delete**.
6. If you want to prevent users from leaving the field blank, select the **Mandatory** check box. Mandatory fields will be identified with a red border.
7. If you want the field to remember the last entered value, select the **Remember** check box.
8. In the **Audit File Key** field, enter the name for the variable (key) that will store the entered value in the audit snapshot file.
9. Click **OK**.

Changing the Display Order of Custom Fields

The custom fields appear in the order you added them. To change the order in which the custom fields appear on the splash screen:

- To move a field up, select the field in the list and click **Field Up**.
- To move a field down, select the field and click **Field Down**.

Modifying Custom Fields

To modify a custom field:

1. Double-click the field. The **Edit Field Definition** dialog box appears.
2. Make the necessary changes and click **OK**.

Removing Custom Fields

- To remove a custom field, select the field and click **Remove**.

Displaying Custom Fields

After defining custom fields, configure *Alloy Discovery Express* to display them in the Computer List:

1. Select **Tools > Configure Computer List** from the main menu.
2. Expand the **Custom Fields** node and double-click each field you want to be displayed.
3. Click **OK**.

For details, see the *Customizing Computer List* section in the embedded Help system.

Configuring the Exclusion Rules

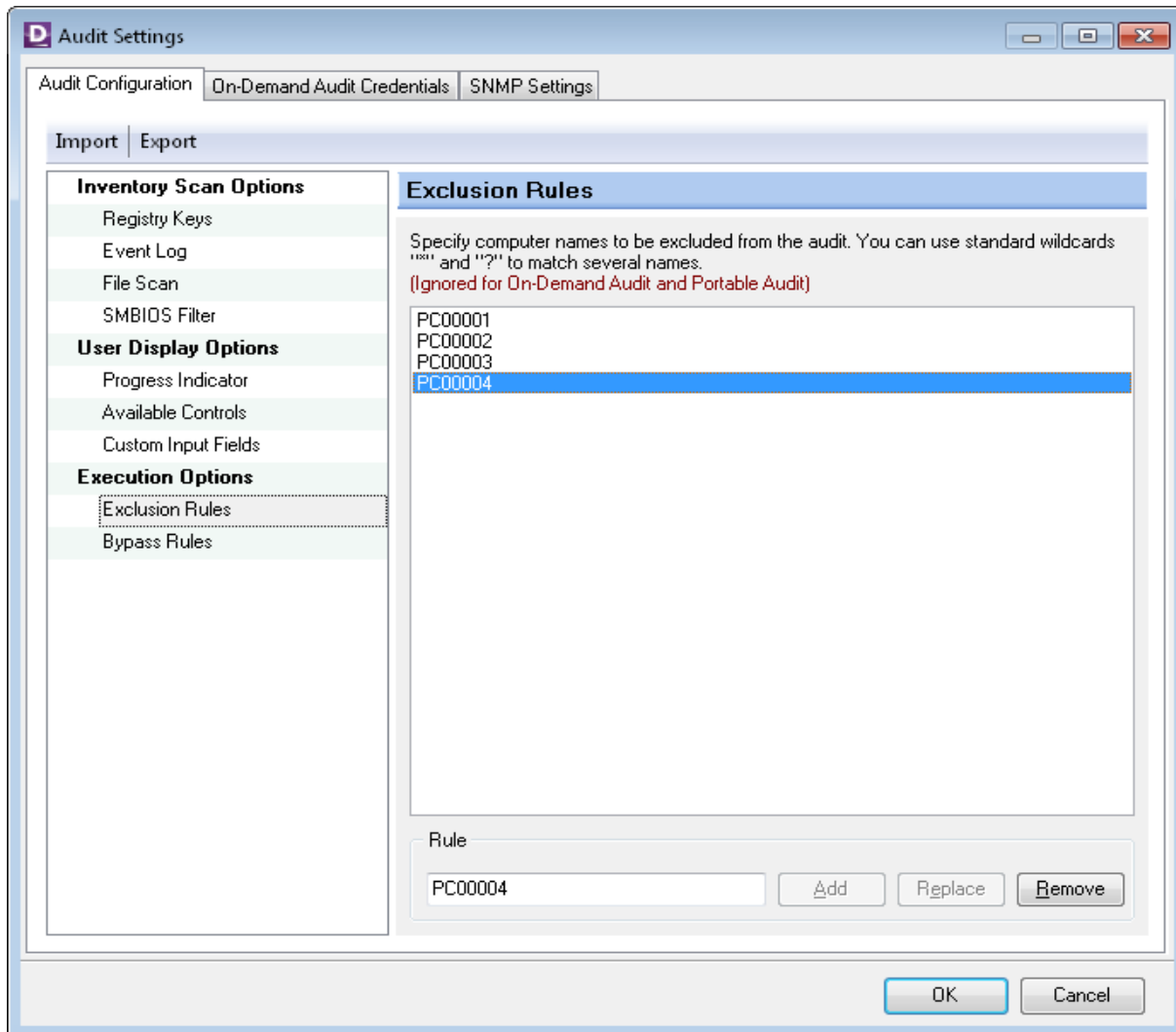


Figure 21: Exclusion Rules

The **Exclusion Rules** screen lets you specify a list of computers that must not be audited.



Exclusion Rules affect only the Scriptable Audit and Audit via E-mail methods. These rules are ignored in the On-Demand Audit and Portable Audit methods.

Excluding computers from the audit

- To add a new computer to the exclusion list, type its name in the text field at the bottom and click **Add**.

You can use the standard wildcards: an asterisk (*) to represent any number of characters, including zero, and the question mark (?) to represent any single character. For example, to match all of the three computers shown in the picture above, you could type in a single 'TS00?' value.

Modifying the exclusion list

- To edit an existing computer name, select it, edit the name in the text field at the bottom, and then click **Replace**.

Removing computers from the exclusion list

- To remove a computer from the exclusion list, select its name and click **Remove**.

Setting the Bypass Rules

With some audit methods the audit is triggered from the client computer, typically when a user logs on the network. Besides the regular users, computers can be accessed by the system administrator or by technicians performing maintenance. In such situations, you wouldn't want the audit to run.

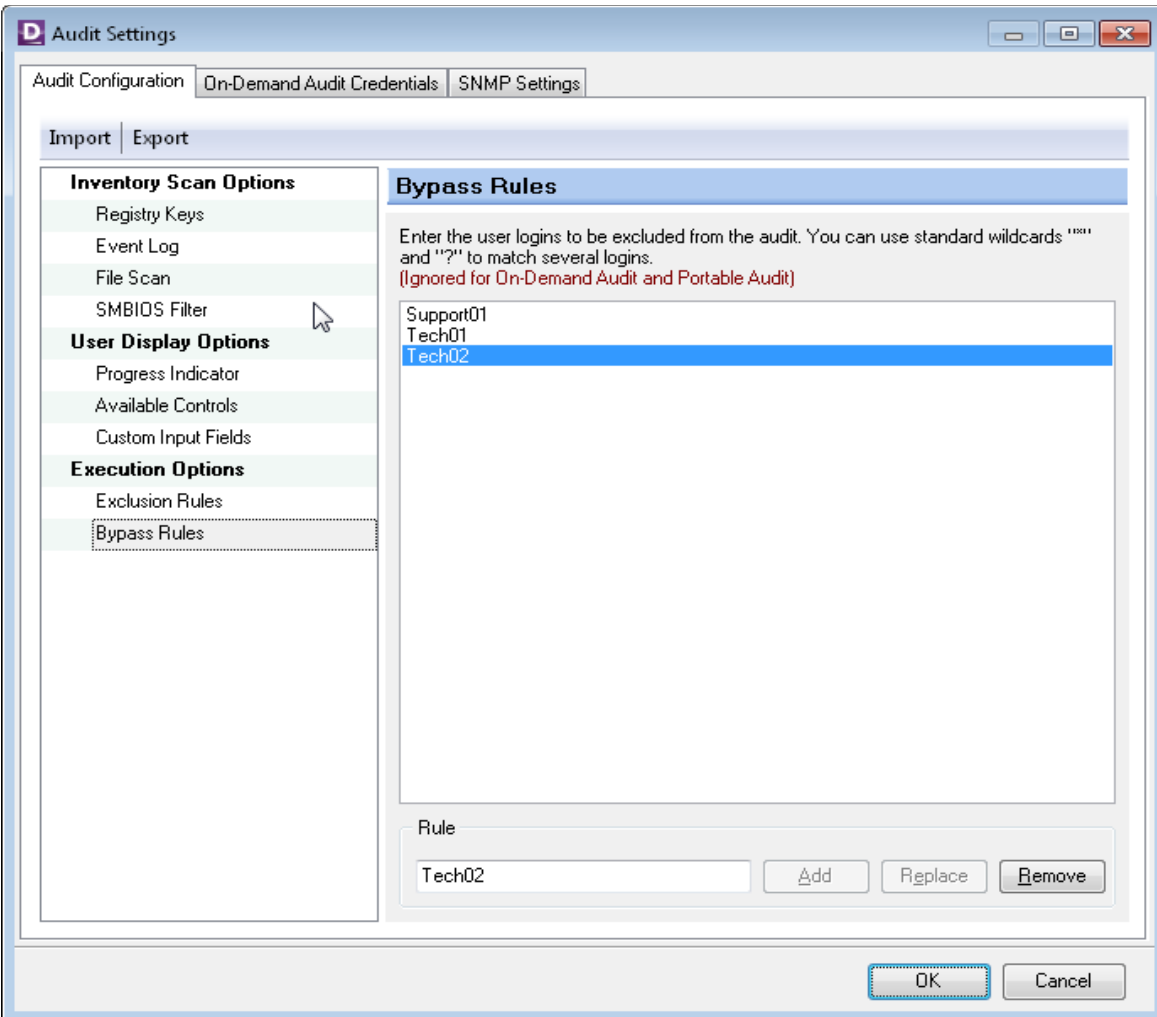


Figure 22: Bypass Rules

Using the **Bypass Rules** screen you can specify a list of user accounts for which you don't want the audit to run.



The list of Bypass Rules affects only the Scriptable Audit and Audit via E-mail methods. These rules are ignored in the On-Demand Audit and Portable Audit methods.

Excluding users from the audit

- To add a user account to the bypass list, type the user name in the text field at the bottom and click **Add**.

You can use the standard wildcards: an asterisk (*) to represent any number of characters, including zero, and the question mark (?) to represent any single character.

Modifying exclusion list

- To edit an existing user name, select it, edit the name in the text field at the bottom, and then click **Replace**.

Removing names from the bypass list

- To remove a user account from the bypass list, select its name and click **Remove**.

Next Steps

Now that you have learned about various audit methods and configured the audit, start auditing computers using any of the following methods:

- To audit the local network at your request, use the On-Demand Audit method. For details, see ["On-Demand Audit" on page 51](#).
- To audit the local network on a regular basis, use the Scriptable Audit. For details, see ["Scriptable Audit" on page 70](#).
- To audit a remote site, use the Audit via E-mail. For details, see ["Audit via E-mail" on page 79](#).
- To audit stand-alone computers or locked-down network segments, use the Portable Audit. For details, see ["Portable Audit" on page 89](#).

CHAPTER 6. Auditing Computers with Alloy Discovery Express

This chapter provides a detailed description of available audit methods.

On-Demand Audit

The On-Demand Audit is an agentless method of auditing LAN computers and network devices at a user's request. Multiple networked computers running on Windows, Mac or Linux can be audited simultaneously for up-to-the-minute audit snapshots. For detailed information on supported operating systems, see ["Supported Platforms and System Requirements" on page 8](#).

The On-Demand Audit is initiated from the host computer to audit any remote computer or device, as long as there is a direct network access from the host and remote computers, and the user is successfully authenticated as an administrator at the remote computer.

You can audit a single or multiple nodes using the on-demand audit:

- **Audit a group of computers or devices** – First you need to create an on-demand audit group. An On-Demand Audit group represents a physical or logical subset of your network, such as a Microsoft Windows domain or an IP address range. For details, see ["Auditing Groups of Computers and Devices" on page 55](#).
- **Auditing a single computer or device** – You can specify a single computer or device by its computer name or IP address. For details, see ["Auditing Standalone Computers or Devices" on page 68](#).

Managing Audit Credentials

To audit a remote computer, *Alloy Discovery Express* needs administrative access to the computer. If you are running *Alloy Discovery Express* under a domain administrative account, you can configure the On-Demand Audit to use the currently logged on user. Otherwise, you may specify another account with administrative access rights for accessing the computers in the group. Similarly, a set of valid audit credentials must be specified for computers running either Linux or Mac operating systems if they are included within the audit group.

You have the flexibility to define an administrative account at the global level (the default audit credentials), or override this setting by using unique audit credentials for the individual audit group. In turn, setting unique audit credentials for a individual computer will override any global audit credentials and the audit credentials set for a particular audit group.

If you need to modify the default credentials, select **Audit > Audit Settings** from the main menu and click the **On-Demand Audit Credentials** tab. On this tab, you can specify the Default Audit Credentials for Windows, and Linux and Mac computers.

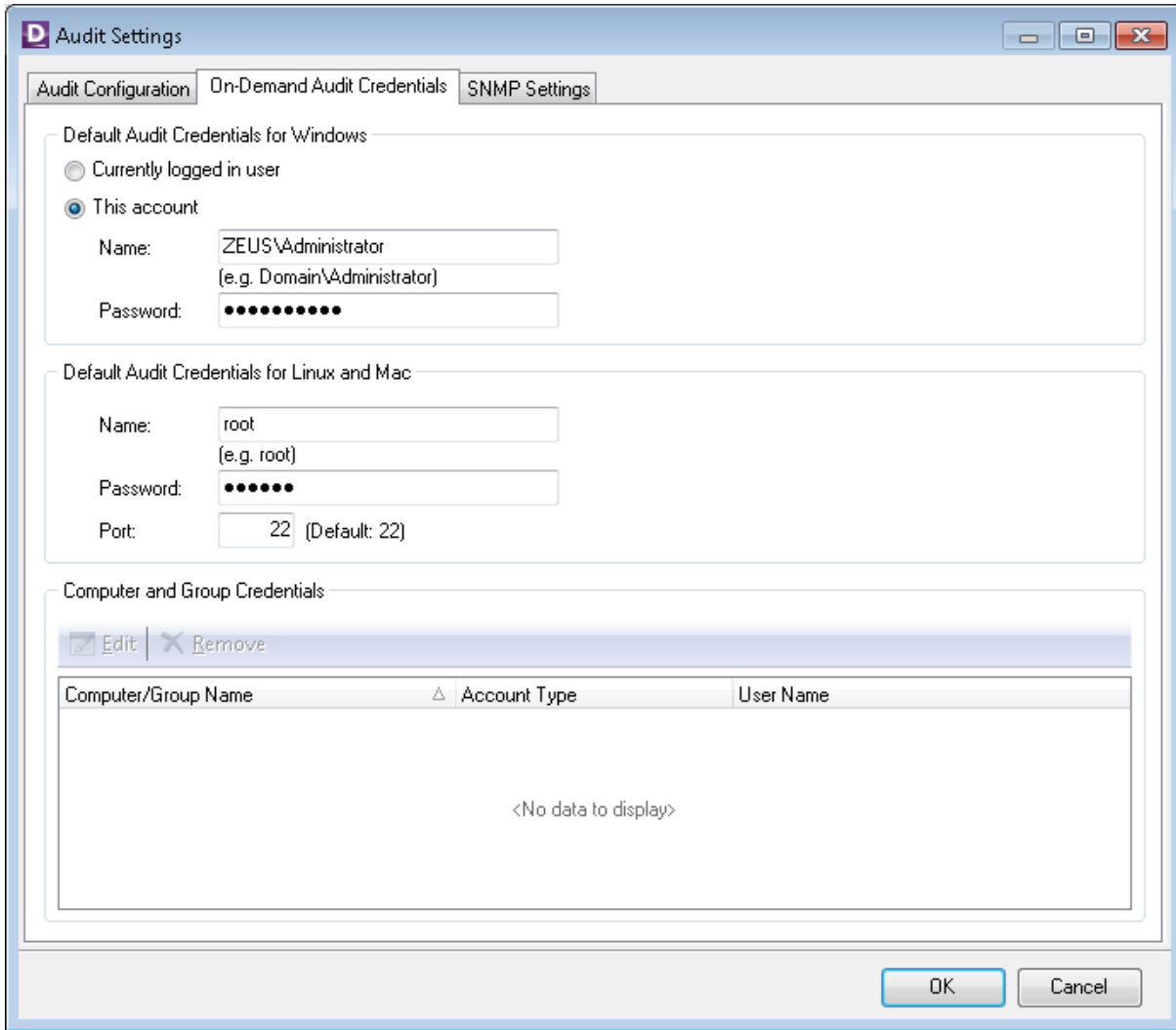


Figure 23: Default On-Demand Audit Credentials

Specifying Default Audit Credentials for Windows Computers

You can specify the Default Audit Credentials for Windows computers in either of the following ways:

- To use the credentials of the logged on user (i.e. use Windows Authentication), select **Currently logged in user**.
- To assign specific credentials, select **This account** and type the login name and password. You can enter either a domain login name (such as ZEUS\Administrator) or a local login name (such as Administrator) as long as this account exists on every computer you want audited as well as on the host machine.

Specifying Default Audit Credentials for Linux and Mac Computers

When specifying the Default Audit Credentials for Linux and Mac computers, enter the **Name** and **Password** to be used. By default, Alloy Discovery Express accesses client Linux and Mac computers using the Secure

Shell protocol (SSH) over the standard TCP port 22. If you want to specify a non-standard TCP port that the SSH server running on client computers listens on, type in its number in the **Port** field.

For Linux and Mac computers, you must assign On-Demand Audit Credentials that allow logging on to these computers. We recommend that you provide credentials for an account with root rights, i.e. the root account or the account which can run the `od` command with elevated (`root`) privileges. Otherwise, *Alloy Discovery Express* will not be able to collect SMBIOS hardware informational on Linux computers. Collecting the list of services (`daemons`) on Mac computers also requires root rights. If you need this information, you should also use the root account or configure the `launchctl` command to run with elevated (`root`) privileges under a non-root account.



Computers with unrecognized operating systems can still be audited only if you assign all the appropriate On-Demand Audit Credentials. Computers with incorrectly recognized operating systems cannot be audited automatically. For details, see ["Incorrectly Recognized Operating System" on page 150](#).

Enabling SNMP Discovery

Alloy Discovery Express uses SNMP to discover, identify, and audit network devices such as switches, routers, and printers in On-Demand Audit groups.



The current version of *Alloy Discovery Express* supports SNMPv1, SNMPv2c, and SNMPv3 versions.

To successfully perform SNMP discovery, the SNMP agent must be configured and running on each target device. You must also specify the SNMP credentials that allow access to the SNMP data on target devices.

You have the flexibility to enable SNMP discovery at the global level and specify the default SNMP credentials, and override these global settings at the group level if necessary.

Global SNMP settings and default SNMP credentials

You can specify global SNMP settings and default SNMP credentials via the **SNMP Settings** tab located on the **Audit Settings** dialog box (**Audit > Audit Settings**):

- **Enable SNMP discovery** – this option enables SNMP discovery globally. However, On-Demand Audit groups may have their own SNMP settings, which would take precedence over these global settings.

If you chose to keep this option selected, specify default SNMP credentials below.



To detect the SNMP version, *Alloy Discovery Express* attempts to connect to a network device using the specified audit credentials for different SNMP versions, starting from Version 3 downward. If, for example, the SNMPv3 credentials are incorrect or not specified, Alloy Discovery Express will have to assume that this device does not support SNMPv3, although the device may support it.

- **Disable SNMP discovery** – this option disables SNMP discovery globally. However, On-Demand Audit groups may have their own SNMP settings, which would override these global settings.
- **SNMP credentials** – specify default SNMP credentials. However, each On-Demand Audit group can use its own SNMP credentials.
- Under **Version v1/v2c**, type in the community string in the **Community** field. An SNMP community is the group that devices running SNMP belong to. The community name is used to identify the group. An SNMP device or agent may belong to more than one SNMP community.



The **Community** field is initialized with the "public" community name, which most SNMPv1-v2c equipment is shipped with by default. However, it is standard practice for system administrators to change community strings so that outsiders cannot see information about the internal network.

- Under **Version v3**, specify the following information for user-based SNMPv3:
 - 1) Type in the SNMP user name.
 - 2) Select the SNMP security level:
 - **No Authentication, No Privacy** — Uses a username for authentication and transmits credentials in clear text.
 - **Authentication, No Privacy** — Provides packet authentication and message integrity, but no encryption. Select the authentication algorithm (MD5 or SHA) in the **Protocol** list and type in the passphrase.
 - **Authentication, Privacy** — Provides the maximal security by combining authentication, message integrity, and encryption. Under **Authentication**, select the authentication algorithm (MD5 or SHA) and type in the authentication passphrase. Under **Privacy**, select the encryption algorithm (DES or AES) and type in the privacy passphrase.

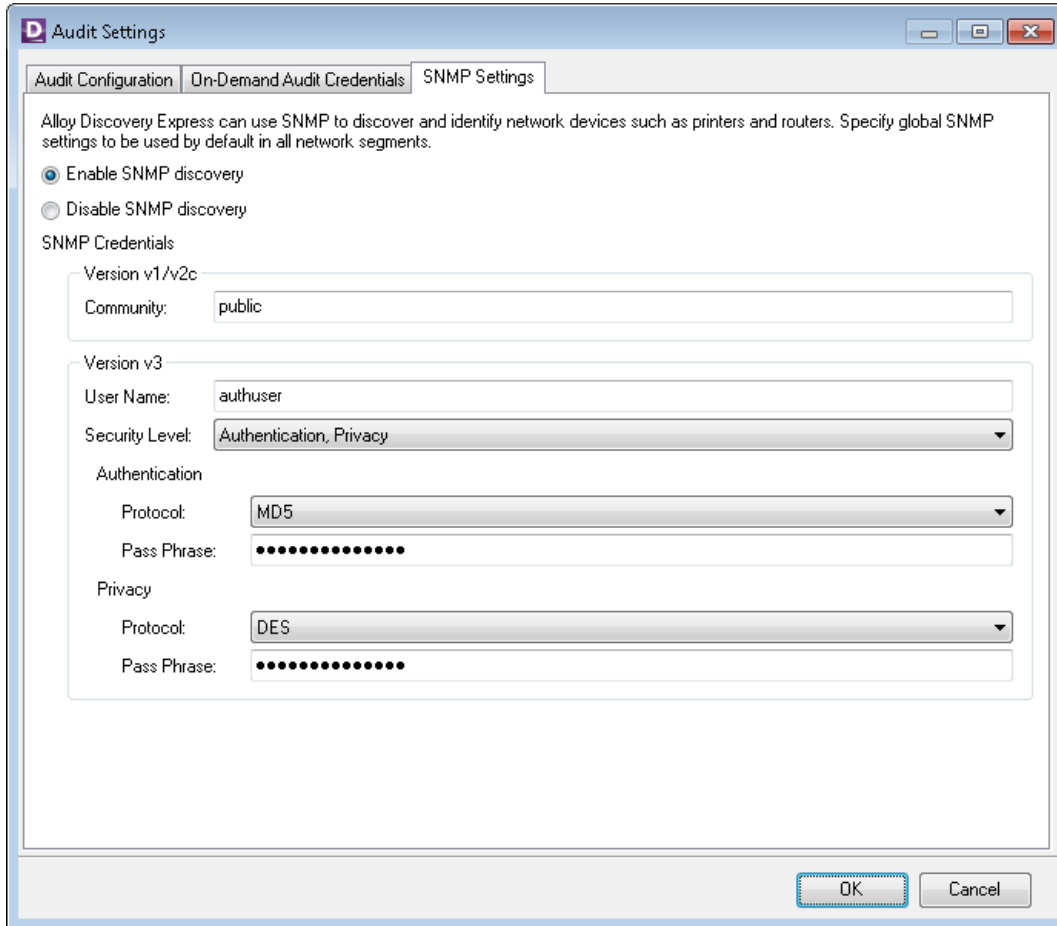


Figure 24: Default SNMP Settings

Group SNMP settings and credentials

You may specify group SNMP settings and SNMP credentials for an individual On-Demand Audit Group. *Alloy Discovery Express* will use these settings when detecting and identifying network devices in that group. Group SNMP settings and credentials can be assigned when creating a new group. If needed, they can be changed at a later time:

- During the creation of the group via the New Group Wizard. For details, see [“Creating On-Demand Audit Groups” on page 56](#).
- By accessing the audit group properties – Right-click on the group, select **Properties**, then select the **SNMP Settings** tab.

Group SNMP settings override global SNMP settings.

Auditing Groups of Computers and Devices

To audit a group of network nodes (computers and network devices) using the On-Demand Audit method, follow the instructions below.

1. Create an On-Demand Audit Group. For details, see ["Creating On-Demand Audit Groups" on page 56](#).
2. Discover nodes within the group. For details, see ["Discovering Computers and Network Devices" on page 63](#).
3. Run the On-Demand Audit for the group. For details, see ["Auditing Computers and Devices" on page 64](#).
4. (Optional) Schedule the On-Demand Audit. For details, see ["Scheduling an On-Demand Audit" on page 69](#).

Creating On-Demand Audit Groups

Each On-Demand Audit Group reflects either logical (a domain or workgroup) or physical (an IP address range or a subnet) structure of your LAN. To create an On-Demand Audit Group, complete the following steps:

1. Select **File > New Group** from the main menu. The New Group Wizard starts.
2. On the **Welcome** page, click **Next** to proceed. The **Group Type** page opens.
3. Click **Audit group** and click **Next**. The **Audit Groups** page opens.
4. Select where to search for computers:
 - If the computers reside within a Windows domain or workgroup, click **On-Demand audit on a Windows domain**, and then click **Next**. The **On-Demand Audit on a Windows Domain** page opens. Proceed to [Step 5](#).
 - If you want to detect network nodes within an IP address range, click **On-Demand audit of an IP address range**, and then click **Next**. The **On-Demand Audit of an IP Address Range** page opens. Proceed to [Step 8](#).
5. On the **On-Demand Audit on a Windows domain** page, click **Browse**. The **Select Domain** dialog box appears.
6. Choose a domain or workgroup in either of the following search areas:
 - To search through the list of all domains and workgroups currently available on your network, select **Network Browser** in the **Search in** list, and then double-click the desired domain or workgroup.
 - To search through the list of domains specified in your Active Directory, select **Active Directory** in the **Search in** list, and then double-click the desired domain or workgroup.Click **Next**. The **Discovery Method** page opens. Proceed to [Step 7](#).
7. On the **Discovery Method** page, choose how to discover computers within a Windows domain:

- For computers registered in the Active Directory, click **Active Directory**.



As long as the information in the Active Directory is accurate, you can use this method to discover computers disconnected at the time of the discovery. However, before starting the discovery process, you should clear the **Discover only computers and devices that respond to ping requests** check box in the group's properties. That check box is available on the **Options** tab of the **Properties** dialog box.

- If you want to query a physical network and discover computers that are not registered in the Active Directory, click **Network Browser**.
- To use both methods, click **Both Active Directory and Network Browser**. *Alloy Discovery Express* will enumerate all computers registered in the Active Directory, and then also perform a network scan to discover other computers that are not currently registered in the Active Directory.

Click **Next**. The **On-Demand Audit Account for Windows computers** page opens.

8. On the **On-Demand Audit of an IP Address Range** page, click **Add** and specify an IP address range to discover computers and network devices on your network in either of the following ways:
 - To specify the IP address range manually, enter the **Start IP Address** and **End IP Address** of the range and click **OK**.
 - To detect the IP address range of your network automatically, click **My Network** and click **OK**.



Depending on your network configuration, the IP address range produced by clicking **My Network** can be unreasonably large so that discovering computers takes a long time. In this case, you can manually edit the start and end IP addresses to narrow down the range as necessary.

If you have a discontinuous network, you can specify its range by adding multiple contiguous segments.

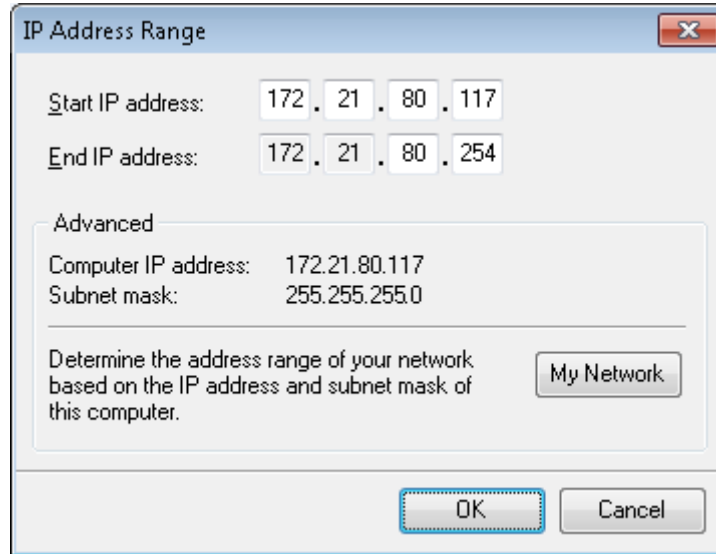


Figure 25: Specifying an IP address range

9. Repeat the previous step to add as many ranges as you need, then click **Next**. The **On-Demand Audit Account for Windows computers** page opens.
10. If you want to use the Default Audit Credentials (for details, see ["Managing Audit Credentials" on page 51](#)), click **Next** to skip this page and proceed to [Step 13](#). If the group contains Linux or Mac computers, the Default Audit Credentials for Linux and Mac computers will be used.
11. If you want to specify custom audit credentials for this On-Demand Audit Group, click **This account** and type in username and password.

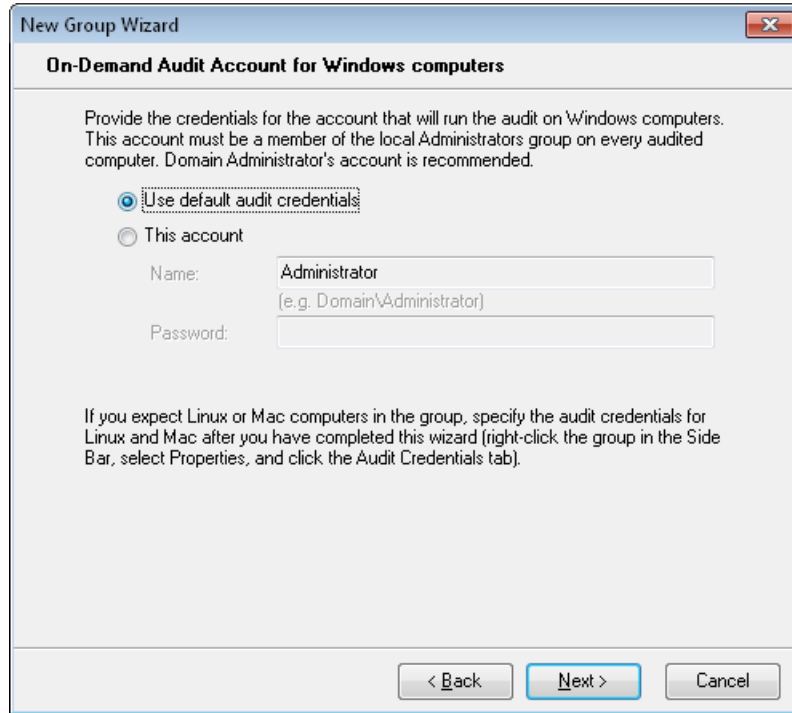


Figure 26: Specifying Custom On-Demand Audit Account

Note that the specified account must be a member of the local Administrators group on every computer in the group and this account must exist on the host machine. Click **Next**.



For any computer where this account does not belong to the local Administrators group, you would need to specify an audit account individually.

For details, see ["Specifying Individual Audit Credentials" on page 114](#).

12. On the **Audit Account for Linux and Mac Computers** page, specify On-Demand Audit Credentials that allow logging on to those computers in the group (for details, see ["Specifying Default Audit Credentials for Linux and Mac Computers" on page 52](#)). Click **Next**.

The **SNMP Discovery settings** page opens.

Figure 27: Specifying group SNMP settings

13. Under **SNMP discovery**, choose whether to enable SNMP discovery for this group.
 - *Alloy Discovery Express* has global SNMP settings, which either enable or disable SNMP discovery globally. If you want to apply global SNMP settings for this group, keep the **Default** option selected. *Alloy Discovery Express* shows the global SNMP discovery status in the parentheses: **enabled** or **disabled**.



For details, see ["Global SNMP settings and default SNMP credentials" on page 53.](#)

- If you want to enable SNMP discovery for this group, regardless of the global SNMP settings, click **Enable SNMP discovery**.

- If you want to disable SNMP discovery for this group, regardless of the global SNMP settings, click **Disable SNMP discovery**.

If SNMP discovery is enabled (either globally or at the group level), under **SNMP credentials**, specify which SNMP credentials *Alloy Discovery Express* should use for this group.

- To discover nodes in this group under the default SNMP credentials, keep the **Default** option.



For details, see ["Global SNMP settings and default SNMP credentials" on page 53](#).

- If you want to specify group SNMP credentials, select the **Use these credentials** option, then specify SNMP settings as needed.



Alloy Discovery Express supports SNMPv1, SNMPv2c, and SNMPv3. We recommend supplying both Version v1/v2c and v3 credentials to let Alloy Discovery pick the appropriate credentials automatically based on the SNMP version supported by the queried network device.

Click **Next**. The **Group Name and Description** page opens.

14. Review the group name and modify it, if necessary. Optionally, enter a description for the group. Then click **Next**. The **Ready to Create New Group** page opens.
15. Review your settings. If you want to change any settings, click **Back** to return to the previous pages and make the necessary changes. When you are ready to create the group, click **Next**. After the wizard finishes creating the group it will display the **Group Created** page.
16. If you want to discover nodes in this group and audit them immediately once you have completed the wizard, keep both the **Discover computers in this group now** and **Audit computers in this group** check boxes selected. Click **Finish** to complete the wizard.

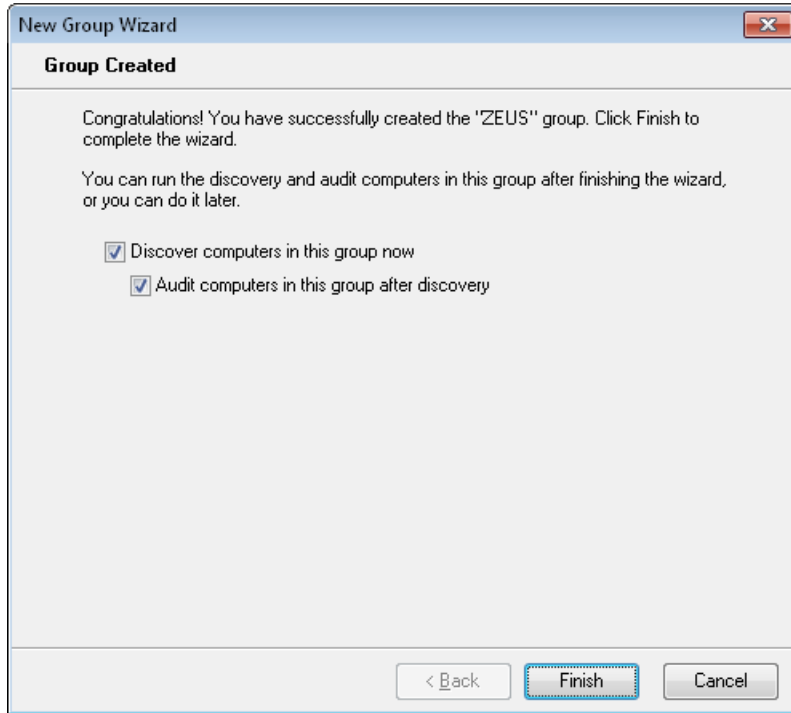


Figure 28: Finishing the New Group Wizard

After the group has been created, it appears in the Sidebar in the structure that represents the group hierarchy. From there you can navigate through existing audit groups and computer groups down to individual computers or devices. Next to each audit group you will see two counters showing the number of audited nodes and total number of nodes in the group. For example 3/10 means the group of 10 nodes has 3 audited nodes. Computer groups display a single counter showing the number of nodes in the group.

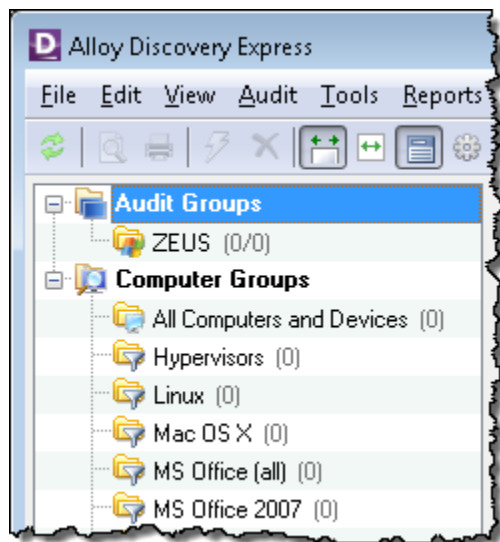


Figure 29: On-Demand Audit Group Created

Discovering Computers and Network Devices

Once you have added an On-Demand Audit Group, you need to populate it with computers and network devices through the process of discovery.

If you left the **Discover computers in this group now** check box selected on the last page of the New Group Wizard, the discovery process starts automatically upon the completion of the wizard. Otherwise, you can start the discovery by right-clicking the group in the Sidebar and selecting **Discover** from the pop-up menu. During the discovery process, *Alloy Discovery Express* displays a status dialog box where you can monitor the progress.

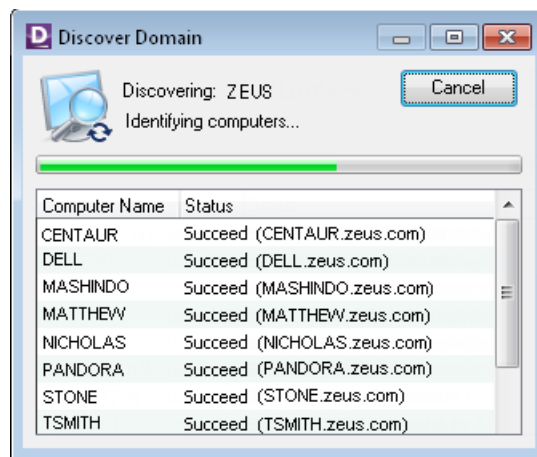


Figure 30: Status of the Discovering Process

Each row in the **Discover Domain** dialog box shows the computer name and current operation status. The **Discover IP Range** dialog box displays the IP address, name (if known), and the current operation status. For explanation of these statuses, see the *Discovering Computers and Devices* section in the embedded Help system.



In case you decide to terminate the discovery process, you can keep already discovered nodes and upload the ir data to the Inventory Repository.

For details, see the *Discovering Computers and Devices* section in the embedded Help system

Computers and network devices that have been discovered appear in the Sidebar along with an icon representing the node type and its state. Discovered but not yet audited nodes show up with a grayed out icon. Once the node has been audited, the icon turns colored.

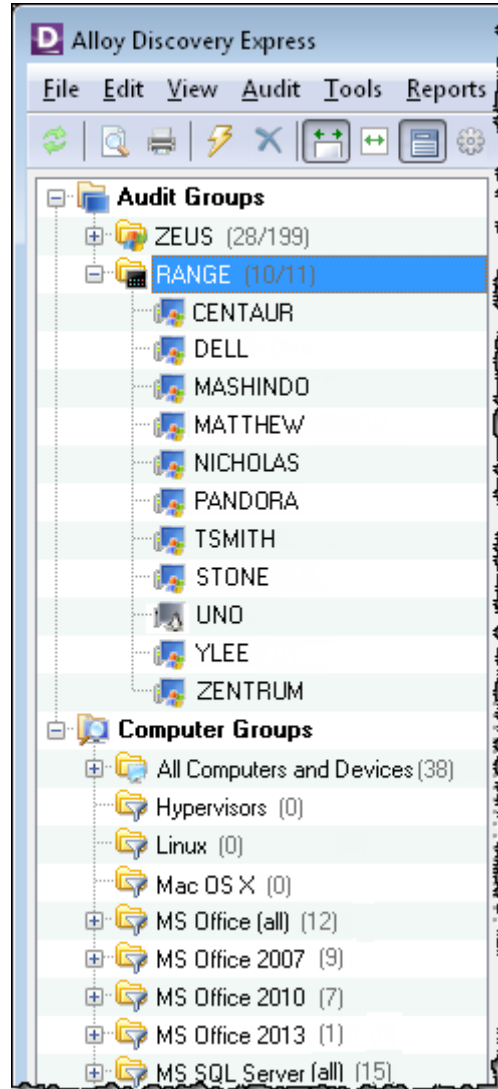


Figure 31: Computers Discovered


Whenever new computers and devices are added to the network, repeat the discovery to add those nodes to the appropriate audit group.

Auditing Computers and Devices

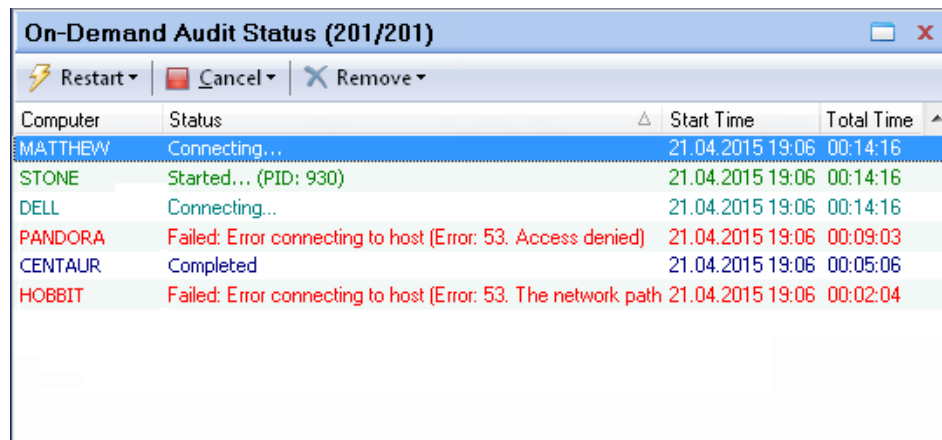
When an audit group is populated with network nodes, you can start auditing this group.

If you left both the **Discover computers in this group now** and **Audit computers in this group** check boxes selected on the last page of the New Group Wizard, the audit starts automatically after the discovery is finished. Otherwise, select the group to audit and click the lightning icon ⚡ on the Standard Toolbar. Alternatively, you can right-click the group in the Sidebar and select **Audit This Group** from the pop-up menu.

Alternatively, you can choose to audit only nodes in a group that been discovered but have yet to be audited, right-click the group in the Sidebar and select **Audit This Group > Audit Never Audited Computers** from the pop-up menu.


If you want to audit an individual computer or device within an On-Demand Audit Group, select it and click the lightning icon  on the Standard Toolbar. Alternatively, you can right-click the computer or device and select **Audit Now** from the pop-up menu. For information how *Alloy Discovery Express* looks for the On-Demand Audit account, see ["Managing Audit Credentials" on page 51](#).


When you start the On-Demand Audit, the **On-Demand Audit Status** pane appears under the preview pane. In the window title bar, you will see two counters showing the number of audited nodes and total number of nodes in the group. For example, 12/20 means the group of 20 nodes has 12 audited nodes.



Computer	Status	Start Time	Total Time
MATTHEW	Connecting...	21.04.2015 19:06	00:14:16
STONE	Started... (PID: 930)	21.04.2015 19:06	00:14:16
DELL	Connecting...	21.04.2015 19:06	00:14:16
PANDORA	Failed: Error connecting to host (Error: 53. Access denied)	21.04.2015 19:06	00:09:03
CENTAUR	Completed	21.04.2015 19:06	00:05:06
HOBBIT	Failed: Error connecting to host (Error: 53. The network path	21.04.2015 19:06	00:02:04

Figure 32: On-Demand Audit Status pane

You can undock the **On-Demand Audit Status** pane by clicking the **Undock** icon  on the upper right top of the pane. To dock the **On-Demand Audit Status** floating dialog box, click the **Dock** button.

You can hide the **On-Demand Audit Status** pane by clicking the **Hide** icon . To hide the **On-Demand Audit Status** floating dialog box, click the **Hide** button or choose **View > On-Demand Audit Status** from the main menu. To restore the **On-Demand Audit Status** pane or dialog box, press F8 or choose **View > On-Demand Audit Status** from the main menu.

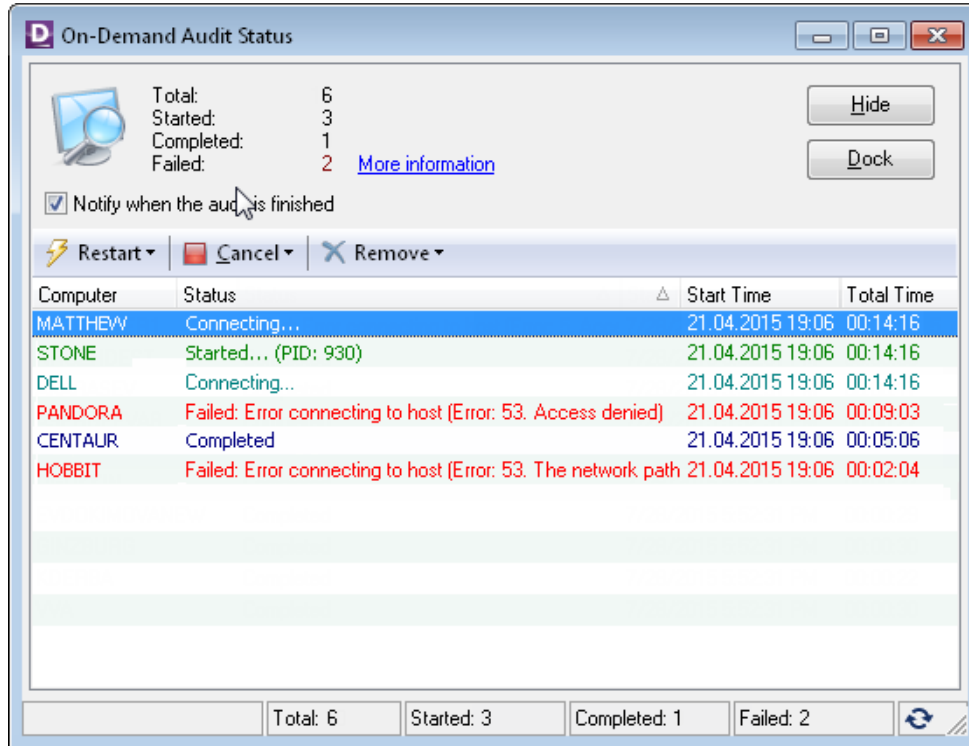


Figure 33: On-Demand Audit Status dialog box

Both the **On-Demand Audit Status** pane and dialog box display the list of all nodes scheduled for On-Demand Audit so you can monitor the audit process and track possible errors. Each entry in the list represents a single computer or device. It shows the name, current status, the time when the audit has started, and the duration of the process. When a node is being audited, the audit process ID is displayed in the **Status** column. For more information about the **On-Demand Audit Status** dialog box and its functions, see the *On-Demand Audit Status* section in the embedded Help system.

When the audit finishes, you will be prompted to refresh the data. Click **Yes**, and the **Loading Audit Snapshots** dialog box appears. For details on this dialog box and the information it displays, see the *On-demand Audit Status* section in the embedded Help system.

Audited computers and devices appear in the Sidebar under their respective groups, where each node is represented with an icon corresponding to its type. Next to each group, you can see two counters showing the number of audited nodes and total number of nodes in the group. You preview the details of any audited network node by clicking its icon. Double-click a computer to open the corresponding audit snapshot in the Audit Snapshot Viewer. Double-click a device icon to open the corresponding device details in the **Network Device Details** dialog box.

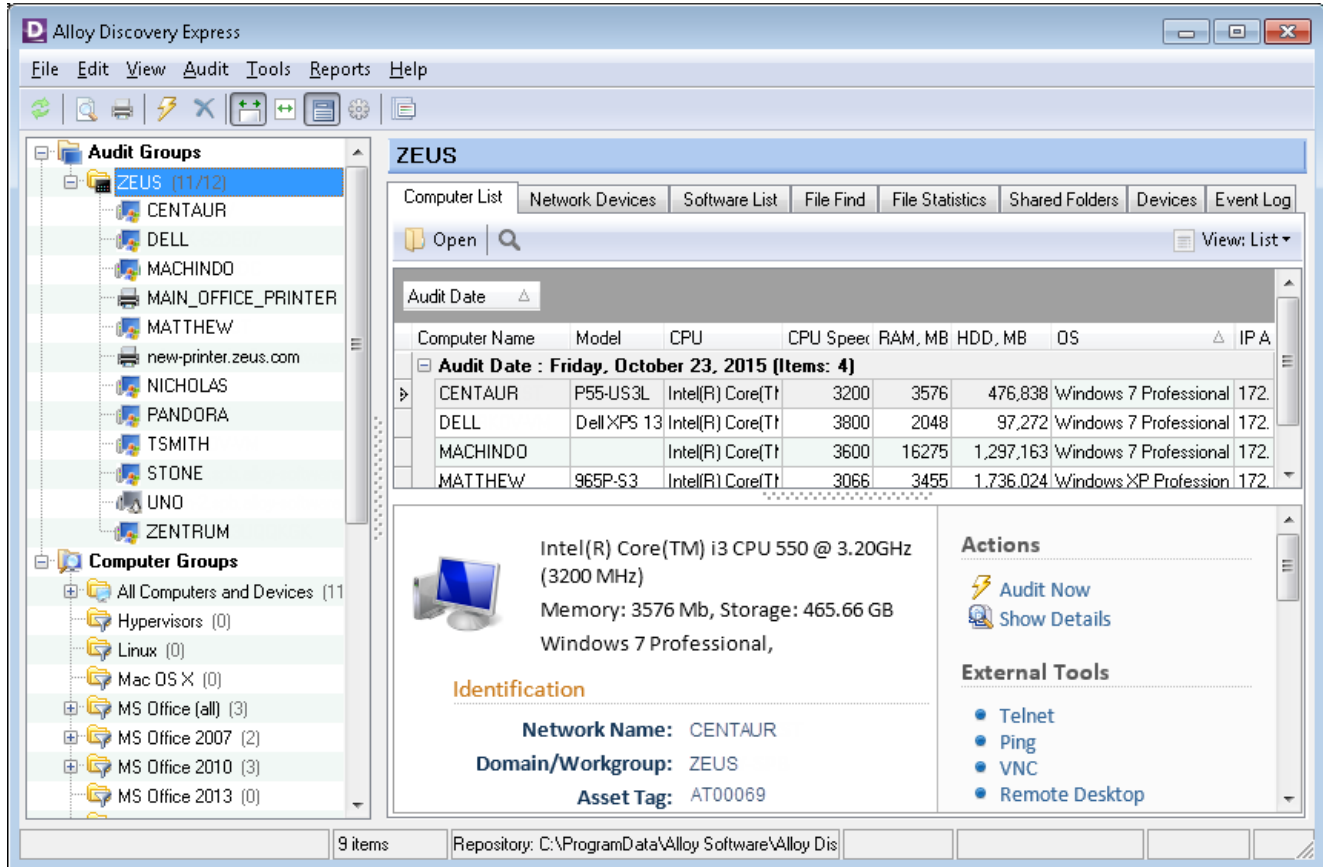


Figure 34: Audited On-Demand Audit Group

Next Steps

The New Group Wizard assigns default values to some of the advanced properties of new groups. To modify them, right-click a group in the Sidebar and select **Properties** from the pop-up menu. For instructions, see the *Configuring Groups for the On-Demand Audit* sections in the embedded Help system.

Auditing Standalone Computers or Devices

If you know the name or IP address of a networked computer or a network device, you can audit that node on demand without adding it to an audit group. You can also quickly audit your own computer (the machine hosting *Alloy Discovery Express*) at any time you want.

Auditing Standalone Remote Computers or Devices

To audit a standalone remote computer or device, complete the steps below:

1. Select **Audit > Audit Computer by Name/IP** from the main menu. The **Audit Computer by Name or IP Address** dialog box appears.

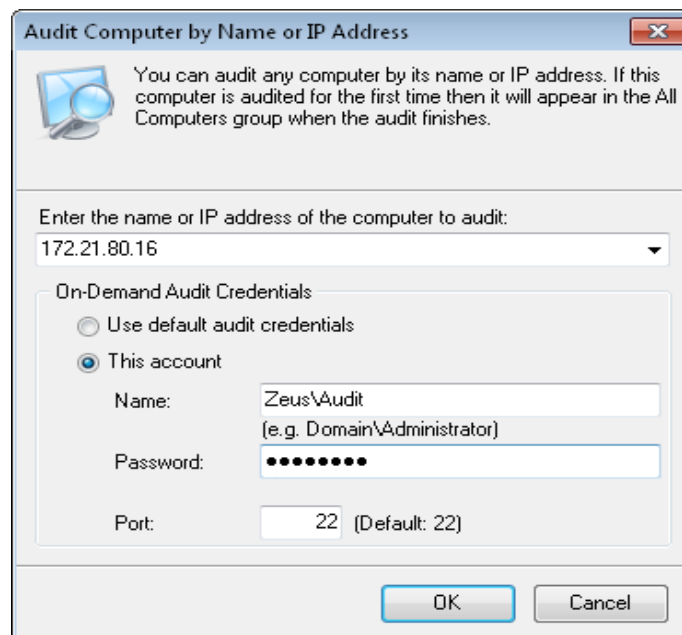


Figure 35: Auditing a Single Computer

2. Enter the node name or its IP address.
3. If the Default On-Demand Audit Credentials cannot be used to access that computer, click **This account** and specify the username and password below.

For a Windows computer, the account you specify here must be a member of the local Administrators group on the computer you want audited (either directly or through the membership in a Windows domain group). You can specify the username as a domain account name (for example, `Zeus\Audit`) or a local account name (for example, `Audit`) as long as this account exists on every computer you want audited as well as on the host machine.

For a Linux or Mac computer, you must specify the credentials that allow logging on to this computer, preferably this should be an administrative account.

4. Click **OK**. The audit starts, and the **On-Demand Audit Status** dialog box appears, where you can monitor and manage the process.

To find this computer or device, you can double-click a record in the **On-Demand Audit Status** dialog box, and *Alloy Discovery Express* will automatically select the corresponding node in the Sidebar. You can also right-click a record and choose **Find Computer in Side Bar**.

Audit Your Computer

If you want to audit your own computer, select **Audit > Audit My Computer** from the main menu. The audit starts, and the **On-Demand Audit Status** dialog box appears, where you can monitor the progress. The audit runs under your current account, and no administrative privileges are needed. To find this computer, you can double-click a record in the Audit Status dialog box, and *Alloy Discovery Express* will automatically select the corresponding computer in the Sidebar. You can also right-click a record and choose **Find Computer in Side Bar**.

Scheduling an On-Demand Audit

You can audit one or several audit groups or computer groups by running `AlloyDiscoveryExpress.exe` from the command line. This executable file is located in your *Alloy Discovery Express* installation folder (typically, `\\Program Files\Alloy Software\Alloy Discovery Express 8\Bin\`).

With this feature, you can initiate the silent agentless On-Demand Audit method to audit the specified network nodes from a script or a scheduled task. For example, you may create a scheduled task that runs a batch file on a regular basis at your desired interval. For detailed information on how to automate the Inventory Analyzer to produce audit snapshots on a regular basis, see ["Automating the Scriptable Audit" on page 72](#).

When `AlloyDiscoveryExpress.exe` is launched from the command line with the `/Audit` option, the *Alloy Discovery Express's* Main Console remains hidden and the application runs in the background, minimized to the notification area.

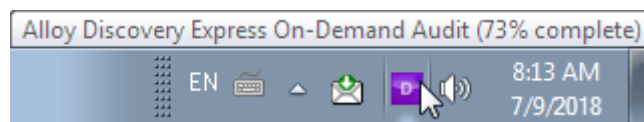


Figure 36: Scheduled On-Demand Audit Status shown in the System Tray

To view the audit status, double-click the application icon in the notification area. The **Alloy Discovery Express On-Demand Audit** dialog box opens, where the progress is displayed.

The following command-line options are available:

/Audit=[GroupName]	<p>This option is required to run <i>Alloy Discovery Express</i> in a hidden mode.</p> <p>Specifies the name of the audit group or computer group to audit. If needed, you can specify multiple groups by using the /Audit option several times.</p> <p>Examples:</p> <p>/Audit="Windows Server (all)" /Audit=ZEUS</p>
/Log=[Path]	<p>Specifies the output directory for log files. Every <i>Alloy Discovery Express</i> instance creates its own log file.</p> <p>If this option is not specified, the default /log sub-folder is created in your ProgramData folder where Alloy Discovery Express stores program data for users, typically:</p> <p>C:\ProgramData\Alloy Software\Alloy Discovery Express\8.0\log</p>



The "All Computers and Devices" group can not be audited.

Scriptable Audit

The Scriptable Audit is an agent-based method of LAN audit. Using this method you can audit networked computers that cannot be normally audited using the On-Demand Audit (for example, when some computer are turned off during the time the On-Demand Audit runs). It involves two steps: the deployment of the Inventory Analyzer to a network share and its automation using domain logon scripts or scheduled tasks.

When you deploy the Inventory Analyzer, you create a shared folder that will serve as an intermediary repository for captured audit snapshots. Automating the Inventory Analyzer, enables *Alloy Discovery Express* to automatically scan intermediary repository and load detected snapshots to the database. If you change audit configuration, *Alloy Discovery Express* will also reflect these changes in the configuration of the deployed audit agent. For more information on the different types of audit methods available see ["Overview of Audit Methods" on page 5](#).

To audit computers using the Scriptable Audit method, follow the instructions below:

1. Deploy Inventory Analyzer to a shared folder. See ["Deploying the Inventory Analyzer onto a Shared Folder" on page 70](#)
2. Automate the audit. See ["Automating the Scriptable Audit" on page 72](#)

Deploying the Inventory Analyzer onto a Shared Folder

First, review the requirements for computer hosting the shared folder (see ["Shared Folder Machine" on page 11](#)). Depending on your environment, the following scenarios are possible:

The Shared Folder is hosted on a server on your network

- In that case, you must complete the following steps prior to deploying the Inventory Analyzer there:
 - Create a dedicated folder on the server and assign both the “Modify” permission and the “Change Permissions” special permission for the account for this folder.
 - Share this folder and grant the Full Control share permission to your user account for this network share.

The Shared Folder is hosted on your computer

- In that case, you will create a shared folder when deploying the Inventory Analyzer.

You deploy the Inventory Analyzer onto a network share by creating a Scriptable Audit group as follows:

1. Select **Audit > New Group** from the main menu. The New Group Wizard starts.
2. On the **Welcome** page, click **Next** to proceed. The **Group Type** page opens.
3. Click **Audit Group** and click **Next**. The **Audit Groups** page opens.
4. Click **Scriptable Audit** and click **Next**. The **Shared Folder** page opens.
5. Choose where you want to deploy the Inventory Analyzer:
 - If you have a network share on another remote server, click **Yes, I already have a shared folder** and then click **Next**. The **Shared Folder Location** page opens. Proceed to [Step 6](#).
 - If you want to configure the computer hosting *Alloy Discovery Express* as the Shared Folder machine, click **No, I do not have a shared folder** and click **Next**. The **Share Folder** page opens. Proceed to [Step 7](#).
6. On the **Shared Folder Location** page, type in the UNC path to the share or click **Browse** and select one from the folder tree. Click **Next**. The **Recommended Permissions** page opens. Proceed to [Step 8](#).
7. On the **Share Folder** page, click **Browse** and click **New Folder** to create a new folder in the folder tree. Then type the share name for the folder in the **Shared as** field. Click **Next**. The **Recommended Permissions** page opens.

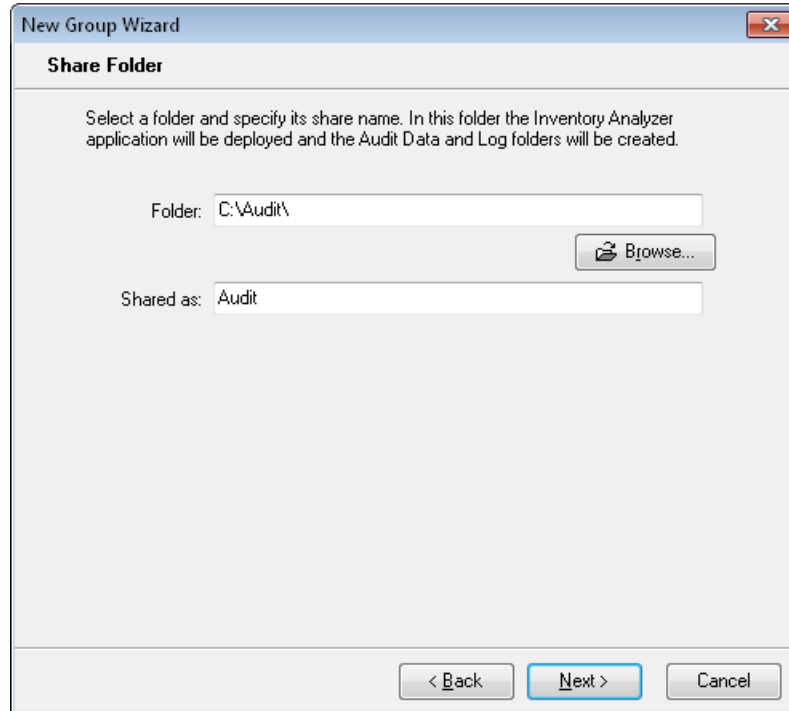


Figure 37: Creating Network Share on the Alloy Discovery Express Host Machine

8. On the **Recommended Permissions** page, keep the **Set recommended permissions** check box selected and click **Next**. This will apply the minimally necessary permissions to perform the audit; for details, see ["Minimally Necessary Permissions" on page 166](#). The **Group Name and Description** page opens.
9. Review the group name and modify it, if necessary. Optionally enter a description for the group. The click **Next**. The **Ready to Create New Group** page opens.
10. Review your settings and click **Next** to proceed with creating the group. Click **Back** to make changes if needed. The wizard will display the **Group Created** page once the group has been created.
11. Click **Finish** to complete the wizard.

Automating the Scriptable Audit

When launched, *Alloy Discovery Express* can automatically scan intermediary repositories (if you have multiple instances of the Scriptable Audit), and load the audit snapshots from there into the main Inventory Repository. For more information on the different types of audit methods available see ["Overview of Audit Methods" on page 5](#)

After you have installed and configured the Inventory Analyzer, you need to automate the Inventory Analyzer to take audit snapshots on a regular basis. There are two main scenarios for automating the audit, depending on your environment:

- Windows domain networks. See ["Automating the Scriptable Audit on Windows Domains" on page 73](#).

- Windows non-domain networks. See [“Automating the Scriptable Audit on Windows Non-Domain Networks” on page 75.](#)
- For networked computers running Linux or Mac OS, you can use the Linux and Mac OS features such as the cron daemon to automate the Inventory Analyzer for Linux (lina) or the Inventory Analyzer for Mac (ina_mac) from the shared folder where the Inventory Analyzer has been deployed. See your Linux or Mac OS documentation for details.

Novell users who have ZenWorks installed should note that it can be configured to run `ina32.exe` on startup. For details, please see your Novell documentation.

Automating the Scriptable Audit on Windows Domains

Windows 2000 and later domain controllers provide the logon scripting facility for configuring desktop environments for users. The default location for logon scripts is the special `NETLOGON` shared folder built during the Active Directory installation.

To automate the audit:

1. In your domain logon script, add a line for launching the deployed Inventory Analyzer.
2. Assign this script for each domain member. For instructions, see the Microsoft TechNet topic "Assign User Logon Scripts" at [https://technet.microsoft.com/en-us/library/cc770908\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc770908(v=ws.11).aspx).

This will run the Inventory Analyzer on each domain member when logging on to the domain, as shown in [Figure 38 on page 73.](#)

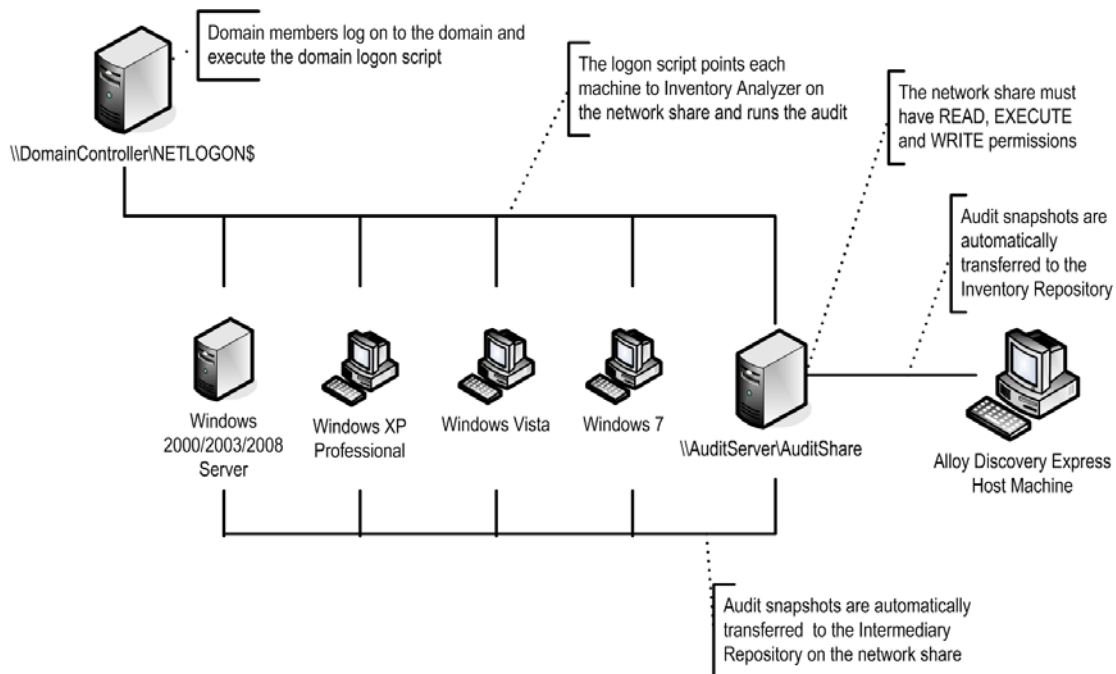


Figure 38: Auditing Computers on a Windows Domain

The command for running the audit can be as simple as the following:

```
\\AuditServer\AuditShare\ina32.exe
```

The above should work fine for scanning Windows workstations. However, the above script won't detect the user's login name of Novell users, so it won't be recorded in the computer's audit snapshot.

To solve the above problem, the Inventory Analyzer has the /userid command-line option to pass a username from the Novell environment:

```
\\AuditServer\AuditShare\ina32.exe /userid="%LOGIN_NAME"
```

This should correctly pass the Novell username to the Inventory Analyzer using the Novell scripting macro %LOGIN_NAME.

Automating the Scriptable Audit on Windows Non-Domain Networks

Once you've deployed the Inventory Analyzer onto the network share, configure each client computer to run it automatically. There are several ways to automate the Scriptable Audit:

- Using the Windows registry startup keys. See ["Using the Windows Registry Startup Keys" on page 75](#).
- Using the Windows startup group. See ["Using the Windows Startup Group" on page 76](#).
- Using the Windows Task Scheduler. See ["Using the Task Scheduler" on page 77](#).

Using the Windows Registry Startup Keys



Editing the Windows registry can cause a total system failure if done incorrectly. Please **do not edit your registry unless** you have experience editing it.

To automate running the audit on startup, complete the following steps on each client computer:

1. Open the Windows Registry Editor and browse to the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2. Create a new string value named "Inventory Analyzer" and enter the Inventory Analyzer's UNC path as the data value. Windows will now run the Inventory Analyzer on startup.

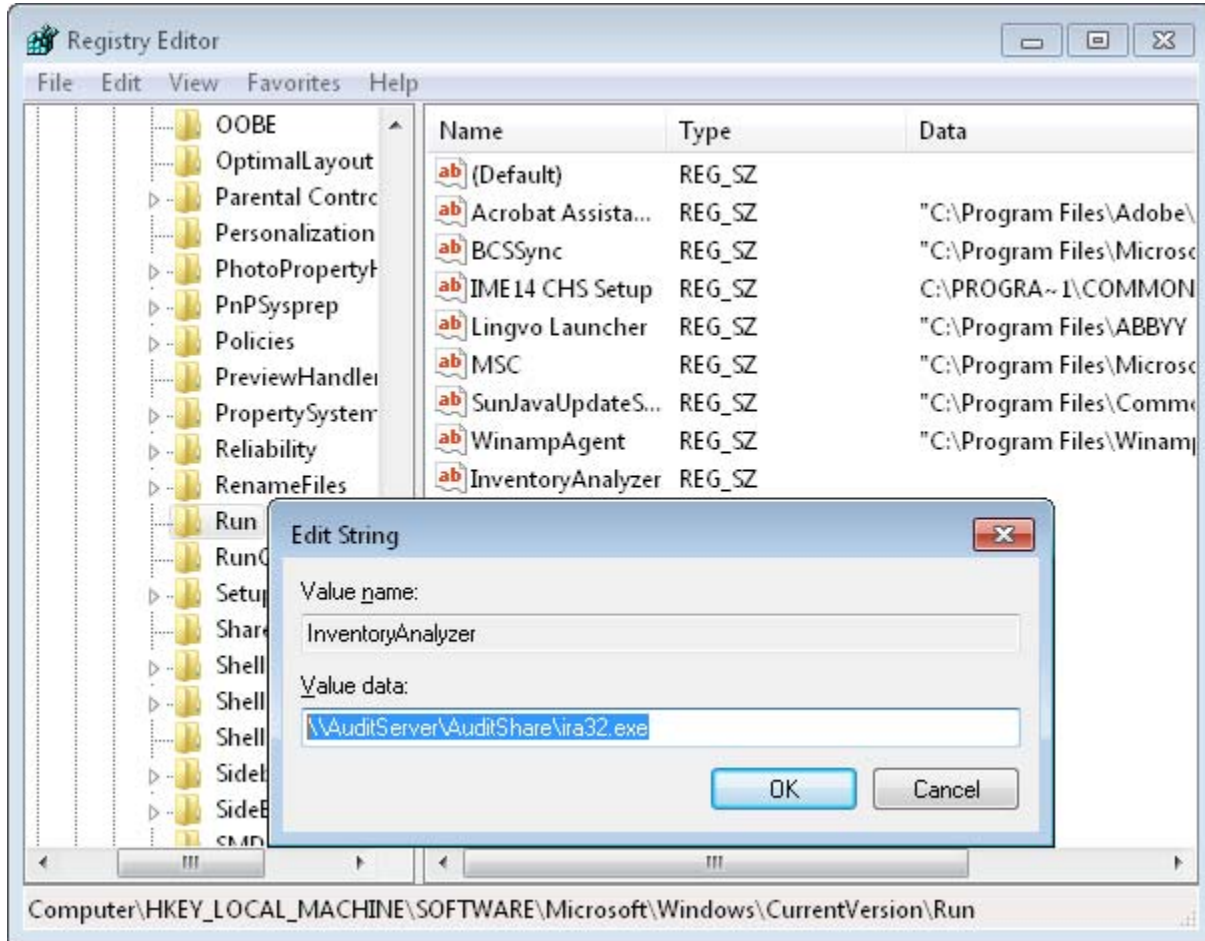


Figure 39: Registry Editor

Using the Windows Startup Group

On startup, Windows computers run all items in the Start Menu folder named "Startup". This folder is located under **Start > All Programs**.

To add a shortcut for the Inventory Analyzer to the Startup folder, complete the following steps on each client computer:

1. Right-click the **Start** button and click **Explore All Users**
2. Browse to **Start Menu > Programs > Startup**.
3. Click **File > New > Shortcut**. The **Create Shortcut** dialog box opens.

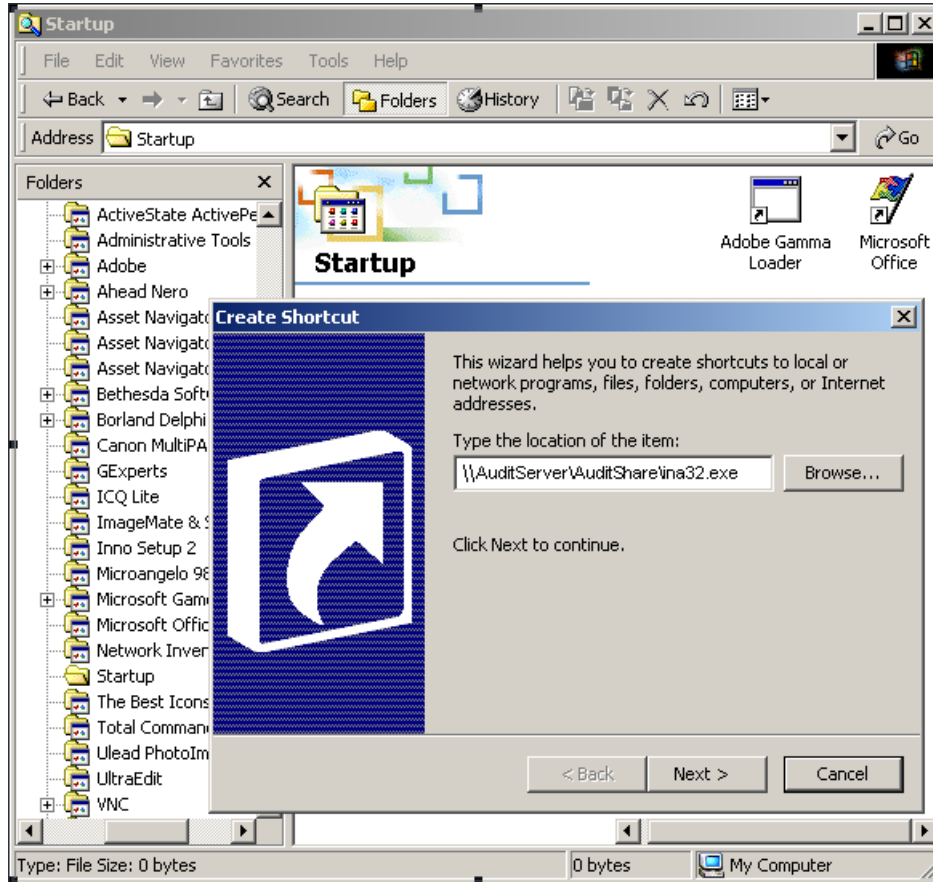


Figure 40: Startup Menu Items

- Specify the location of the Inventory Analyzer (ina32.exe) and complete the wizard.



Use this method with caution, since users may disable scheduled audits by removing startup entries.

Using the Task Scheduler

You can use the Windows Task Scheduler to start the audit at a specified date and time.

The steps below show how to create a scheduled task in Windows 7.

To open the Task Scheduler, click the Start button, click Control Panel, click **System and security**, click **Administrative Tools**, and double-click **Task Scheduler**.

To create a scheduled task, complete the following steps on each client computer:

- Double-click **Add Scheduled Task** to start the Scheduled Task Wizard, and then click **Next**.

2. Click **Browse**, navigate to the Inventory Analyzer (ina32.exe), and click **Open**.
3. Type in a name for the task and choose how often the task should run. Click **Next**.
4. Specify the information about the day and time to run the task, and then click **Next**.
5. Type in the name and password of the user who is associated with this task. Make sure that you choose a user with sufficient permissions to run the program. By default, the wizard selects the name of the user who is currently logged on. Click **Next**.
6. Review the settings and click **Finish** to complete the creating of a new scheduled task.

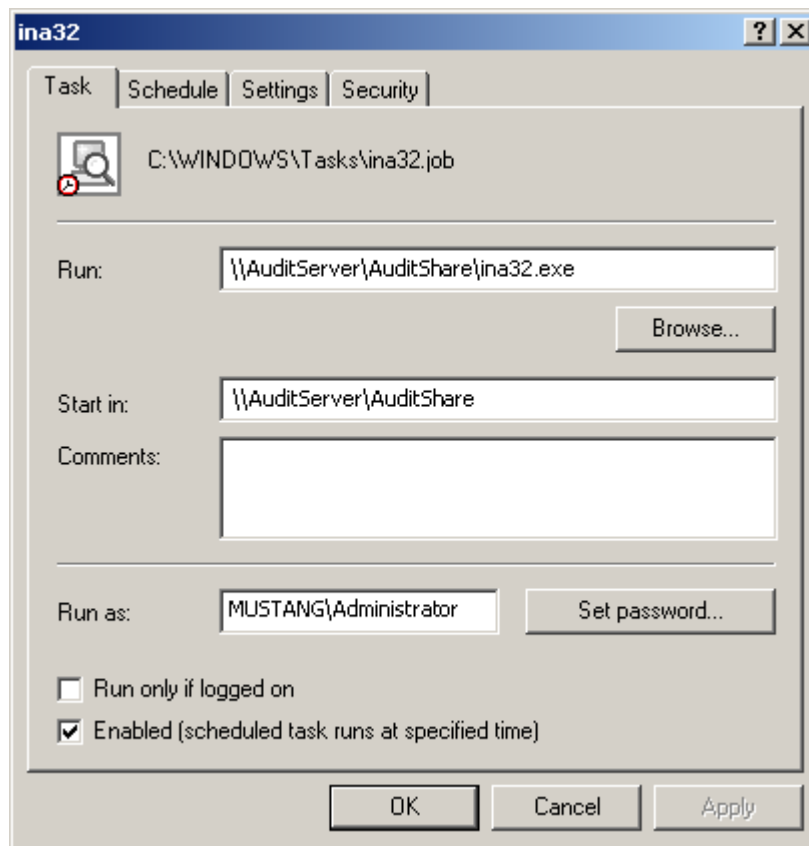


Figure 41: Inventory Analyzer as a Scheduled Task

The new task appears on the list of Scheduled Tasks. If you want to modify any of the task's properties, or to change the advanced configuration, double-click the task to open its **Properties** dialog.

Automating the Scriptable Audit on Linux and Mac Machines

For networked computers running Linux or Mac OS, you can use the cron daemon to automate the inventory analyzers for Linux (lina) or for Mac (ina_mac) from the shared folder where the inventory analyzer has been deployed.

Cron is a time-based scheduling service in Unix-like computer operating systems. Each crontab file entry contains six fields separated by spaces or tabs in the following form:

```
minute hour day_of_month month day_of_week command_to_be_executed
```

Users can have their own individual crontab files and often there is a system-wide crontab file (usually in /etc or a sub-directory of /etc) which is also used but can be modified only by the system administrator.

For details on scheduling tasks using cron, see the following manpages:

- crontab(1) at <https://www.manpagez.com/man/1/crontab/>
- crontab(5) at <https://www.manpagez.com/man/5/crontab/>

For the list of switches you can use with `lina` and `ina_mac`, see "[Linux Inventory Analyzer Command-Line options](#)" on page 134 or "[Mac Inventory Analyzer Command-Line options](#)" on page 136.

Next Steps

Now that you have deployed the Inventory Analyzer to a network share and automated the audit to produce audit snapshots on a regular basis, you can customize the Scriptable Audit. Some properties of the Scriptable Audit group have been set to their default values when you created the group. You can fine-tune group's settings in the **Properties** dialog box. To access the **Properties** dialog box, right-click the group in the Sidebar and select **Properties** from the pop-up menu.

Audit via E-mail

The Audit via E-mail is an agent-based method of WAN audit using standalone audit agents. This audit method is similar to the Scriptable Audit method, however the network share where the Inventory Analyzer package is deployed, typically has no direct connection from the local network.

This method involves two steps: deploying the Inventory Analyzer Package to the target network and automating the Inventory Analyzer using domain logon scripts or scheduled tasks. The audit snapshots are delivered to host machine via e-mail. When using this audit method, there is no direct link between the host machine and the deployed audit agents; this is why any configuration changes or updated versions of the audit agents must be manually re-deployed.



Any configuration changes or updated version of the Inventory Analyzer need to be manually re-deployed.

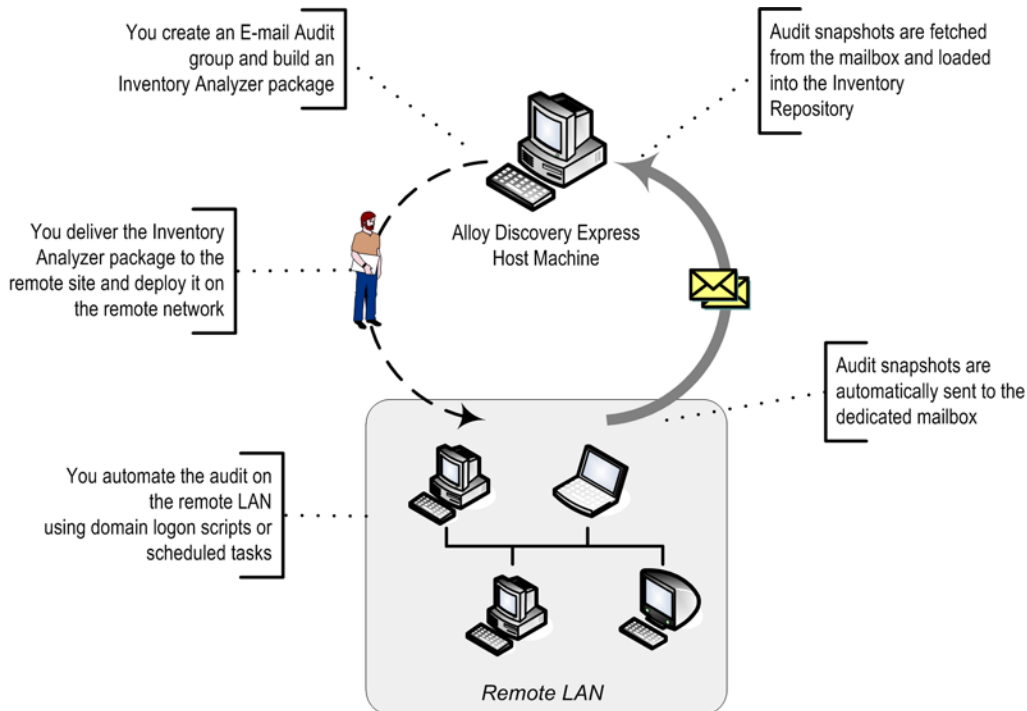


Figure 42: Auditing Computers via E-mail

To configure the Audit via E-mail, follow the instructions below:

1. Create an E-mail Audit Group. See ["Creating E-mail Audit Groups" on page 80](#).
2. Prepare the Inventory Analyzer package for the E-mail Audit Group. See ["Building Inventory Analyzer packages for the Audit via E-mail" on page 84](#).
3. Deploy the package on the target network and run the audit. See ["Running the Audit via E-mail on the Target Network" on page 86](#).
4. Load the audit results. See ["Checking E-mail Audit Groups for New Snapshots" on page 87](#).

Creating E-mail Audit Groups



Before you begin, make sure to complete setting the Audit Configuration, as the Inventory Analyzer package you will create in the following steps would need to be rebuilt after making any Audit Configuration changes. See ["Configuring the Audit" on page 24](#). Also, make sure to designate a mailbox on the Mail Server for handling incoming audit snapshots.

To create an E-mail Audit Group:

1. Select **File > New Group** from the main menu. The New Group Wizard starts.
2. On the **Welcome** page, click **Next** to proceed. The **Group Type** page opens.
3. Click **Audit group** and click **Next**. The **Audit Groups** page opens.

4. Click **Automated audit via e-mail**, then click **Next**. The **E-mail Address** page opens.
5. Specify the email address where the Inventory Analyzer will be delivering audit snapshots in the form of email messages. Optionally, specify the "From" address that will appear on these e-mail messages. Click **Next**. The **Incoming Mail Server** page opens.
6. Configure the settings for the mail server which will be receiving incoming audit results.
 - 1) Enter the name and port number of your mail server.
 - 2) If the mail server requires authentication, select the **Server Requires Authentication** check box and enter the user name and password. If the server requires SPA, select the **Require Secure Password Authentication (SPA)** check box.
 - 3) If you want to use secure connection, select one of the following options under **Secure Connection**:
 - **TLS, if available** – This establishes a secure connection using the Transport Layer Security (TLS) protocol. If TLS protocol is not available, establishes non-secure connection.
 - **TLS** – This establishes a secure connection using the Transport Layer Security (TLS) protocol.
 - **SSL** – This establishes a secure connection using the Secure Sockets Layer (SSL) protocol.
 - 4) If you want to terminate the connection established via an TLS/SSL-encrypted channel when a certificate validation error occurs, select the **Reject invalid certificates** check box.
 - 5) Optionally: click **Test Connection** to make sure that the settings are correct. Click **Next**. The **Testing Mail Server Settings** page opens.

New Group Wizard

Incoming Mail Server

Specify the mail server which will handle incoming messages containing audit snapshots.

Server Type: POP3 IMAP4

Server Name: Port:

Server Logon Information:

User Name:

Password:

Require Secure Password Authentication (SPA)

Secure Connection

Never TLS, if available TLS SSL

Reject invalid certificates

< Back Next > Cancel

Figure 43: Configuring Incoming Mail Server Settings

7. Make sure that the settings are tested successfully, then click **Next**. The **Outgoing Mail Server** page opens.
8. Optional: Configure the settings for the outgoing SMTP server, which will be used for e-mailing out audit snapshots from audited computers.



You will be able to configure the settings for the outgoing SMTP server when building the Inventory Analyzer package.

- 1) Enter the name and port number for the SMTP server. The default port number is 25 for insecure connection. For secure connection via SSL, the default port number is 465.
- 2) If the outgoing mail server requires authentication, select the **Server Requires Authentication** check box and enter the username and password. If the server requires SPA, select the **Require Secure Password Authentication (SPA)** check box.
- 3) If you want to use secure connection, select one of the following options under **Secure Connection**:
 - **TLS, if available** – This establishes a secure connection using the Transport Layer Security (TLS) protocol. If TLS protocol is not available, establishes non-secure connection.
 - **TLS** – This establishes a secure connection using the Transport Layer Security (TLS) protocol.

- **SSL** – This establishes a secure connection using the Secure Sockets Layer (SSL) protocol.
- 4) If you want to terminate the connection established via an TLS/SSL-encrypted channel when a certificate validation error occurs, select the **Reject invalid certificates** check box.
 - 5) Click **Test Connection** to make sure that *Alloy Discovery Express* is able to connect to the server with these settings, and then click **Next**. The **Group Name and Description** page opens.

The screenshot shows a 'New Group Wizard' window with the 'Outgoing Mail Server' step. The text reads: 'Specify the outgoing (SMTP) server. Audit agents will use this server for sending audit snapshots.' The 'Server Name' field contains 'mail.zeus.com' and the 'Port' field contains '465'. The 'Server requires authentication' checkbox is checked. The 'User Name' field contains 'audit' and the 'Password' field is masked with dots. The 'Require Secure Password Authentication (SPA)' checkbox is unchecked. The 'Secure Connection' section has three radio buttons: 'Never', 'TLS, if available', and 'SSL', with 'SSL' selected. The 'Reject invalid certificates' checkbox is unchecked. A 'Test Connection' button is located below the 'Secure Connection' section. At the bottom of the dialog are '< Back', 'Next >', and 'Cancel' buttons.

Figure 44: Configuring Outgoing Mail Server Settings (New Group Wizard)

9. Review the group name and modify it, if necessary. Optionally enter a description for the group. Click **Next**. The **Ready to Create New Group** page opens.
10. Review your settings. When you are ready to create the group, click **Next**. If you want to change any settings, click **Back**. The wizard will display the **Group Created** page once it has finished.
11. Some properties of the new E-mail Audit Group acquire default values:
 - If you want to use the default properties and immediately create an Inventory Analyzer package for this group, keep the **Build Inventory Analyzer package(s) after finish** check box selected. Then click **Finish** to complete the wizard.
 - If you want to fine-tune some properties before creating an Inventory Analyzer package, clear the check box, then click **Finish** to complete the wizard.

To review and modify the properties of any group, right-click the group in the Sidebar and select **Properties** from the pop-up menu. For instructions, see the *Configuring E-mail Audit Groups* section in the embedded Help system.

Building Inventory Analyzer packages for the Audit via E-mail

To create an Inventory Analyzer package for the Audit via E-mail, run the Portable Audit Wizard as follows:

- If you kept the **Build Inventory Analyzer package(s) after finish** check box selected on the last page of the New Group Wizard, the Portable Audit Wizard starts automatically after the E-mail Audit Group is created.
- To start the Portable Audit Wizard manually, right-click the created E-mail Audit Group in the Sidebar, click **Properties**, and then click **Create** under **Inventory Analyzer packages**. The Portable Audit Wizard opens.

To create an Inventory Analyzer package:

1. On the **Welcome** page of the Portable Audit Wizard, click **Next**. The **Operating System** page opens.
2. Select the check boxes for each operating system type that you want to audit (the wizard will create separate packages for each of the selected OSes). Click **Next**.
 - If you selected Windows OS, the **Audit Mode** page opens. Proceed to [Step 3](#).
 - If you selected Linux and/or Mac OS, the **E-mail Address** page opens. Proceed to [Step 4](#).
3. Select one of the following audit modes:
 - If you want the Inventory Analyzer to prompt the user before the audit, click **Interactive Mode**.
 - If you want the to run the audit silently without any interaction with the user, click **Silent Mode**.
 - If you want the Inventory Analyzer to prompt the user only at the first audit, then run all the subsequent audits silently, click **Interactive Once**.



In the Silent Mode, the User Input Options configured in Audit Configuration will be ignored (see ["Configuring Available Controls" on page 42](#) and ["Configuring Custom Input Fields" on page 44](#)).

Click **Next**. The **E-mail Address** page opens.

4. Enter the e-mail address for sending audit snapshots to. Optionally, enter the "From" e-mail address to appear on the sent messages. Click **Next**.
 - If you selected Windows OS in Step 2, the **Outgoing Server (SMTP) Settings** page opens. Proceed to [Step 5](#).
 - If you did not selected Windows OS in Step 2, the **Destination Folder** page opens. Proceed to [Step 6](#).

- Configure the outgoing server (SMTP) settings, which the Inventory Analyzer will be using for sending out audit snapshots (the page may be populated with the values you entered when creating the E-mail Audit Group):

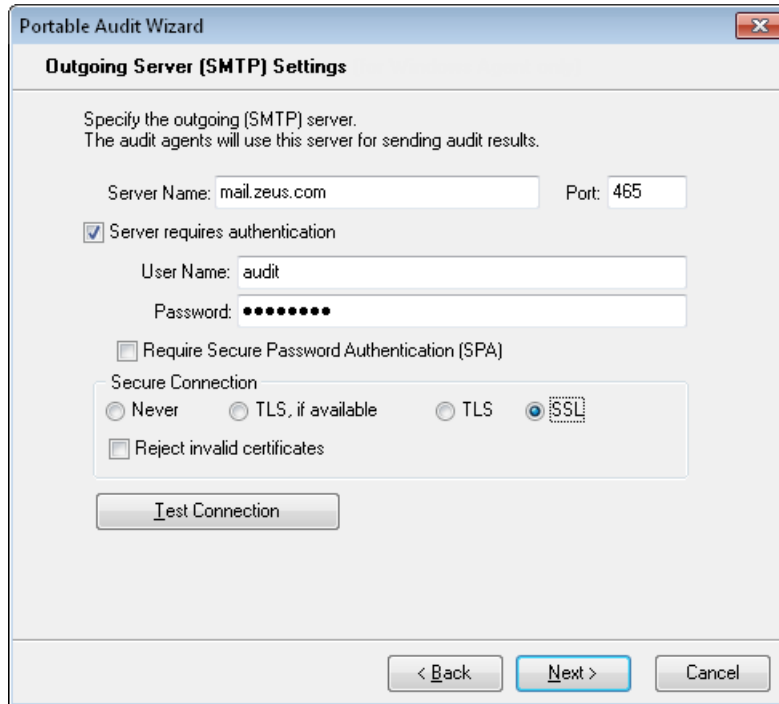


Figure 45: Configuring Outgoing Mail Server Settings (Portable Audit Wizard)

- Enter the name and port number for the SMTP mail server. The default port number is 25 for insecure connection. For secure connection via SSL, the default port number is 465.
- If the outgoing mail server requires authentication, select the **Server Requires Authentication** check box and enter the user name and password. If the server requires SPA, select the **Require Secure Password Authentication (SPA)** check box.
- If you want to use secure connection, select one of the following options under **Secure Connection**:
 - TLS, if available** – This establishes a secure connection using the Transport Layer Security (TLS) protocol. If TLS protocol is not available, establishes non-secure connection.
 - TLS** – This establishes a secure connection using the Transport Layer Security (TLS) protocol.
 - SSL** – This establishes a secure connection using the Secure Sockets Layer (SSL) protocol.
- If you want to terminate the connection established via an TLS/SSL-encrypted channel when a certificate validation error occurs, select the **Reject invalid certificates** check box.
- Optionally: click **Test Connection** to make sure that the settings are correct. Click **Next**. The **Destination Folder** page opens.
- Click **Next**. The **Destination Folder** page opens.

6. Specify the output folder for the prepared Inventory Analyzer package. If you want the package to be compressed, select the **Compress the package** check box. This can be useful if you intend to deploy the package via e-mail or via File Transfer Protocol (FTP) because compressing ensures the integrity of file attributes during the transfer.

Click **Next**. The **Finish** page opens.

7. Review your settings. If you want to change any settings, click **Back**. When you are ready, click **Finish** to complete the wizard.

Alloy Discovery Express creates the following folders and files in the destination folder:

- `AuditData` — the folder where the Inventory Analyzer saves audit snapshots before sending them to the *Alloy Discovery Express* host machine.
- `Log` — the folder in which the Inventory Analyzer will store logged events (the folder is created for the Windows pack only).
- *The Windows pack — for auditing Windows computers:*
 - `ina32.cfg` — the configuration file for the Windows Inventory Analyzer.
 - `ina32.exe` — the Windows Inventory Analyzer executable file.
- *The Linux pack — for auditing Linux computers:*
 - `lina` — the script that automatically detects the kernel version and launches the appropriate Linux Inventory Analyzer executable.
 - `lina24` — the Linux Inventory Analyzer executable for Linux kernel version 2.4 and earlier.
 - `lina26` — the Linux Inventory Analyzer executable for Linux kernel version 2.6 and later.
 - `lina.ini` — the configuration file for the Linux Inventory Analyzer.
 - `README-lina.txt` — the Readme file for the Linux Inventory Analyzer.
- *The Mac pack — for auditing Mac OS computers:*
 - `ina_mac` — the Mac Inventory Analyzer executable.
 - `ina_mac.ini` — the configuration file for the Mac Inventory Analyzer.
 - `README-ina_mac.txt` — the Readme file for the Mac Inventory Analyzer.

Running the Audit via E-mail on the Target Network

After building the Inventory Analyzer package, deploy it to the target network and run the audit as follows:

- If you want to audit multiple computers on a remote network:
 1. Deliver the Inventory Analyzer Package to the remote site.
 - 2) Deploy the Inventory Analyzer Package. You would need to create a shared folder and set its permissions manually. For instructions on creating shared folders, see your Microsoft Windows documentation. For information on setting the minimally necessary permissions to perform the audit, see [“Minimally Necessary Permissions” on page 166](#).
 - 3) Make sure the Internet connectivity is available to allow for sending e-mail.

- 4) Automate the audit using the domain logon script or a scheduled task. For instructions, see ["Automating the Scriptable Audit" on page 72](#).
- If you want to audit a standalone computer:
 1. Deliver the Inventory Analyzer package to the client machine (for example, using a USB flash drive).
 - 2) Make sure the Internet connectivity is available to allow for sending e-mail.
 - 3) Run the Inventory Analyzer.

The Inventory Analyzer will send audit snapshots as e-mail messages to the specified mailbox.

Checking E-mail Audit Groups for New Snapshots

To load to the Inventory Repository audit snapshots collected using the Audit via E-mail method, you should check the E-mail Audit Group as follows:

- To make *Alloy Discovery Express* check an E-mail Audit Group for new snapshots each time the application starts, right-click the group in the Sidebar and select **Properties** from the pop-up menu. Click the **Options** tab, select the **Look for new audit snapshots** check box, and click **OK**.
- To check an E-mail Audit Group for new snapshots when the application is already running, right-click the group in the Sidebar and choose **Check for New Audit Snapshots** from the pop-up menu.

E-mail messages are handled in accordance with the options you specified for the E-mail Audit Group (you can view these options on the **Options** tab of the group's **Properties** dialog box). The following statuses describe various processing stages for each individual email message in the mailbox:

- **Succeeded** – The audit snapshot has successfully imported from the e-mail message into the Inventory Repository.
- **Failed** – The e-mail message has been identified as containing an audit snapshot, however the snapshot could not be imported.

- **Skipped** – No audit snapshot has been found in the e-mail message.

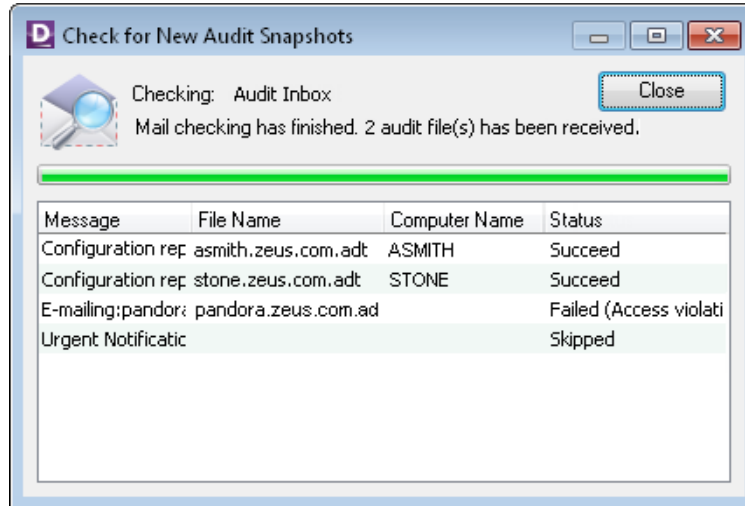


Figure 46: Processing E-mail Messages

After you close the **Check for New Audit Snapshots** dialog box, click **Yes** when prompted to reload data from the Inventory Repository.



If you change the Audit Configuration after deploying Inventory Analyzer packages, or install newer versions of the audit agents, you'll need to re-create the Inventory Analyzer packages and re-deploy them.

For details on Audit Configuration, see ["Configuring the Audit" on page 24](#).

Next Steps

Now that you have created the E-mail Audit Group, built the Inventory Analyzer package, and deployed the Inventory Analyzer on the remote site, you can customize the properties of the E-mail Audit Group. Some properties of the group were set to their default values when you created the group. You can fine-tune group's settings in the **Properties** dialog box.

To access the **Properties** dialog box, right-click the group in the Sidebar and select **Properties** from the pop-up menu. There, on the **Options** tab, you can modify the settings for scanning the mailbox for audit snapshots and handling e-mail. For instructions, see the *Configuring E-mail Audit Groups* section in the embedded Help system.



If you modify other properties of E-mail Audit Groups, you will need to re-create the Inventory Analyzer package and re-deploy it to reflect your changes.

Portable Audit

The Portable Audit is an agent-based method of auditing non-networked computers or isolated network segments. Typically, the audit agent is deployed to a flash drive, which is used to audit individual computers. Audit snapshots are stored on the same flash drive and then manually transported into the main repository.

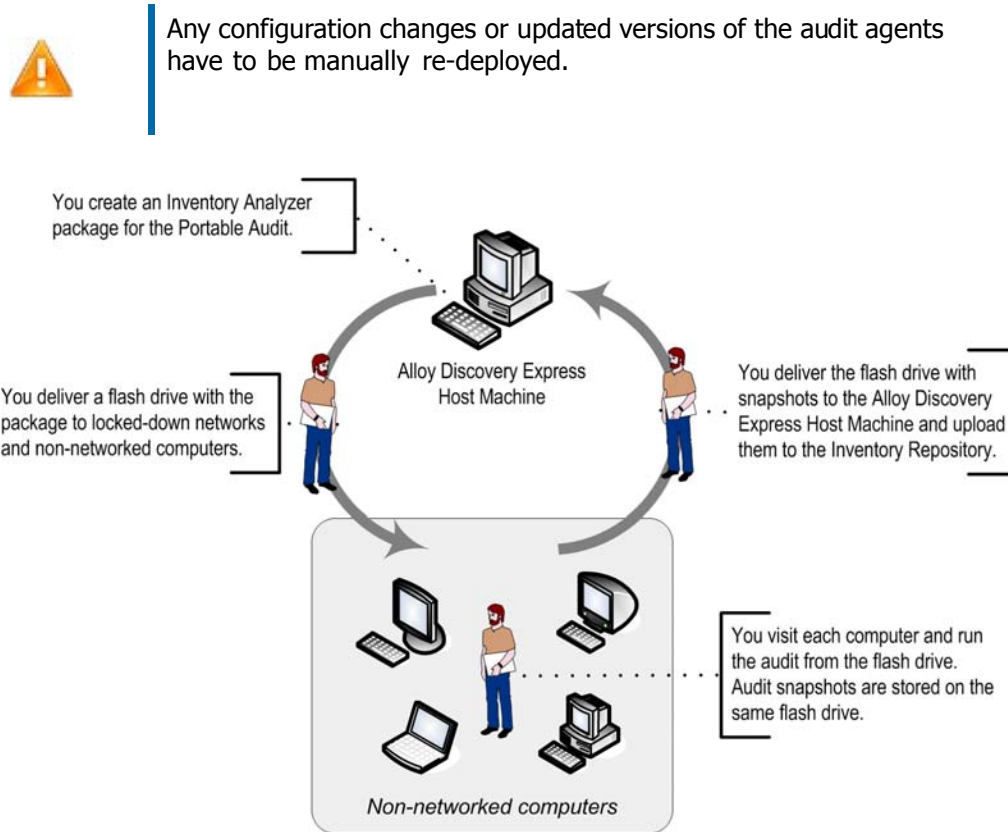


Figure 47: Auditing Non-Networked Computers

See ["Configuring the Audit" on page 24](#) for information on configuring the audit.

To perform the Portable Audit, follow the instructions below:

1. Create the Inventory Analyzer Package. See ["Building Inventory Analyzer Packages for the Portable Audit" on page 90](#).
2. Run the audit. See ["Running the Portable Audit on Client Machines" on page 92](#).
3. Transport the audit snapshots to the main Inventory Repository. See ["Transporting Audit Snapshots to the Inventory Repository" on page 92](#).

Building Inventory Analyzer Packages for the Portable Audit

To create an Inventory Analyzer package for the Portable Audit, complete the Portable Audit Wizard as follows:

1. Choose **Audit > Create Portable Audit Package** from the main menu. The Portable Audit Wizard starts.
2. On the **Welcome** page, click **Next**. The **Operating System** page opens.
3. Select the types of operating systems that you want to audit. Click **Next**.
 - If you selected Windows OS, the **Audit Mode** page opens. Proceed to [Step 4](#).
 - If you didn't select Windows OS, the **Audit Snapshot Viewer** page opens. Proceed to [Step 5](#).
4. Select one of the following audit modes:
 - If you want the Inventory Analyzer to prompt the user before the audit, click **Interactive Mode**.
 - If you want to run the audit silently without any interaction with the user, click **Silent Mode**.
 - If you want the Inventory Analyzer to prompt the user only at the first audit, then run all subsequent audits silently, click **Interactive Once**.



In the Silent Mode, the User Input Options configured in Audit Configuration will be ignored (see ["Configuring Available Controls" on page 42](#) and ["Configuring Custom Input Fields" on page 44](#)).

Click **Next**. The **Audit Snapshot Viewer** page opens.

5. If you are planning to view audit snapshots outside of *Alloy Discovery Express*, keep the **Include the Audit Snapshot Viewer** check box selected. This will add the Audit Snapshot Viewer to your portable Inventory Analyzer package.

Click **Next**. The **Destination Folder** page opens.

6. Specify the output folder for the Inventory Analyzer package. If you want the package to be compressed, select the **Compress the package** check box. This can be useful if you intend to deploy the package via e-mail or via File Transfer Protocol (FTP) because compressing ensures the integrity of file attributes during the transfer.

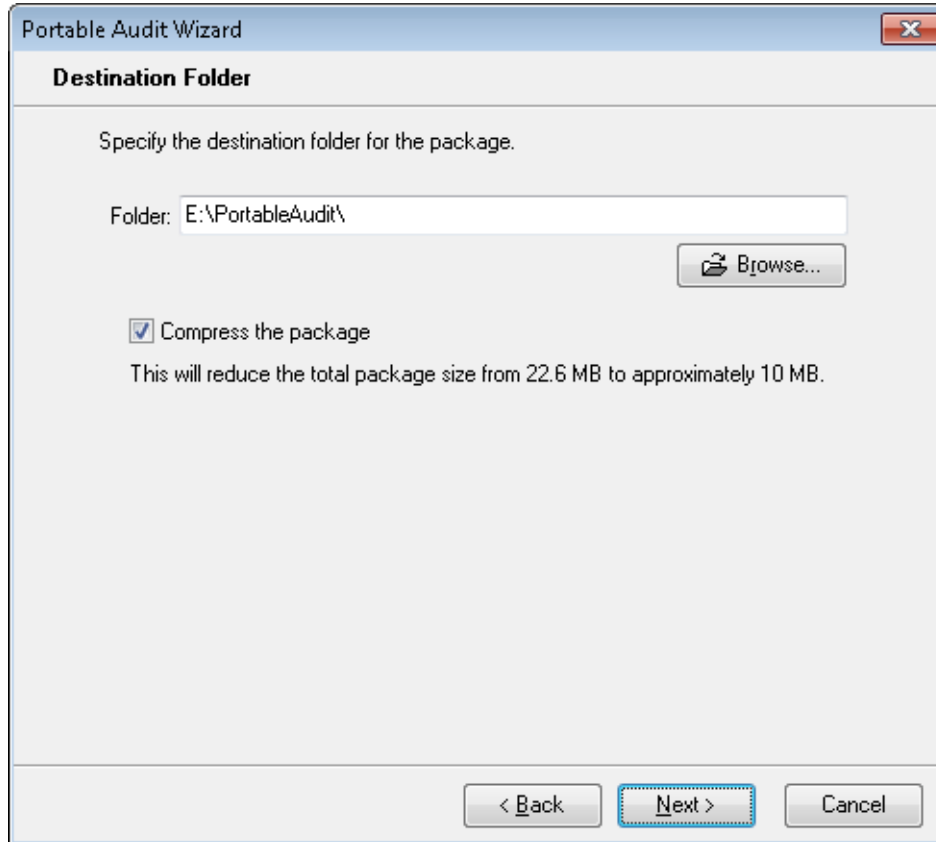


Figure 48: Specifying Destination Folder

Click **Next**. The **Finish** page opens.

7. Review your settings. If you want to change any settings, click **Back**. When you are ready to proceed, click **Finish**.

Alloy Discovery Express creates the following folders and files in the destination folder:

- `AuditData` — the folder where the Inventory Analyzer saves audit snapshots before loading them into the main repository.
- `Log` — the folder in which the Inventory Analyzer will store logged events (the folder is created for the Windows pack only).
- *The Windows pack — for auditing Windows computers:*
 - `ina32.cfg` — the configuration file for the Windows Inventory Analyzer.
 - `ina32.exe` — the Windows Inventory Analyzer executable file.
- *The Linux pack — for auditing Linux computers:*
 - `lina` — the script that automatically detects the kernel version and launches the appropriate Linux Inventory Analyzer executable.
 - `lina24` — the Linux Inventory Analyzer executable for Linux kernel version 2.4 and earlier.
 - `lina26` — the Linux Inventory Analyzer executable for Linux kernel version 2.6 and later.

- `lina.ini` — the configuration file for the Linux Inventory Analyzer.
- `README-lina.txt` — the Readme file for the Linux Inventory Analyzer.
- *The Mac pack — for auditing Mac OS computers:*
 - `ina_mac` — the Mac Inventory Analyzer executable.
 - `ina_mac.ini` — the configuration file for the Mac Inventory Analyzer.
 - `README-ina_mac.txt` — the Readme file for the Mac Inventory Analyzer.
- *The Audit Snapshot Viewer pack — for viewing audit snapshots from outside Alloy Discovery Express:*
 - `AdtViewer.exe` — the Audit Snapshot Viewer executable file
 - `ADTViewerEng.dll` — the Audit Snapshot Viewer Engine for displaying audit snapshots.
 - `pcidevs.txt` — the dictionary file for identifying PCI device manufacturers.



If you change the Audit Configuration or install a newer version of the Audit Tools module, you need to re-create the Inventory Analyzer package and re-deploy it.

For details on Audit Configuration, see ["Configuring the Audit" on page 24](#).

Running the Portable Audit on Client Machines

After building the Inventory Analyzer package, run the Inventory Analyzer from the flash drive on each individual client machine.

Transporting Audit Snapshots to the Inventory Repository

After running the audit and collecting audit snapshots, transport the flash drive with audit results to the computer that hosts *Alloy Discovery Express*.

Load the audit snapshot files into the Inventory Repository as follows:

1. Choose **Audit > Load Audit Files from Media** from the main menu.
2. Browse to and select the audit snapshot files to load. Click **OK**. *Alloy Discovery Express* loads selected snapshots into the Inventory Repository.

The audited computers appear in the pre-defined **All Computers and Devices** group.

Next Steps

Now that you have created your Inventory Analyzer package, ran the Portable Audit, and imported the audit snapshots into the Inventory Repository on the host machine, you may want to create a Computer Group to view the results. For instructions, see ["Working with Static and Dynamic Computer Groups" on page 115](#).

Auditing Linux and Mac Computers

With *Alloy Discovery Express*, you can audit computers running Linux and Mac OS X. Depending on your environment, the following audit methods apply:

- If the Linux and Mac machines are part of your LAN, you may use either the On-Demand Audit method (See [“On-Demand Audit” on page 51](#)), or the Scriptable Audit method (see [“Scriptable Audit” on page 70](#)).
- If the Linux and Mac machines are part of a remote site, use the Audit via E-mail method. See [“Audit via E-mail” on page 79](#).
- If the Linux and Mac machines are on an isolated network or standalone, use the Portable Audit. See [“Portable Audit” on page 89](#).

For details about the configuration files and command-line parameters you can use with `lina` and `ina_mac`, see [“Linux Inventory Analyzer Command-Line options” on page 134](#) or [“Mac Inventory Analyzer Command-Line options” on page 136](#).



Make certain that the computers you are going to audit meet Client Machines requirements (see [“Audit Clients” on page 9](#)).

Specifying Connection Parameters for VMware ESX / ESXi Hypervisors

Alloy Discovery Express establishes connection to VMware ESX/ESXi hypervisors with the WS-Management service over HTTP or HTTPS protocols. Use the **ESX/ESXi Options** tab of the computer’s audit properties dialog box to view or specify connection parameters for VMware ESX/ESXi hypervisors.



If you plan to audit VMware ESX and VMware ESXi hypervisors using WS-Management, the computer hosting your Alloy Discovery Express must have Microsoft .NET Framework 4.6.1 or later installed.

For details, see [“Microsoft .NET Framework 4.6.1” on page 12](#).

For computers running VMware ESX (but not ESXi) hypervisor with the SSH protocol enabled, *Alloy Discovery Express* uses the options configured for Linux machines and audit such hypervisor as a Linux computer.



The audit of the VMware ESXi hypervisor can be performed only via WS-Management protocol.

To specify connection parameters for VMware ESX/ESXi hypervisors, follow these steps:

- 1) In the Audit Group, locate the Computer for which you want to specify connection parameters.

- 2) Right-click its record and choose **Properties** from the pop-up menu. The computer's audit properties dialog box opens.
- 3) Switch to the **ESX/ESXi Options** tab. If this tab is not displayed, ensure that **VMware ESX/VMware ESXi** is selected as the Hypervisor within the **General** tab of the computer's audit properties dialog box.
- 4) On the **ESX/ESXi Options** tab, under **Transport**, specify the parameters of the transport protocol for the WS-Management connection:

Select one of the following transport protocols:

- **HTTP** — establishes non-secure connection using the Hypertext Transfer Protocol (HTTP) protocol. The default port number is 80. However, if the server on your client computers listens on a non-standard TCP port, you can specify another port number.
- **HTTPS** — establishes secure connection using the Hypertext Transfer Protocol Secure (HTTPS) protocol. The default port number is 443. However, if the server on your client computers listens on a non-standard TCP port, you can specify another port number.
- For **HTTPS** protocol: If you want to prevent communication with the server via an HTTPS-encrypted channel when a certificate validation error occurs, select the **Reject invalid certificates** check box.



To access VMware ESX or VMware ESXi hypervisors *Alloy Discovery Express* uses Linux credentials as follows. If the computer has individual audit credentials specified, *Alloy Discovery Express* uses these credentials. Otherwise, it applies Linux credentials from the computer's Audit Group.

- 5) Click **OK**.

CHAPTER 7. Analyzing Audit Snapshots

This chapter explains how to view and analyze audit snapshots.

Viewing Software and Hardware Inventory

Analyzing Inventory Data using Groups

Alloy Discovery Express collects in-depth hardware and software inventory information from computers and network devices. This includes information about hardware configurations, installed software, files on the hard drive, event log records, and more.



File information is collected only when the File Scan is enabled. For details, see ["Configuring File Scan Options" on page 34](#).

Once your computers and network devices have been audited, their audit snapshots have been collected and uploaded into the Inventory Repository, you can browse and analyze their inventory data.

When you select a particular audit or computer group, the contents of that group populates the data grids. If you apply filters to the Computer List (i.e., narrow down the visible contents of the current group), the information associated with these hidden computers will also be hidden from other data grids.

The preview pane (located below the Computer List or Network Devices) provides a digest of information about the selected network node. The preview pane also enables you to access the following commands:

- Initiate an on-demand audit by selecting **Audit Now**.
- View the audit snapshot details for the selected node via **Show Details**. For details, see ["Viewing Audit Snapshots" on page 103](#) or ["Viewing Network Device Details" on page 108](#).
- Launch various external commands. For details, see ["External Tools" on page 125](#).

Audit data is organized on the following tabs:

- **Computer List** — lists computers in the current group and displays their key parameters, such as CPU type and speed, memory size, operating system details, network card and address, etc.



You can also configure the **Computer List** tab to show the user-defined fields. For details on configuring and populating user-defined fields, see ["User-Defined Fields" on page 129](#).

- **Network Devices** — lists network devices of the selected group.
- **Software List** — displays software inventory data for the current group.

- **File Find** — allows you to search through file scan data.



To enable the File Find option, you must configure the File Scan feature. The results will be searchable only after auditing at least one Computer with the Detailed Scan option applied for at least one file mask. For details, see ["Configuring File Scan Options" on page 34](#).

- **File Statistics** — shows file statistics collected during the file scan.



To enable Alloy Discovery Express collect file statistics, you must configure File Scan. Statistics results appear only after auditing at least one Computer with the Summary Scan option enabled for at least one file mask. For details, see ["Configuring File Scan Options" on page 34](#).

- **Shared Folders** — lists all shared folders found on the computers in the current group.
- **Devices** — displays devices installed on the computers in the current group.
- **Event Log** — displays event log entries collected from computers in the current group. For detailed information on configuring the audit to capture event log entries, see ["Configuring Event Log Options" on page 31](#).

For details on the contents of the tabs, see the *Viewing Hardware and Software Inventory* section in the embedded Help system.

You can customize the grids as follows:

- Organize the display of columns — You can add more columns to a grid or remove unwanted columns from a grid, change the column order, resize the columns, etc.
- Filter records — You can use the Quick Filter to filter records, or configure the Advanced Filter to retrieve from the repository only the data that meets the filtering criteria.
- Group records — You can group records using various methods.
- Display statistics — You can configure *Alloy Discovery Express* to show statistics for the grid data.
- Sort records — You can sort grid records by any column, or by a series of columns.

After you have customized the visual aspects of a grid, you can save your settings for further use as a "view". You can also export grid records for external analysis, charting, and reporting.

For details on working with the grids, see the *Using Grids* chapter in the embedded Help system.

ZEUS

Computer List | Network Devices | Software List | File Find | File Statistics | Shared Folders | Devices | Event Log

Open | View: List

Computer Name	Audit Date	Model	CPU	CPU Speed	RAM, M	HDD, MB	OS	IP Address
							Windows 7	
CEN TAUR	8/27/2018 1:36:0	P55-US3L	Intel(R) Core	3200	3576	476,838	Windows 7 Professio	172
DELL	8/27/2018 1:36:1	VMware V	Intel(R) Core	3800	2048	97,272	Windows 7 Professio	172
MACHINDO	8/27/2018 1:35:4		Intel(R) Core	3600	16275	1,297,163	Windows 7 Professio	172

(OS LIKE Windows 7%) Customize...

Intel(R) Core(TM) i3 CPU 550 @ 3.20GHz (3200 MHz)
 Memory: 3576 Mb, Storage: 465.66 GB
 Windows 7 Professional,

Identification

Network Name: CEN TAUR
Domain/Workgroup: ZEUS
Asset Tag: AT00069

Actions

- Audit Now
- Show Details

External Tools

- Telnet
- Ping
- VNC
- Remote Desktop

Repository: C:\ProgramData\Alloy Software\Alloy Dis

Figure 49: Computer List tab Being Filtered by Operating System



If you apply a filter to the contents of the Computer List tab, the contents of all the subordinate computer-related tabs will be narrowed down to reflect the effect of the filter.

Viewing File Scan Results

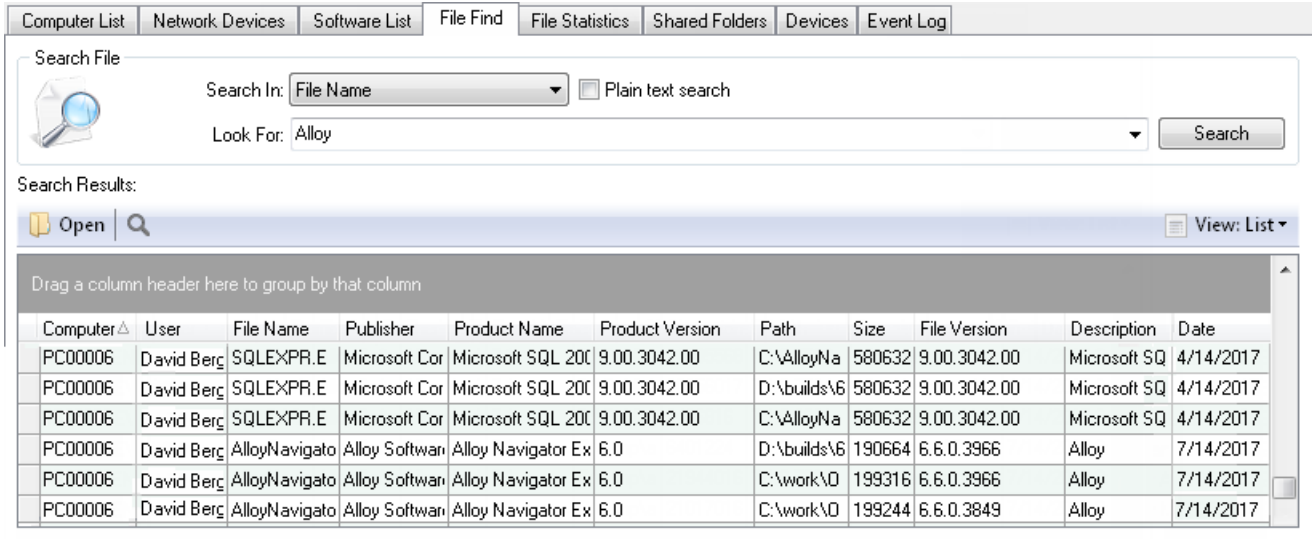
Alloy Discovery Express provides the File Scan feature to analyze files on computers during the audit, search for specific files, or collect volume statistic on specified file types. You can view the file scan results in the **File Statistics** and **File Find** tab.



The file scan feature is applicable only for Windows computers; file scan options are ignored when auditing Linux and Mac computers. For details on enabling and configuring the file scan feature, see ["Configuring File Scan Options" on page 34](#).

Searching For Files

The **File Find** tab allows you to search for a particular file through the results of the Detailed File Scan.



Search File

Search In: Plain text search

Look For:

Search Results:

Drag a column header here to group by that column

Computer	User	File Name	Publisher	Product Name	Product Version	Path	Size	File Version	Description	Date
PC00006	David Berg	SQLXPR.E	Microsoft Cor	Microsoft SQL 200	9.00.3042.00	C:\AlloyNa	580632	9.00.3042.00	Microsoft SQ	4/14/2017
PC00006	David Berg	SQLXPR.E	Microsoft Cor	Microsoft SQL 200	9.00.3042.00	D:\builds\6	580632	9.00.3042.00	Microsoft SQ	4/14/2017
PC00006	David Berg	SQLXPR.E	Microsoft Cor	Microsoft SQL 200	9.00.3042.00	C:\AlloyNa	580632	9.00.3042.00	Microsoft SQ	4/14/2017
PC00006	David Berg	AlloyNavigato	Alloy Softwar	Alloy Navigator Ex	6.0	D:\builds\6	190664	6.6.0.3966	Alloy	7/14/2017
PC00006	David Berg	AlloyNavigato	Alloy Softwar	Alloy Navigator Ex	6.0	C:\work\0	199316	6.6.0.3966	Alloy	7/14/2017
PC00006	David Berg	AlloyNavigato	Alloy Softwar	Alloy Navigator Ex	6.0	C:\work\0	199244	6.6.0.3849	Alloy	7/14/2017

Figure 50: Searching for files within the results of the Detailed File Scan

By default, each entry in the results list contains the following information:

- **Computer Name** — the name of the computer where the file was detected
- **User** — the user name on whose computer the file was detected
- **File Name** — the name of the file
- **Publisher** — the name of the organization that developed or created the file
- **Product Name** — the name of the product with which the file is distributed
- **Product Version** — the version number of the product with which the file is distributed
- **Path** — the full path to the file on the hard drive
- **Size** — the size of the file in bytes
- **File Version** — the version number of the file
- **Description** — the description of the file
- **Date** — the date and time when the file was last modified



You can search for files only if you have performed at least one audit with the Detailed Scan enabled for at least one file mask. Otherwise, the results list of your search will be empty.

To search for a particular file in the results of the Detailed File Scan, do the following:

1. In the Sidebar, select the Audit Group, where you want to search for a file.
2. On the **File Find** tab, define where you want to search for the entered text by selecting a field from the **Search In** drop-down list.



As with the standard file masks, an asterisk (*) matches 0 or more occurrences of any symbol, and the question mark (?) matches any single symbol. If you don't want to use wildcards, you can select the **Plain text search** check box. Pattern (or mask) search always starts at the beginning of the search field and attempts to match the entire value; plain-text search looks for any occurrence of the text in the search field.

3. Specify a search query within the **Look For** field. The drop-down arrow at the far right of the **Look For** field shows a list of text strings that you recently have searched for. You can choose an item from the list to search for it again.



The file search is case-insensitive.

4. Click **Search**. The results of the search operation appear in the grid.

Viewing File Statistics

The **File Statistics** tab displays the volume statistics for every file type (or file mask) requested through the Summary File Scan.

Computer Name	User	File Mask	Count	Size (MB)
PC00003	Armando Suggs	*.JPG	44	6.85
PC00003	Armando Suggs	*.MP3	3	19.79
PC00003	Armando Suggs	*.PNG	06	24.32
PC00006	David Berger	*.AVI	1	1791.03
PC00006	David Berger	*.BMP	11	40.73
PC00006	David Bercoer	*.DLL	20	55.98

Figure 51: Viewing file statistics gathered by the Summary File Scan

To see where the files of a particular type are located on the hard drive, double-click the corresponding record in the grid. A separate dialog box opens with the following information for each folder where matching files were found:

- **Count** — the total number of files detected in the folder
- **Path** — the folder's path

- **Size** — the total size of files of this type in the folder

Viewing Individual Audit Snapshots

Previewing Computer Data

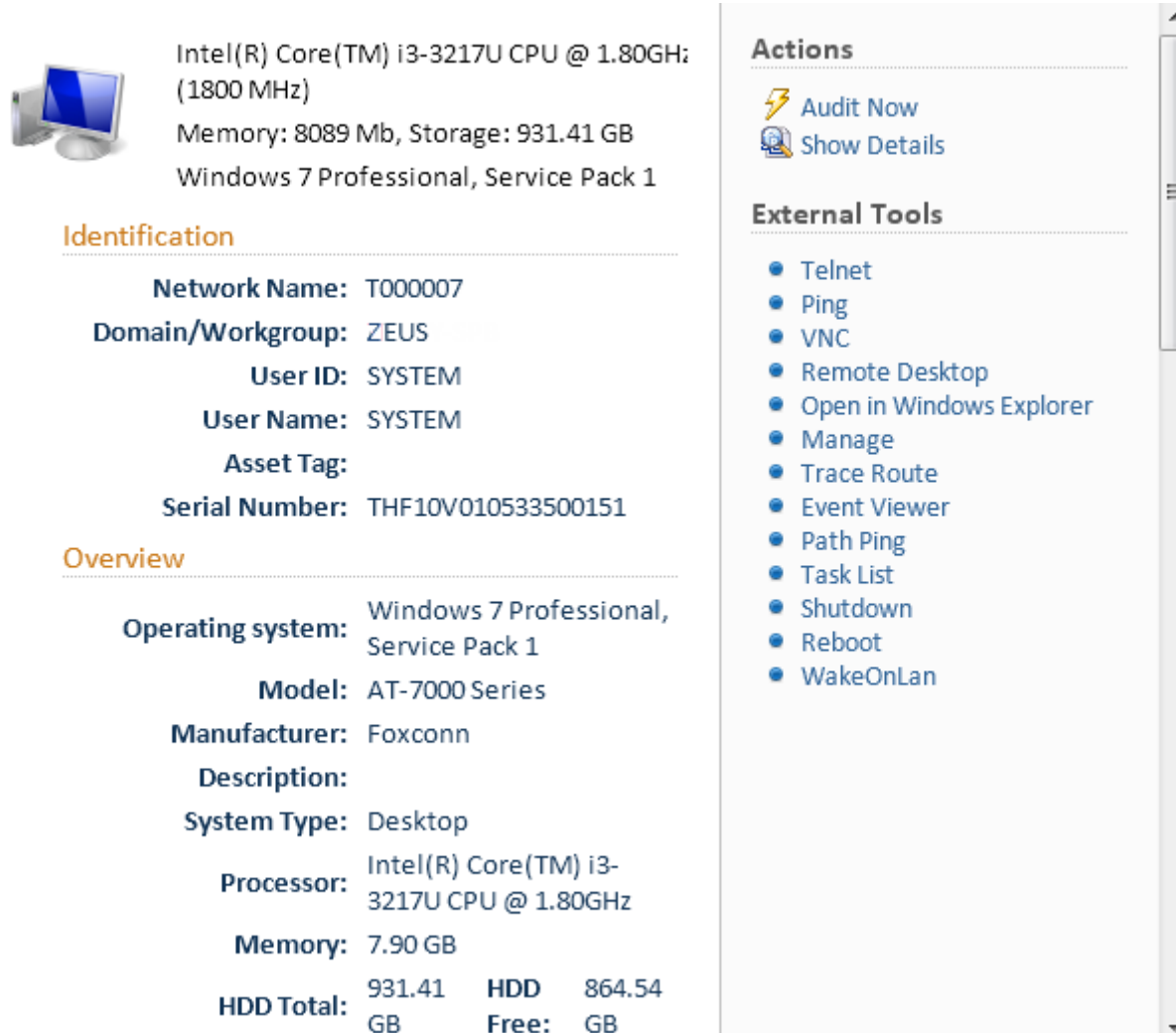
When you select a computer record on the **Computer List** tab, general information about the audited computer is displayed in the preview pane below the computer list. The preview pane shows the basic computer information such as the model, operating system, etc.

When you click a computer in the Sidebar, the preview pane occupies the entire main area and provides a more detailed overview of the computer. For computers that do not yet have audit snapshots, only the computer name is displayed.

On the right-hand side of the preview pane you will find a list of commands (actions) that can be performed on the selected computer. The following commands are available:

- **Audit Now** – initiates the On-Demand Audit of the computer.
- **Show Details** – opens the audit snapshot in the Audit Snapshot Viewer. This option is available only when the audit snapshot for the computer is available.

There are also a number of **External Tools** commands, allowing you to launch external applications using various properties of the selected computer as command-line parameters. For details, see [“External Tools” on page 125](#).



Intel(R) Core(TM) i3-3217U CPU @ 1.80GH:
(1800 MHz)
Memory: 8089 Mb, Storage: 931.41 GB
Windows 7 Professional, Service Pack 1



Identification

Network Name: T000007
Domain/Workgroup: ZEUS
User ID: SYSTEM
User Name: SYSTEM
Asset Tag:
Serial Number: THF10V010533500151

Overview

Operating system: Windows 7 Professional,
Service Pack 1
Model: AT-7000 Series
Manufacturer: Foxconn
Description:
System Type: Desktop
Processor: Intel(R) Core(TM) i3-
3217U CPU @ 1.80GHz
Memory: 7.90 GB
HDD Total: 931.41 **HDD** 864.54
GB **Free:** GB

Actions

-  Audit Now
-  Show Details

External Tools

- Telnet
- Ping
- VNC
- Remote Desktop
- Open in Windows Explorer
- Manage
- Trace Route
- Event Viewer
- Path Ping
- Task List
- Shutdown
- Reboot
- WakeOnLan

Figure 52: Preview Pane

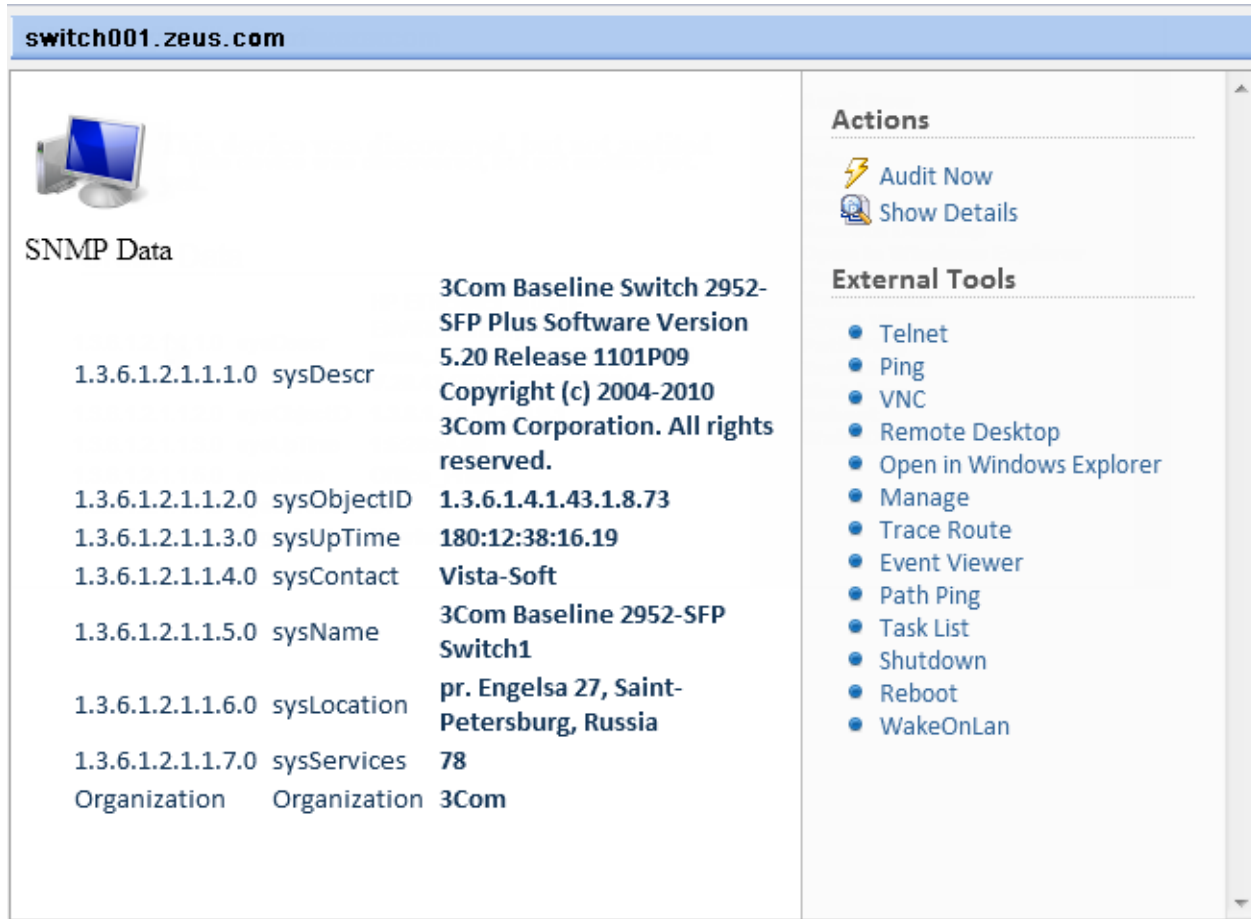
Viewing SNMP Data

When you select a network device record on the **Network Devices** tab, its SNMP information is displayed in the preview pane. The preview pane also appears when you click a network device in the Sidebar. For network devices that have no audit snapshot only the network device name is displayed.

On the right-hand side of the preview pane you will find a list of commands (actions) that can be performed on the selected device. The following commands are available:


- **Audit Now** – initiates the On-Demand Audit of the network device.
- **Show Details** – opens the Network Device Details dialog box. For details, see [“Viewing Network Device Details” on page 108](#).

There are also a number of **External Tools** commands, allowing you to launch external applications using various properties of the selected device as command-line parameters. For details, [“External Tools” on page 125](#).





switch001.zeus.com

SNMP Data

		
1.3.6.1.2.1.1.1.0	sysDescr	3Com Baseline Switch 2952-SFP Plus Software Version 5.20 Release 1101P09 Copyright (c) 2004-2010 3Com Corporation. All rights reserved.
1.3.6.1.2.1.1.2.0	sysObjectID	1.3.6.1.4.1.43.1.8.73
1.3.6.1.2.1.1.3.0	sysUpTime	180:12:38:16.19
1.3.6.1.2.1.1.4.0	sysContact	Vista-Soft
1.3.6.1.2.1.1.5.0	sysName	3Com Baseline 2952-SFP Switch1
1.3.6.1.2.1.1.6.0	sysLocation	pr. Engelsa 27, Saint-Petersburg, Russia
1.3.6.1.2.1.1.7.0	sysServices	78
Organization	Organization	3Com

Actions

-  Audit Now
-  Show Details

External Tools

- Telnet
- Ping
- VNC
- Remote Desktop
- Open in Windows Explorer
- Manage
- Trace Route
- Event Viewer
- Path Ping
- Task List
- Shutdown
- Reboot
- WakeOnLan

Figure 53: Previewing SNMP Data from a Network Device

Viewing Audit Snapshots

The Preview Pane shows only a select portion of data associated with the computer. To view detailed information including a complete listing of system hardware configuration settings and installed software, double-click the computer record or click **Show Details** located on the preview pane. *Alloy Discovery Express* will open the audit snapshot for this computer in the Audit Snapshot Viewer.

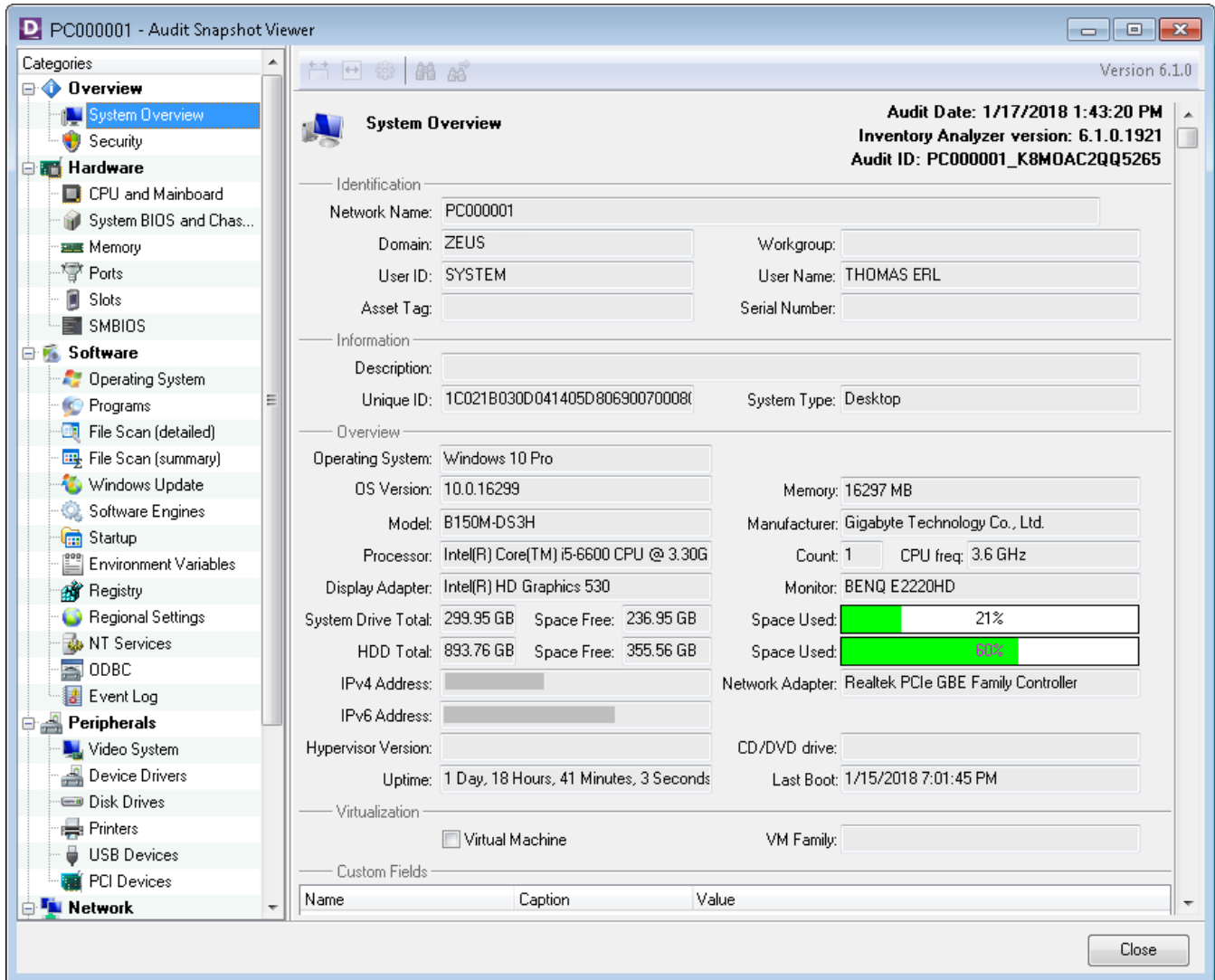


Figure 54: Computer Snapshot, System Overview

The Audit Snapshot Viewer shows the audit information broken down into several categories and sub-categories.



Audit Snapshot information may vary based on the type of the audited device and the computer's operating system.

Overview

The **Overview** category includes the following sub-categories:

Sub-category	Explanation
System Overview	<p>Basic information including the computer name, OS, hardware specs, and custom input fields data (for details, see "Configuring Custom Input Fields" on page 44).</p> <p>For Hypervisors, the Hypervisor Version field shows the product name and version of the hypervisor. Under Virtualization, you can also see read-only parameters collected during the audit:</p> <ul style="list-style-type: none"> Virtual Machine - The check box that indicates whether the computer is a virtual machine. VM Family - The virtualization platform family of the virtual machine.
Security Windows-specific data	<p>Security data including the information from the Windows Security Center (or the Action Center in Windows 7 and later), Windows firewall, installed firewall software, and installed antivirus software. The list of displayed security data varies depending on the Windows OS.</p> <p>The WSC security provider categories can have the following values:</p> <ul style="list-style-type: none"> Good – The status of the category is good and does not need user attention. Not Monitored – The status is not monitored by WSC. Poor – The status is poor and the computer may be at risk. Snooze – The computer is in snooze state. Snooze indicates that WSC is not actively protecting the computer.

Hardware

The **Hardware** category includes the following sub-categories:

Sub-category	Explanation
CPU and Mainboard	Details about the CPU and mainboard.
System BIOS and Chassis	Information about System BIOS and system enclosures.
Memory	Detailed memory specs, including virtual memory information and RAM speed.
Ports Windows- and Linux-specific data	Information about mainboard's internal and external port connectors.
Slots Windows-specific data	Information about data bus slots.

Software

The **Software** category includes the following sub-categories:

Sub-category	Explanation
Operating System	<p>Detailed OS information, including service packs, applied hot fixes, and Product ID.</p> <p>The Operating System section in the Audit Snapshot Viewer includes (when available) the OEM Information sub-section. This sub-section shows the Windows OEM information retrieved on brand name computers: the manufacturer name, computer model, and other support details specified by the original equipment manufacturer (OEM).</p>
Programs	<p><u>Windows computers</u>: Software products based on the information from the Uninstall section of the registry (the information you can see in the Add or Remove Programs tool) To see updates, select the Show Updates check box.</p> <p><u>Linux computers</u>: Software products based on the information from the package management system.</p> <p><u>Mac computers</u>: Software products based on the software information provided by the macOS's System Profiler utility.</p>
File Scan (detailed) Windows-specific data	A list of files created by the detailed portion of the software scan. For details, see "Configuring File Scan Options" on page 34
File Scan (summary) Windows-specific data	A list of files created by the summary portion of the software scan. For details, see "Configuring File Scan Options" on page 34 .
Windows Update Windows-specific data	Information about Windows updates.
Software Engines Windows-specific data	Software engines such as ODBC and DirectX.
Startup Windows- and Linux-specific data	Information about what runs on the computer at boot time, including information about startup folders and registry startup entries.
Environment Variables Windows- and Linux-specific data	Environment variables.
Registry Windows-specific data	A list of captured registry keys. For details, see "Configuring the Capture of Registry Keys" on page 26 .
Regional Settings Windows- and Linux-specific data	Readout of the machine's regional settings.
Services Mac OS-specific data	A list of system-wide launch daemons.

NT Services Windows-specific data	A list of all Windows services.
ODBC Windows-specific data	A listing of ODBC libraries and connections.
Event Log Windows-specific data	<p>A list of event log entries. For details, see "Configuring Event Log Options" on page 31.</p> <p>Here you can translate the time stamps of recorded events in various time zones: Administrator's time zone, user's time zone, and UTC (Universal Time Coordinated, same as GMT or Greenwich Mean Time).</p>

Peripherals

The **Peripherals** category includes the following sub-categories:

Sub-category	Explanation
Video System Windows- and Linux-specific data	Details about the video card, such as chipset and refresh rate.
Device Drivers Windows- and Linux-specific data	Devices installed on the machine.
Disk Drives	All drives on the machine, including floppy, CD/DVD drive, and fixed drives as well as mapped drives.
Printers Windows-specific data	A list of installed printers.
USB Devices Windows-specific data	A list of installed USB devices.
PCI Devices Windows-specific data	A list of installed PCI devices.

Below is an example the Audit Snapshot Viewer showing the device drivers details for a Windows computer:

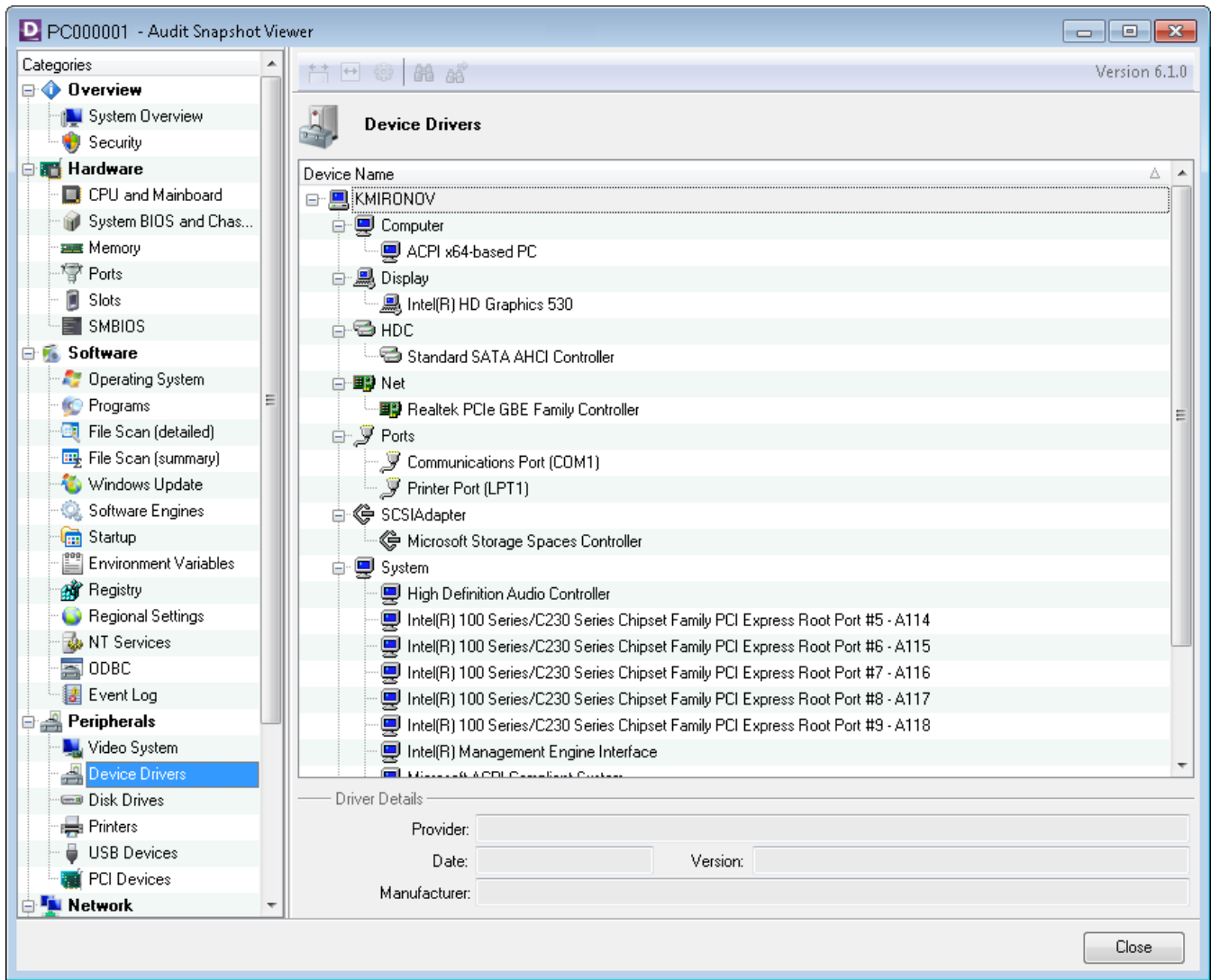


Figure 55: Computer Snapshot, Windows Device Drivers

Network

The **Network** category includes the following sub-categories:

Sub-category	Explanation
Network Configuration Windows-specific data	Miscellaneous network information, such as current user and domain name.
Network Adapters	Parameters (IP Address, DHCP, MAC address, etc.) of each network adapter.

Mapped Network Drivers Windows-specific data	A list of drive mappings.
Shared Resources Windows- and Linux-specific data	A list of shared resources.

User

The **User** category includes the following sub-categories:

Sub-category	Explanation
User Information Windows-specific data	Details about the current user (when available, this shows information from the Active Directory, such as e-mail address, contact numbers, physical address, etc.).
User Accounts	<p><u>Windows and Mac OS machines</u>: A list of local user accounts and user groups.</p> <p><u>Linux machines</u>: A list of local user accounts.</p>

Additional Information

The **Additional Information** category includes the following sub-categories:

Sub-category	Explanation
User-Defined Fields	<p>A list of user-defined fields and their values. For details, see "User-Defined Fields" on page 129.</p> <p>If no user-defined fields are configured or none of them are filled out for this computer or device, the grid is empty. The information for user-defined fields is unavailable when an audit snapshot is opened outside of <i>Alloy Discovery Express</i>, for example by clicking on an .adt file in Windows Explorer.</p>

Viewing Network Device Details

To view detailed information about a network device, double-click a device in the Sidebar or right-click a device in the grid and choose **Show Details** from the context menu. The Network Device Details dialog box opens.

- **General** — This tab shows the SNMP information obtained from the audited device.

- Printer Supplies** — This tab displays textual and graphical information about printer supplies, such as ink or toner. This tab appears only when the device has been detected as printer.

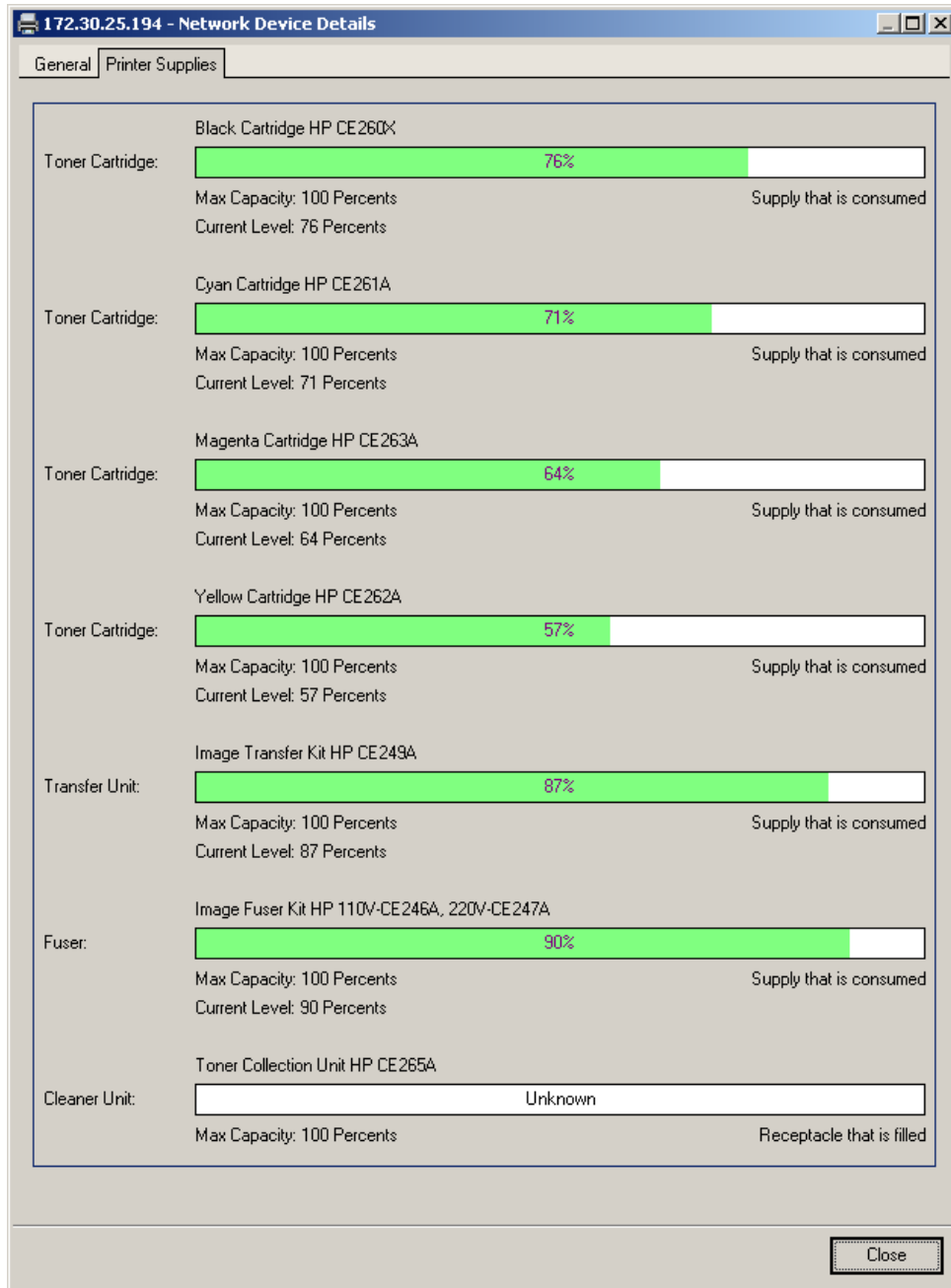


Figure 56: Network Device Details dialog box



The **Printer Supplies** tab does not appear for print servers.

There are two kinds of information that can be displayed on this tab:

- Supplies that are consumed. Levels of these supplies are visualized with progress bars that start at 100% and gradually decrease. For example, see Toner Cartridges, Transfer Unit, and Fuser in the screenshot above.
- Receptacles that are filled. Their levels are visualized with progress bars that start at 0% (empty receptacle) and gradually increase. For example, see Cleaner Unit in the screenshot above.



Information about printer supplies is obtained from the device via SNMP and displayed "as is". Thus, each printer may have a different set of available information, different units of measurement (thousands of ounces, tenths of milliliters), etc.

Working with Audit Properties

Once your network nodes have been audited, their audit snapshots have been imported into the *Alloy Discovery Express* database, you can modify their properties by specifying individual SNMP credentials, audit credentials or reclassifying types of unrecognized computers and network devices.



For details, see ["Specifying Individual SNMP Credentials" on page 113](#) and ["Specifying Individual Audit Credentials" on page 114](#).

Reclassifying Unrecognized Computers or Network Devices

To reclassify an unrecognized computer or network device, follow these steps:

1. In the Sidebar, right-click a node you want to reclassify and choose **Properties** from the pop-up menu. The **Audit Properties** dialog box opens.
2. You can correct the automatic recognition results as follows:
 - Unrecognized devices receive the **Unknown** type. Network devices that respond to SNMP requests but do not match any of the supported types receive the **Other** type. If you know the type, you can choose it from the **Type** drop-down list.



To make your inventory more accurate, every time *Alloy Discovery Express* runs the discovery, it removes previously discovered but unrecognized devices (**Unknown** devices) that are no longer found on the network.

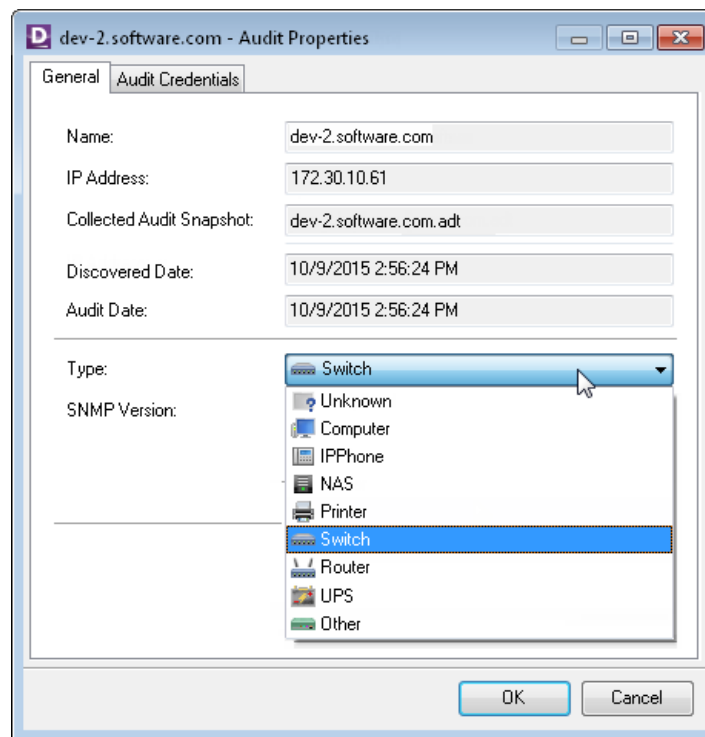


Figure 57: Specifying the type of unrecognized network device

For example, to specify that an unrecognized device is a computer, choose **Computer** from the **Type** list and choose its OS from the **Operating System** list.

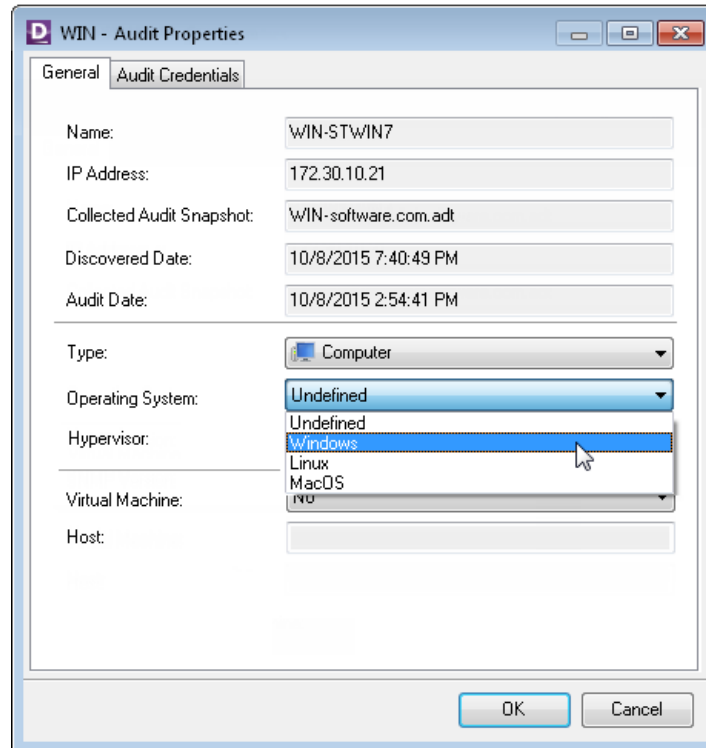


Figure 58: Specifying the OS type of unrecognized computer

- For computers running a hypervisor, you can change the **Hypervisor** type, such as **Microsoft Hyper-V**, **VMware ESX**, **VMware ESXi**, **Xen**, or **Citrix XenServer**. If you mark a hypervisor as **Undefined**, *Alloy Discovery Express* will update this value next time you run the discovery of the Audit Group where that hypervisor belongs. The system will attempt to automatically determine whether the computer is running a hypervisor and if it is, detect its type.



Alloy Discovery Express automatically sets the operating system (**OS Type** value) for the computer in accordance with the hypervisor type specified. This does not apply to computers defined as **Not a Hypervisor** or **Undefined**.



For computers running VMware ESX/ESXi hypervisors, the **Audit Properties** dialog box also displays an additional **ESX/ESXi Options** tab. To audit those computers, you must specify connection parameters. For details, see ["Specifying Connection Parameters for VMware ESX / ESXi Hypervisors"](#) on page 93.

3. Click **OK**.



Additionally, you can specify individual SNMP credentials for a network device or individual audit credentials for a computer.

For details, see ["Specifying Individual SNMP Credentials" on page 113](#) and ["Specifying Individual Audit Credentials" on page 114](#).

Specifying Individual SNMP Credentials

By default, Alloy Discovery Express accesses SNMP data on devices in the Audit Group using SNMP credentials that you have provided when configuring the On-Demand Audit Group (see ["Creating On-Demand Audit Groups" on page 56](#)). However, you may need to specify different SNMP credentials for a particular network device.

To specify an individual set of SNMP credentials for a particular device, follow these steps:

1. In the Sidebar, locate the network device for which you want to specify individual SNMP credentials.
2. Right-click the record and choose **Properties** from the pop-up menu. The **Audit Properties** dialog box opens.
3. Choose the version from the **SNMP Version** drop-down list and click **OK**.

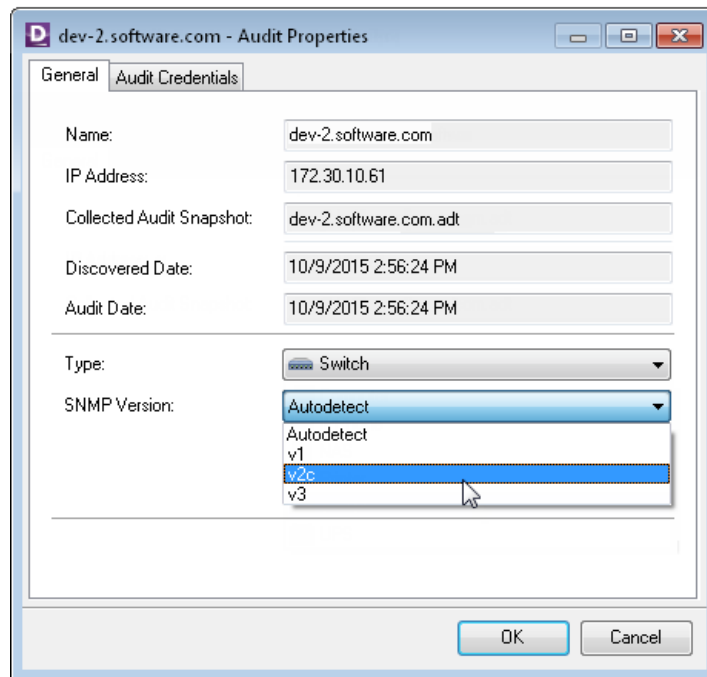


Figure 59: Specifying individual SNMP credentials



Individual SNMP credentials for a network device take precedence over the credentials specified in its Audit Group.

Specifying Individual Audit Credentials

By default, Alloy Discovery Express computers within a group use audit credentials that you have provided when configuring the On-Demand Audit Group (see [“Creating On-Demand Audit Groups” on page 56](#)). However, you may need to specify individual credentials for a particular computer or a network device.

To specify individual credentials for a particular network node, follow these steps:

1. In the Sidebar, locate the computer or network device for which you want to specify individual audit credentials.
2. Right-click its record and choose **Properties** from the pop-up menu. The **Audit Properties** dialog box opens.
3. In the **Audit Credentials** tab, select **This Account** and type in the username and password. You can enter either a domain login name (such as ZEUS\Administrator) or a local login name (such as Administrator) as long as this account exists on every computer you want audited as well as on the host machine.

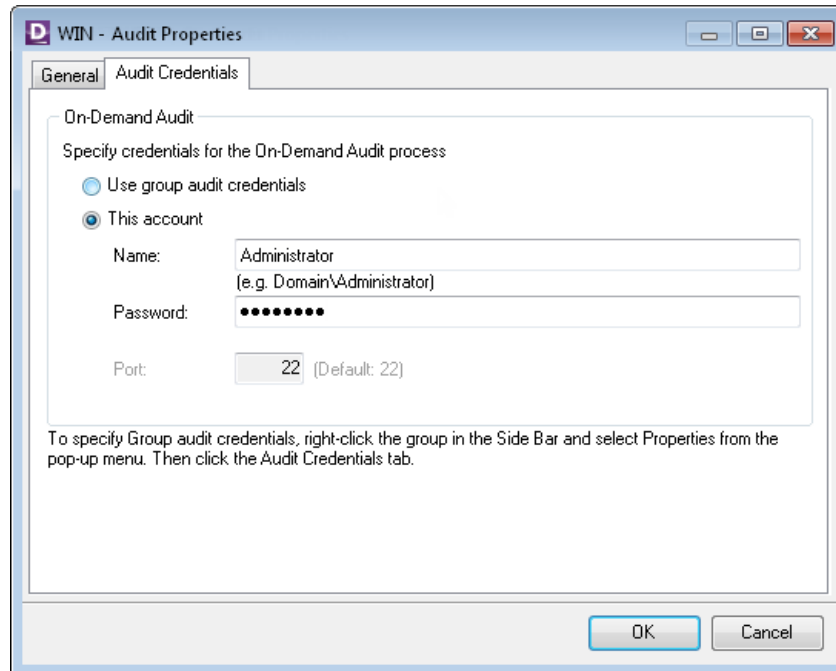


Figure 60: Specifying individual audit credentials

4. Click **OK**.



Individual audit credentials for a node take precedence over the credentials specified in its Audit Group.

For details, see ["Managing Audit Credentials" on page 51](#).

Working with Static and Dynamic Computer Groups

Once you have audited your computers and obtained their audit snapshots, you can create computer groups to analyze your inventory.

A computer group can be one of the following types:

- **Dynamic** – these groups are populated automatically based on a combination of criteria you specify for the group. *Alloy Discovery Express* provides a number of pre-defined dynamic groups, such as Windows 10, Linux, Mac OS, MS Office 2016, MS SQL Server 2017, Hypervisors, Computers with SSD, etc.
- **Static** – these groups are created by manually assigning computers. For example, you can use static groups to independently analyze and report inventory data from multiple networks or subdivisions within your organization.

For details on working with these groups, see the *Working with Computer Groups* section in the embedded Help system.

Although computer groups are meant for analyzing audit data, you can also perform the On-Demand Audit of a computer group: right-click the group in the Sidebar and choose **Audit this Group** from the pop-up menu. For static computer groups, you can also start the On-Demand Audit of never audited computers: right-click the group in the Sidebar and choose **Audit This Group > Audit Never Audited Computers** from the pop-up menu. The audit will run under the default On-Demand Audit credentials, unless different On-Demand Audit credentials are specified for individual computers in this group. For details, see ["Managing Audit Credentials" on page 51](#).

Configuring Dynamic Computer Groups

The Group Properties dialog box shows the current settings for a Dynamic Group and lets you modify these settings. To open this dialog box, right-click a Dynamic Computer group in the Sidebar and choose **Properties** from the pop-up menu.

The properties are organized on the following tabs: **General** and **Description**.

General tab

On this tab you can view and edit the name of the group and its inclusion rules.

- **Name** – shows the name of the group.

The **Inclusion Rules** section shows the criteria for adding computers to this group. The criteria are a combination of logical expressions (rules) based on the values reported in audit snapshots.

You can work with the inclusion rules using the following functions:

- **Add** – creates a new inclusion rule.
- **Edit** – modifies the selected rule.
- **Remove** – removes the selected rule.

You can select one of the following options in conjunction with the **Include computers matching** field:

- **all rules** – if you want to include in the group only those computers that match all rules in the list.
- **any of rules** – if you want to include in the group any computer that matches at least one inclusion rule.

Specifying Inclusion Rules

In this dialog box, you can define an inclusion rule as follows:

1. Select a field (a computer attribute available in audit snapshots) that you want to use in the rule. Click the plus icon to expand the category which contains the attribute. Attributes can be singular (containing a single value) or plural (containing a list of values). Define the rule condition:
 - For singular attributes, such as **CPU Architecture**, **Operating System**, or **System Drive Free Space**:
 - 1) Select an attribute field.

- 2) In the **Operator** list, select an operator.
- 3) If the selected operator requires a value to compare the field with, type in a value in the **Value** field.

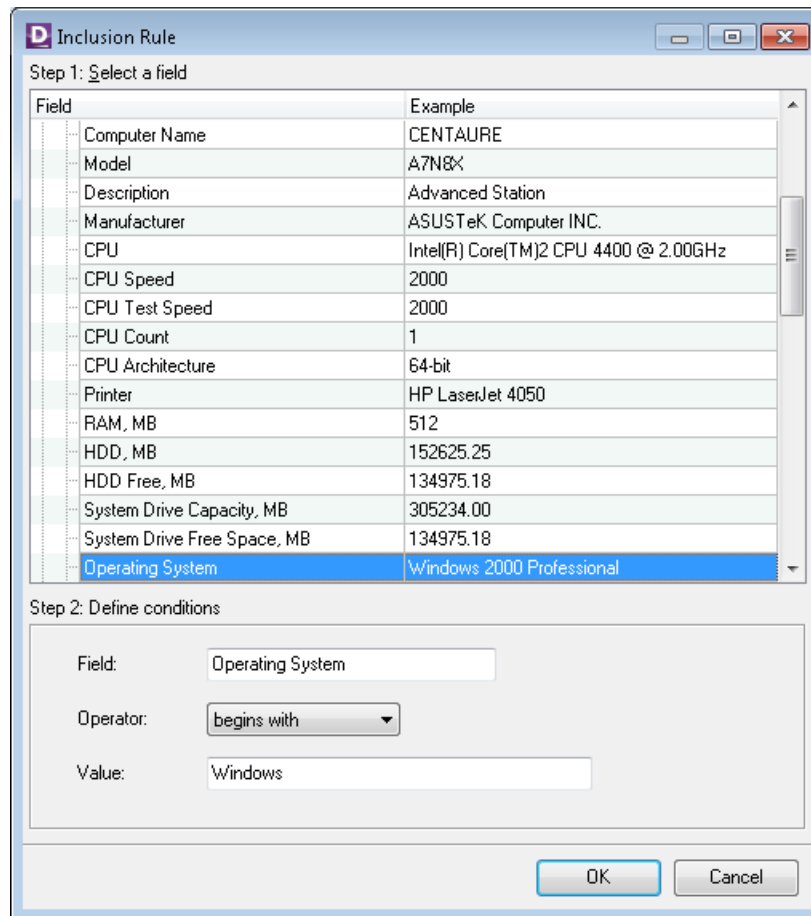


Figure 61: An inclusion rule for a single attribute

- 1) Select a general logical condition, either positive or negative (such as "Shares Exist" or "Shares Not Exist", "Product Discovered" or "Product Not Discovered", "User Account Found" or "User Account Not Found").
 - 2) Under **Define rule condition**, supplement the general condition with additional conditions (these simple conditions will be connected with AND logic, meaning that every sub-condition must be satisfied in order for the inclusion rule to result in a match):
 - 1) Select an operator for a computer attribute you want to use. If the selected operator requires a value, type in the value.

Repeat this step for each field you want to use.

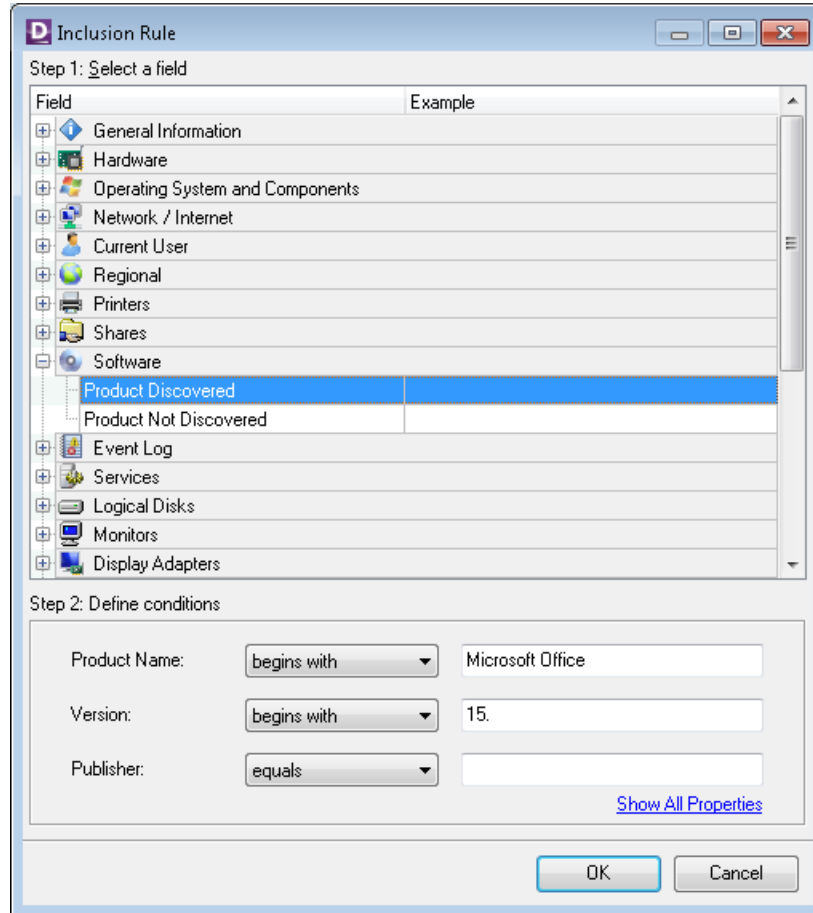


Figure 62: An inclusion rule for a multiple attribute

- 2) If you want to view all available properties, click the **Show All Properties** link. The **Advanced Fields** dialog box opens. Using this dialog box, you can specify additional conditions for advanced attributes (such as **Product ID** or **Install Date**).
3. Click **OK**. The rule is added to the inclusion rule list.

CHAPTER 8. Advanced Options

This chapter explains audit snapshots and provides a list of command-line options for the Inventory Analyzer.

Understanding Audit Snapshots

Audit snapshots are the end result of the audit. Each snapshot contains various hardware and software details for an individual computer or device. An audit snapshot can consist of one or several files all having the same base name. The base name is comprised of the fully qualified domain name of the computer if such name is available (for example, `jdoe.zeus.com`). Otherwise, in some cases it is the computer name followed by a unique identifier (for example, `jdoe_IXHERTR6247`). The file name extension identifies the contents of the snapshot file:

- **ADT file** — An `.adt` file is a mandatory part of an audit snapshot. An `.adt` file contains information about hardware configuration of the device. For computers, this file also contains information about installed software products.
- **SCN file** — An `.scn` file contains file scan information of the audited node. It is created if you have configured the file scan option in the audit configuration. For details, see [“Configuring File Scan Options” on page 34](#).
- **SNMP file** — An `.snmp` file contains SNMP information about the node. It is created if you have enabled discovery via SNMP. For details, see [“Enabling SNMP Discovery” on page 53](#).
- **UDF file** — An `.udf` file contains information about user-defined fields. It is created if you have configured one or several user-defined fields and filled out at least one of these fields for a computer or device. For details on configuring and populating user-defined fields, see [“User-Defined Fields” on page 129](#).

You can determine the name of the `.adt` file for an audited computer as follows:

1. Right-click the computer in the Sidebar and select **Properties** from the pop-up menu. The **Audit Properties** dialog opens.
2. The base name of the audit snapshot will be displayed in the **Collected Audit Snapshot** field.

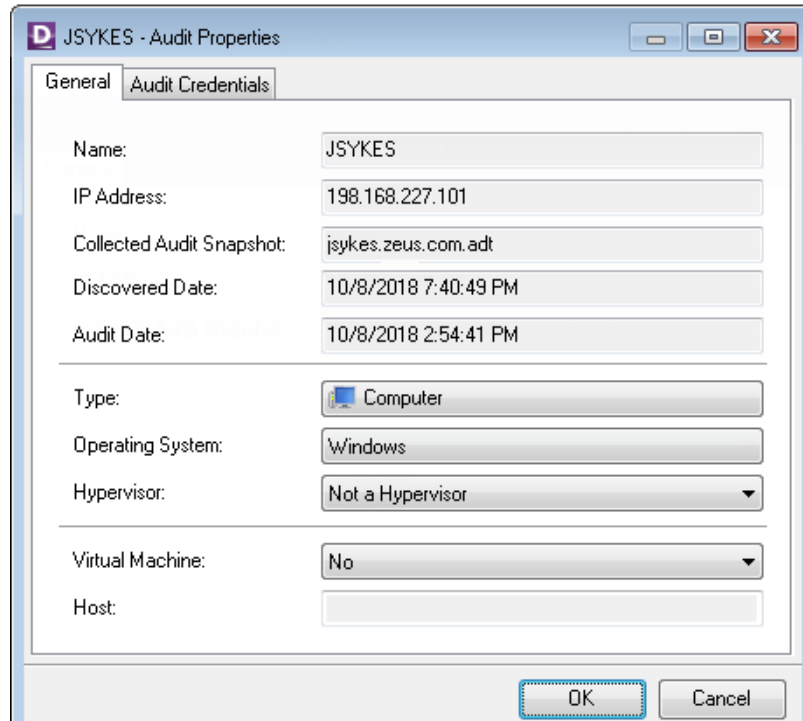


Figure 63: Viewing Snapshot File Name

Comparing Audit Snapshots

With *Alloy Discovery Express* you can compare two computers and easily determine differences in their configuration.



Comparison can only be initiated for two audited computers. For two network devices this option is unavailable.

To compare two computers:

1. Right-click the first computer in the Sidebar or in the Computer List and select **Compare With** from the pop-up menu. The Compare With dialog box opens.

The **Compare With** dialog box displays a hierarchical tree of audit groups and computer groups containing audited nodes.

2. Select the second computer from one of the groups shown in the hierarchical tree and click **OK**.

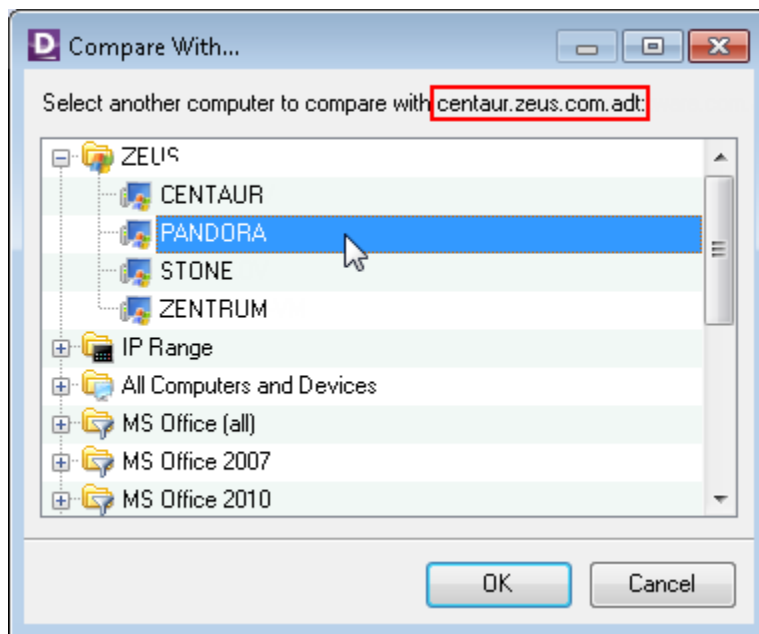


Figure 64: The Compare With dialog box

The **Audit Files Compare** dialog box opens (see [Figure 64 below](#)).

3. The **Audit Files Compare** dialog box provides a side-by-side comparison of audit snapshots for both computers. Navigate through the **Parameter** tree and view the result of the comparison. Items that have different values show up in red.

If you want to exclude items that have identical values from the list, select the **Show differences only** check box. Since the **Parameters** tree will display only items with different values, red color will not be used to indicate differences.

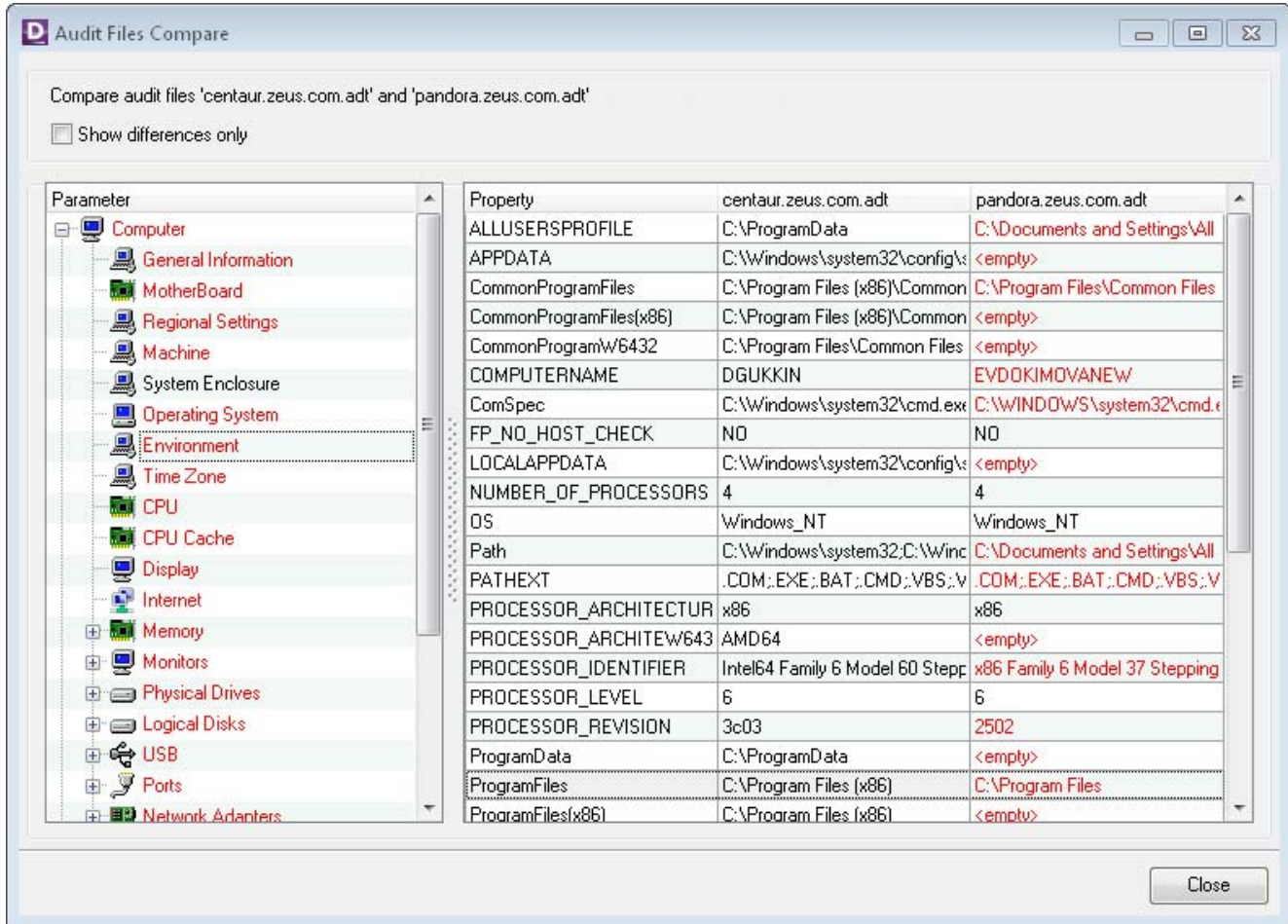


Figure 65: Comparing Audit Snapshot Files

4. Click **Close** to exit the **Audit Files Compare** dialog box.

Understanding the Audit Snapshot Viewer

Alloy Discovery Express includes the Audit Snapshot Viewer for displaying audit snapshot data in a convenient human-readable form. When you install *Alloy Discovery Express*, the installer associates the .adt file extension with the Audit Snapshot Viewer so you can view the contents of audit snapshots from Windows Explorer or from the command line. To open an audit snapshot from Windows Explorer, simply double click the snapshot's .adt file. To open an audit snapshot from the command line, supply the name of the snapshot's .adt file as a parameter to the Audit Snapshot Viewer executable (typically, the executable is installed in the \Program Files\Common Files\Alloy Shared\AuditViewer\Bin folder). You can also launch the Audit Snapshot Viewer without any parameters, it will prompt you for the audit snapshot to open.

The Audit Snapshot Viewer doesn't open scan (.scn) or user-defined field (.udf) files directly. However, it displays the information from .scn files in the **File Scan (detailed)** and **File Scan (summary)** sections when viewing the related .adt file, as illustrated in [Figure 66 below](#). Data from user-defined fields is shown in the Additional Information section.

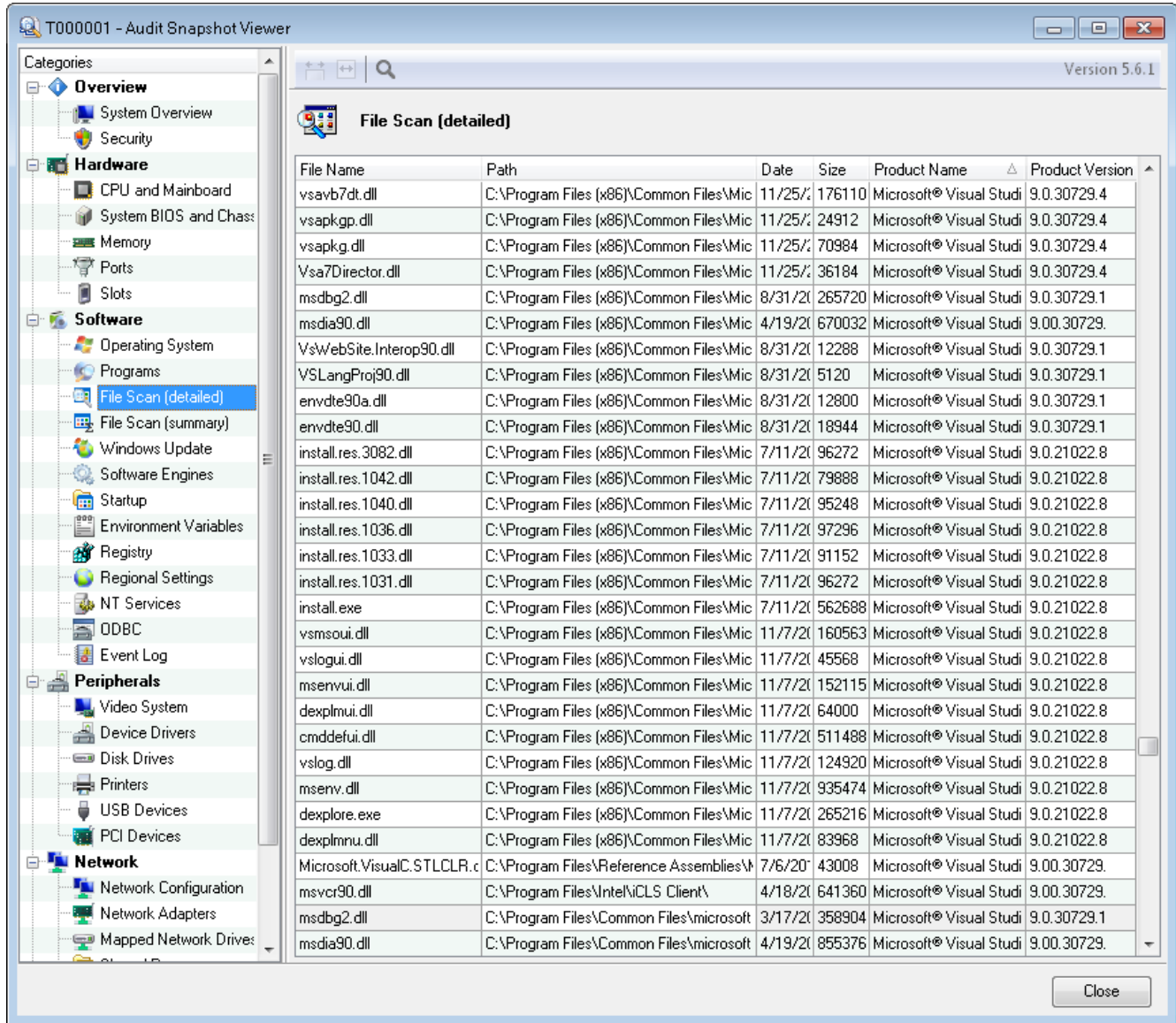


Figure 66: Viewing File Scan results in Audit Snapshot Viewer

Configuring Computer List

Audit snapshots contain many fields, but only few of them are displayed in the Computer List. You can customize the columns that appear in the Computer List using the **Computer List Configuration** dialog box by adding or removing certain fields. To customize the Computer List, select **Tools > Computer List Configuration** from the main menu.

Under **Available fields** you will find the list of all fields available for mapping into the Computer List. Under **Show these fields in the Computer List** is the list of currently selected columns.

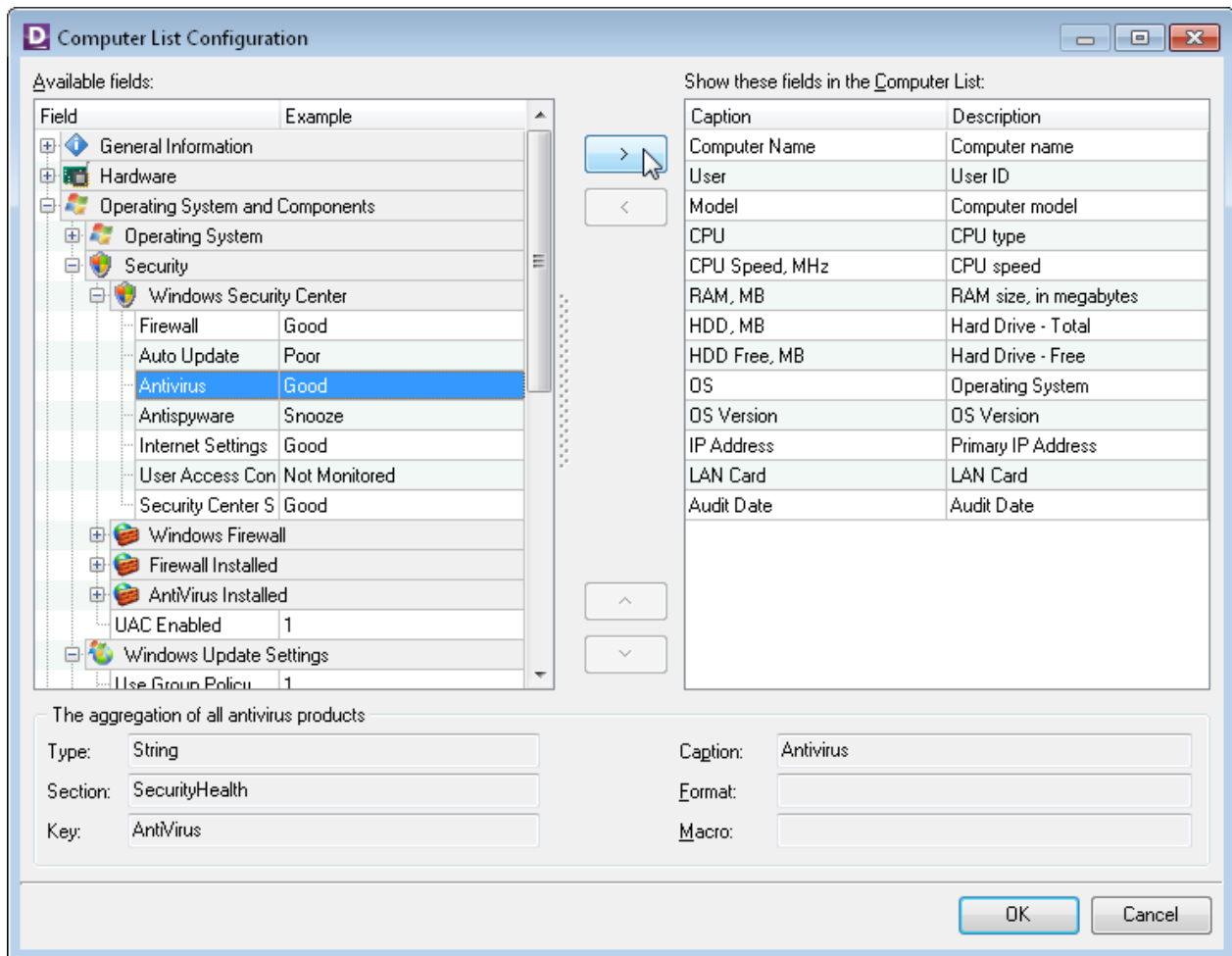


Figure 67: Configuring the Computer List

- The **Custom Fields** section appears if you have defined custom input fields in the Audit Configuration (for details, see ["Configuring Custom Input Fields" on page 44](#)).
- The **Registry Fields** section appears if you have added registry keys to capture (for details, see ["Configuring the Capture of Registry Keys" on page 26](#)).
- The **User-Defined Fields** section appears, if you have added user-defined fields. For details on using this feature, see ["User-Defined Fields" on page 129](#).

To include a snapshot field in the Computer List, select a field in the **Available Fields** section and click the right arrow button (>).

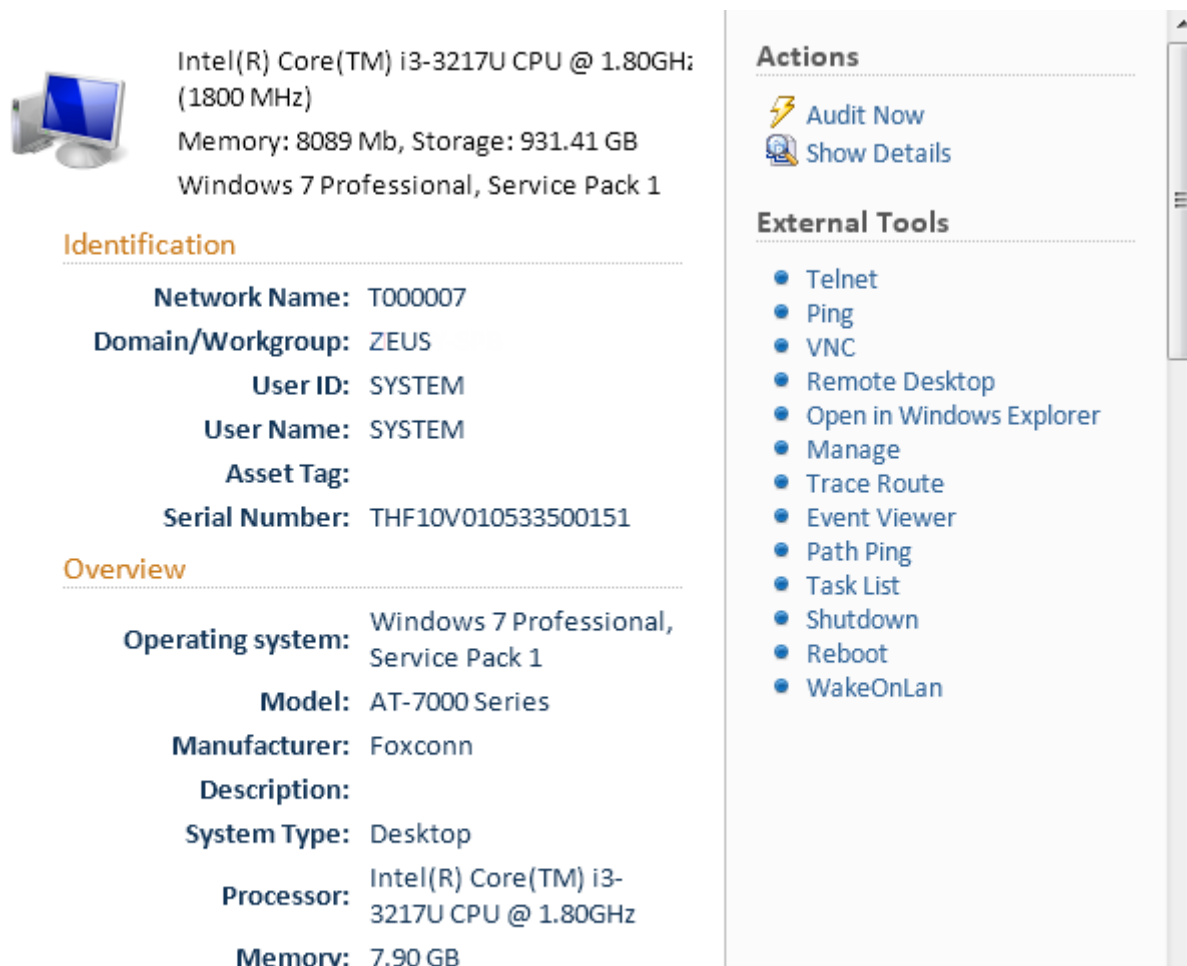
To remove a column from the Computer List, select a field in the **Show these fields in the Computer List** section and click the left arrow button (<).

Using the up and down arrow buttons, you can rearrange columns in the Computer List grid.

External Tools

External Tools is an *Alloy Discovery Express* feature which helps you launch various external commands for a node. For instance, you can use this feature to connect to remotely manage computers via Remote Desktop, VNC, or PC Anywhere, telnet or SSH to a device, or simply ping it.

External tools are shown on the right side of the preview pane when selecting a computer from the Sidebar, or via the **Computer List** tab. The preview pane for an audited computer is shown below.



Intel(R) Core(TM) i3-3217U CPU @ 1.80GHz:
(1800 MHz)
Memory: 8089 Mb, Storage: 931.41 GB
Windows 7 Professional, Service Pack 1

Identification

Network Name: T000007
Domain/Workgroup: ZEUS
User ID: SYSTEM
User Name: SYSTEM
Asset Tag:
Serial Number: THF10V010533500151

Overview

Operating system: Windows 7 Professional,
Service Pack 1
Model: AT-7000 Series
Manufacturer: Foxconn
Description:
System Type: Desktop
Processor: Intel(R) Core(TM) i3-
3217U CPU @ 1.80GHz
Memory: 7.90 GB

Actions

- Audit Now
- Show Details

External Tools

- Telnet
- Ping
- VNC
- Remote Desktop
- Open in Windows Explorer
- Manage
- Trace Route
- Event Viewer
- Path Ping
- Task List
- Shutdown
- Reboot
- WakeOnLan

Figure 68: External Tools (Preview Pane)

Alloy Discovery Express comes with a number of pre-configured external tools. For instructions on configuring additional external tools, see ["Configuring External Tools" on page 127](#):

- **Telnet** — connects to a remote device via Telnet.
- **Ping** — runs ping.
- **VNC** — runs Virtual Network Computing, which is a popular graphical desktop sharing and remote computer access tool. To use this tool, VNC must be installed on both the host and remote computers.

- **Remote Desktop** (RDC) — runs the Remote Desktop Connection, which is a Microsoft client tool (included by default in Windows XP and above) for accessing the desktop, applications, and data on a remote computer and controlling it remotely.
- **Open in Windows Explorer** — lets you access the computer's shared resources using Windows Explorer.
- **Manage** — allows you to open the Computer Management console for the chosen computer.
- **Trace Route** — runs the TRACERT (Trace Route) tool, which is a command-line utility that traces the path that an Internet Protocol (IP) packet takes to its destination.
- **Event Viewer** — allows you to open the Event Viewer for the chosen computer.
- **Path Ping** — runs the PathPing tool, which is a TCP/IP based utility (command-line tool) that provides useful information about network latency and network loss at intermediate hops between a source address and a destination address.
- **Task List** — allows you to view applications and services for all tasks running on a remote computer.
- **Shutdown** — shuts down a remote computer.
- **Reboot** — restarts a remote computer.
- **WakeOnLan** — turns on a remote computer via a network connection.



Executing the **WakeOnLan** command requires that the computer meets the technical conditions of the Wake on LAN (WOL) standard. Also, you may need to make some changes in the target computer's BIOS configuration in order to enable this feature.

To launch an external tool, select a node in the Sidebar or in the Computer List, and perform either of the following operations:

- From the main menu, choose **Tools > External Tools** and click the tool name.
- From the preview pane, click the tool name in the External Tools list.

Configuring External Tools

To configure external tools, open the **External Tools** dialog box by choosing **Tools > External Tools > Configuring External Tools**. From this dialog box you can add new tools, edit and delete existing tools.

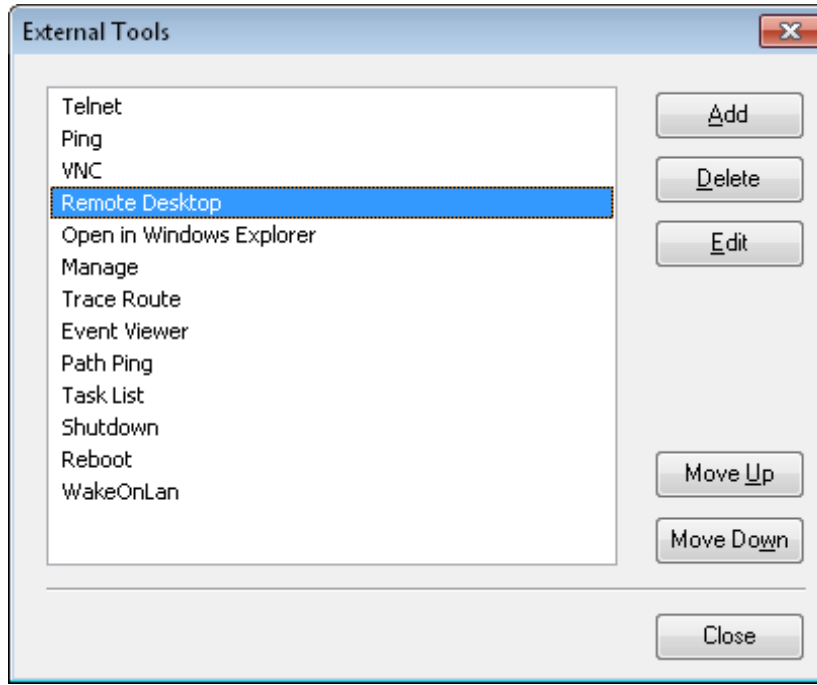


Figure 69: The External Tools dialog

The following functions are available in the External Tools dialog box:

- **Add** — adds a new external tool.
- **Delete** — removes the selected tool.
- **Edit** — edits the settings of the selected tool.



To access these functions you can also right-click any tool name in the External Tools list (see [Figure 69 above](#)).

- **Move Up and Move Down** — change a tool's position in the list.
- **Close** — saves the changes, if any, and closes the dialog box.

When you launch an external tool, *Alloy Discovery Express* executes the command specified in that tool's configuration. The command parameters specified via placeholders are replaced with appropriate values from that node's audit snapshot.

For example, `$COMPUTER_NAME` is replaced with the computer name. The provided placeholders will fit most users' needs. However, you can create new ones in the Customizing Computer List dialog, if you want.

Below is an example of the parameters available for the Ping tool.

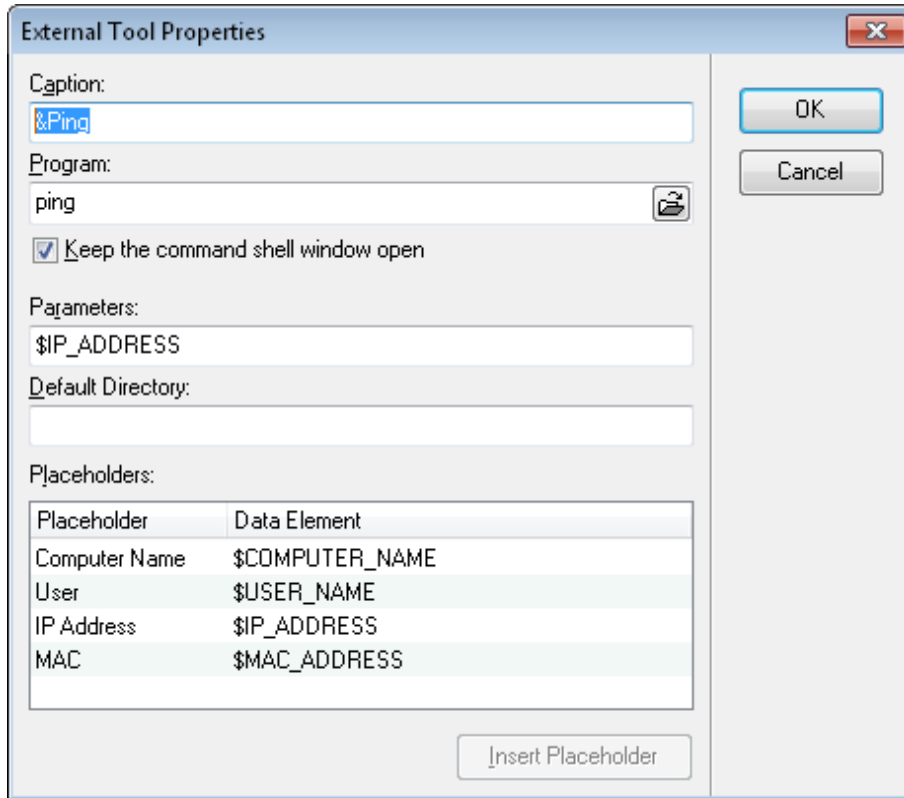


Figure 70: "Ping" Properties

The following parameters can be customized:

- **Caption** — This is the name of the tool, as it appears in the external tools list. The name must be unique among other names, and can't be blank. To include a keyboard accelerator (for example, Ping), which is the standard Windows ALT+<character> combination, for your tool, include an ampersand (&) before the character. For example, to use the ALT+P combination as an accelerator for the Ping action, enter the caption as "&Ping". To display the ampersand character in the caption, use two ampersands (&&).
- **Program** — This is the path and the name of the program you want to run. You can specify a name without path only if the program is a system command or if it's located on the system search path.
- **Keep the command shell window open** — For DOS commands and scripts, such as ping or TRACERT, check this box to keep the command shell dialog box open after the command is executed to review its output.
- **Parameters** — You can enter any command line options as necessary. For example, use the computer name placeholder to pass the name of the currently selected computer as a parameter for the tool's program. Use the **Insert Placeholder** button to insert the selected placeholder into the **Parameters** field.
- **Default Directory** — You can optionally specify the default folder where your command should run. You can use this option when your tool relies on "current directory" to search for additional files (e.g. configuration files) or to generate an output file.

User-Defined Fields

Alloy Discovery Express lets you configure user-defined fields to store custom information about computers. For example, this allows you to track financial information, barcode numbers, your notes, etc. Once created, the user-defined field will be available for all node records. You can see user-defined fields in the Computer List (you need to customize the Computer List to show these fields).



If an audit snapshot is opened from within *Alloy Discovery Express*, user-defined fields are shown in the **Additional Information > User-Defined Fields** sub-category. When you open audit snapshots outside of *Alloy Discovery Express* (e.g from the command line or from Windows Explorer), user defined fields will not be shown.

Working with User-Defined Fields

To customize user-defined fields, open the User-Defined Fields dialog box by selecting **Tools > User-Defined Fields > Configure** from the main menu.

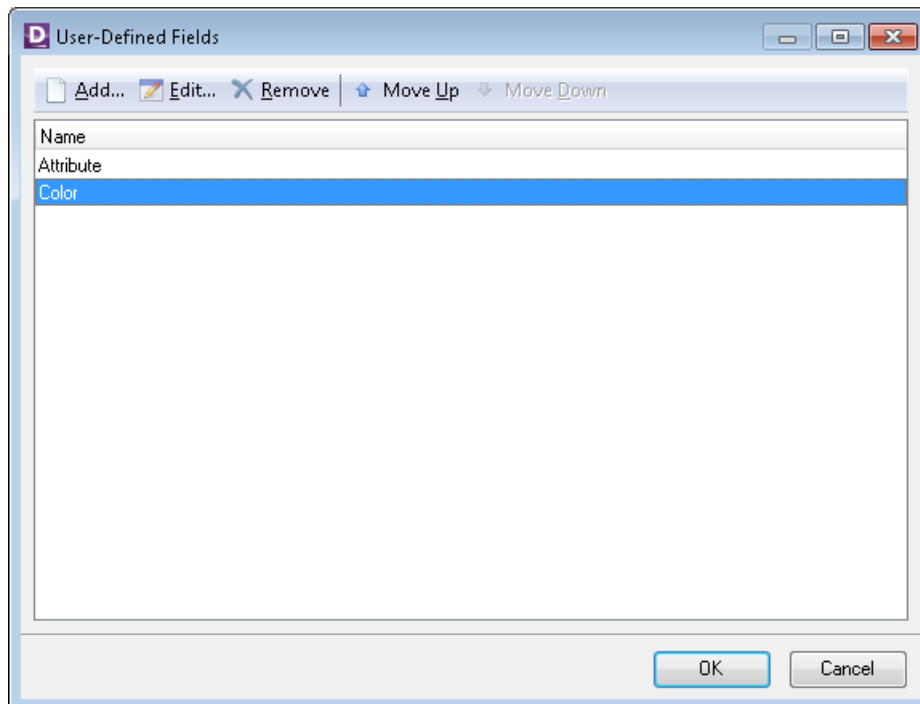


Figure 71: Configuring user-defined fields

To add a user-defined field, click **Add**, specify the field name, and click **OK**.



If you want the user-defined field to appear in the Computer List, you need to explicitly add it as a column. You can do this by selecting **Tools > Configure Computer List** from the main menu.

To rename a user-defined field, select the field in the list, click **Edit**, type in a new name for the field, then click **OK**. To delete a user-defined field, select the field and click **Remove**.

You can assign an accelerator key for a user-defined field (for example, **C**olor). This accelerator key can be used to select the field in the **Tools > User-Defined Fields > Batch Update** menu by pressing the standard Windows ALT+<accelerator_key> combination. To assign an accelerator key, when you are editing the field name, insert an ampersand (&) before the character you want to use as an accelerator key. If you want to display an ampersand character in the field name, use two ampersands (&&).

Use the **Move Up** and **Move Down** buttons to rearrange fields in the list. The user-defined fields will be shown in the same order also in the **User-Defined Fields** section of the **Available fields** pane in the Computer List Configuration and Inclusion Rule dialog boxes.

Storing Data in User-Defined Fields

To set a value of a user-defined field:

1. Right-click the node either in the Sidebar or in the Computer List and choose **Edit User-Defined Fields** from the pop-up menu.
2. Type in a value for the required field.
3. Click **OK**.

Batch Updating User-Defined Fields

The Batch Update feature helps you change the values of a user-defined field in multiple computer records at once.

To update a user-defined field in multiple computer records:

1. In the Computer List, select the computer records you want to update using the following methods:
 - To select adjacent records, hold down SHIFT and click the first and the last record of the desired selection;
 - To select non-adjacent records, hold down CTRL and click each record you want to update;
 - To select all records in the grid, press CTRL+A.
2. Choose **Tools > User-Defined Fields > Batch Update** from the main menu and select the field to update.

3. Choose one of the following:
 - To set a value for the field, type the required value in the text field and click **OK**.
 - To clear the field, click **Clear**.

Associating Virtual Machines with Host Machines

Alloy Discovery Express automatically identifies different types of virtual machines and hypervisors. *Alloy Discovery Express* also provides the ability to associate virtual client computers with their host machines (physical computers running the virtualization platform). For a number of popular virtualization platforms, *Alloy Discovery Express* performs the association automatically. When the automatic association is not possible, you can establish the association manually.



Alloy Discovery Express puts virtual computers and hypervisors detected during the audit into the pre-defined **Virtual Machines Collection** and **Hypervisors** collections respectively.

Automatic Association of Virtual Machines to their Hypervisor Hosts

By default, *Alloy Discovery Express* associates virtual guest computers with their hypervisor host by the MAC address of the network adapter. Mac addresses of virtual machines are collected from the hypervisor during the audit. However, there are rare cases when MAC addresses can not be detected or when virtual machines hosted on different hypervisors may have the same MAC addresses. In these cases automatic association may not work properly. You can correct that by establishing the association manually. For details, please refer to ["Manual Association of Virtual Machines to their Hypervisor Hosts" on page 131](#).



Make sure to keep MAC addresses of virtual machines unique to establish correct auto-association of virtual machines to their hypervisors. Otherwise, the manually established association may be lost next time you audit the virtual guest computer.

You can check whether the hypervisor host for the virtual machine was detected correctly in the **Host** field of the **Computer Audit Properties** dialog box.

Manual Association of Virtual Machines to their Hypervisor Hosts

To associate a virtual guest computer to a host, follow these steps:

- 1) Right-click an audited Computer in the Sidebar.
- 2) In the **General** tab of the **Computer Audit Properties** dialog box, do one of the following:
 - If the Computer was not detected as a virtual machine, select **Yes** from the **Virtual Machine** drop-down list. In the enabled **Host** drop-down list, select the host where the virtual guest computer resides, then click **OK**.

- If a Computer is already detected as a virtual machine, select its host from the **Host** drop-down list, then click **OK**.

Inventory Analyzer Command-Line Options

You can use the Inventory Analyzer command-line options for overriding the audit configuration settings when running the Inventory Analyzer manually, or automating it in Scriptable Audit scenarios.

The following table explains the available options. For convenience the options are grouped by their purpose. To see a full listing of these options on the screen, enter `ina32.exe /?` at the command prompt.

Option	Description
Output Options	
<code>/out=[Path]</code>	Specifies the output directory for audit snapshot files. You can use environment variables in the path.
<code>/ini=[Path]</code>	Specifies the path to the <code>ina32u.ini</code> . When the Inventory Analyzer runs, it leaves behind the <code>ina32u.ini</code> file on every audited computer. This file contains the identification data for both the computer and the user. Since this information is required for subsequent audits. You can use environment variables (such as <code>%SYSTEMROOT%</code>) as part of the path specification. However, the path must be a local path. If the specified path does not exist or the <code>ina32u.ini</code> file can't be found there, the Inventory Analyzer ignores this option. Instead, the default location of the Windows system folder is used. If the logged on user doesn't have permissions to write to this folder, the root folder of the first available fixed disk is used.
<code>/cfg=[FileName]</code>	Specifies the configuration file for the Inventory Analyzer. The full path of the file is required; for example, <code>C:\audit\deployment\green.cfg</code> . You can use environment variables in the path.
<code>/log=[Path]</code>	Specifies the output directory for log files. You can use environment variables in the path.
User ID Options	
<code>/user=[FullName]</code>	Specifies (overrides) the user's full name. When this option is used without the <code>/userid</code> option, user information will not be collected from the Active Directory.
<code>/userid=[LoginName]</code>	Specifies (overrides) the user's login name.
<code>/email=[Email]</code>	Specifies (overrides) the user's e-mail address.

/nameformat=[Format]	<p>Specifies the format for the user's full name.</p> <p>The \$FN\$ and \$LN\$ placeholders designate the placement of the first name and last name respectively. If the format contains spaces, it must be enclosed in double quotes.</p> <p>Example:</p> <p>"\$LN\$, \$FN\$" — outputs "Doe, John"</p> <p>"\$FN\$ \$LN\$" — outputs "John Doe"</p>
Mode Options	
/q or /silent	Forces the Inventory Analyzer to run in the silent mode.
/i or /interactive	Forces the Inventory Analyzer to run in the interactive mode.
Inventory Options	
/forceinventory	Forces an immediate hardware and software inventory, ignoring the schedule from the audit configuration file (ina32.cfg) and exclusion rules for computers and users.
/forcescan	Forces an immediate file scan, ignoring the file scan schedule from the audit configuration file (ina32.cfg) and exclusion rules for computers and users.
/force	Forces an immediate audit process, ignoring any schedule settings and exclusion rules from the audit configuration file (ina32.cfg). This option is a combination of the /forceinventory and /forcescan options.
/auditdelay=[Delay]	<p>Specifies the time delay in minutes before starting the audit process. If no value is specified, the time delay is set to 1 minute.</p> <p>Use this option to ensure that any resource-intensive tasks that may take place at logon are finished and the initialization is complete.</p>
/samba	Prevents the Inventory Analyzer from setting permissions to the audit data files. Use this option if your audit snapshot files are stored on a non-Windows file server.
/logsize=[Size]	Automatically rotates the log file when it reaches the specified size (in kilobytes)
Interactive Mode Options	
These options apply only when the Inventory Analyzer runs in the interactive mode and define the appearance of the Inventory Analyzer splash screen. When the Inventory Analyzer runs in the silent mode, these options are ignored.	
/nocancel	Hides the Cancel button.
/nosaveto	Hides the Save To option.
E-mail Options	

Any of the /smtp_* options forces the Inventory Analyzer to send audit snapshot files by e-mail. The /smtp_to and /smtp_server options are required to send e-mail, the rest of the e-mail options are optional.	
/smtp_to=[ToAddress]	Specifies the "To" e-mail address where audit snapshots should be sent.
/smtp_from=[FromAddress]	Specifies the "From" address.
/smtp_server=[ServerName]	Specifies SMTP server name.
/smtp_port=[PortNumber]	Specifies SMTP listening port. If this option is not specified, the default port number 25 is used for non-secure connection and 465 for secure connection.
/smtp_user=[UserID]	Specifies the user ID for authorization if the SMTP server requires authorization.
/smtp_password=[Password]	Specifies the password for authorization if the SMTP server requires authorization.
/UseSSL=[NO TLS SSL TRYTLS]	Forces the Inventory Analyzer to use SSL in e-mail related operations. If no other SMTP options are specified this option is ignored. Valid values: NO — uses non-secure connection TLS — establishes secure connection using TLS protocol, aborts connection if TLS is not available SSL — establishes secure connection using SSL protocol, aborts connection if SSL is not available TRYTLS — establishes secure connection using TLS protocol, establishes non-secure connection if TLS is not available.
/UseSPA	Forces the Inventory Analyzer to use Secure Password Authentication on the SMTP server. If no other SMTP options are specified this option is ignored.
/RejectInvalidCerts	Terminates the connection established via an TLS/SSL-encrypted channel when a certificate validation error occurs.

Linux Inventory Analyzer Command-Line options

You can use the Linux Inventory Analyzer command-line options for overriding the settings in the lina.ini configuration file and for applying some advanced options.

Option	Description
-h, --help	Prints the list of command-line options.
-m, --mail [EmailAddress]	Specifies the e-mail address where audit snapshots should be sent. Example: -m collector@example.com

Option	Description
-mf, --mail-from [EmailAddress]	Specifies the "From" address. Example: -mf sender@example.com
-of, --out-file [FileName]	Specifies the base name (without extension) of the audit snapshot. Example: -of example.adt
-od, --out-dir [Path]	Specifies the path to the folder where to store audit snapshots. Example: -od /var/audit/
-sp, --smtp-port [PortNumber]	Specifies the SMTP listening port. Example: -sp 25
-ss, --smtp-server [ServerName]	Forces the Linux Inventory Analyzer to send e-mail via SMTP server. Example: -ss smtp.example.com
-u, --username	Specifies the username for SMTP authentication. Example: -u jdoe
-p, --password	Specifies the password for SMTP authentication. Example: -p verysecret
-V, --version	Forces the Linux Inventory Analyzer to display the program version and exit.

Note that some parameters are mutually exclusive: either the output file or e-mail address can be specified, but not both.

If the output file is not explicitly specified in the `lina.ini` configuration file or with the `--out-file` command-line option, it is assigned automatically. The format is `hostname_MACaddress.adt`. If neither host name nor MAC address can be determined, then the Inventory Analyzer names the file `lina.adt`.

When run with the `--mail` command-line option, the Linux Inventory Analyzer looks for `sendmail` in `PATH`. If it is not there by default, you can use the following syntax:


```
PATH=/usr/local/lib:$PATH ./lina -m collector@example.com
```

The following values are used for illustrative purposes:

- `/usr/local/lib` – This is the folder where sendmail resides.
- `collector@example.com` – This is the e-mail address where to send the audit files.

To send audit snapshots from Linux machines by e-mail, you can use one of the following options:

- Send snapshots via a SMTP server. For details on specifying the SMTP server, see ["Building Inventory Analyzer packages for the Audit via E-mail" on page 84](#).
- Send snapshots using the Mail Transfer Agent (MTA). This option is used when the SMTP server is not specified. To send the snapshots using the MTA, execute `./lina -m collector@example.com` (make sure to replace the e-mail address with a real one) from the command line. The snapshots will be sent directly to the specified e-mail address via the sendmail-compatible MTA installed locally. Note that MTA can be used only when the SMTP server is not specified.



For details on installing MTA, see your Linux documentation or Linux Internet recourses.

Mac Inventory Analyzer Command-Line options

You can use the Mac Inventory Analyzer command-line options for overriding the settings in the `ina_mac.ini` configuration file and for applying some advanced options.

Option	Description
<code>-h, --help</code>	Prints the list of command-line options.
<code>-m, --mail [EmailAddress]</code>	Specifies the e-mail address where audit snapshots should be sent. Example: <code>-m collector@example.com</code>
<code>-mf, --mail-from [EmailAddress]</code>	Specifies the "From" address. Example: <code>-mf sender@example.com</code>
<code>-of, --out-file [FileName]</code>	Specifies the base name (without extension) of the audit snapshot. Example: <code>-of example.adt</code>

Option	Description
-od, --out-dir [Path]	Specifies the path to the folder where to store audit snapshots. Example: -od /var/audit/
-sp, --smtp-port [PortNumber]	Specifies the port for the SMTP server to listen on. Example: -sp 25
-ss, --smtp-server [ServerName]	Forces the Mac Inventory Analyzer use an SMTP server. Example: -ss smtp.example.com
-u, --username	Specifies the username for SMTP authentication. Example: -u jdoe
-p, --password	Specifies the password for SMTP authentication. Example: -p verysecret
-V, --version	Forces the Mac Inventory Analyzer to display the program version and exit.
-v, --verbose	Verbose output.

Note that some parameters are mutually exclusive: either the output file or e-mail address can be specified, but not both.

If the output file is not explicitly specified in the `ina_mac.ini` configuration file or with the `--out-file` command-line option, it is assigned automatically.

If you want to run `ina_mac` with `--mail` command-line option, you must configure and start a sendmail-compatible Mail Transfer Agent (for example, postfix) on each Mac machine, and the `PATH` environment variable should contain the sendmail directory. The postfix tool ships with OS but is not started by default. For details, see your macOS documentation or macOS Internet resources, such as <https://egopoly.com/2006/08/15/enable-postfix-mail-on-mac-os-x-tiger/>.

To send audit snapshots from Mac machines by e-mail, you can use one of the following options:

- Send snapshots via a SMTP server. For details specifying the SMTP server, see [“Building Inventory Analyzer packages for the Audit via E-mail” on page 84](#).

- Send snapshots using the Mail Transfer Agent (MTA). This option is used when the SMTP server is not specified. To send snapshots using the MTA, execute `./ina_mac -m collector@example.com` (make sure to replace an example e-mail address of the recipient with the real one) from the command line. The snapshots will be sent directly to the specified e-mail address via the sendmail-compatible MTA installed locally.



For details on configuring and starting postfix on Mac OS client machines, see your Mac OS documentation or Mac OS Internet resources such as <https://egopoly.com/2006/08/15/enable-postfix-mail-on-mac-os-x-tiger/>.

Report Designer

Alloy Discovery Express includes the following pre-configured reports:

- Asset Summary
- Asset Tag Stickers
- Assets by Operating System
- Assets by Platform
- Assets by Software
- Computer Cards
- Discovered but Not Audited
- Disk Usage
- SNMP Devices
- Software by Asset
- Software by Publisher
- Software Summary by Title
- Top 10 Software

To generate a report:

1. Select **Reports > [Report Name]** from the main menu.
2. Some reports require an additional input. If the **Report Options** dialog box opens, specify the required options for the report and click **OK**. The report preview dialog box opens.
3. You can view the report on the computer screen or send it to the printer. Additionally, you can export the report in one of the supported formats: PDF file, HTML file, RTF file, Excel (XML) file, CSV file, text file.

The *Alloy Discovery Express* reporting component is based on the FastReport designer (<https://www.fast-report.com>). You can access the Report Designer by selecting **Reports > Create Report** from the main menu of *Alloy Discovery Express*, or from the report preview dialog box by clicking **Design Report**.

The Report Designer contains its own Help system (Report Designer Help). Please refer to this help system for more information. To access this Help, open the FastReport designer (**Reports > Create Reports**), then select **Help > Help Contents** from the module's main menu.

CHAPTER 9. Troubleshooting

Troubleshooting the On-Demand Audit

Windows On-Demand Audit

Summary

The Windows On-Demand Audit feature relies on the hidden administrative share (ADMIN\$) that Windows uses to manage the computer environment on the network. Typically, computers that are running Windows automatically create the administrative share during the install of the operating system. Normally, the On-Demand Audit works right out of the box; however, the feature requires a few things to be in place.

This section will explain most common issues and known solutions for them. Some of these issues might have to do computers being audited (for details, see ["Remote Computers" on page 139](#)), other - with the computer hosting Alloy Discovery Express (for details, see ["Host Machine" on page 148](#)).

Remote Computers

The most common issues related to client computers are:

- [Administrative Shares are Disabled](#)
- [File and Printer Sharing Components are Disabled](#)
- [Configuration Issues Preventing Access to Administrative Shares](#)
- [Audit Account Does Not Exist on Client Computer](#)
- [Error Messages](#)

Administrative Shares are Disabled

Some administrators consider administrative shares a security risk and disable them completely. This is a result of certain vulnerabilities found in early versions of Windows. However, these were mostly issues with the local administrator password being blank, which allowed for unauthorized access to the administrative share.

Since then, Microsoft has restricted file sharing and significantly improved security. Today, with reasonable precautions in place, it is quite safe to have administrative shares enabled. Without them the On-Demand Audit will not work. Moreover, you may experience a variety of other issues unrelated to Alloy Discovery Express when administrative shares are unavailable. For details, see *Microsoft Knowledge Base article 842715 "Overview of problems that may occur when administrative shares are missing"* at <http://support.microsoft.com/kb/842715>.

File and Printer Sharing Components are Disabled

You will be unable to remotely audit Windows computers unless the File and Printer Sharing for Microsoft Networks component and the Server service is enabled there.

Make sure that the File and Printer Sharing for Microsoft Networks component is installed and enabled:

1. Select **Control Panel** from the Start menu.
2. Open the Network Connections folder:
 - 1) *For Windows XP*. Click **Network Connections**.
 - 2) *For Windows Vista or Windows Server 2008*:
 - 1) Start Network and Sharing Center:
 - If you use the **Control Panel Home** view, under the **Network and Internet** section, click **View network status and tasks**.
 - If you use the **Classic View**, double-click **Network and Sharing Center**.
 - 2) In the **Tasks** pane, click **Manage network connections**.
 - 3) *For Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016*:
 - 1) Start Network and Sharing Center:
 - In **Control Panel**, when **View by** is set to **Category**, click **Network and Internet**, and then click **Network and Sharing Center**.
 - In **Control Panel**, when **View by** is set to either **Large icons** or **Small icons**, click **Network and Sharing Center**.
 - 2) In the **Tasks** pane, click **Change adapter settings**.
3. Click the network connection associated with the LAN.
4. On the **General** tab, select **Properties** and verify that **File and Printer Sharing for Microsoft Networks** appears on the list of installed items (i.e. the check box next to this component is selected).

The File and Printer Sharing for Microsoft Networks component corresponds to a Windows network service named **Server**. Configure the **Server** service as follows:

1. In Control Panel, open **System and Security > Administrative Tools**, and then double-click **Services**.
2. Double-click the **Server** service.
3. Set the startup type to **Automatic**.
4. Make sure the service status is **Started**. Otherwise, click **Start**.

Please note that additional steps are required on computers running Windows Vista and above:

1. *For Windows Vista*:
 - 1) Open **Network and Sharing Center** dialog box (for example, click **Start**, right-click **Network**, then select **Properties**).

- 2) In the **Sharing and Discovery** section, click the down arrow next to **File sharing** and under **File sharing settings**, click **Turn on file sharing**. Click **Apply**.
 - 3) Set the Network Location Type to either Private or Domain as follows:
 - 1) To the right of the network name and location type, click **Customize**.
 - 2) In the **Set Network Location** dialog, click **Private** or **Domain**, and then click **Next**.
 - 3) In the **Successfully set network settings** dialog box, click **Close**.
2. *For Windows 7, Windows 8, Windows 8.1, or Windows 10:*
- 1) Start Network and Sharing Center (for example, in **Control Panel**, when **View by** is set to **Category**, click **Network and Internet**, then click **Network and Sharing Center**).
 - 2) In the **Network and Sharing Center** left pane, click **Change advanced sharing settings**. The **Advanced sharing settings** folder opens.
 - 3) In **Advanced sharing settings**, click the arrow next to the network profile that you want to configure (Home or Work).
 - 4) In **File and printer sharing**, click **Turn on file and printer sharing**. Then click **Save changes**.
 - 5) Set **Network Location Type** to **Home** or **Work** network profile as follows:
 - 1) In **Network and Sharing Center**, under the **View your active networks** section, click the link below the active network name. For example, if you have a network named **Network 1** and there is a link below the network name, click it. The **Set Network Location** dialog box opens.



If your network is a domain network and you are unable to change the network location, contact your network administrator.

- 2) In the **Set Network Location** dialog box, click **Work network** or **Home network**.
- 3) Review the summary of your network location, and then click **Close**.

Configuration Issues Preventing Access to Administrative Shares

Simple File Sharing

The Simple File Sharing feature is always turned on for Windows XP Home Edition. By default, Simple File Sharing is also turned on for Windows XP Professional when the computer is in a workgroup environment. Starting with Windows Vista, Simple File Sharing is not enabled by default.

When Simple File Sharing is turned on, access to the administrative share is disabled because all remote users authenticate as "Guest", and guest accounts do not have administrative rights. Therefore, you must turn off Simple File Sharing to allow the On-Demand Audit feature to work.

To turn off Simple File Sharing in Windows XP Professional, follow these steps:

1. Double-click **My Computer** on the desktop or select **My Computer** from the Start menu.
2. Select **Tools > Folder Options**.
3. Click the **View** tab, and then clear the **Use Simple File Sharing (Recommended)** check box.

Windows Firewall

Since the release of Windows XP SP2, the File and Printer Sharing component is blocked by default in Windows Firewall. This causes the *"Network path not found"* error message when attempting to perform the On-Demand Audit.

In order to allow the On-Demand Audit through Windows Firewall, you must enable the File and Printer Sharing exception in the Windows Firewall configuration. When client computers running Windows XP SP2 or later are part of an Active Directory domain, you can use Group Policy to change the Windows Firewall configuration on multiple computers at once.



In certain cases, the File and Printer Sharing exception in Windows Firewall may allow unauthorized access to your files, printers, and network.

For details, see *Microsoft Knowledge Base article 199346 "Disable File and Printer Sharing for Additional Security"* at <https://support.microsoft.com/kb/199346>.



The steps below show how to change the Windows Firewall Group Policy settings for a Windows Server 2008 R2 domain. Steps for Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 domain are very similar.

For details on enabling the File and Printer Sharing in a Windows Server 2003 R2 domain, see the Knowledge Base article KB002165 *"Enabling File and Printer Sharing component in Windows 2003 R2 Server based Active Directory domain"* on the Alloy Software Support Portal at <https://support.alloysoftware.com/?mode=page&aid=KB002165>. Steps for Windows Server 2003 domain are very similar.

To enable the File and Printer Sharing exception in Windows Firewall using Group Policy, follow these steps:

1. Log on to the domain controller.
2. Open the Microsoft Group Policy Management Console (for example, click **Start > Run**, type `gpmc.msc` in the text box, then click **OK**).
3. Determine what group of machines your policy is going to be applied to. The steps below show how to change the group policy for the entire domain.
4. In the console tree, right-click **Default Domain Controllers Policy** in **Domains\[Current Domain]**, and then click **Edit**.

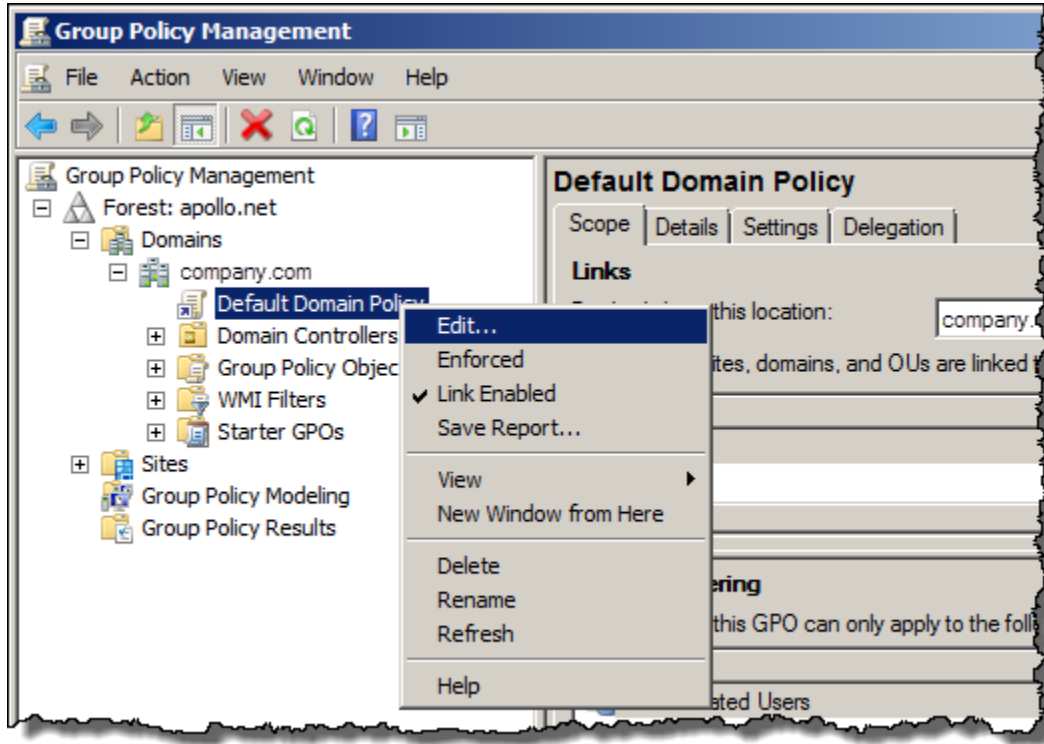


Figure 72: Accessing the default domain policy

The **Group Policy Management Editor** dialog box opens.

5. Navigate to **Computer Configuration > Policies > Administrative Templates: Policy definitions > Network > Network Connections > Windows Firewall**. The **Windows Firewall** area contains two sections: **Domain Profile** and **Standard Profile**. Domain computers will automatically determine which profile they should use by the type of network they are connected to:
 - *The domain profile* is a set of Windows Firewall settings that are needed when the computer is connected to the managed network. For example, the domain profile might contain settings for excepted traffic for the applications and services needed by a managed computer in an enterprise network.
 - *The standard profile* is a set of Windows Firewall settings that are needed when the computer is connected to another network. A good example is when a laptop is taken on the road and connects to the Internet using a public broadband or wireless Internet service provider. Because the laptop is directly connected to the Internet, the standard profile should contain more restrictive settings than the domain profile.

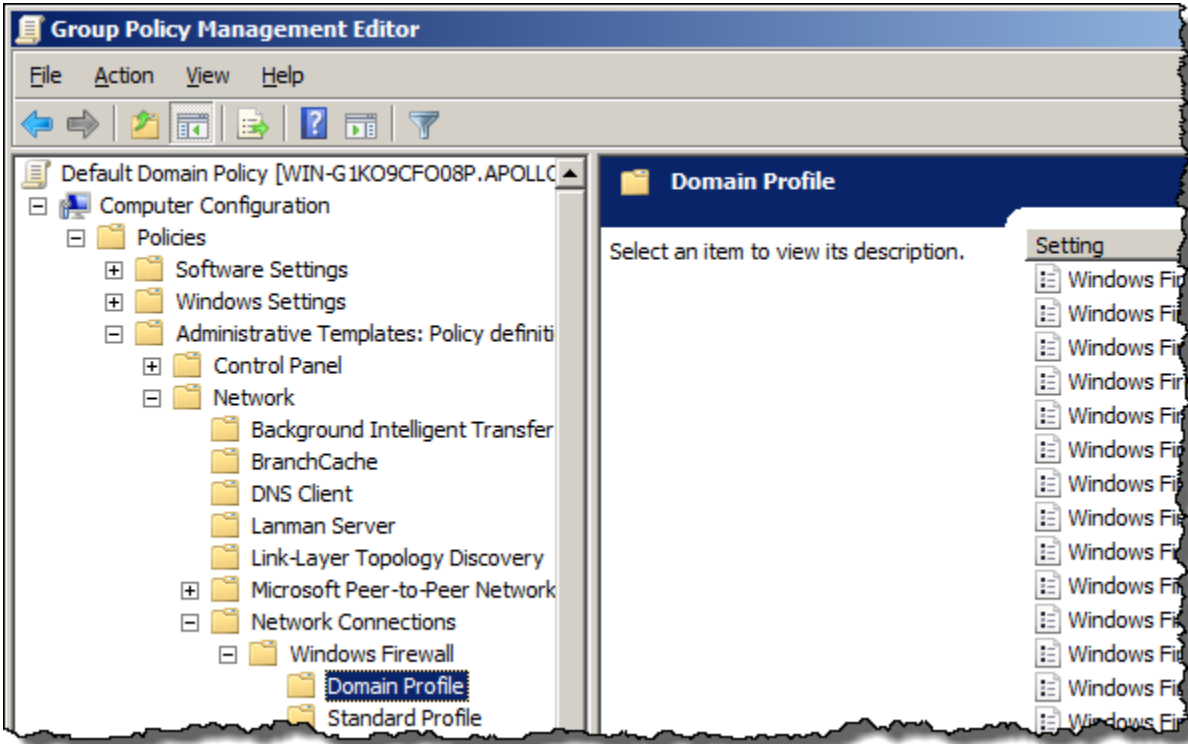


Figure 73: Accessing the domain profile

6. Select the appropriate profile. In the right pane, double-click the **Windows Firewall: Allow inbound file and printer sharing exception** item.

Setting	State
Windows Firewall: Allow local program exceptions	Not configured
Windows Firewall: Define inbound program exceptions	Not configured
Windows Firewall: Protect all network connections	Not configured
Windows Firewall: Do not allow exceptions	Not configured
Windows Firewall: Allow inbound file and printer sharing exception	Not configured
Windows Firewall: Allow ICMP exceptions	Not configured
Windows Firewall: Allow logging	Not configured
Windows Firewall: Prohibit notifications	Not configured
Windows Firewall: Allow local port exceptions	Not configured
Windows Firewall: Define inbound port exceptions	Not configured
Windows Firewall: Allow inbound remote administration exception	Not configured
Windows Firewall: Allow inbound Remote Desktop exceptions	Not configured
Windows Firewall: Prohibit unicast response to multicast or broad...	Not configured
Windows Firewall: Allow inbound UPnP framework exceptions	Not configured

Figure 74: Selecting the profile item

The **Windows Firewall: Allow inbound file and printer sharing exception** dialog box opens.

- Click **Enabled**. Under **Options**, enter a filter value to tell the group policy which computers are allowed to connect to the machine. Use * to allow all computers to connect.

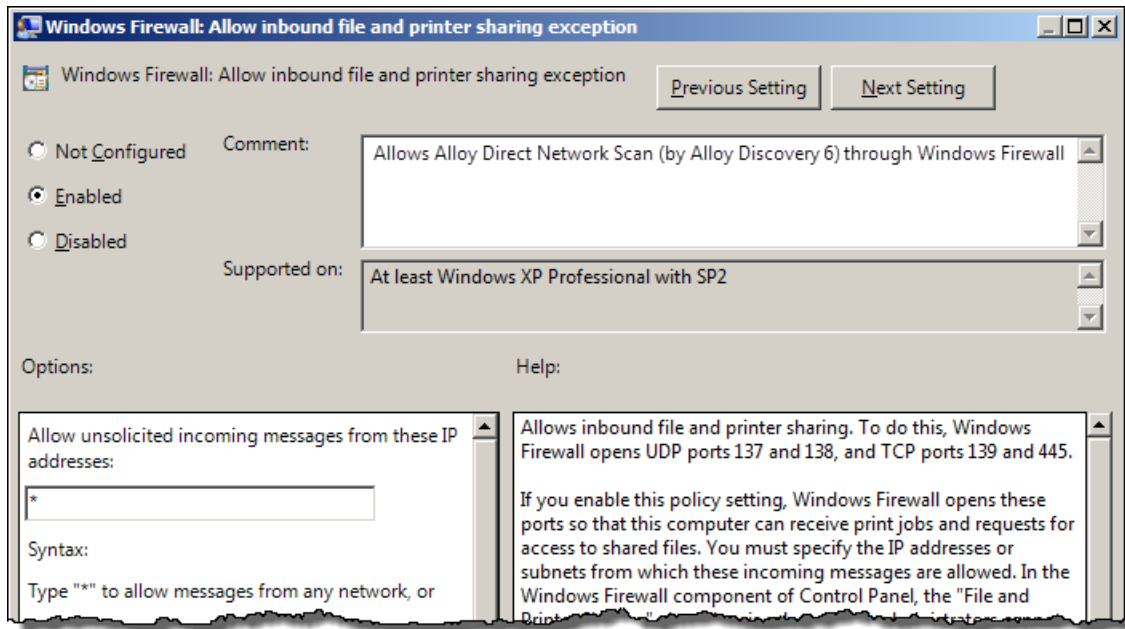


Figure 75: Enabling the File and Printer Sharing Exception

- Click **OK**. After about 30 minutes your computers should pick up the new policy.



On a client machine, you can immediately refresh Group Policy settings by going to the command line and typing in the following command:
`GPUPDATE /force`

After the new policy has been applied, you will see the **File And Printer Sharing** item (it will appear dimmed) in the list of Windows Firewall exceptions on domain computers. To access the list of Windows Firewall exceptions, open Control Panel, open Windows Firewall, and click **Allow a program or feature through Windows Firewall**.

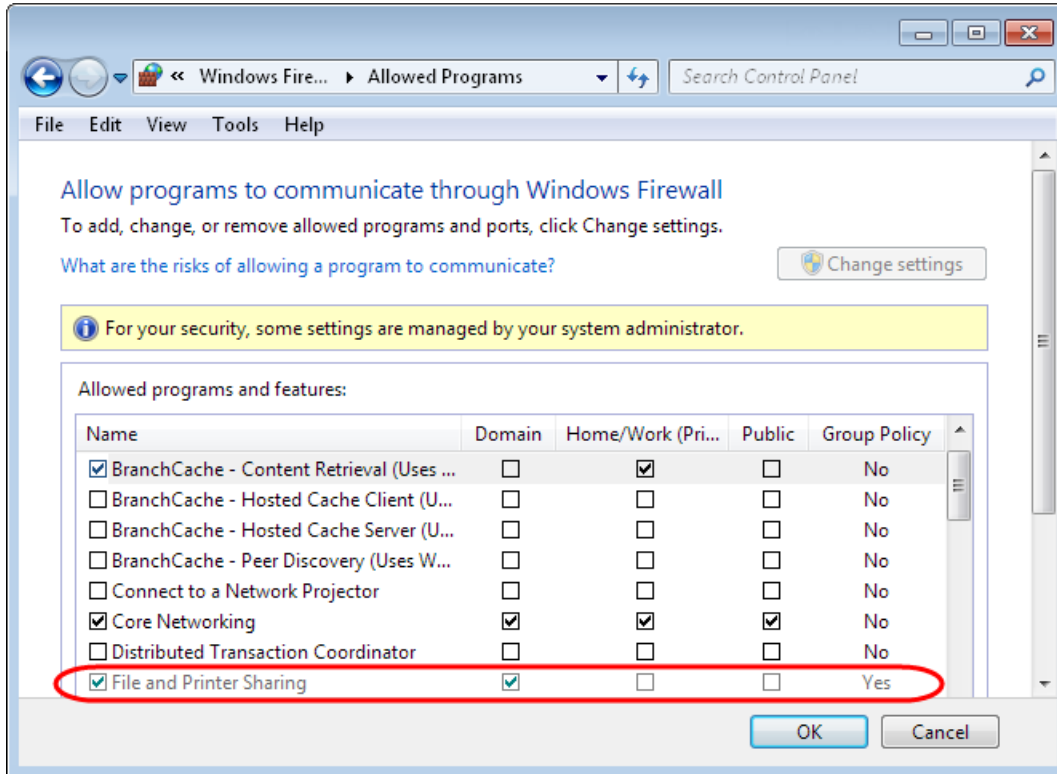


Figure 76: Viewing the File and Printer Sharing firewall exception on a Windows 7 computer

Third-Party Firewall Products

Third-party firewall products may also close the ports used for file and print sharing to prevent Internet computers from accessing your resources. In order to allow the On-Demand Audit through a firewall between the Alloy Discovery Express host machine and remote computers, open the ports for your local network.



For details, see *Microsoft Knowledge Base article 298804 "Internet firewalls can prevent browsing and file sharing"* at <http://support.microsoft.com/kb/298804/>.

User Account Control (UAC) - Windows Vista and above

User Account Control (UAC) is a security component introduced in the Microsoft Windows Vista operating system. UAC enables users to perform common tasks as non-administrators, called standard users in Windows Vista, and as administrators without having to switch users, log off, or use Run As. Microsoft developed the UAC feature in Windows Vista to prevent silent installation of malware. UAC is enabled by default. Windows 7, Windows 8, Windows 8.1, and Windows 10 have inherited UAC from Windows Vista.

UAC also affects remote connections to computers. When a local user account is used to connect to a machine, the user is identified as a standard user even if the account is in the Administrators group. Since regular users do not have administrative rights, the system refuses access to administrative shares and the On-Demand Audit fails.

The method of solving this issue depends on whether you are connecting to remote computers in a domain or in a workgroup, since this determines whether UAC filtering is enabled.

If your computer is part of a Windows domain network, the audit credentials used by the On-Demand Audit should be for a domain account that is in the local Administrators group on the remote computer because UAC does not affect domain accounts in the local Administrators group. Do not use a local, non-domain account on the remote computer, even if it is in the Administrators group. In a workgroup, you must disable UAC for remote connections (remote UAC) by changing the registry entry that controls remote UAC.

Disable remote UAC as follows:

1. Start Registry Editor: Click **Start**, type `regedit` in the **Start Search** field, and then click **regedit.exe** in the **Programs** list.
2. Locate and then click the following registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type `LocalAccountTokenFilterPolicy` for the name of the DWORD, and then press ENTER.
5. Right-click **LocalAccountTokenFilterPolicy**, and then click **Modify**.
6. In the **Value data field**, type `1`, and then click **OK**.
7. Exit Registry Editor.

Both solutions are a security risk. However, the latter may be necessary in a workgroup environment.

Other Issues

This section applies to Windows XP SP2 and higher.

Access to administrative shares and file sharing may also fail for the following reasons:

1. Windows will deny access under accounts with a blank password.
2. Windows will deny access if there are DNS issues related to the name of the host machine or the IP address of the client machine. For example, the name of the DNS entry for the host machine must match its computer name, and the IP address of the client machine must be unique within the DNS. If there is an issue with your DNS configuration, audit snapshots for computers with identical names overwrite each other in the Inventory Repository.

Audit Account Does Not Exist on Client Computer

We recommend that you use credentials for a domain administrative account for the On-Demand Audit of Windows computers. If you use a local account (for example, in a non-domain network), must be a member of the local Administrators group.



For details, see ["Managing Audit Credentials" on page 51](#).

The administrative account must exist on the Host Machine (see ["Audit Account Does Not Exist on the Host Machine" on page 150](#)) and on every client computer you want audited. Otherwise, the On-Demand Audit may fail with the following error messages:

Failed: Error connecting to host (Error 5. Access is denied)

Failed: Error connecting to host (Error 1331. This user can't sign in because this account is currently disabled)

As a workaround, on the client computer, create the account that you use for the On-Demand Audit, and add this account to the local Administrators group.

Error Messages

When the operating system denies access to the administrative share due to authentication - or network-related issues, Windows will report a generic error code. Keep in mind that in some cases this error code and the corresponding system error message may not reflect the actual cause of the failure and be misleading.

Troubleshooting Administrative Shares

Microsoft offers a guide for troubleshooting file and printer sharing in Windows which is available for download at Microsoft Download Center.

File Name: FP_Tshoot.doc

Title: **Troubleshooting File and Printer Sharing in Microsoft Windows XP**

Host Machine

The most common issue and known solution referring to the host machine is the following:

- [Client for Microsoft Networks Component is Disabled](#)
- [Audit Account Does Not Exist on the Host Machine](#)
- [Audit Account Does Not Exist on Client Computer](#)

Client for Microsoft Networks Component is Disabled

On computers running Windows XP / Windows Server 2003 or later, you are unable to remotely audit computers when the Client for Microsoft Networks component and Workstation service is not installed and configured.

Make sure that the Client for Microsoft Networks component is installed and enabled as follows:

1. Select **Control Panel** from the Start menu.
2. Open the Network Connections folder:
 - 1) *For Windows XP.* Click **Network Connections**.
 - 2) *For Windows Vista or Windows Server 2008:*
 - 1) Start Network and Sharing Center:
 - If you use the **Control Panel Home** view, under the **Network and Internet** section, click **View network status and tasks**.
 - If you use **Classic View**, double-click **Network and Sharing Center**.
 - 2) In the **Tasks** pane, click **Manage network connections**.
 - 3) *For Windows 7 and above:*
 - 1) Start Network and Sharing Center:
 - In **Control Panel**, when **View by** is set to **Category**, click **Network and Internet**, and then click **Network and Sharing Center**.
 - In **Control Panel**, when **View by** is set to either **Large icons** or **Small icons**, click **Network and Sharing Center**.
 - 2) In the **Tasks** pane, click **Change adapter settings**.
3. Click the network connection associated with the LAN.
4. On the **General** tab, select **Properties** and verify that **Client for Microsoft Networks** appears on the list of installed items (i.e. the check box next to this component is selected).

The Client for Microsoft Networks component corresponds to Windows network service **Workstation**. Configure the **Workstation** service as follows:

1. In Control Panel, open **System and Security > Administrative Tools**, then double-click **Services**.
2. Double-click the **Workstation** service.
3. Set the startup type to **Automatic**.
4. Make sure that the service status is **Started**. Otherwise, click **Start**.

Audit Account Does Not Exist on the Host Machine

We recommend that you use credentials for a domain administrative account for the On-Demand Audit of Windows computers. If you use a local account (for example, in a non-domain network), such account must be a member of the local Administrators group.



For details, see ["Managing Audit Credentials" on page 51](#).

The administrative account must exist on every client computer you want audited (see ["Audit Account Does Not Exist on Client Computer" on page 148](#)) and on the Host Machine. Otherwise, the On-Demand Audit may fail with the following error messages:

Failed: Error connecting to host (Error: 1331. Logon failure: account currently disabled)

Failed: Error starting the audit ([...] Error: 1327. Logon failure: user account restriction. Possible reasons are blank passwords not allowed, logon hour restrictions, or a policy restriction has been enforced

As a workaround, on the computer hosting Alloy Discovery Express, create an account which you will use for the On-Demand Audit, and add this account to the local Administrators group.

Linux and Mac On-Demand Audit

Incorrect SSH Protocol Configuration for Linux and Mac

The On-Demand Audit of Linux and Mac computers, Alloy Discovery Express establishes connection to the audited computers using the Secure Shell protocol (SSH). By default, the standard TCP port 22 is used. However, you can supply a different port number when you specify audit credentials.



For details, see ["Specifying Default Audit Credentials for Linux and Mac Computers" on page 52](#), ["Creating On-Demand Audit Groups" on page 56](#), and ["Specifying Individual Audit Credentials" on page 114](#).

Make sure that all remote computers have the SSH server running. Otherwise, the On-Demand Audit will fail.

If you want to use a SSH private key instead of a password, make sure the SSH public/private key pair is properly set up and the public key is uploaded to all Linux and Mac computers you want to audit. For more information on SSH public key authentication, see: <http://the.earth.li/~sgtatham/putty/0.58/html/doc/Chapter8.html>.

Incorrectly Recognized Operating System

Before starting the On-Demand Audit, Alloy Discovery Express performs the discovery operation to enumerate computers within the specified audit scope. An important phase of discovery is the identification of the

computer's operating system, because the operating system type determines how On-Demand Audit, Alloy Discovery Express will later audit the computer.



Computers with unrecognized operating systems can still be audited only if you assign the appropriate On-Demand Audit Credentials. For details, see ["Specifying Default Audit Credentials for Linux and Mac Computers" on page 52.](#)

There can be rare cases when the operating system of a Linux or Mac computer is recognized incorrectly or remains unrecognized. Specifically, a Linux machine running a Samba service sometimes may be recognized as a Windows computer. In this case, the computer cannot be audited. You can solve this problem by assigning the operating system type by hand:

1. In Alloy Discovery Express, in the Sidebar, locate the problematic computer and right-click its record, then choose Properties from the pop-up menu. The [**Computer Name**] - **Audit Properties** dialog box opens.
2. Review the **Operating System** field value. If you need to correct it, select a value from the drop-down list.
3. Click **OK**.
4. Audit the computer again.

Extended Hardware Information Is Not Collected

In order to access low-level hardware information (hardware serial numbers and asset tags) from a Linux system during the On-Demand Audit, the user account used for auditing the system must have root privileges. This is due to the fact that this information is retrieved from the BIOS storage and root privileges are required to get access to the BIOS. The implementation of the On-Demand Audit relies on the `dmidecode` command to read BIOS data hence root privileges are only required to run this command.



For details, see ["Specifying Default Audit Credentials for Linux and Mac Computers" on page 52.](#)

If you want to collect extended hardware information, make sure that `dmidecode` is installed on each Linux computer you want audited. You may need to install the `dmidecode` package via your Linux package manager.

Some administrators consider providing credentials for the root account a security risk. The instructions below provide two methods of configuring the `dmidecode` command to run with elevated (root) privileges, which allows the On-Demand Audit to collect extended hardware information using audit credentials for a non-root account. These instructions have been tested using the Ubuntu Linux distribution. For other distributions the procedure should be very similar.

Setting the `setuid` bit on the `dmidecode` file

1. Log in to the client Linux machine.
2. Open a console dialog box.

- Find the `dmidecode` file (typically, it is in the `/usr/sbin/` folder):

```
which dmidecode
```

- Get root privileges. For example:

```
sudo su
```

- Make sure the `dmidecode` file is owned by `root:root`:

```
ls -l /usr/sbin/dmidecode
```

If it is, the output will contain "root" twice. For example:

```
-rwxr-xr-x 1 root root 42812 2008-04-04 02:42 /usr/sbin/dmidecode
```

If it is not, set the ownership to `root:root`:

```
chown root:root /usr/sbin/dmidecode
```

- Set the `setuid` bit for the `dmidecode` file:

```
chmod 4755 /usr/sbin/dmidecode
```

After doing this, any users or processes running the `dmidecode` file will have permissions of its owner, within the executed process. Since the owner is set to `root`, `dmidecode` will run with root privileges.

- Test that the `dmidecode` command runs as `root` under a non-root user account. For example, by running the following:

```
dmidecode -u
```

If `dmidecode` runs as `root`, this command will return SMBIOS data.



The `setuid` bit is disabled on many Linux implementations due to security reasons. If `dmidecode` does not run as `root` with the `setuid` bit set, chances are that your Linux distribution has `setuid` disabled.

Using the `sudo` command

The `sudo` command offers another approach to giving users root access. When trusted users precede an administrative command with `sudo`, they are prompted for their own password. Once authenticated, the administrative command is executed as if by the `root` user, assuming the command is permitted.

However, `sudo` can be configured not to ask for the user's password.

In order to run the `dmidecode` command with root privileges using the `sudo` approach, a bit of tweaking is needed:

- Log in to your Linux machine and open a console dialog box.

2. Get root privileges. For example,

```
sudo su
```

3. Find the location of your `sudo` and `dmidecode` files. Typically, they are both in the `/usr/sbin` folder:

```
which sudo
which dmidecode
```

4. Add the user account that you intend to use as a dedicated audit account to the `sudoers` list on the client Linux machine. To do so, edit the `/etc/sudoers` file and add the following line:

```
username ALL=(root)NOPASSWD:/usr/sbin/dmidecode2
```

Where *username* is a user name of the dedicated audit account.

This allows the dedicated audit account to run the `/usr/sbin/dmidecode2` command as root using the `sudo` command on any host without being asked for the password.

5. Rename the original `dmidecode` file to `dmidecode2`:

```
mv /usr/sbin/dmidecode /usr/sbin/dmidecode2
```

6. Run the following commands to create a new script file named `od`:

```
echo '#!/bin/bash' > /usr/sbin/dmidecode
echo '/usr/sbin/sudo /usr/sbin/dmidecode2 "$@"' >> /usr/sbin/dmidecode
chown root:root /usr/sbin/dmidecode
chmod 755 /usr/sbin/dmidecode
```

7. Test that the `dmidecode` command is now replaced with the `dmidecode` script. For example, run the following command:

```
dmidecode -u
```

If the `sudoers` file is configured correctly, this command will output SMBIOS data.

8. To test remote execution, run the following from the machine on which Alloy Discovery Express is installed:

```
"C:\Program Files\Common Files\Alloy Shared\RemoteAudit\bin\plink.exe"
-batch -t -l username -pw password 192.168.0.1 "dmidecode -u"
```

Where

- `"C:\Program Files\Common Files\Alloy Shared\RemoteAudit\bin\plink.exe"` is the path to the `plink.exe` file,
- *username* is the username of the dedicated audit account,
- *password* is the password for the dedicated audit account,
- `192.168.0.1` is the IP address of the audited Linux machine.

If this command returns SMBIOS data, you will be able to run On-Demand Audit of the computer remotely.



If there are some issues with the `dmidecode` command in your environment, preventing the On-Demand Audit from locating or using this command, it will attempt to access the BIOS storage using the `od` command. Using `od` is not recommended due to its limitations with memory access, and can serve only as a last resort.

The `od` command requires the same privileges as `dmidecode`.

Hypervisor On-Demand Audit

Incorrectly Recognized Hypervisor Type

Before starting the On-Demand Audit, Alloy Discovery Express performs the discovery operation to identify computers within the specified audit scope. Alloy Discovery Express supports multiple types of hypervisors and in most cases automatically identifies them during the discovery operation. However, there can be rare cases when the hypervisor type is defined incorrectly or remains undefined, which prevents a successful audit of the hypervisor and its association with hosted virtual machines. In such cases, you can check whether Alloy Discovery Express has identified the hypervisor type correctly as follows:

1. Alloy Discovery Express locates the problematic hypervisor in its respective audit group and right-click this record, then choose **Properties** in the pop-up dialog box. The computer's audit properties dialog box opens.
2. Review the value displayed in the **Hypervisor** field. If you need to correct it, select the correct value from the drop-down list.
3. If you have selected **VMware ESX** or **VMware ESXi** as hypervisor type, you can also modify the connection settings for these hypervisors in the **ESX/ESXi Options** tab.



For details, see ["Specifying Connection Parameters for VMware ESX / ESXi Hypervisors" on page 93](#).

4. Click **OK**.
5. After correcting the hypervisor type, audit the computer again.

Incorrect SSH Protocol Configuration for Linux-based Hypervisors

In order to perform the On-Demand Audit of hypervisors based on Linux (VMware ESX, Xen, Citrix XenServer), Alloy Discovery Express attempts to establish the connection with the server using the Secure Shell Protocol (SSH).

By default, Alloy Discovery Express accesses Linux-based hypervisors over the standard port (22). However, if the SSH server on your hypervisors listens on a non-standard TCP port, you can specify a different port number when configuring audit credentials.



For details, see ["Specifying Default Audit Credentials for Linux and Mac Computers" on page 52](#), ["Creating On-Demand Audit Groups" on page 56](#), and ["Specifying Individual Audit Credentials" on page 114](#).

Before performing an On-Demand Audit of a Linux-based hypervisor (other than VMware ESX or VMware ESXi), make sure that the hypervisor runs the SSH server. Otherwise, the On-Demand Audit will fail.



When On-Demand Audit via SSH fails for a VMware ESX hypervisor, Alloy Discovery Express audits it using the WS-Management protocol. VMware ESXi hypervisors can be audited via WS-Management protocol only. For details, see ["Specifying Connection Parameters for VMware ESX / ESXi Hypervisors" on page 101](#).

Microsoft .NET Framework 4.6.1 Is Missing

The On-Demand Audit of computers running VMware ESXi hypervisors requires that the computer hosting Alloy Discovery Express has Microsoft .NET Framework 4.6.1 or later installed. This component is also required when hypervisors running VMware ESX have their SSH service turned off.



Windows 10 and Windows Server 2016 include .NET Framework 4.6.1 or later. Therefore, you do not have to install Microsoft .NET Framework 4.6.1 if you have one of these operating systems.

Incorrect Connection Parameters for VMware ESX/ESXi Hypervisors

When SSH protocol is disabled on a VMware ESX hypervisor, Alloy Discovery Express attempts to establish connection using the WS-Management protocol over HTTP or HTTPS. The audit of VMware ESXi hypervisors cannot be performed via SSH and is always performed via WS-Management protocol.

Therefore, if the On-Demand Audit fails for a VMware ESXi hypervisor or a VMware ESX hypervisor with disabled SSH, check the WS-Management parameters.



For details, see ["Specifying Connection Parameters for VMware ESX / ESXi Hypervisors" on page 101](#).

After correcting the connection parameters, audit the hypervisor again.

Troubleshooting Agent-Based Audit

Alloy Discovery Express offers three agent-based audit methods: Scriptable Audit, Audit via E-Mail, and Portable Audit. Those methods involve deploying the Inventory Analyzer to a target network or to a flash drive and launching the audit from the deployment location.



For details, see ["Overview of Audit Methods" on page 5](#).

Alloy Discovery Express supports the agent-based audit of all supported types of hypervisors, except for VMware ESXi, which can be audited only via the On-Demand Audit. The agent-based audit of hypervisors is performed using the same standalone audit agents that are used for regular computers. Thus, please refer to the section corresponding to the operating system of your hypervisor, if its agent-based audit is not working as expected.

Windows Audit

In some cases, the standalone Windows Inventory Analyzer (`ina32.exe`) may not work as expected. For instance, it may be unable to collect some information about the computer, or in some rare cases it may terminate with an error message. Usually this indicates a problem with the operating system, device driver, or hardware. To resolve such issues, contact Alloy Software Technical Support. Before contacting, you should prepare troubleshooting information for the Technical Support representatives as follows:

1. Build a debug version of the Inventory Analyzer package and deploy it to a flash drive:
 - 1) In the Sidebar, right-click the E-mail Audit Group and choose Properties from the pop-up menu.
 - 2) On the **General** tab of the group's properties dialog box, click **Create**.
 - 3) On the **Welcome** page of the Portable Audit Wizard, click **Next**. The **Operating System** page opens.
 - 4) Select **Windows (for auditing Windows computers)** check box, click **Next**.

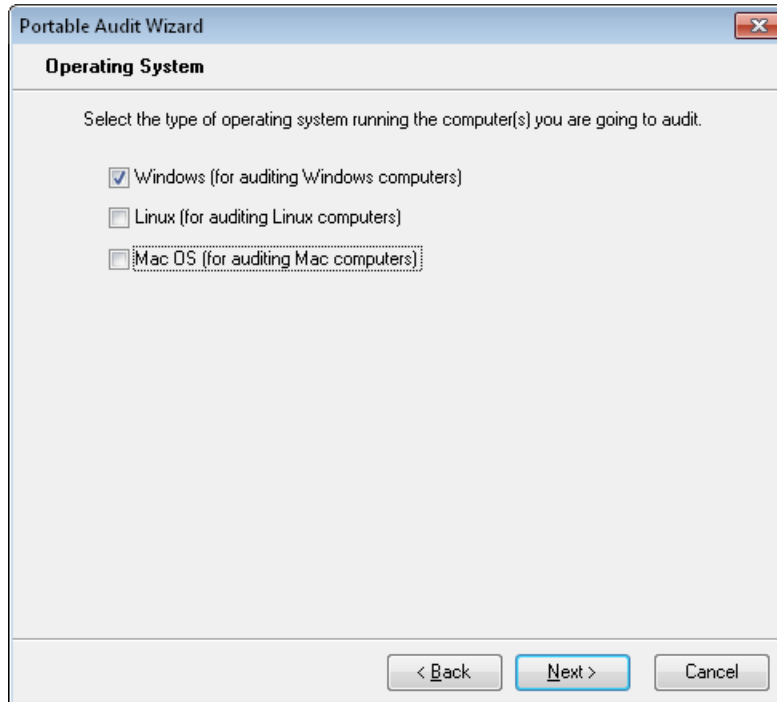


Figure 77: Creating a Windows Inventory Analyzer debug package

- 5) Complete the Portable Audit Wizard (for details, see ["Building Inventory Analyzer packages for the Audit via E-mail" on page 84](#)).
 - 6) Click **OK**. The created package contains the following files and folders:
 - `ina32.exe` — the Windows Inventory Analyzer executable file.
 - `ina32.cfg` — the configuration file for the Windows Inventory Analyzer.
 - `Log` — the folder in where the Windows Inventory Analyzer will store logged events and debug log files.
 - `AuditData` — the folder in which audit snapshots will be stored.
 - 7) Click **OK** to close the **Group [Group Name]** dialog box.
2. Modify the Windows Inventory Analyzer's configuration file:
 - 1) In the deployment folder, open the `ina32.cfg` file in a text editor.
 - 2) At the end of the `[Options]` section, add the following line:


```
Debug=1
```
 - 3) Save the `ina32.cfg` file.
 3. Run the Windows Inventory Analyzer from the flash drive on the client machine where the problem was encountered.

3. When the audit finishes, the audit snapshot is saved to the same flash drive in the `AuditData` folder. The log file and the debug log file are saved in the `Log` folder.
4. Compress the `AuditData` and `Log` folders into one archive file (for example, using WinZip or WinRAR).

Contact Alloy Software Technical Support by e-mail, describe the problem, and attach the archive file.



For details, see ["Contact Information" on page 161](#).

Linux Audit

In some cases, a standalone Linux Inventory Analyzer (`lina`) may not work as expected. For instance, it may be unable to collect some information about the computer, or in some rare cases it may terminate with an error message. Usually this indicates a problem with the operating system, device driver, or hardware. To resolve such issues, contact Alloy Software Technical Support. Before contacting, you should prepare troubleshooting information for the Technical Support representatives as follows:



Note that `$(hostname)` is a command and it must be used as is; do not replace "hostname" with the computer name.

1. Open the terminal.
2. Change working directory to the `lina` folder:


```
cd <path_to_lina>
```
3. Run `lina` in the debug mode:


```
sudo ./lina -n -d -w $(hostname).bin -of $(hostname).adt
```
4. Wait until the information message is displayed confirming that the audit snapshot file has been created. Three output files should be created in the current folder:

- `<your_computer_name>.adt`
- `<your_computer_name>_Debug.log`
- `<your_computer_name>.bin`

Note that `<your_computer_name>` is the computer name.

5. Compress the created files into the `<your_computer_name>.tgz` archive file:

```
tar czvf $(hostname).tgz $(hostname)*
```

Contact Alloy Software Technical Support by e-mail, describe the problem and attach the archive file.



For details, see ["Contact Information" on page 161](#).

Mac Audit

In some cases, a standalone Mac Inventory Analyzer (`ina_mac`) may not work as expected. For instance, it may be unable to collect some information about the computer, or in some rare cases it may terminate with an error message. Usually this indicates a problem with the operating system, device driver, or hardware. To resolve such issues, contact Alloy Software Technical Support. Before contacting, you should prepare troubleshooting information for the Technical Support representatives as follows:



Note that `$(hostname)` is a command and it must be used as is; do not replace "hostname" with the computer name.

1. Open the terminal.
2. Change directory into your `ina_mac` directory:

```
cd <path_where_'ina_mac'_resides>
```

3. If you use the `ina_mac.ini` file to store your Mac OS audit settings and it includes the `out-dir` key, you need to temporarily comment the key (just add the semicolon character at the start of the line) in order for the next step to work as expected.
4. Run `ina_mac` in the debug mode:

```
ina_mac -w $(hostname).spx -of $(hostname).adt &> $(hostname).log
```

Wait until the information message is displayed confirming that the audit snapshot file has been created. Three output files should be created in the current folder:

- `<your_computer_name>.adt`
- `<your_computer_name>.spx`
- `<your_computer_name>.log`

Note that `<your_computer_name>` is the computer name.

5. Compress all the created files into the `<your_computer_name>.tgz` archive file:

```
tar czvf $(hostname).tgz $(hostname)*
```


Contact Alloy Software Technical Support by e-mail, describe the problem and attach the archive file.



For details, see ["Contact Information" on page 161.](#)

CHAPTER 10. Contact Information

About Alloy Software

Established in 2002, Alloy Software, Inc. is a leading provider of service management, asset management, and network inventory software solutions that help organizations of all sizes automate IT operations. For more information, visit our website at <https://www.alloysoftware.com/>.

Follow Us

Follow us on Twitter, Facebook, or LinkedIn to stay on top of the latest events and developments regarding Alloy Software.

- Twitter: <https://twitter.com/AlloySoftware>
- Facebook: <https://www.facebook.com/Alloy-Software-121393101252093/>
- LinkedIn: <https://www.linkedin.com/company/alloy-software/>

Obtain Technical Support

Using the online Support Portal you can manage your support tickets, download product updates and search our product Knowledge Base which includes a comprehensive collection of searchable articles, answers, tips, tricks, videos and solutions from our Technical Services team.

- Alloy Software Support Portal: <https://support.alloysoftware.com>

Contact Us

We want to hear from you! Contact us online, by e-mail, phone, fax, or regular mail using the contact information below.

Online

Use our short **Contact Us** form to leave a question, comment, or concern, and we will get back to you within one business day.

- Contact Alloy Software online: <https://www.alloysoftware.com/company/contact-us/>

E-Mail

Sales and licensing:	sales@alloysoftware.com
Technical support:	support@alloysoftware.com
General inquiries:	admin@alloysoftware.com

Phone

US and Canada:	(800) 810-9020
International:	+1 (973) 661-9700

Fax

US and Canada:	(866) 422-1658
International:	+1 (973) 661-9777

Mailing Address

All correspondence:	Alloy Software, Inc. 400 Broadacres Dr, Suite 100 Bloomfield, NJ 07003 USA
---------------------	---

CHAPTER 11. **Glossary**

This chapter explains terms used throughout this document.

A

Audit

Audit is the process of collecting hardware and software information from computers. The audit results are stored in audit snapshot files.

Audit Agent

An audit agent is a tool that captures the information about hardware configurations and installed software, and produces audit snapshots. The audit agent of *Alloy Discovery Express* the Inventory Analyzer. There are three platform-dependent versions of the Inventory Analyzer: Windows Inventory Analyzer, Linux Inventory Analyzer, and Mac Inventory Analyzer.

Audit Configuration

Audit configuration is a combination of options that define how to collect the data is collected during the audit.

Audit Snapshot

Audit snapshots contain information about an individual computer or network device. This information is collected during the audit and optionally supplemented with data entered in user-defined fields.

An audit snapshot can consist of four files:

- .adt file contains the hardware and basic-level software information;
- .scn file (optional) contains the results of the detailed and summary file scans;
- .snmp file (optional) contains SNMP data;
- .udf file (optional) contains the values specified for user-defined fields.

All audit snapshot files are located in the Inventory Repository. You can view audit snapshots in Alloy Discovery Express or in the standalone Audit Snapshot Viewer.

Audit Snapshot Viewer

Audit Snapshot Viewer is an Alloy Software tool for displaying audit snapshots in a convenient form. *Alloy Discovery Express* uses the Audit Snapshot Viewer to display the content of audit snapshots in the Main Console. The Audit Snapshot Viewer can also be used as a standalone tool for viewing audit

snapshots from the command line.

This tool is installed into the \\Program Files\Common Files\Alloy Shared\AuditViewer\Bin\ folder; the name of its executable file is `AdtViewer.exe`.

Audit Group

Audit group is a combination of nodes sharing a single audit method. There are the following types of audit groups: On-Demand Audit Groups, Scriptable Audit Groups, and E-mail Audit Groups.

Audit via E-mail

Audit via E-mail is an agent-based method of WAN audit. This method involves two steps: deploying the Inventory Analyzer package to the target network and (optionally) automating the Inventory Analyzer using domain logon scripts or scheduled tasks. In contrast to the Scriptable Audit method, there is no direct link between the host machine and the deployed audit agents. Audit snapshots are delivered directly to the host machine via e-mail. Also, any configuration changes or updated versions of the audit agent needs to be manually re-deployed.

B

Built-in Mode

The build-in mode does not require preliminary installation of the audit agent on remote computers. *Alloy Discovery Express* runs the audit agent from the Host Machine, interrogating client computers remotely. In order for the build-in mode to work, remote computers should be accessible over the local network.

Alloy Discovery Express uses the built-in mode for the On-Demand Audit of Windows, Linux, and Mac OS computers on the internal network.

C

Client Machine

Client machine is a computer tracked and audited with *Alloy Discovery Express*.

Computer Group

Computer group is a combination of computers for analyzing their audit results. A computer group can be either dynamic or static. Static groups can also include network devices.

D

Default On-Demand Audit Credentials

Default On-Demand Audit Credentials are the On-Demand Audit Credentials that are used by default for the On-Demand Audit if the target computer (or the target on-demand audit group) doesn't have custom credentials assigned.

Dynamic Group

Dynamic group is a computer group maintained by *Alloy Discovery Express* automatically, based on the inclusion criteria configured for the group.

E

E-mail Audit Group

E-mail Audit Group is an audit group created for the Audit via E-mail method.

External Audit Snapshot Source Group

External Audit Snapshot Source group is an audit group created to import audit snapshots from the designated source folder to the Inventory Repository. These groups are necessary to integrate *Alloy Discovery Express* with *Alloy Navigator*, when the audit facilities of *Alloy Navigator* are used to provide audit snapshots to *Alloy Navigator* and *Alloy Discovery Express*.

G

Group for the On-Demand Audit of an IP Address Range

Group for the On-Demand Audit of an IP Address Range is an audit group created for the On-Demand Audit of computers and network devices within a specified IP address range.

Group for the On-Demand Audit on a Windows Domain

Group for the On-Demand Audit on a Windows Domain is an audit group created for the On-Demand Audit of computers that belong to a specified Windows domain or a workgroup.

H

Hardware and Software Inventory

Hardware and Software Inventory is a collection of hardware configuration data and information about software products installed.

Host Machine

Host machine is the computer hosting *Alloy Discovery Express*.

Hypervisor

Hypervisor, also called virtual machine manager (VMM), is a specific software system that allows multiple operating systems, called guests or virtual machines, to run concurrently on a host machine and manages the host's processor, memory, and other resources allocated to each guest operating system. Hypervisors are typically installed on server hardware to host virtual machines that themselves act as servers.

I

Interactive Mode

Interactive mode is a method of running the audit allowing the audit agent to interact with the user. In this mode the Inventory Analyzer can be configured to ask the user for certain information, such as their name, location, or any other custom information. You can choose an audit mode for auditing Windows computers using the Scriptable Audit, Audit via E-mail, or Portable Audit methods.

Interactive Once Mode

Interactive Once mode is a combination of the Interactive mode and the Silent mode. In the Interactive Once mode, the users are prompted to enter their information only at the first run of the Inventory Analyzer. Subsequent audits run silently.

Note that in the Interactive Once mode the Inventory Analyzer will run interactively not only at the first audit, but also every time after you modify the audit configuration.

You can choose an audit mode for auditing Windows computers using the Scriptable Audit, Audit via E-mail, or Portable Audit methods.

Intermediary Repository

Intermediary Repository is a shared folder where the results by the Scriptable Audit are collected (typically, it is the /AuditData sub-folder of the shared folder designated for the Scriptable Audit Group).

Inventory Analyzer

Inventory Analyzer is the audit agent that *Alloy Discovery Express* uses for auditing computers. It captures the information about hardware configurations and installed software, and produces audit snapshots. There are three platform-specific versions of the Inventory Analyzer: Windows Inventory Analyzer, Linux Inventory Analyzer, and Mac Inventory Analyzer.

Inventory Analyzer Package

Inventory Analyzer Package consists of an Inventory Analyzer executable and a configuration file. The Inventory Analyzer is a deployable agent used for scriptable audits. It captures information about hardware configurations and installed software, within audit snapshots. There are separate Inventory Analyzers executable modules for Windows, Linux, and Mac operating systems.

Inventory Repository

Inventory Repository is a folder maintained by *Alloy Discovery Express* to store audit snapshots.

The Inventory Repository is located in the Repository sub-folder under the ProgramData folder where *Alloy Discovery Express* stores data for users: \\ProgramData\Alloy Software\Alloy Discovery Express\8.0\Repository\.

M

Minimally Necessary Permissions

Minimally necessary permissions are the permissions for the shared folder that are absolutely necessary for the *Inventory Analyzer* and *Alloy Discovery Express* to operate. They include the following permissions granted to the Everyone group:

Permission	Shared Folder (and all files in it)	Audit Snapshots Folder (and all files in it)	Log Folder (and all files in it)
Traverse Folder/Execute File	Yes		
List Folder/Read Data	Yes	Yes	Yes
Read Attributes	Yes	Yes	Yes
Read Extended Attributes	Yes	Yes	Yes
Create Files/Write Data	Yes	Yes	Yes
Create Folders/Append Data	Yes	Yes	Yes
Write Attributes	Yes		Yes
Write Extended Attributes	Yes		Yes
Delete Subfolders and Files		Yes	
Read Permissions	Yes	Yes	Yes
Change Permissions	Yes	Yes	Yes

Minimally necessary permissions are used for the Scriptable Audit and Audit via E-mail methods to create the most secure environment for the Shared Folder and audit snapshot files stored there.

O

On-Demand Audit

On-Demand Audit is an agentless method of auditing LAN Windows, Linux, and Mac OS X computers at user's request. Multiple networked computers that are members of a Windows domain or a workgroup can be audited simultaneously for up-to-the-minute audit snapshots. Network devices can also be discovered and audited using this audit method.

On-Demand Audit Credentials

On-Demand Audit Credentials are a combination of a user name and password for an administrative account, which is used for the On-Demand Audit.

On-Demand Audit Group

On-Demand Audit group is an audit group created to audit computers and devices on demand. Each On-Demand Audit group is defined by specifying either a Windows domain (Group for the On-Demand Audit on a Windows domain) or an IP address range (Group for the On-Demand Audit of an IP address range).

P

Portable Audit

Portable Audit is an agent-based method of auditing computers on locked-down networks and non-networked computers. Typically, the audit agent is deployed to a flash drive, which is used to audit individual computers in walk-around mode. Audit snapshots are stored on the same flash drive and then manually transported into the main Inventory Repository.

S

Scriptable Audit

Scriptable Audit is an agent-based method of LAN audit. Using this method you can audit networked computers on a regular basis. It involves two steps: the deployment of the Inventory Analyzer to a network share, and its automation using domain logon scripts or scheduled tasks. Audit snapshots are stored in an intermediary repository on the same network share until they are processed by *Alloy Discovery Express* and loaded into the main Inventory Repository. *Alloy Discovery Express* automatically reflects changes of the audit configuration on the host machine in the configurations of its deployed audit agents.

Scriptable Audit Group

Scriptable Audit group is an audit group created for the Scriptable Audit.

Shared Folder Machine

The Shared Folder Machine is the server hosting the shared folder where the Inventory Analyzer is deployed to. The Shared Folder machine is essential for the Scriptable Audit.

Sidebar

Sidebar is the left navigation pane in *Alloy Discovery Express* interface that displays the group hierarchy and allows you to navigate through audit groups and computer groups down to individual computers and devices.

Silent Mode

Silent mode is an audit mode that allows you to audit computers silently without requiring interaction with the user. You can choose an audit mode for auditing Windows computers using the Scriptable Audit, Audit via E-mail, or Portable Audit methods.

SMBIOS Filter

SMBIOS Filter is an *Alloy Discovery Express* feature that allows you to ignore placeholder values (such as No Asset Information, System Product Name, None, etc.) found in SMBIOS tables when auditing computers. The SMBIOS Filter is made up of the built-in filter and the user-defined filter.

SNMP

SNMP (that is short for Simple Network Management Protocol) is a protocol used to monitor and perform basic configuration of network devices. Examples of these devices include network printers, routers, switches, and network UPS devices. SNMP presents management data as variables on the managed systems, which describe the system configuration. The values of these variables can be obtained (and sometimes set) by managing applications.

Alloy Discovery Express uses SNMP to discover, identify, and audit network devices such as switches, routers, and network printers. To successfully perform SNMP discovery, the SNMP agent must be configured and running on each target device. You must also specify the SNMP credentials that allow access to the SNMP data on target devices.

Standalone Mode

The standalone mode of using audit agent involves deploying audit agents onto the client side and running the audit outside of *Alloy Discovery Express*.

Alloy Discovery Express offers three audit methods, based on audit agents in the standalone mode: the Scriptable Audit, the Audit via E-mail, and the Portable Audit. Those methods involve the deployment of the Inventory Analyzer Package to a target location (a network share or a flash drive) and running the audit from that deployment location.

Static Group

Static group is a group populated by manually adding computers and network devices to that group. For example, you can use static groups to independently analyze and report inventory data from multiple networks or subdivisions within your organization.

Style

Style is a custom visual appearance that can be applied to various elements of application's graphical interface: grids, menus, tabs, check boxes, buttons, and others. A style determines the look of the application but does not affect its functionality.

U

UNC

UNC, short for Universal Naming Convention or Uniform Naming Convention, specifies a common syntax to describe the location of a network resource, such as a shared file, directory, or printer. The UNC syntax for Windows systems is as follows:
`\\ComputerName\SharedFolder\Resource`