SERENA

SERENA®
SERVICE MANAGER

Serena Asset Manager iScanner Guide

Serena Proprietary and Confidential Information

Trademarks

U.S. Government Rights

Part number: Serena Asset Manager 5.0.1

Publication date: 2014-10-02

Table of Contents

Chapter 1: Introduction

Welcome to the *Serena Asset Manager iScanner Guide*. This chapter provides an overview of the iScanner documentation and application.

Document Overview

This document covers the following topics:

- Chapter 1: Introduction [page 5] – This chapter provides an overview of the major components of iScanner.
- Chapter 2: Getting Started [page 9] – This chapter provides instructions on setting up the scanner and an introduction to the scanner interface.
- Chapter 3: Running a Scan [page 29] – This chapter provides information on executing a scan of your network. A scan can be run immediately or scheduled to run for a later time.
- Chapter 4: Scheduling a Scan [page 31] – This chapter provides information on scheduling scans at specific dates and times.
- Chapter 5: Troubleshooting [page 33] – This chapter covers common errors and their resolution.
- Chapter 6: Device Inspector [page 37] – This chapter covers the stand-alone Device Inspector utility.

About Serena Asset Manager iScanner

The Serena Asset Manager iScanner application enables you to quickly scan your network, or a selected portion of the network, and gather relevant data pertaining to the devices on that network.

The discovery phase is the initial step in gathering information about devices on a network. iScanner searches your network to locate (discover) the devices operating on that network. After a device is discovered, it can then be inventoried using a set of standard methods and protocols. No agent needs to be installed on your network devices to allow the scanner to find them; the inventory process leverages existing network and system protocols to find them or they can be inventoried with Serena Asset Manager's Device Inspector, which is not dependent on any protocols. iScanner can explore a variety of networked devices including devices running Windows, UNIX and LINUX, along with devices supporting SNMP like switches, network printers, controllers and routers or anything using a TCP/IP stack.

During the inventory phase, iScanner gathers hardware, configuration, and software information from devices that it has discovered. After discovering a device, the inventory process determines hardware, software and configuration information.

For example, when iScanner queries a machine, it gathers:

- Asset intelligence on all the hardware attributes (which can include hundreds of attributes based on the device instrumentation).
- Configuration information such as local user accounts, and information on services, processes, and all the installed applications and software.

It also collects valuable data on the TCP/UDP ports in use, shares available, date, time, and the total "up-time" of the machine. The iScanner application can also perform a security scan to determine if current patches have been applied to the system and if a potential security breach could occur due to an open port or poor policy setting.

Who Can Use This Data?

The IT asset intelligence data collected by iScanner can provide information which, when used effectively, becomes vital knowledge to many organizational functions.

The following list contains the types of employees and departments who can use this data as business information:

- Employees with network management responsibilities can use the data to analyze devices on the network
- Employees responsible for software license compliancy
- During hiring or exit interviews, HR departments can use this data to gain a better understanding of systems in inventory (or soon to be collected)
- Departments responsible for Sarbanes-Oxley compliancy audits
- Employees responsible for software version control
- Mergers and acquisitions teams to gather essential information on assets and the configuration of the new environment
- Asset management teams for financial and IT information
- Helpdesk teams can use the data to gain knowledge of user systems to solve problems
- Capacity planning teams can use the information to assess if new hardware is required
- Employees involved in special IT projects or roll-outs can assess the environment where new changes are to be made
- Desktop teams are able to gain valuable configuration information that help to keep the environment under management
- Security teams are able to assess security vulnerabilities such as open ports and shares, and Windows patch management

Introduction to Discovery

Discovery locates devices on TCP/IP-based networks. When a device is discovered, high-level, network-specific data, is gathered.

IP Discovery

The IP discovery process enables you to search specified IP address ranges to locate devices and gather information. This can include the entire network or specific areas of that network by way of TCP/IP seed ranges (a start IP and end IP). When the scanner discovers an IP device, it records the IP address to the asset repository, and attempts to determine other network-specific information, such as the host name, MAC address, vendor information, and operating system class.

Windows Discovery

The Windows discovery process enables you to use Windows Network Browsing technology to identify the domains and machines on your network. This enables you to include the entire Windows Network or specific domains of that network. When the scanner discovers a Windows device, it records the host name to the inventory, and it attempts to determine other network-specific information, such as the IP address, MAC information, and basic operating system information.

Introduction to Inventory

After a device has been discovered, the inventory process identifies specific detailed information about that device. Hundreds of attributes and values can be gathered based on the device instrumentation.

After the scanner has gathered data from a discovered device an inventory file is created. The extracted data includes, but is not limited to, information about the hardware, software and general device configuration. The inventory information for a machine contains data on many system areas including the processor, RAM, network adapter, attached peripherals, and operating system to name a few.

If the device is a Windows machine, the inventory data includes host, registry and WMI information, plus lists of the users, shares, services on the machine and details on security patches that are installed. For Windows devices that do not have any standard manageability enabled (such as WMI), the stand-alone Device Inspector (DI) utility can be configured to collect detailed information.

The Device Inspector is a utility you invoke from the command line that can be used as a stand-alone inventory application. The DI can be installed on devices that do not connect to your network when an inventory is required from them. The DI can be invoked from the agent-less iScanner to inventory operating systems that do not have any manageability. Currently only Windows and LINUX operating systems are supported for the Device Inspector. For detailed information on the Device Inspector, refer to Chapter 6: Device Inspector [page 37].

If enabled, iScanner can leverage the Web-Based Enterprise Management protocol (WBEM), which can extend the amount of information that can be gathered on UNIX and LINUX systems. The Device Inspector is available for the LINUX platform.

For network devices such as switches, routers, and networks printers iScanner can collect data using the Simple Network Management Protocol (SNMP). Data from all MIBs can be captured by iScanner. SNMP v1, v2 and v3 are supported and configurable within iScanner.

Note: If Access Control Lists (ACL) are implemented in your environment, please ensure that the iScanner server is listed in the Access Control List.

The data is stored temporarily in XML format, and then processed by the Business Logic Technology (BLT) and stored in the Serena Asset Manager SQL Server database.

Licensing iScanner

A separate license is required for iScanner. The iScanner license is generated using your server's unique license code, which is based on the machine's active NIC MAC address. Servers with multiple Network Interface Cards, including wireless, each require a license. If the NIC card is replaced or a separate internal NIC card is activated, you must request a new license.

There are two methods for obtaining an iScanner license:

- Run the **Ident.exe** utility and send the output and license request to Support.
- Run the **Installation Report** utility and send the output and license request to Support.

To obtain the license code using the Ident.exe utility:

1. Run the ICT MAC application (`Ident.exe`) from the installation directory. The default directory is:

   ```
   installDirectory\Serena\Solutions\SAM\iScanner
   ```

2. In the application, click **Export**.

   You are prompted to save the MAC `Ident.ict` file.

3. Save the file, and then send it to Serena Support with your license request.

To obtain a code using the Installation Report:

1. From the Windows **Start** menu, click **All Programs**, and then select Serena Asset Manager.
2. Launch the **Installation Report** utility.
3. Click **Export**, and send a copy to Support with your license request.

To apply the license in iScanner (once you have received it):

1. Open the iScanner application.
2. In the iScanner menu, click **Options**, and then select **License Update**.
3. Apply the license code or codes you received.

Chapter 2: Getting Started

This chapter provides an introduction to the iScanner interface and instructions on setting up the scanner.

About the File Menu

The **File** menu allows you to create, edit, and select iScanner configurations. The following options are available from this menu:

- **New Configuration** – This option creates a new iScanner configuration file (`*.isc`). This file can be used to select specific targets and the type of discovery or inventory to be performed on the target devices.
  Provide a name that enables you to easily identify the purpose of the scan configuration file. For example:
  - `DallasOffice.isc`
  - `SDDataCenter.isc`

  The new configuration contains default settings according to the settings created by the **Save as Default** option below.
- **Open Configuration** – Open an existing configuration file to either edit or run a scan against.
- **Save as Default** – Create a baseline default template to be used for all new configuration files, based on the current settings.
- **Setup Directory Locations** – Specify the location for the configuration files (`*.isc`) and the output folder for the iScanner output files. One output file is created per device. Use the default values unless you will use iScanner in distributed or scan and forward mode. You must change these settings if you are using iScanner on a system that is not the core Serena Asset Manager application server. You can also set overrides for the location of the Device Inspector and Application Tracker files.

  

  Important: If iScanner is located on the core Serena Asset Manager system, if you modify any of the paths, you must also change the paths for the Business Logic Technology (BLT) in the `BLTConfig.xml` file to ensure proper operation of the import process. If these will be your new default paths, then use the **Save as Default** option to save them.

About the Options Menu

The **Options** menu provides the configuration of discovery and inventory settings, and the iScanner licenses.

Clear Scan

The **Clear Scan** option clears any information inside the **Network Layout Tree** and **Progress** text box from any prior scans. This does not clear any of the configuration settings.

Discovery

The **Discovery** sub-menu enables you to configure iScanner for IP Address Ranges, Windows Network targets, and directed scanning.

Discovery Configuration

Select this option to open the **Discovery Configuration** dialog box. The **Discovery Configuration** dialog box enables you to select **Discovery Types** and enter administrative information that is required for access to gather device information.

Hostnames and Fully Qualified Domain Names (FQDN) are automatically discovered if available. In order for hostnames to be identified, a reverse DNS zone (IP to hostname) must be configured appropriately on the DNS server. To test if reverse DNS lookups are properly configured, open a command window and perform a NSLOOKUP on any valid IP address: the result should be the IP's hostname or FQDN. If the result is not found, then reverse DNS is not configured correctly on the DNS Server. Contact your network administrator to resolve this issue.

Select the type of discovery you would like the scan to run (you can select multiple options):

- **Enable IP Range Network Discovery** – Select this option to scan the IP address range as configured in the IP Range dialog. For details, refer to IP Discovery [page 14].
- **Enable Windows Browser Discovery** – Select this option to scan the Windows network domains and workgroups. For details, refer to Windows Discovery [page 15].
- **Enable Directed Scans** – Select this option to scan IP addresses, hostnames, and FQDNs stored in a plain text file. For details, refer to Directed Scanning [page 16].

Select additional discovery options:

- **Ping IP Before Inventory** – If you are going to scan a network LAN or WAN that does not allow ICMP (PING), do not select this option. This option dramatically lengthens the amount of time that is required for the discovery process to complete because an attempt to access every IP address in the seed range is tried. Once the request times-out, then iScanner moves on to the next IP address.

- **Read MAC Address via NetBIOS** – If you are scanning Windows machines on the same subnet on which iScanner is running, you can collect MAC addresses of computers with this option. For subnets on which iScanner does not reside, or if the subnet local to iScanner does not have a majority of Windows devices, clear this option to improve scanning times.

Account Credentials Setup

Select this option to open the **Setup Account Credentials** dialog box. The following tabs appear in the **Setup Account Credentials** dialog box.

Credential Set

Multiple credential sets can be created. The individual credential sets can be applied to IP seed ranges, Windows domains, or directed scan lists. Click **New** to create a new set of credentials or **Delete** to remove a credential set. The **Default** credential set cannot be deleted.

The following list describes the account type privileges required by the vendors and publishers to ensure proper authentication to the systems and protocols:

- **Windows** – Administrator access to ALL machines. Ability to access WMI, DCOM, Remote Registry.
- **Macintosh** – Non-Admin account. Ability to SSH into the box. The same user and password must be replicated to all machines.
- **VMware vSphere** – Read-only account that has access to Web services. The same user and password must be replicated to all machines.
- **SNMP v1/v2** (Printers, switches, routers) – Read-only community string. Either the same community string across all machines, or all variations of a read community string. If ACL's (Access Control List) are used, ensure the iScanner server is granted access and privileges.
- **SNMP v3** – SNMP user account that has read access.
- **Linux** – Root level account. Ability to SSH into the target without any log in/log out error or warning messages. Same user and password replicated to all machines. SNMP can also be used.
- **Solaris** – Non-root account. Ability to SSH into the target without any log in/log out error or warning messages. Same user and password replicated to all machines. SNMP can also be used.
- **AIX** – Root level account. Ability to SSH into the target without any log in/log out error or warning messages. Same user and password replicated to all machines. SNMP can also be used.
- **HP-UX** – Root level account. Ability to SSH into the target without any log in/log out error or warning messages. Same user and password replicated to all machines. SNMP can also be used.

Windows

In order to fully inventory Windows-based systems, proper and valid credentials must be provided. An administrator domain type account and privileges are required to fully

inventory and obtain forensic level information for hardware, software applications, and configuration.

1. In the **Domain** field, enter the domain name. To use a local system account, enter ".” or leave the field empty.

2. Enter the default administrative login credentials for your Windows network discovery. This grants the scanner permissions to scan your Windows domains or workgroups on the network and Windows devices within the IP range on the network that you provide.

   - **User Name** – The administrative account that will be used to provide valid credentials to the target system. This is required to ensure that proper security is set within your environment.

   - **Password** – A valid password is required for the account that you specify.

   

   Tip: This is a blanket account. Different targeted administrator logins can be defined on both the Windows Discovery configuration and on the IP Range Configuration.

3. Test the credentials to verify that the scanner can gather data from the target systems. Click **Test Access** and enter a valid machine name or IP address. Immediate positive or negative validation is provided. If the connection is not successful, please check the information with your network administrator.

4. Click **OK** to save the settings.

Macintosh

If you are scanning any Macintosh computers, enter the **User Name** and **Password** of a common user account that has SSH privileges to the machines.

UNIX/Linux

FOr UNIX/Linux machines, enter the **User Name** and **Password** of a Root (superuser) class of account that access to the systems.

SNMP V1/V2

SNMP (Simple Network Management Protocol) requires proper authentication in order to request data from the devices. For SNMP v1/v2, iScanner requires read-only access to the device. Enter your community strings in the text field, and then click **Add Community String**. This adds the new community string to the list. iScanner attempts to access the device with the community strings in the order listed. To change the order, select the community string from the list and use the **Move Up** or **Move Down** buttons accordingly. To remove a community string, select the string, and then click **Remove**.

Note: Many network environments have ACL (Access Control Lists) in place. If you have ACLs for your network devices, please ensure that the iScanner server is listed in the ACL.

SNMP V3

SNMP v3 provides additional security when iScanner accesses data from the device.

Configure the following:

- **User Name** – Enter the User Name to access v3.

- **Authentication** – Select the protocol (**None**, **MD5**, or **SHA**) based on the **User Name** policy. Enter the assigned passphrase in the **Passphrase** and **Confirm Passphrase** fields.
- **Privacy** – Select the protocol (**None** or **DES**) based on the **User Name** policy. Enter the assigned passphrase in the **Passphrase** and **Confirm Passphrase** fields.

There are three levels of security and levels supported by v3:

Model	Level	Authentication	Encryption	Result
v3	noAuthnoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Note the following about SNMPv3 objects:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy is what SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users.

vSphere

If you are planning to scan VMware ESX, ESXi, or vCenter Server machines, enter a **User name** and **Password** that is common to all VMware machines.

Note: If you are using Active Directory credentials, do not specify the user name in the standard Windows format: "domain\username". Specify only the user name.

Note: For Active Directory credentials to work, they must be granted a minimum of read-only permission to every vSphere server. For more information, refer to Enabling Access to ESX and ESXi for Active Directory Accounts [page 52].

IP Discovery

Select this option to open the **IP Scan Range Setup** dialog box. The **IP Scan Range Setup** dialog box enables you to set the range or ranges of IP addresses for the scanner to explore. iScanner is most efficient when it is configured with narrow IP ranges. Class C subnets are typically suggested.

Note: An IP range must be set if **IP Discovery** is selected, otherwise the scanner will not scan your IP network. If the ranges are left blank, a discovery is not run.

To add an IP range:

1. In the **From** field, enter the IP address for the start of the range.
2. In the **To** field, enter the IP address for the end of the scan range.
3. Select the **Credential Set** that should be applied to the IP seed range that is created if it does not use the default account credentials.
4. Click **Add**.

   The range is added to the list of scan ranges and the credentials that will be used for the scan range are displayed.
5. Repeat these steps to include additional ranges.
6. Click **OK** to save the ranges.

To remove an IP range:

1. Select the range that you want to remove from the scan.
2. Click **Remove**.

   The range is removed from the list of scan ranges.
3. Repeat these steps to remove additional ranges.
4. Click **OK** to save your changes.

To modify an IP range:

1. Select the range that you want to modify.
2. Click **Modify**.
3. Make the appropriate changes to this seed range.
4. Click **Modify** again when you are finished.
5. Repeat these steps to modify additional ranges.
6. Click **OK** to save your changes.

Windows Discovery

Select this option to open the **Windows Scan Range Setup** dialog box. The **Windows Scan Range Setup** dialog box enables you to configure which Windows domains, workgroups, or individual computers are explored by the scanner.

To explore domains and workgroups:

1. Click **Explore Network Layout**.
2. iScanner examines the Microsoft Windows Network and enumerates all available domains and machines in the **Current Network Layout** section.

   

   Note: This operation can be time consuming on very large networks.

3. Double-click on a Microsoft Windows Network icon to display the domains within that network.

   The domains that reside on the network are displayed in the **Current Network Layout** list.
4. Select a domain in the list.
5. Select the **Credential Set** to be used for the domain (**Default** is used if none is selected).
6. Decide if you want to exclude a domain or a specific computer system from the scan. To include everything, click **Include Everything**.

   To exclude a domain or system:

   a. Select the domain or computer system in the **Current Network Layout** list.

   b. Select **Exclude Target From Scans**.
7. Click **OK** to save the ranges.

If you have a requirement to target scans on specific PCs or Windows servers with high security or non-default credentials, you scan individual Windows computers.

To scan individual Windows computers:

1. Click **Explore Network Layout**.
2. Double-click on a domain or workgroup to display individual PCs or servers.
3. Select the appropriate credentials from the **Credential Set** if the default credentials are not used.
4. Decide if you want to exclude a computer from the scan.

   To exclude a computer:

   a. Select the computer in the **Current Network Layout** list.

   b. Select **Exclude Target From Scans**.
5. Click **OK** to save your changes.

Directed Scanning

Select this option to open the **Directed Scan Range Setup** dialog box. The **Directed Scan Range Setup** dialog box enables you to perform a scan against a directed list of IP addresses, hostnames, and fully qualified domain names (FQDN). Use this option to generate a custom text report from sources such as Serena Asset Manager, Active Directory, LDAP, a DNS lookup zone list, and other sources to focus scanning on known machines.

Consider utilizing directed scanning over broad IP address for:

- A quick refresh of selected assets inside Serena Asset Manager that have already been discovered and inventoried.
- A targeted re-scan of assets inside Serena Asset Manager that have been discovered but not yet inventoried.
- A targeted nighttime scan of known desktops and laptops for off-hours energy consumption reporting.
- A targeted scan of devices known to Active Directory, LDAP, or DNS to give the user fast inventory of machines known from other sources, as well as enabling the user to use these known sources to help identify IP subnets for use with larger IP scan sweeps later.

The file that is used is a plain text file that contains one IP address, hostname, or FQDN per line, and nothing else on the line. You can mix and match IP addresses, hostnames, and FQDNs in the same file. You may specify more than one file to be used for directed scans.

To set up directed scanning:

1. Enter the path name to the file that contains the list of machine addresses, or click **Browse** to navigate to it.
2. Select **Retry Directed Scans** to automatically retry machines in the list that could not be pinged.

   

   Note: This option causes iScanner to continually loop and re-scan until all entries in the directed scan files have been scanned once. If the list contains machines that are always off or otherwise permanently unreachable, iScanner will continue running indefinitely until you click **Abort Scan button**, or until iScanner is stopped either through the Windows Scheduler or the Task Manager (if iScanner is being run in the background).
3. Select the **Credential Set** that should be applied to the directed scan list.
4. Click **Add**.

To remove a directed scan file from the scan process:

1. Select the directed scan file that you want to remove from the scan.
2. Click **Remove**.
3. Repeat this process to remove additional scans.

4. Click **OK** to save your changes.

To modify a directed scan:

1. Select the directed scan file that you want to modify.
2. Click **Modify**.
3. Make the appropriate changes.
4. Click **Modify** again.
5. Click **OK** to save your changes.

Advanced SSH Configuration

Select this option to open the **Advanced SSH Setup** dialog box. Certain iScanner discovery and inventory options use Secure Shell (SSH) to communicate with target devices to be scanned. When iScanner establishes an SSH connection to a machine, it requests a public key from that machine, and attempts to verify the key with a copy stored locally in the Windows registry. If the key does not exist, or if the key has changed, iScanner needs to know how to correctly respond before proceeding.

A copy of the key might not exist on the iScanner machine if iScanner has never connected to this machine via SSH before. However, consider the following security issues when the cached key does not exist:

- Someone could have deleted the cached keys from the Windows registry.
- If the IT Administrator is satisfied that all machines have been previously scanned and that there should be no additional machines that iScanner needs to connect to via SSH, then the sudden and unexpected appearance of a new machine that iScanner wishes to connect to via SSH could be a security concern.

By default, if iScanner encounters a machine for which it does not have a copy of the public SSH key, iScanner accepts the connection and stores the key in the cache inside the Windows Registry. However, this behavior can be changed, if the administrator desires, by using the **Advanced SSH Configuration** dialog box as follows:

- **Accept connection but do not cache, and warn** – iScanner will still connect, but will not store the key, and it will log a warning message into the scan output file. Each subsequent time iScanner connects, a warning message will be generated until the behavior is changed again.
- **Reject connection and log error** – iScanner will not connect to the target machine and will log an error in the scan output file. An administrator might choose this option if he or she is satisfied that all of the SSH keys from target machines that they wish to inventory are cached, and that any additional SSH connections that iScanner attempts to make represents a security concern.

In the case where the cached copy of the SSH key is different than the key that is sent by the target machine, iScanner rejects the connection and logs an error to the scan output file by default. This situation can is caused by either a benign or a potentially malicious condition, and the IT Administrator needs to carefully determine what has happened before changing iScanner's behavior.

Benign reasons for the SSH key changing include:

- The SSH password on the target machine has been changed.
- The SSH key has been regenerated. This can occur if the SSH service is re-installed, or if the operating system on the target machine is removed and re-installed.
- A new physical machine has legitimately replaced an old machine with the same hostname and IP address.

Potential malicious reasons for the SSH key changing include:

- A "man in the middle" attack where another machine is attempting to intercept SSH connections.
- An unauthorized replacement of the physical machine with a new machine that has the same hostname and IP address.
- The target machine has been hacked, and the SSH server has been compromised or replaced with a malicious SSH service that may be performing unauthorized activities such as logging keystrokes and passwords.

If the IT Administrator is confident that the reason for an SSH key changing is benign and acceptable, then he or she can change iScanner's default behavior when encountering a changed SSH key as follows:

- **Accept connection and cache new key** – iScanner will permanently accept the new key and allow scanning to proceed.
- **Accept connection but do not cache, and warn** – iScanner will still connect, but will not store the key, and will log a warning message into the scan output file. Each subsequent time iScanner connects, a warning message is generated until the behavior is changed again.

Inventory

The **Inventory** sub-menu contains a **Configuration** option to set up the type of inventory data collected by the scanner, and a **Remote Execution Configuration** option.

Inventory Configuration

Select this option to open the **Inventory Configuration** dialog box. The **Inventory Configuration** dialog box enables you to determine what information is written to the inventory files for each device.

To set up the Inventory Configuration, complete the following sections.

Scan Type

Select the applicable boxes for the data that you want the scan to collect in the Windows and IP networks.

- **Forensic** – A very detailed scan is performed. This enables all possible features and collects from every protocol and data point available to the scanner. This excludes the ability to enable the Device Inspector.

For SNMP-based devices, the scanner collects data from every MIB-enabled on the device. This includes all pubic and proprietary MIBs.

Note: Complex SNMP devices can create very large files.

For Windows machines, iScanner will collect more WMI attributes, including: MSI product info, performance metrics, and plug and play components. In addition, the Windows software will collect additional attributes about all installed software. This can create large scan files that can significantly slow down load times.

- **Lightweight With Software** – iScanner only retrieves select attributes when scanning, which limits the size of scan files and improves load times. The attributes that are selected include most or all that are deemed critical to successful IT Asset Management. This is the normal mode of operation for iScanner.
- **Lightweight Without Software** – This is similar to the option above, but no installed software data is retrieved. This can significantly reduce the size of scan files even further if you do not need to collect installed software data from machines.
- **Power Information Only** – This mode collects very minimal hardware information and no software information.
- **Custom** – This mode enables you to completely customize which attributes to scan. For more information, refer to the Advanced Settings for each applicable section.

Windows Specific Inventory

The inventory scanner automatically gathers Windows networking information about the host, including the computer name and operating system. Access to this data usually requires that you configure the proper access credentials in the scanner.

The following data can also be captured:

- **Application Tracker** – If you have deployed the Application Tracker agent to target machines, use this option to retrieve the AppTracker data.
- **Registry** – Gathers select registry information, including installed software and additional information on installed SQL Server instances such as the SQL Server edition. If you select the **Lightweight Without Software** scan type, installed software is not retrieved.
- **Security** – Verifies that the latest security patches are installed on the scanned device. Also identifies configuration issues and verifies local accounts.
  Click **Advanced** to launch the **Windows Security Scan Advanced Settings** dialog box. Use the following advanced settings to modify the behavior of the security scan:
  - **Unapproved WSUS Updates** – If your IT department is using WSUS (Windows Software Update Service) servers in-house to update Windows machines instead of the external Microsoft Update site, you can specify how security updates that have not been approved by WSUS should be deployed to your machines.
  - **Automatically Configure Target Machines** – Includes the following options:
    - **Update the prerequisite Windows Update Agent components during a scan** – Select this option to install the current version of the Windows Update

Agent on the target computer if it is absent or out-of-date. Also configures the target computer to meet other scanning requirements for security updates.

- **Configure target to use the Microsoft Update site for updates** – Select this option configure computers to use the Microsoft Update site on the computer that is being scanned.

- **Edit Inclusion / Exclusion Lists** – These options enable you to add or edit entries to two sets of inclusion and exclusion lists:
  - **NoExpireOk.txt** – Account names listed in this file are not reported as potential security problems in the **Password Expiration** test. If the name ends with an asterisk (*), all accounts with that initial string are not reported. Account names are not case-sensitive.
  - **Services.txt** – Services included in this file are checked during scans and listed in the resulting security report. The status of each service (stopped or started) is listed. When editing this list, include the service name for each service that you want to be scanned on a separate line. Find the service name by looking at the **Properties** for the service in the **Services Control Panel** applet.

- **Services** – Lists the services on each scanned device.
- **Shares** – Lists the shares available for other computers to connect to on each scanned device.
- **Users** – For non-domain controllers, this option gathers the list of local user accounts for each scanned device. For domain controllers, this option gathers the list of all domain user accounts.

  

  Note: Both primary and backup domain controllers produce the same list of users, and these lists can create very large scan files that can take a long time to load. Serena recommends, at a minimum, that you isolate all backup domain controllers from the main scan configuration files and place them in a separate scan configuration file, and then de-select the **Users** inventory option. If you are using the LDAP / Active Directory scanner (whic is recommended), then place the primary domain controller in this scan configuration as well.

- **WMI** – Gathers WMI (Windows Management Instrumentation) information from a scanned device.

  Click **Advanced** to launch the **WMI Advanced Settings** dialog box. Use the options in the **WMI Advanced Settings** dialog box to enable, disable, or add additional WMI classes to iScanner.

  Select **Custom** to enable the **Custom WMI Classes** section. To add a class, specify the Win32 class name in the **Class Name** text field. You can find WMI classes here: Microsoft WMI Classes.

  Certain pre-selected WMI classes are not scanned by default to reduce the size of the scan file and improve loading times. For information on which classes to enable for certain additional attribute scanning scenarios, refer to Appendix [page 49].

IP Inventory

This section provides inventory options for machines not running Microsoft Windows.

- **Device Inspector for Linux** – Enables detailed hardware and software scanning of Linux machines. To use this option, you must provide account credentials with root-level access to the Linux machines.

  

  Note: Device Inspector for Linux will not run on UNIX machines, nor on Linux machines that have a hardware platform other than Intel or AMD (i686 / x86_64). For these kinds of machines please use the **Unix Script** option below.

  Click **Advanced** to launch the **Device Inspector for Linux Advanced Setup** dialog box. Use the options in the **Device Inspector for Linux Advanced Setup** dialog box to fine tune and select the class attributes that will be collected when using the Linux Device Inspector (LDI) for collecting data, including **Custom Scan Categories**:

  - **Scan Type** – The scan type settings are inherited from the **Scan Type** selected in the parent **Inventory Configuration** dialog box. The most common setting for the **Scan Type** is **Lightweight with Software**.

    If required, you can override the parent scan type by selecting a different type. Select **Custom** to enable the **Custom Scan Categories** options.

  - **Remote Execution Method** – If scanning older Linux machines without Secure Shell (SSH) support, you can select a legacy method of remotely executing LDI on the target machine.

    

    Note: If iScanner is installed on Windows Server 2008 or later, you must first install Microsoft Windows Services for UNIX on the application server in order to use the legacy remote execution options.

  - **Remote Copy Options** – If scanning older Linux machines without Secure Copy (SCP) support, you can select a legacy method of remotely copying LDI to the target machine.

    

    Note: If iScanner is installed on Windows Server 2008 or later, you must first install Microsoft Windows Services for UNIX on the application server in order to use the legacy remote copy (RCP) option.

  - **Custom Scan Categories** – This section performs the LDI actions depending on the category selected. These categories are automatically set for any scan type other than **Custom**.

  - **Enable Logging** – Select this option if directed by Support.

  - **Retrieve BIN File** – Select this option if directed by Support to retrieve the intermediate BIN file for analysis.

  - **Destination Temporary Path** – If the location of the temporary directory on the target Linux machines is different from the default location (which is typically `/var/tmp`, but can be `/tmp`), you can change it here.

- **Macintosh** – Gets hardware and installed software information from Apple Macintosh computers.

  

  Note: iScanner supports scanning Mac OS X 10.4 (Tiger) and later. You may encounter issues attempting to scan 10.3 or lower. iScanner does not support Mac OS 9 or lower.

- **Ports** – Lists select TCP ports that are in use on a device, and what processes are running on those ports.

- **Remote Command Execution** – Enables iScanner to process ad-hoc commands on the remote system that is being scanned.

- **SNMP V1/V2** – This option gets select MIB data for devices that have the SNMP service using the version 1 or version 2 protocols. The data is listed by ISO number in the inventory file.

- **SNMP V3** – Select this option if you have devices that use version 3 of SNMP. SNMP v3 provides secure access to devices.

  Click **Advanced** to launch the **SNMP Advanced Setup** dialog box. Use the options in the **SNMP Advanced Setup** dialog box to add or remove OIDs (Object Identifiers for SNMP MIBs), configure Forensic SNMP scans, change the default OIDs that are selected, or add your own. To modify the selection or add your own OIDs, select the **Custom** radio button. You must use the OSI format.

- **Time of Day** – Lists the current up-time of the device, the time on the device's clock, the Greenwich Mean Time (GMT) when the device was scanned, and the date when the device was scanned.

- **Unix Script** – If you have any UNIX hardware (AIX, HP-UX, or Solaris), enable this option to collect hardware and software inventory information from these machines. This option attempts to run a Bourne shell script on the target devices; therefore, if Device Inspector fails on Linux machines, this option may be able to inventory a more limited set of data.
  Click **Advanced** to launch the **UNIX Inventory Script Advanced Options** dialog box. Use the following options in the **UNIX Inventory Script Advanced Options** dialog box to change how the script is executed and where it is located on the source and target machines:

  - **Remote Execution Method** – If iScanner will be scanning older UNIX machines without Secure Shell (SSH) support, you may select a legacy method of remotely executing the UNIX script on the target machine.

    

    Note: If iScanner is installed on Windows Server 2008 or later, you must first install Microsoft Windows Services for UNIX on the application server in order to use the legacy remote execution options.

  - **Remote Copy Options** – If scanning older UNIX machines without Secure Copy (SCP) support, you may select a legacy method of remotely copying the UNIX script to the target machine.

    

    Note: If iScanner is installed on Windows Server 2008 or later, you must first install Microsoft Windows Services for UNIX on the application server in order to use the legacy remote copy (RCP) option .

- **Script Source** – Select the location of the Bourne shell script on the iScanner application server.
- **Script Destination** – If the location of the temporary directory on the target UNIX machine is different from the default location (which is typically `/var/tmp`, but can be `/tmp`), you can change it here.

- **VmWare vSphere** – If you have VMware ESX, ESXi, or vCenter Server virtual machine servers, select this option to collect hardware inventory information and a list of guest VMs that are installed that can be cross-referenced with the actual VMs once they are scanned.

Device Inspector for Windows

Device Inspector (DI) for Windows has three different modes of operation:

- **Disabled** – Device Inspector for Windows will never run.
- **Enable When WMI Fails** – Some corporate networks disable WMI on their networks, or other network settings block WMI scanning. If **WMI** is selected, and iScanner cannot connect to WMI on the remote target, it will attempt to launch Device Inspector for Windows instead.
- **Enable for All Targets** – A Device Inspector for Windows scan will be performed against all Windows machines.

Click **Advanced** to launch the **Device Inspector for Windows Advanced Setup** dialog box. Use the following options in the **Device Inspector for Windows Advanced Setup** dialog box to fine tune and select the class attributes that will be collected when using the DI for collecting data, including **Custom Scan Categories**:

- **Scan Type** – The scan type settings are inherited from the **Scan Type** selected in the parent **Inventory Configuration** dialog box. The most common setting for the **Scan Type** is **Lightweight with Software**.

  If required, you can override the parent scan type by selecting a different type. Select **Custom** to enable the **Custom Scan Categories** options.
- **Logging** – If directed by Support, enable the appropriate logging level, and select the option to retrieve the intermediate BIN file for analysis. This option produces Device Inspector log files in the destination scan file folder.
- **BIOS Scan Method** – If you are scanning legacy Windows 95, 98, ME machines, change this setting to **Windows 9x** to retrieve hardware inventory information from these machines, otherwise leave this set to **Windows NT**.

  

  Tip: Because only one type of hardware scan can be selected, it is recommended that you isolate any legacy Windows 9x machines into a separate iScanner configuration, and then change this option in that configuration. This ensures that modern Windows machines are not excluded from hardware inventory scanning.

- **Custom Scan Categories** – This section performs the DI actions depending on the category selected. These categories are automatically set for any scan type other than **Custom**.

  Note: If **Software** is selected, this enables the **Advanced** option. Click Advanced to launch the **Advanced Software** dialog box.

  This option causes Device Inspector to bypass checking the registry directly for installed software items, and instead causes it to rely only on a Microsoft Windows call that retrieves software items that have been installed by the Microsoft Installer (MSI). This option might not return all installed software on the target machine. Please consult with Support before setting this option.

Remote Execution Configuration

Select this option to open the **Remote Execution Configuration** dialog box. The **Remote Execution Configuration** dialog box enables iScanner to perform actions on the target scanned devices. These actions can be performed in the form of a script, an executable, or a direct command to the device.

CAUTION:

Serena is not responsible for the use of any macro—even if provided by Serena—or for any legal, financial, or other implications resulting from the use of any macro. The use of any and all macros is the complete and sole responsibility of the user.

The following sections describe the tabs that appear in the **Remote Execution Configuration** dialog box.

Command Tab

The following options appear on the **Command** tab:

- **Description** – Enter a human readable description of the command to perform.
- **Command** – Enter the command to be performed on the device. For examples, see Executing an Executable [page 26] and Running a Script [page 26].
- **Remote Execution Method** – If you are scanning older UNIX or Linux machines without Secure Shell (SSH) support, you can select a legacy method of remotely executing the UNIX script on the target machine. For Windows target machines this should usually be set to "Windows RPC".

  Note: If iScanner is installed on Windows Server 2008 or later, you must first install Microsoft Windows Services for UNIX on the application server in order to use the legacy remote execution options .

- **Target Platform** – Select **Windows** for Microsoft Windows targets or **POSIX** (Portable Operating System Interface for UNIX) for UNIX, Linux, or Mac OS X machines. The default is **Windows**.
- **RLogin / Telnet Logout Method** – If you have selected a legacy remote execution method (RLogin or Telnet), iScanner might have difficulty logging out of the target machine when it has finished executing the command. Either specify that iScanner send the control sequence `<CTRL><D>` to the target machine to log out, or specify a specific command to execute to attempt to log out (typically `logout`).

- **Cancel if Error Message Returned** – iScanner attempts to intercept error messages written to the standard error output from remote targets. In some cases, these error messages are non-fatal, and iScanner might still be able to collect data that is returned. If this is true, then clear this option.

- **Advanced SSH Setup** – Please refer to Advanced SSH Configuration [page 17]. Changes made here affect SSH behavior on a global scale for iScanner, so this is functionally identical to selecting the **Advanced SSH Configuration** option from the **Discovery** menu.

Copy Options Tab

The following options appear on the **Copy Options** tab:

- **Copy Command to Target Machine** – Select this option if you need to copy an executable or script to perform an action on the target device.

- **Remote Copy Options** – If you are scanning older UNIX or Linux machines without Secure Copy (SCP) support, you can select a legacy method of remotely copying the script or executable to the target machine. If the target machine is a Windows machine, select **Windows Copy** instead.

  

  Note: If iScanner is installed on Windows Server 2008 or later, you must first install Microsoft Windows Services for UNIX on the application server in order to use the legacy remote copy (RCP) option.

- **Command Source** – Enter the full pathname to the script or executable on the application server, or click the **Browse** button to locate it.

- **Command Destination** – Enter the location of the standard temporary folder or directory on the target machine. For Microsoft Windows, this is usually `Admin$\Temp\`. For UNIX and Linux this is usually either `/tmp` or `/var/tmp`.

- **Delete Command When Finished** – Select this option to cause iScanner to attempt to delete the script or executable file off of the target machine. This is the default behavior.

Command Output Tab

The following options appear on the **Command Output** tab:

- **Retrieve Standard Output** – Select this option if you need to capture the data from the "standard output" of the target device, based on the type of command you are executing on the target device.

- **Standard Output Parsing**:

  - **Delimiters** – Specify any characters that should be used to denote a separation of data, such as a comma (`,`) or a vertical line (`|`).

  - **Non-Printing Delimiters** – If the **Newline** (end-of-line), **Space**, or **Tab** character denotes data separation, select these options as appropriate.

  - **Remove Last Line of Data Returned** – Some types of standard output data captures might require that the last line of data be removed to make it readable. In this scenario, select this option to remove the last line.

- **XML Data Returned** – If the data is output as Extensible Markup Language (XML), select this option.

Once all of your settings have been configured, click **Add** to save the command. If required, you can repeat the process to add additional commands for the devices that will be scanned.

Executing an Executable

Windows Shutdown:

1. Press F7 to launch the **Remote Execution Options**.
2. Enter a **Description**. For example: `Shut Down Idle Windows Sessions.`
3. Enter `ICWindowsShutdown.exe` in the **Command** field.
4. Ensure **Windows** is selected for the **Target Platform**.
5. Click the **Copy Options** tab.
6. Select **Copy Command To Remote Machine**.
7. Change **Command Source** and **Command Destination** if necessary from the defaults. By default, it should point to the correct source directory to find the command:

   ```
   INSTALL_PATH\iScanner\Remote Utilities
   ```

8. Ensure **Delete Command When Finished** is selected.
9. Click **Add**.

Running a Script

UNIX / Linux / Mac OS Inventory Scripts:

Note: These scripts are now superseded by the inventory options Device Inspector for Linux, Macintosh, and Unix Script. This example demonstrates how to set up a script for remote execution. Please enable the above options under **Options** | **Inventory** | **Configuration** to correctly gather inventory information from these machines.

1. Press F7 to launch the **Remote Execution Options**.
2. Enter a **Description**. For example: `Linux Inventory Info.`
3. For general and hardware, enter `Posix-Info.sh` in the **Command** field; for Linux distributions with RPM, enter `Linux-Software-Info.sh`.
4. Ensure **POSIX** is selected for the **Target Platform**.
5. Click the **Copy Options** tab.
6. Select **Copy Command To Remote Machine**.

7. Change **Command Source** and **Command Destination** if necessary from the defaults. By default, it should point to the correct source directory to find the command:

   ```
   INSTALL_PATH\iScanner\Remote Utilities
   ```

8. Ensure **Delete Command When Finished** is selected.
9. Click the **Command Output Tab**.
10. Select **Retrieve Standard Output**.
11. Select the **Newline** option in the list of **Non-Printing Delimiters**.
12. Click **Add**.

License Update

For details on adding or updating your iScanner license, refer to Licensing iScanner [page 8].

Debugging Trace Messages

Selecting this option to add additional message to the scan file output. You do not need to select this for normal, day-to-day scans. You should only select this option if instructed to do so by Support.

Chapter 3: Running a Scan

This chapter provides instructions to start a scan.

Starting a Scan

To run a scan using the opened configuration, click Scan in the main window. The progress of the scan is tracked in the status box. When the scan is complete, the results are displayed in the Network Layout Tree and written to the inventory files.

Network Layout

The **Network Layout Tree** lists the information gathered during the most recent scan. This section displays the data that you requested in the Inventory Configuration.

The **Network Layout Tree** is arranged in a hierarchical order: the discovered networks are listed on the top level; domains are listed on the second level; servers are listed on the third level.

To navigate the Network Layout:

1. Double-click on a network icon to navigate to the next layer.
2. Continue to double-click to navigate down through the layout, which is displayed in a tree format.

Status Information

As the scan runs, a series of messages are displayed in the status box of the main window. The status box is scrollable, and it contains messages that describe the progress of the scan. The status informs you of what is being scanned, the type of data that is being retrieved, and if the scan was successful.

For example, the following messages are displayed for a successful scan of port 80 on a network PC:

```
Scanning Port 80
  Scanning Users
    Success
  Scanning Shares
    Success
  Scanning Services
    Success
  Retrieving TOD
  Retrieving Registry
  Retrieving MAC
  Security Scan initiated
  Security Scan ended
```

```
Retrieving SNMP Data
Retrieving WMI data
```

Aborting a Scan

To abort a scan, click the **Abort** button in the main window. The scanner finishes processing the current device before it aborts the scan; this may take a minute or more depending on the progress of the device being scanned.

Chapter 4: Scheduling a Scan

This chapter provides instructions to schedule a scan.

Scheduling a Scan

iScanner can be launched automatically using the scheduling system built into the Windows Operating System. This enables the OS to manage the scheduling and settings that are required to launch the scanner and run as an unattended background process.

Note: To create scheduler jobs for multiple iScanner configuration files, use the utility application found here: `<installDirectory>\InControl\Tools\ScanConfigUpdate`. Please contact Support for guidance on using this utility.

Scheduling on Windows Server 2003

To access the built-in scheduling system provided in Windows:

1. Open the Control Panel and select **Scheduled Tasks**.
2. Select **Add Scheduled Task** to create a new task for launching iScanner.

   

   Note: If iScanner does not appear in the list of applications, click **Browse** to navigate to the location of the iScanner executable. The default location is `<installDirectory\InControl\iScanner\iScanner.exe`.

   The Scheduled Task Wizard begins.
3. Follow the wizard to configure the schedule. You typically schedule the scanner for periods that provide enough time for it to complete any previously scheduled scans.

   

   Tip: Running the scanner once a week is sufficient in a typical environment.
4. You must associate the iScanner process with a user account on the machine. Typically the Administrator account is used.
5. Once the wizard is complete, the Task Scheduler prompts you to open the **Advanced Settings** for the newly-defined task. Proceed to the task settings window. You can also access this window by double-clicking on the task name within the **Scheduled Tasks** window of the Control Panel.
6. Modify the Run section to launch the task with the `/silent` parameter. This enables the scanner to run as an unattended background process without the iScanner user interface.
   To use an alternate configuration file in scheduled mode, include the parameter `/config filename`. For example:

```
"installDirectory\incontrol\iScanner\iScanner.exe" /silent /config myconfig.isc
```

The Task window can also be used to make modifications to the scheduling of the task, or some of the advanced settings that are associated with the task. Ensure that the **Stop Task if it runs for X Hours** option is not selected within a range that is normally expected for the scanner to complete. This could cause the scanner to be terminated before it has time to complete its task.

Scheduling on Windows Server 2008 and later

To access the built-in scheduling system provided in Windows:

1. In the Windows **Start** menu, click **Administrative Tools**. Select **Task Scheduler**.

   The **Task Scheduler** dialog box appears.

2. In the **Actions** pane, click **Create Task**. (Two advanced setting options are required to create the schedule; therefore, do not select **Create Basic Task**.)

   The **Create Task** dialog box appears.

3. Enter a **Name** and **Description** for the task. If you are not logged in to the machine as the user that will be used to run the schedule, click **Change User or Group** and select the correct account.

4. In the **Security options** section, select **Run whether user is logged on or not** and **Run with highest privileges**.

   Important: You must select both of these options, otherwise iScanner will not run.

5. On the **Triggers** tab, click the **New** button.

   The **New Trigger** dialog box appears.

6. Set up a schedule to run the task. A weekly task is usually sufficient. Click **OK** when you are finished.

7. On the **Actions** tab, click the **New** button.

   The **New Action** dialog box appears.

8. In the **Action** drop-down list, select **Start a program**. Click **Browse** to navigate to the location of the iScanner executable. The default location is `<installDirectory\InControl\iScanner\iScanner.exe`

9. In the **Add arguments** field, type `/silent`. This switch ensures that the iScanner user interface is not used. If you are using a configuration file other than the default `ScanConfig.isc`, include the `config filename.isc` switch and replace `filename.isc` with the name of the iScanner configuration file.

10. In the **Start In** field, enter the path to iScanner. The default is: `<installDirectory\InControl\iScanner`.

11. When you are finished, click **OK**. Click **OK** again on the main **Create Task** dialog box.

Chapter 5: Troubleshooting

This chapter provides common troubleshooting tips.

Common Errors and Resolutions

This section lists types of common errors and their resolutions.

SNMPData

`Timeout: No Response from <Hostname or IP Address> using community string: <read community string>`

SNMP V1 and V2 do not return any value other than "success" or "timeout" when attempting to connect to the SNMP service on a target machine. A timeout, therefore, can mean many different things, from "invalid community string" to "SNMP Service unavailable".

Resolution:

Check to see if the error message `all community strings failed` occurs, and see below for resolutions. If this message is not returned, then SNMP data should have been returned with a different community string.

`All community strings failed.`

This indicates that all SNMP V1/V2 community strings have been tried, and none returned any SNMP data.

Resolutions:

- Does the machine have SNMP on it? Most Windows machines do not have SNMP, so they will almost always return this error message if you have selected to scan with SNMP. Other machines, such as those with the Linux and Macintosh operating systems, often do not have SNMP turned on by default. Contact the system administrator to see if they wish to activate SNMP on these machines.
- Have you entered a valid community string for the machine? Contact the system administrators for all of their SNMP read community strings, and enter them in the SNMP V1/V2 Credentials tab.
- Are you blocked by an Access Control List (ACL)? Contact the system administrator to find out if ACLs are in place, and if so, have them add the machine to the ACL.
- Is the SNMP port blocked by a firewall or router? SNMP uses UDP port 161. See if there are any firewall settings on the local machine, or a policy on the routers, that blocks port 161. If so, open the port.

WMI

Microsoft has implemented security guidelines that might affect remote access to the WMI service. To ensure proper implementation, follow the requirements set by Microsoft.

Error #80070005: Access is denied.

This error normally indicates that a connection could be made to WMI, but invalid credentials were passed. Occasionally, it indicates that the WMI service is unavailable. Refer to `The RPC Server is unavailable` error below if the following resolutions do not help.

Resolutions:

- Is the target machine attached to a domain controller? If so, have the system administrator provide you with a domain level account that has administrator privileges on the machine, and enter the credentials into a credential set under the Windows tab. Be sure to enter the domain name in the domain field, and also ensure that the credential set is selected for either the IP scan rage that the machine is in, or for the selected Windows machine in the **Windows Scan Range Setup** dialog box.
- If the target machine is not attached to a domain controller, you must use a local account with administrator privileges. Enter this account in the Windows tab, and leave the domain name field blank.
- Additional Reference Links:
  - Connecting Through Windows Firewall
  - http://support.microsoft.com/kb/909444

Error #800706ba: The RPC server is unavailable.

iScanner was unable to connect to the WMI Service on the target machine.

Resolutions:

- Is the target machine a Windows machine? WMI is only available on machines with the Microsoft Windows operating system installed. All other devices will display this error, and it should be ignored in these cases.
- Does the target machine have a version of Windows earlier than Windows 2000? Older editions of Windows do not have WMI installed and activated by default.
- Is a firewall or router blocking ports? Check with the system administrator to see if RPC (Port 135), NetBIOS (Ports 137-139), or SMB (Port 445) are being blocked, and have these ports opened if they are blocked.
- If the target machine is attached to a domain controller, are the domain policies too restrictive? Check with the domain administrator to see if there are policies in place prohibiting WMI, DCOM, RPC, or Remote Registry access, or if the domain policy forces any or all of these services to be turned off by default. Also, check to see that the domain controller automatically relaxes Windows XP and Vista firewall settings to allow connection to these services. In addition, policies may need to be changed in accordance with the Microsoft article "Connecting to WMI Remotely Starting with Vista".

- If the target machine is not attached to a domain controller, and the operating system is Windows XP Professional with Service Pack 1 or later, you must run `ICT XP.exe` found in *`installDirectory`*`\InControl\InControlMgmt\Tools` on these machines to set the correct permissions.
- If the target machine is not attached to a domain controller, and the operating system is Windows Vista or Windows Server 2008, please refer to the Microsoft article Connecting to WMI Remotely Starting with Vista for further instructions.
- If the target machine is Windows XP Home Edition or Windows Vista Home (basic or premium), WMI does not run on these machines, and iScanner will not scan them.

`Error #80070005: Access is denied.`

On Windows Server 2003 with Service Pack 1, the WMI class Win32_Product (Installed Software) is unavailable by default, and the Windows Installer Provider must be installed.

Resolution:

Refer to the FAQ in the *Serena Asset Manager Installation Guide* for instructions on installing the Windows Installer Provider.

Registry

`Error #5: Access is denied.`

This error normally indicates that a remote registry connection could be made, but invalid credentials were passed.

Resolution:

The resolution is the same as the WMI `Access is denied` error message in the previous section.

`Error #53: The network path was not found.`

iScanner was unable to establish a remote registry connection on the target machine.

Resolution:

The resolution is the same as the WMI `The RPC Server is Unavailable` error message in the previous section, with the exception that the second bullet does not apply.

WindowsSession

`Unable to create a trusted Windows connection with supplied user credentials.`

iScanner was unable to establish an SMB or CIFS (Windows File and Print sharing) connection to the target machine, or invalid credentials were used to establish the connection.

Resolution:

The resolution is the same as all WMI errors in the previous section.

Windows DI

ScanSystemDI: Remote Copy \\<IP Address>\ADMIN$\Temp\deviceinspector.exe failed: Error #5: Access is denied.

When attempting to remotely copy Windows Device Inspector, this error normally indicates that an SMB/CIFS connection to the remote machine was established, but invalid credentials were passed.

Resolution:

The resolution is the same as all WMI errors in the previous section.

ScanSystemDI: Remote Copy \\<IP Address>\ADMIN$\Temp\deviceinspector.exe failed: Error #35: The network path was not found.

When attempting to remotely copy Windows Device Inspector to the target machine, iScanner could not establish a network connection.

Resolution:

The resolution is the same as the WMI `The RPC Server is Unavailable` error message in the previous section, with the exception that the second bullet does not apply.

Chapter 6: Device Inspector

The Serena Asset Manager Device Inspector (DI) for Windows is a standalone utility designed to extract information from Windows computer systems (Including Windows 95/98/ME, NT4.0, Windows 2000, Windows XP, Windows 2003, Vista Windows 7, Windows 2008 /R2). The DI examines many aspects of a computer system, collecting information from a large number of sub-systems, and provides the results in a XML format. The DI is able to determine hardware characteristics, installed software, and configuration details from the target system while also being configurable in the type data it collects.

Using the Device Inspector

The Device Inspector is a command line utility that can be installed on any Windows computer system or in a Domain Login script and executed. Executing DI on a local system from a command line prompt invokes the product to analyze the system and store its details in an XML file in the current working directory. More advanced usage of the Device Inspector can be accomplished through the use of a configuration file or command line switches that can determine the different types of information to be collected, for specifying the output file name, or for automatically transferring the file to a remote FTP server.

The Device Inspector can also be executed from a shared network drive, a CD, or any portable drive or disk. Invoking the Device Inspector from this type of media should use the `-d` option described below to direct temporary and output files to a writeable directory.

The Device Inspector for Windows can also be used and launched within Windows Server or Active Directory Logon Scripts. This assists you in capturing devices that log into your network infrequently or for RAS/VPN users. The command lined method should be used under these circumstances to interact with your target machine. Contact Support to obtain additional assistance in using WHS or VBS scripting assistance.

Using a Configuration File

The DI looks for a `DIConfig.ini` configuration file in the same directory where the executable resides. The format of a sample configuration file is as follows:

- **FtpHostName=value**

  The 'value' is the name of the FTP Server to connect to. It can be specified in decimal notation like `192.168.123.102` or it can be a host name text like `SG-12` or `localhost`.

- **FtpUserName=value**

  The 'value' is The user name that will be used to authenticate with the FTP server.

- **FtpPassword=value**

  The 'value' is the password of the corresponding user.

- **FtpRemoteDirectory=value**

  The 'value' is the FTP virtual directory in the FTP server where the files are to be put. If not provided, then it does not change to any remote directory.

- **TimeOut=value**

  The 'value' is the time in milliseconds to wait before terminating the program. If not provided, the program takes a default value of `600000` (ten minutes).

- **LogType=value**
  This is the level of output detail to place into a log file. The 'value' is one of the following:

  - `error`
  - `detail`
  - `normal`
  - `nolog`

- **Include=value**

  The 'value' is the option or options you want to include in the search. See Include/Exclude Options below.

- **Exclude=value**

  The 'value' is the option or options you want to exclude from the search. See Include/Exclude Options below.

- **OutputFileName=value**

  The 'value' is the name of the output file.

- **OutputDirectory=value**

  The 'value' is the path to the directory in which the output file is created.

- **IncludeDirectories=value**

The 'value' is the list of directories that you want to search for specific patterns. The directory paths should be separated by a comma (,).

- **ExcludeDirectories=value**

  The 'value' is the list of directories that you want to exclude from a search for specific patterns. The directory paths should be separated by a comma (,).

- **FileSearchPattern=value**
  The 'value' is the list of the patterns you want to search for. The patterns can be any wildcard combination delimited by ','. For example:

  ```
  *.dll,*.doc
  ```

- **SearchWindowsDirectory=value**

  The 'value' is `yes`, if you want to search in WINDOWS directory. Otherwise, specify `no`.

If the DI is not able to find the configuration file, then the arguments given in the command line will be used.

Using Command Line Switches

Command line switches take precedence over configuration file settings. The switches that can be used in command line include:

- **-ftpoff**

  Disables transfer of the Device Inspector output file to a remote machine using FTP. Additional parameters `-hostname`, `-username`, `-password`, and `-remotedir` are ignored, as are any FTP options specified in the configuration file.

- **-hostname value (or) -h value**

  This option specifies the hostname of the remote machine to transfer the Device Inspector output file to using FTP. The 'value' can either be the IP address or a hostname.

- **-username value (or) -u value**

  This option specifies the user account name to use when transferring the Device Inspector output file using FTP. The 'value' here must be a valid user name on the FTP Server.

- **-password value (or) -p value**
  This option specifies the password of the corresponding user to use when transferring the Device Inspector output file using FTP. For example:

```
DeviceInspector.exe -[hostname/h] [hostname] -[username/u] [user name]
→-[password/p] [password]
DeviceInspector.exe -h ftp.mycompany.com -u anonymous -p MyPassword
```

- **-remotedir value (or) -r value**

This option specifies the FTP Virtual Directory on the FTP Server where the files are to be put. If not provided, then it does not change to any remote directory. For example:

```
DeviceInspector.exe -[h] [host name] -[u] [username] -[p] [password]
→-[r] [remote directory]
DeviceInspector.exe -h ftp.mycompany.com -u anonymous -p MyPassword
→-r /public/di_dest_directory
```

- **-timeout value (or) -t value**
  The 'value' is the time in milliseconds to wait before terminating the program. If not provided, the program uses a default value of `600000` (ten minutes). For example:

```
DeviceInspector.exe -[timeout/t] 300000
```

- **-include value (or) -i value**
  The 'value' is the scan option or options you only want to include. If this switch is not specified, all scan options are included by default. For all options, see Include/Exclude Options below. For example:

```
DeviceInspector.exe -[include/i] [options]
DeviceInspector.exe -i dmi,app,share
```

- **-exclude value (or) -x value**
  The 'value' is the scan option or options you want to exclude. This option is useful when you do not specify the `–include` option, but wish to exclude only a few scan options. If the `–include` option is specified, it overrides any options specified by `–exclude`. For all options, see Include/Exclude Options below. For example:

```
DeviceInspector.exe -[exclude/x] [options]
DeviceInspector.exe -x edi,net,file
```

- **-log value (or) -l value**
  Generate a log text file named `DIFullLog.txt`. The 'value' is the level of detail that you wish to log. The options include:
  - `error`
  - `detail`
  - `normal`
  - `nolog`

  For example:

```
DeviceInspector.exe -[log/l] [log type]
DeviceInspector.exe -[log/l] detail
```

- **-bioscall value**

Determines the method used to retrieve DMI (BIOS) information. Use this option if you select the DMI option from the Include/Exclude options described below. The 'value' is one of the following:

- **dos** – Get DMI information using the MS-DOS program `SMBDMP.EXE`. Use this option for scanning BIOS information on Windows 95, 98, and ME machines. The `SMBDMP.EXE` file must be present in the same directory as `DeviceInspector.exe` in order for this option to work.
- **nt** – Get DMI information using NT routines. Use this option for scanning BIOS information on Windows NT, 2000, XP, 2003 Server, and Vista machines. The `SMBDMP.EXE` program should not be present on the target machine, or it may cause problems with BIOS scanning.

For example:

```
DeviceInspector.exe -i DMI -bioscall nt
```

- **-output value (or) -o value**
  The 'value' here is the name of the Device Inspector scan output file. The file name is automatically appended with a `.xml` extension. For example:

```
DeviceInspector.exe -[output/o] [file name]
DeviceInspector.exe -[output/o] DI_Scan
```

- **-directory value (or) -d value**
  The 'value' is the directory path where the output file will get created. For example:

```
DeviceInspector.exe -[directory/d] [directory path]
DeviceInspector.exe -d "c:\MyWorkspace"
```

- **-searchinclude value (or) -si value**
  Use this option to specify a list of directories you want to include in searches if you have scanning files enabled. The 'value' is the list of the directories you want to search in, enclosed in double quotes and separated by commas. For example:

```
DeviceInspector.exe -[searchinclude/si] [DirectoryNames]
```

(Where `[DirectoryNames]` can be any wildcard combination delimited by ',' .

```
DeviceInspector.exe -i FILE -si "c:\mysql,c:\Program Files\"
```

- **-searchexclude value (or) -sx value**
  Use this option to specify a list of directories you want to exclude from searches if you have scanning files enabled. The 'value' is the list of the directories you want to exclude, enclosed in double quotes and separated by commas. For example:

```
DeviceInspector.exe -sx [DirectoryNames]
```

(Where `[DirectoryNames]` can be any wildcard combination delimited by ',' .

```
DeviceInspector.exe -i FILE -sx "c:\Program Files\"
```

- **-searchpattern value (or) -sp value**
  This option is used to specify the file patterns to match if you have scanning files enabled. The 'value' is the search patterns you want to search, separated by commas. For example:

```
DeviceInspector.exe -[searchpattern/sp] [Pattern]
```

  (Where `[DirectoryNames]` can be any wildcard combination delimited by ',' .

```
DeviceInspector.exe -i FILE -sp ACME*.doc,*.jpg
```

- **-searchwindows value (or) -sw value**
  This option is used to specify if you want to search in the WINDOWS directory when the option to scan files is specified. Specify the 'value' as `yes` or `no`. For example:

```
DeviceInspector.exe -[searchwindows/sw] [value]
DeviceInspector.exe -i FILE -sw no
```

- **-donotdelbin**
  If this switch is given at the command line, an intermediate binary file (`DI.BIN`) that is generated during DMI (BIOS) scans will not get deleted automatically at the end of the scan. This can be useful to send to Support for debugging and diagnostic checks if there are concerns or issues with Device Inspector. The `.bin` file is deleted by default. For example:

```
DeviceInspector.exe -i DMI -donotdelbin
```

- **/?**
  This switch is used to view the help. For example:

```
DeviceInspector.exe /?
```

Include and Exclude Options

These options are used with the Device Inspector configuration file settings `Include=` and `Exclude=` as well as the command line switches `-include` and `-exclude`.

Note the following:

- The options must be separated by commas (`,`).
- If both include and exclude lists are specified, then exclude list gets precedence over include list.

Operating System and Software Related Options

- **app/APP**
  Get the Installed Applications information. For example:

```
DeviceInspector.exe -[i/I] [app/APP]
```

- **appapi/APPAPI**

Get the Installed Applications only from the Windows MSI API Call. This advanced option causes Device Inspector for Windows to bypass checking the registry directly for installed software items and will instead cause it to only rely on a Microsoft Windows call which will retrieve software items that have been installed with the Microsoft Installer (MSI). If both `app` and `appapi` are specified, `appapi` are used. Please consult with Support before using this option. For example:

```
DeviceInspector.exe -[i/I] [appapi/APPAPI]
```

- **srvc/SRVC**
  Get the Windows Services information. For example:

```
DeviceInspector.exe -[i/I] [srvc/SRVC]
```

- **share/SHARE**
  Get the Windows Shared Folders information. For example:

```
DeviceInspector.exe -[i/I] [share/SHARE]
```

- **os/OS**
  Get the Operating System information. For example:

```
DeviceInspector.exe -[i/I] [os/OS]
```

- **lsa/LSA**
  Get the Local Security Policy information. For example:

```
DeviceInspector.exe -[i/I] [lsa/LSA]
```

- **profile/PROFILE**
  Get the User Profiles information. For example:

```
DeviceInspector.exe -[i/I] [profile/PROFILE]
```

- **user/USER**
  Get the Windows Users information. For example:

```
DeviceInspector.exe -[i/I] [user/USER]
```

- **inet/INET**
  Get the Internet Settings information. For example:

```
DeviceInspector.exe -[i/I] [inet/INET]
```

- **iis/IIS**
  Get the IIS Settings information. For example:

```
DeviceInspector.exe -[i/I] [iis/IIS]
```

- **file/FILE**

Gets file information of the files that matches the search pattern specified. By default search pattern is `*.exe`. For example:

```
DeviceInspector.exe -[i/I] [file/FILE]
DeviceInspector.exe -i file -sp ACME*.pdf,ACME*.xml
```

Hardware Related Options

- **net/NET**
  Get the Network information. For example:

```
DeviceInspector.exe -[i/I] [net/NET]
```

- **dmi/DMI**
  Get the BIOS information. For example:

```
DeviceInspector.exe -[i/I] [dmi/DMI]
```

- **Pnp/PNP**
  Get the plug-n-play hardware information. For example:

```
DeviceInspector.exe -[i/I] [pnp/PNP]
```

- **hdd/HDD**
  Get the hard disk information. For example:

```
DeviceInspector.exe -[i/I] [hdd/HDD]
```

- **drv/DRV**
  Get the logical drives information. For example:

```
DeviceInspector.exe -[i/I] [drv/DRV]
```

- **mon/MON**
  Get the monitor information. For example:

```
DeviceInspector.exe -[i/I] [mon/MON]
```

- **prn/PRN**
  Get the printer information. For example:

```
DeviceInspector.exe -[i/I] [prn/PRN]
```

- **disp/DISP**
  Get the display adapter information. For example:

```
DeviceInspector.exe -[i/I] [disp/DISP]
```

- **edi/EDI**
  Get the monitor EDID information. For example:

```
DeviceInspector.exe -[i/I] [edi/EDI]
```

- **pow/POW**
  Get the information related to the power supply and heat. For example:

```
DeviceInspector.exe -[i/I] [pow/POW]
```

When no switches are given, the FTP is disabled.

If `-ftpoff` switch is given, then the FTP service is disabled and the other FTP parameters, even when given, will not be considered.

Running the executable with the `/?` switch provides a help message with the possible arguments and their meaning.

Example Execution Commands

The following is a typical **Lightweight With Software** scan:

```
deviceinspector -bioscall nt -sw no -sp *.exe,*.dll -i NET,DMI,PNP,
→HDD,DRV,MON,DISP,EDI,PRN,SRVC,SHARE,USER,OS,APP,FILE -o DIOutput
```

In this example, the Device Inspector will:

- Query the system for network, BIOS, Plug and Play devices, hard disks, logical disk drives, monitors, monitor EDID information, printers, services, network shared folders, users, operating system information, installed applications, and file information.
- Use the Windows NT method for acquiring DMI (BIOS) information.
- Exclude the Windows directory from a file scan.
- Report only on files matching `*.exe` and `*.dll` for the file scan.
- Store the output in a file named `DIOutput.xml`.

As an alternative, the above command could be expressed with the exclude switch as follows:

```
deviceinspector -bioscall nt -sw no -sp *.exe,*.dll -x
→PROFILE,INET,IIS,LSA  -o DIOutput
```

A **Forensic scan** would be achieved as follows:

```
deviceinspector -bioscall nt -o DIOutput
```

CAUTION:

Use a comprehensive (forensic) scan with caution, as this can create very large XML scan files and take a long time to complete. Consider at least limiting the file scan with `-scanwindows no` and `-searchinclude <Directory List>` command line switches or configuration file equivalents.

Specify a **Power Information Only** scan (for use with a feature like ITGreen) as follows:

```
deviceinspector –i POW
```

To transfer the file across FTP using command line options, use a command such as:

```
deviceinspector –bioscall nt –sw no -sp *.exe,*.dll -x PROFILE,INET,IIS,LSA
→-o DIOutput –h ftp.yourcompany.com –u joeuser –p passwd –r /private/di_folder
```

The above command accomplishes everything for a **Lightweight With Software** scan, and then FTPs `DIOutput.xml` to `ftp.yourcompany.com` using `joeuser` and `passwd`, and places the file into the FTP virtual directory named `/private/di_folder`.

If you need to provide Support with detailed information regarding an issue with Device Inspector, you could specify a command line such as:

```
deviceinspector –noftp –d c:\temp –l detail –donotdelbin –o DIOutput –si
→"C:\Program Files" –sp *.exe
```

In this example, the Device Inspector will:

- Query all subsystems.
- Not use any FTP settings specified in the Device Inspector Configuration File.
- Use the directory `c:\temp` to store all temporary and output files.
- Generate a detailed log file named `DIFullLog.txt`.
- Keep the `DI.BIN` file, which can be sent along with the log and output file to Support for analysis.
- The final output is written to a file named `DIOutput.xml`.

Device Inspector Output

The Device Inspector creates an XML containing all the requested information. The default name for the output file is `DeviceInspectorOutput` with the date and time values of the XML creation time. This can be overridden using the command line switches with the `–o` option or the configuration file.

For example:

```
DeviceInspectorOutput_02112013_18545589.xml
```

Where 02112013 stands for 02 November 2013 and 18545589 stands for 18 hours 54 minutes 55 seconds and 89 milliseconds.

You can automatically upload the generated XML file to an FTP server by providing the connection parameters when you invoke the program.

Error Logging

Errors and important information are written to the `log.txt` file. This file is created in the same directory where the `.exe` resides. Normally only important information is logged. If

detailed logging is needed for debugging purposes, use the command line switch `-log`. Alternatively, set it in the Configuration File.

The log file is structured as follows:

- The first field in any line identifies whether that line contains error, information, or detailed Info.
- The second field contains the date and time of the event.
- The third field contains the actual message.

Advanced Information on Data Acquisition

Each of the data gathering methods function differently depending on the Windows operating system. The functionality of each method is detailed in this section.

- **Installed Applications Information Gatherer**
  Windows NT and Above:
  - The installer APIs (like `MsiEnumProducts`) are used to get information about installed products. If it fails, the registry is used to get the information.
  - After this, the information from `.dll`, `.exe`, and `.com` files are written to the XML file.

  Windows 9x Systems:
  - The registry is used to gather information, followed by `.dll`, `.exe`, and `.com` files
- **Windows Services Information Gatherer**
  Windows NT and Above:
  - The Win32 API `EnumServiceStatus` is used to get information about services. If it fails, the registry is used to get the information.

  Windows 9x Systems:
  - As there are no services in 9X systems, no service data is generated in the output.
- **Windows Share Data Information Gatherer**
  Windows NT and Above:
  - The Win32 API `NetShareEnum` is used to get information about shared folders. If it fails, the registry is used to get the information.

  Windows 9x Systems:
  - The Win32 API `NetShareEnum` is used. However, because this API is declared in `svrapi.lib`, this function is put into a separate DLL (`SoftwareInformation9x.dll`).
- **Windows User Information Gatherer**
  Windows NT and above:
  - The Win32 API `NetUserEnum` is used to get information about Windows users. If it fails, the registry is used to get the information.

Windows 9x Systems:

- The registry is used to get the User Names.

- **Local Security Policy Information Gatherer**
  Windows NT and above:
  - Win32 APIs (like `LsaQueryInformationPolicy`) are used. For security options, the registry is used.

  Windows 9x systems:
  - No local security policy information.

- **Operating System Information Gatherer**

  Windows NT and above, Windows 9x systems: A combination of Win APIs and registry calls are used.

- **Internet Settings Information Gatherer [Both Windows NT and Windows 9x]**

  The Windows registry is used to get the values.

- **IIS Settings Information Gatherer [Only Windows NT and Above]**

  This uses the COM object `IMSAdminBase` to get the IIS Settings. The settings are like those that can be seen using the MetaEdit Tool. All Keys under LM and SCHEMA are enumerated and their properties are retrieved.

Appendix

This appendix covers additional iScanner configuration topics.

Configuring the Power User Account

Microsoft security has been enhanced and updated as new service packs and operating systems have been released. In order to adapt to the security settings enforced by Microsoft, special care must be given to allow the user account configured in iScanner to access the data and protocols. Microsoft recommends using an administrator type of account to ensure proper authentication.

If you encounter environments that do not permit administrator privileges as outlined by Microsoft, you can make the following changes to the Power User account to permit access to the WMI service.

Perform the following steps:

1. From the Windows **Start** menu, click **Administrative Tools** and select **Computer Management** or right-click **My Computer** and select **Manage**.
2. Expand the **Services and Applications** node, right-click **WMI Control**, and select **Properties**.

   The **WMI Control Properties** dialog box appears.
3. Click the **Security** tab.
4. Expand the Root tree to display all the of the security namespaces. Select **CIMV2**, and then click the **Security** button.

   The **Security for ROOT\CIMV2** dialog box appears, and all of the accounts that have access to the WMI services are listed.
5. If the power user account is not listed, add the account to the list.
6. Select the power user account, and select **Allow** for the following permissions:
   - Execute Methods
   - Enable Account
   - Remote Enable
   - Read Security
7. Apply the changes, and click the **OK** button.

All the changes necessary to access the WMI components are now enabled. These settings will not allow the Device Inspector to run; that operation requires full Administrator rights based on Microsoft requirements.

Enabling Additional Attributes by Performing Custom Scans

To limit the size of scan output files and facilitate faster load times as a result, some less common attribute groups are disabled by default for **Lightweight With Software** and **Lightweight Without Software** types of scans. You may either perform a Forensic scan to get all attributes, or you can select **Custom** for the scan type and add the attributes that you are looking for. This section describes how to enable various component and attribute groupings in custom scans that you might find useful.

Windows Performance Metrics

WMI is able to collect Windows performance metrics, and Serena Asset Manager has tables that can report on this data. To enable collection of performance metrics, open the **Options** menu, select **Inventory**, and then **Configuration** (or press F6). In the **Inventory Configuration** dialog box, click the **Advanced** button next to the **WMI** check box. The **WMI Advanced Setup** dialog box appears.

Class to Activate	Description
Win32_PerfFormattedData_PerfDisk_LogicalDisk	Logical Disk
Win32_PerfFormattedData_PerfDisk_PhysicalDisk	Physical Disk
Win32_PerfFormattedData_PerfOS_Memory	Memory
Win32_PerfFormattedData_PerfOS_Processor	Processor
Win32_PerfFormattedData_PerfProc_Process	Process
Win32_PerfFormattedData_Tcpip_NetworkInterface	Network Interface

Plug and Play Attached Devices

To gather additional information about devices attached via the "Plug and Play" interface, enable the `WMI class Win32_PnPEntity` in the **WMI Advanced Setup** dialog box.

Additional WMI Hardware Attributes

The following additional WMI hardware classes have database tables for additional data gathering:

Class to Activate	Description
Win32_BaseBoard	Base Board
Win32_ComputerSystemProduct	Computer System Product

Class to Activate	Description
Win32_USBControllerDevice	USB Controller Device

WMI Software

The following software tables do not need to be activated if the **Registry** option is checked under the Windows Specific Inventory section:

Class to Activate	Description
Win32_Product	Installed Software (MSI Only)
Win32_QuickFixEngineering	Quick Fix Engineering

Important: It is not recommended to activate the class `Win32_Product` as this class does not always collect all installed software. In addition, there is a known issue with calling this class in which the target machine can have its installed software reconfigured back to original settings.

Device Inspector for Windows File Scanning

Device Inspector for Windows has the capability to scan a target machine for all executable (`*.exe`) files present on the system, and it can also be customized to scan for any type of file. This can sometimes be helpful in tracking down software that does not report itself to Windows as being installed (for example, it does not appear in the Control Panel section to remove software). However, enabling this option produces very large scan files that can take a long time to load. It is recommended that this option only be enabled if you have a specific need to track down executables or other file types.

To enable this feature, open the **Options** menu, select **Inventory**, and then **Configuration** (or press F6). In the **Inventory Configuration** dialog box, click the **Advanced** button in the **Device Inspector for Windows** section. The **Device Inspector for Windows Advanced Setup** dialog box appears. Select the **Custom** scan type, and select the **Files** option in the **Custom Scan Categories** section.

The following additional Device Inspector classes have database tables for additional data gathering that are not enabled by default:

- Internet Explorer Settings
- IIS Settings
- Local Security Policy
- Profiles
- Registry

Enabling Access to ESX and ESXi for Active Directory Accounts

Starting with ESX 4.1, you can use Active Directory accounts to scan ESX and ESXi servers for inventory. iScanner does not require root or administrator privileges to perform this operation; the account may be granted a minimum read-only permission.

To add Active Directory accounts, the ESX and ESXi servers must allow authentication against a domain controller. Please refer to your ESX administration guide for complete details on how to do this.

Once your ESX servers are set up to authenticate to your domain controller, you must perform one of the following two tasks to grant permission to the iScanner credentials to allow inventory:

- Assign Read-Only permission on each ESXi server by performing the following steps:
  1. Launch vSphere Client, and connect to the ESX/ESXi server.
  2. Click the **Permissions** tab.
  3. Right-click the list of users, and select **Add Permission**.
  4. Click **Add**.
  5. Select **AD** in the **Domain** drop-down list.
  6. Select the credentials you will use from the list of users.
  7. Click **Add**.
  8. Click **OK**.
  9. Set **Assigned Role** to **Read-only**.
  10. Click **OK**.
  11. Repeat for each ESXi server.
- Add the credentials you will use for scanning into the Active Directory group named `ESX Admins`. This automatically propagates rights to all ESX servers that authenticate against the domain controller, at the expense of placing the selected credential in the Administrator group on all ESX machines. Please refer to your ESX administration guide for complete details.