CONFIGURATION GUIDE

Product	Snow Inventory Agents
Version	5
Release date	2016-09-27
Document date	2020-11-19

CONTENTS

1 INTRODUCTION

This document describes the configuration of the Snow Inventory Agents.

The Snow Inventory Agents are part of the Snow Inventory solution. They are used for inventory of Windows, Linux, macOS, and Unix computers. The agents scan the computers and save the collected data to encrypted files, which are sent to a Snow Inventory server (Master Server or Service Gateway).

2 AGENT CONFIGURATION

The configuration file of the Snow Inventory Agents is named **snowagent.config**, an XML file stored in the installation folder or directory. The file contains settings defining what to inventory, when to inventory, and where to send the inventory result.

Agent configurations are created and edited in the Snow Inventory Admin Console which is accessed via Snow Management and Configuration Center.

A configuration can be deployed to all, or to a subset of devices. Configuration updates can be deployed remotely if the agent has been configured to check for updates (recommended). For manual deployment of updates, it is possible to create the configuration in the Admin Console and then export it to an XML file.

For a complete list of all configuration parameters, refer to the *configuration-doc.html* file available in the Snow Support portal: *Configuration document for all Inventory agents*.

NOTE

- To ensure correct functioning of the agent, the syntax of the agent configuration file must be correct. Manual editing of this file is not recommended. As far as possible, any changes should be made via the Snow Inventory Admin Console.
- All elements in the agent configuration file are case-sensitive.

3 VIRTUALIZATION AND TERMINAL SERVERS

NOTE

- Configuration for virtualization and Terminal servers is only available for the Snow Inventory Agent for Windows.

3.1 VIRTUAL DESKTOPS

When using the Snow Inventory Agent in a Virtual Desktop Infrastructure (VDI), there are some configuration settings that need to be applied to ensure accurate capture of all activities on each virtual desktop.

3.1.1 VDI AWARENESS

To utilize the functionality for VDI and VDA license calculations in Snow License Manager, the computer needs to be aware of that it is a part of a VDI. This is done using a system setting in the configuration file:

env.is_virtual_desktop_infrastructure=true

Typically this configuration is set during the creation of the MSI package but can also be modified after deployment using the Snow Inventory Admin Console.

3.1.2 AGENT INSTALLATION

The Snow Inventory Agent needs to be installed on all virtual desktops. This can be achieved either by installing the agent in the global image (a.k.a. Golden Image), or by deploying it as a part of the VDI provisioning process.

3.1.3 CAPTURE ASSURANCE

To ensure that all VDI sessions and application usage within the VDI are captured, a script needs to be executed as a part of closing down the Virtual Desktop session. The script will trigger the scan and send the result to a Snow Inventory Server before allowing the session to terminate. Depending on what infrastructure the VDI is running on, different solutions exist for running scripts as a part of the VDI decommission. For more information, contact Snow Support.

3.2 VIRTUAL APPLICATIONS

The Snow Inventory Agent for Windows has support for several technologies for application virtualization, including Microsoft App-V (previously known as SoftGrid App-V). Both inventory and usage of virtual applications are performed.

As from Microsoft App-V version 5.0 the agent is able to identify what applications are running virtualized and correctly identify them as such, as with any other application that is locally installed.

The agent will also recognize VMware ThinApp and Citrix Virtual Apps applications as virtual.

3.3 TERMINAL SERVERS

The Snow Inventory Agent for Windows has support for monitoring remote usage on Citrix and Windows Remote Desktop servers. No additional configuration is required.

4 WEB APPLICATIONS

NOTE

- Metering of Web applications is only available for the Snow Inventory Agent for Windows.

The Snow Inventory Agent for Windows can meter usage of web applications. The configuration of which web applications to meter is done in the web user interface of Snow License Manager.

To enable web application metering **legacy_webmetering.is_enabled** must be configured to **true**.

NOTE
From Snow Inventory Agent 6.2 for Windows, the setting **idx.endpoint** is deprecated. Snow Inventory Agent 6.2 for Windows will retrieve the web application patterns from the first available endpoint in the Snow Inventory Agent configuration file.

Web application patterns will be retrieved every eight hours and when the Snow Inventory Agent is started or restarted.

If new or updated patterns are available they will be downloaded by the agent and stored in the file **webapps.config**.

All web application patterns in the **webapps.config** file are monitored for usage. The usage is recorded independently of which type of application connects to the web host, i.e. a web browser or any other application.

Web applications are monitored by the explicit host names and ports that are configured for use. For example, if a user has Snow Inventory Agent for Windows installed, web application metering is enabled, and Snow Inventory Agent is configured to monitor use of www.google.com on port 80, usage of that site will be metered. If the same user is using a proxy, or some other kind of technology that redirects network traffic, so that www.google.com looks like proxy.external.example.com, and/or port 80 is redirected to port 3128, metering will not be possible.

5 ORACLE DATABASE PRODUCTS

NOTE

- Inventory of Oracle database products is only available for the Snow Inventory Agents for Linux, Unix, and Windows

The Snow Inventory Agent can perform inventory of Oracle database products. Automatic discovery and inventory of all Oracle instances on the computer is achieved by the Snow Inventory Oracle Scanner (SIOS).

NOTE
SIOS requires Java Runtime Environment 6.0 (1.6) or later to be installed. Due to an internal defect in Java, Java Runtime Environment 1.7.0_7 must not be used.

When Oracle scan is enabled in the configuration, the agent will be triggered to run SIOS as part of the inventory process, and automatically perform an inventory of all Oracle database instances found. For information on advanced configuration options for the Oracle database inventory, refer to the User guide for *Snow Inventory Oracle Scanner*.

If multiple versions of Java are installed on a computer and the default Java version available in the path is not version 1.6 or later, the system setting named **env.java_home** in the configuration file can be used to specify the location to the Java installation to use. The agent will then try to run Java using the following path to the executable:

<Setting key="env.java_home" value="/usr/bin/java"/>

This setting controls the Java version of the SIOS, and is applicable to the Windows and Linux agents.

6 SCHEDULING

NOTE

- Configuration for scheduling is only available for the Snow Inventory Agent for Windows.

The Snow Inventory Agent for Windows can be configured to run on a daily, weekly, or monthly basis or at system start-up. Configuration of the schedule is done via the Snow Inventory Admin Console.

Randomization can be applied to the daily, weekly, and monthly occurrence types. It adds a random delay each time a scan is scheduled which will spread the start time among the agents and distribute the load when many agents are configured to scan at the same time.

When a scheduled scan is completed, the result will be sent immediately to an Inventory server.

7 OUTPUT DATA

The output of the inventory scan is an encrypted and compressed file containing inventory data, meta-information on the inventoried client, current configuration file of the agent (snowagent.config), and any critical events from the agent log.

The output file will be placed in the **data** subdirectory if no other output path has been specified in the configuration.

NOTE
Since the log data is sent once a day, a comparison of the local log file (in real time) and the log file displayed in the Snow Inventory Admin console (updated daily) at a given point in time will probably show differences.

8 SERVER ENDPOINTS AND DROP LOCATIONS

The agents can deliver the encrypted files in different ways, for example over HTTPS, which is the most common (and recommended) way, or by writing the result to a file share. For this, server endpoints and drop locations are configured.

8.1 SERVER ENDPOINT

A server endpoint represents a possible path for delivery. The Snow Inventory Agent establishes a connection and sends the output file to an Inventory server endpoint defined in the configuration. When several endpoints have been defined, the agent randomly selects one from the list. It tries at least once for each endpoint. As soon as it has successfully managed to negotiate a connection it will use that one for the remainder of the session.

NOTE
The more server endpoints defined in the agent configuration, the longer it will take to negotiate a connection. This is typically not an issue but when writing scripts, keep in mind that it may introduce a significant delay since the agent has to timeout on a bad server endpoint configuration before it can try the next one.

8.2 DROP LOCATION

A drop location represents an additional location for delivery of the scan result. It can be network folder, an HTTP endpoint, or an UNC file path. If several one drop locations have been defined, the scan result will be sent to all of them.

NOTE
If the agent cannot reach a drop location during the send activity, it will not try to resend the file later.

9 SECURITY

9.1 ENCRYPTION OF PASSWORDS

Passwords used in the configuration file are automatically encrypted when the configuration file is managed via the Snow Inventory Admin Console.

9.2 DATA ANONYMIZATION OPTIONS

The Snow Inventory Agent can be configured to send anonymous user data from the inventoried computer. It can also be configured not to inventory any IP addresses assigned to the network interfaces of the computers.

9.2.1 ANONYMOUS USER DATA

Both usernames of logged on users and usernames within the software metering (i.e. users who have used applications on the computer) can be replaced with SHA-1 hash. The same encrypted string will be used for the same user each time, even if the user uses multiple computers, no duplicate entries are created.

To enable the anonymous user data option, the following system setting needs to be added to the configuration file:

privacy.hide_user=true

EXAMPLE

Default setting (not anonymous):

With **privacy.hide_user=true** (anonymous):

9.2.2 ANONYMOUS IP ADDRESSES

The IP addresses assigned to the network interfaces of the computer can be replaced with SHA-1 hash. Add the following system setting to the configuration file:

privacy.hide_ip=true

NOTE
When this option is enabled, it is not possible to use Auto Connect Rules in Snow License Manager based on computer IP addresses for allocation of computers to different units in the organization structure. However, other criteria can still be used for Auto Connect Rules, such as computer hostnames and site names.

9.3 COMMUNICATION

It is possible to use any combination of X.509 certificates to secure and authenticate communication between the agent and the server.

If the server certificate has been issued by a trusted root certificate authority (CA), no additional configuration is required other than to configure the agent to use the HTTPS (or HTTP) URI scheme.

9.3.1 SELF-SIGNED OR SELF-ISSUED CERTIFICATES

If a self-signed or self-issued certificate is used to secure communication, i.e. a certificate that is not installed in the trusted root certificate store of the computer, the agent needs to be configured to ignore warnings about unknown CA's. Use the following system setting in the configuration:

http.ssl_verify=false

This setting is disabled by default.

NOTE
The system setting **http.ssl_verify=false** does not work on Mac OS X 10.8. Even if the setting is set to false, the agent will still try to verify the server's CA certificate.

NOTE
Read Configuring the agent for public key pinning for more security-related information in regards to certificates.

9.3.2 CLIENT AUTHENTICATION USING CERTIFICATES

The Snow Agent supports use of client certificates. The certificates need to be password protected, and the password must be stored (encrypted) in the agent configuration file.

A common practice is to distribute the client certificate alongside the agent as part of the update package. The agent is then configured to look for a **certificate.pfx** file that contains the client certificate for client authentication and use that (provided it has the correct password).

If the server endpoint is used with a client certificate and the password does not match, an error is generated in the **snowagent.log**. The agent will continue with other server endpoint configurations, if any have been set.

NOTE
Specify one client certificate per server endpoint. It is possible to have multiple entries for the same server endpoint with different client certificates

9.3.3 COMMUNICATION USING TLS

To be able to use Transport Layer Security (TLS) 1.2 for the communication between the Inventory agent and the Inventory server, the following requirements need to be met:

- The Windows operating system of the Inventory server (both Master Server and Service Gateway) must be updated to enable the TLS 1.2 protocol for SHA512 certificates. See article https://support.microsoft.com/en-us/help/2973337/sha512-is-disabled-in-windows-when-you-use-tls-1-2.
- **Windows agent**
  The root certificate (.cer) must be installed in the Trusted Root Certification Authorities of the computer to be inventoried.
- **Linux and macOS agents**
  In the configuration file of the agent, the setting **<Setting key="http.ssl_capath" value="" />** must point to the certificate file (.pem).
- **Unix agent**
  The certificate file (.cer) needs to be put in the **/opt/snow/** directory of the computer to be inventoried.
  If the "RSA premaster secret error" entry is shown in the log, the components **local_policy.jar** and **US_export_policy.jar** need to be updated in Java.

10 TROUBLESHOOTING

10.1 COMMUNICATION

If a computer with the Snow Agent installed is unable to send inventory result to the server, the following steps can be performed.

10.1.1 VERIFY COMMUNICATION

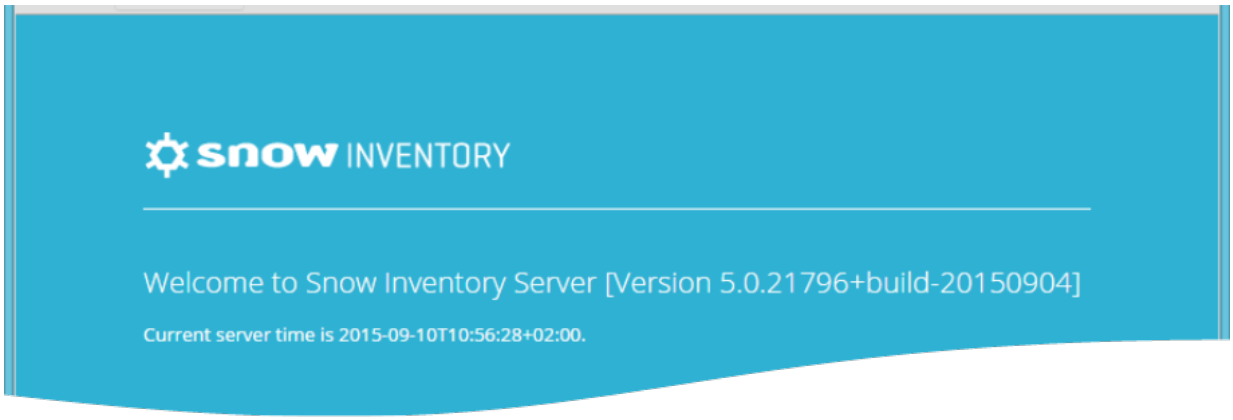
From a command prompt, use the following command to run a self-test that checks server connectivity, and then exits with a 0 (if successful) or a non-zero exit code:

```
snowagent.exe test
```

- or -

```
snowagent test
```

To test that the Snow Agent can communicate with the server, open a browser and browse for the server endpoint. After a successful connection a page similar to this is opened:



NOTE
When performing this manual test towards the Inventory server, do not type /inventory.asmx or /v1/inventory.ashx at the end of the server address.

Example of URL: https://myserver