

User Agent Options and Troubleshooting How-To

Table of Contents

Introduction to the User Agent	3
System Requirements	4
Supported Operating Systems	4
Other Requirements	4
User Agent Options	5
Options in the User Agent Interface	5
Blacklisting.....	5
Registry Options	6
Troubleshooting	6
DNS Resolving	6
Syntax for Username.....	6
User Information in Files	7
Running the User Agent Troubleshooting Tool	8
Using the Windows Management Instrumentation Tester	9
Configuring Windows Server 2008 R2 and Windows Server 2003 R2	11
Collecting Diagnostics	12

Introduction to the User Agent

The User Agent is an optional software component that can be installed either locally on the Active Directory Domain Controller or on another Windows system in the domain. The User Agent communicates with the Domain Controller to associate users with IP addresses. If a domain has many Domain Controllers one User Agent can be set to collect user information from them all. The same User Agent can send user information to several Security Engines.

Preparing the Windows environment for the User Agent to be able to collect user information is presented in a separate document. See [KB 78750](#).

This document outlines additional configuration options available in the User Agent interface and also describes troubleshooting steps if the User Agent is not able to retrieve user information or the User Agent is not forwarding user information to the engine.

The initial configuration for the User Agent is exported from the SMC and imported to the User Agent. Further configuration information is received from the engine when the engine's policy is refreshed. When communication has been established between an engine and the User Agent, you must refresh the engine's policy every time the User Agent or Active Directory Domain Controller settings are modified in the engine's properties. The engine then forwards the new configuration to the User Agent. You only need to manually re-import the configuration to the User Agent if the connecting Security Engine or User Agent elements change.

System Requirements

Supported Operating Systems

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

All the systems must have Microsoft .NET Framework version 2.0 and Microsoft Visual C++ Redistributable installed. Both of these are included with the User Agent installer.

Other Requirements

- 4GB of RAM, depending on the number of users and groups in the Active Directory database
- 5GB free disk space

Note! Do not install the User Agent on a network drive.

- The Domain user used by User Agent must have access rights to security event logs on each Domain Controller and permission to execute LDAP queries. WMI connections use TCP/135 (DCOM). Reverse connections use a high random port.
- Domain Controllers must have a non-SSL port open for LDAP queries (usually TCP/389).
- The system on which the User Agent runs must be able to receive connections from Security Engines on port 16661.

Note! Execution of WMI queries may consume a large amount of system resources. This may decrease the performance of the Domain Controller.

User Agent Options

Some User Agent options can be configured in the User Agent interface. Other options can be configured through Windows registry keys.

Options in the User Agent Interface

The following options can be configured in the User Agent interface:

Option	Description
Port	This option allows you to change the default port used for communication with the Security Engine. You must also change the port in the properties of the User Agent in the Management Client.
Backread	When the User Agent is started, it queries the Domain Controller's security logs backwards in time to detect users who have recently logged in. The Backread option defines (in minutes) the time period for which this check is done.
Logs Path	This option allows you to change the location in which the logs are saved.
Workstation Monitoring	The User Agent can be set periodically to send ICMP echo (ping) requests to users' workstations to monitor whether the workstation is still connected to the network. If a user's workstation does not respond, the workstation's IP address-to-username binding is removed from the list of IP addresses. In cases where ping requests to workstations are not allowed or are unreliable, Workstation Monitoring should not be enabled.
Diagnostics Log Level	The User Agent creates logs related to its operation. By default User Agent writes Medium level log. At setup time it is reasonable to set the Diagnostics Log Level to High .

Blacklisting

Some users and IP addresses can be ignored by adding them to the blacklist file. Information about events associated with these users or IP addresses is not sent to the Security Engine. This may be useful with terminal servers or other machines where several users are connected at the same with their domain user accounts.

By default, the blacklist file is located in `C:\Program Files (x86)\Stonesoft\Stonesoft User Agent\Logs\blacklist.txt`. The file name and path can be modified using the `BlacklistFileLocation` and `BlacklistFileName` keys in the Windows registry.

To add blacklist entries

1. Edit the blacklist file.
2. Add blacklist entries in one the following formats:
 - User name (for example, Alice)
 - IP address (for example, 192.168.1.1)
 - User@IPAddress (for example, Alice@192.168.1.1)

Note! Each line in the blacklist file is treated as a separate entry.

Registry Options

There are some local settings for the User Agent that you can edit in the Windows registry. Normally there is no need to change the default values. The settings are available under the following paths:

- 32-bit systems: HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\Stonesoft
- 64-bit systems:
HKLM\Software\WoW6432\Microsoft\Windows\CurrentVersion\Uninstall\Stonesoft

Troubleshooting

DNS Resolving

The computer on which the User Agent is installed must be able to resolve all of the Domain Controllers from which it collects logs.

Starting from version 1.1.6, the User Agent is able to operate in environments where the DNS domain name is not the same as the AD domain name. Starting from version 1.1.6, the User Agent no longer performs reverse DNS queries to the IP addresses found from the Event log to verify the workstation name and DNS name.

Syntax for Username

The username that the User Agent uses to collect login events from the Domain Controller is defined on the Domain Controllers tab in the Active Directory Server element properties in the Management Client. The syntax for the username is **username** or **username@domain**. If the username is specified without the domain name, the DNS suffix of the computer where the User Agent is installed must match the Active Directory domain name.

User Information in Files

CacheDiagnostic.txt

The User Agent periodically makes LDAP queries to the Domain Controller to query all users and their groups. The LDAP query results are written to the `CacheDiagnostic.txt` file stored in the User Agent log directory.

When the User Agent retrieves user login information, it uses the LDAP query results to forward both the user name mapping to IP addresses, and the user groups to the Security Engine. Group information forwarded to the Security Engine is based solely on these LDAP query results. Matching in the Security Engine's Access rules is based on user names and groups found from the LDAP query results.

An Event log query is different from an LDAP query. Event log query results must have a match in the `CacheDiagnostic.txt` file based on an earlier LDAP query for user information to be forwarded. If the User Agent gets an "Event log for user not found" response, user information based on the query is not forwarded to the Security Engine.

UserDiagnostic.txt

The `UserDiagnostic.txt` file is located in the User Agent log directory. This file lists the user information that the User Agent has been able to retrieve from the Domain Controller(s), information that has passed verification, and user name mapping to IP addresses that has been sent to the Security Engine. In addition to user names and IP addresses, the file also lists the time when the User Agent detected the login. The content of this file should match the name cache on the Security Engine in `/proc/stonegate/name_cache/names`.

storeUsers.txt

The `storeUsers.txt` file is written when the User Agent is shut down. When the User Agent restarts, this file is read, and user information is sent to the Security Engine as the last known status of the user name mapping to IP addresses. You can reset the information learned by the User Agent by stopping the User Agent, removing this file, and restarting the User Agent. Otherwise, the User Agent continues to report the last user name associated with a particular IP address to the Security Engine based on information in the file.

Running the User Agent Troubleshooting Tool

The User Agent Troubleshooting Tool is a testing tool that allows you to diagnose some common configuration problems. The Troubleshooting Tool is installed as part of the User Agent installation. The Troubleshooting Tool runs tests by making connections and queries in a similar way to the User Agent. Run the Troubleshooting Tool separately for each Domain Controller monitored by the User Agent.

If a test fails, the Troubleshooting Tool displays errors that provide information about which settings in the configuration should be checked. The Troubleshooting Tool also proposes a possible solution.

Note! Some problems in the User Agent configuration may be outside the scope of the Troubleshooting Tool.

To run the troubleshooting tool

1. Click **Start**.
2. Browse to **Stonesoft→Stonesoft User Agent→Troubleshooting Tool**. The User Agent Troubleshooting Tool starts.
3. Enter the following information:
 - **Domain Controller:** IP address of the Domain Controller that the User Agent connects to while running the diagnostics.
 - **Username / Password:** Credentials of the domain user account used by the User Agent to monitor the Domain Controller.
4. Click **Run Tests** and wait for diagnostic process to finish. This may take several minutes. The progress and results of the tests are displayed in the Progress field.

Using the Windows Management Instrumentation Tester

Issues related to Windows Management Instrumentation (WMI) can be diagnosed using the Windows Management Instrumentation Tester (wbemtest) tool. The Management Instrumentation Tester makes connections and queries in a similar way to the User Agent. This allows you to verify whether the Management Instrumentation Tester can successfully make connections and queries that fail for the User Agent. If the Management Instrumentation Tester communication also fails, there is likely a configuration issue with the access rights for the User Agent user. Run the Windows Management Instrumentation Tester separately for each Domain Controller monitored by the User Agent.

To start the Windows Management Instrumentation Tester

1. Click **Start** and type **wbemtest.exe**. The Windows Management Instrumentation Tester starts.
2. Click **Connect**. You are prompted to enter the connection details.
 - If you are connecting to a remote Domain Controller, proceed to step 3.
 - If you are running tests locally on the Domain Controller, proceed to step 4.
3. *(If connecting to a remote Domain Controller)* Enter the following information and proceed to step 5.

Option	Value
Namespace	\\<IP address of Domain Controller>\root\cimv2
User	Credentials for the domain user account used by the User Agent to monitor the Domain Controller.
Password	
Impersonation Level	Impersonate.
Authentication Level	Packet privacy.

4. *(If running tests locally on the Domain Controller)* Enter the following information:

Option	Value
Namespace	root\cimv2
User	Leave empty (tests are run as the currently logged in user).
Password	
Impersonation Level	Impersonate.
Authentication Level	Packet privacy.

5. Click **Connect**. A WMI connection is established to the Domain Controller and the options in the Windows Management Instrumentation Tester dialog are enabled.

To run tests using the Windows Management Instrumentation Tester

1. Select **Synchronous** in the Method Invocation Options section.
2. Click **Query**. The Query dialog opens.
3. Enter `SELECT * FROM Win32_OperatingSystem` and click **Apply**. The query result opens in a new dialog and the result status is "Done".

Tip: It may be helpful to take screen captures of the query results to provide to McAfee support if a support request needs to be opened.

4. Click **Close**.
5. Repeat steps 2-4 with one of the following queries depending on the Windows Server version that the Domain Controller runs:

Windows Server Version 2003

```
SELECT * FROM Win32_NTLogEvent WHERE Logfile="security" AND EventType=4 AND EventCode=673
```

Windows Server Version 2008

```
SELECT * FROM Win32_NTLogEvent WHERE Logfile="security" AND EventType=4 AND EventCode=4769
```

6. Select **Semisynchronous** in the Method Invocation Options section.
7. Click **Notification Query**. The Query dialog opens.
8. Enter one of the following queries depending on the Windows Server version that the Domain Controller runs:

Windows Server Version 2003

```
SELECT * FROM __InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32_NTLogEvent' AND (TargetInstance.SourceName='Security' OR TargetInstance.LogFile='Security') AND TargetInstance.EventIdentifier=673
```

Windows Server Version 2008

```
SELECT * FROM __InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32_NTLogEvent' AND (TargetInstance.SourceName='Security' OR TargetInstance.LogFile='Security') AND TargetInstance.EventIdentifier=4769
```

9. Click **Apply**. This query may take some time to finish. The query result opens in a new dialog and the result status is "Done".

Configuring Windows Server 2008 R2 and Windows Server 2003 R2

On Windows Server 2008 R2 and 2003 R2, Kerberos settings may prevent the User Agent user from accessing the Security Event logs. You may need to configure the following settings depending on the server's configuration.

Note! Enabling these settings may cause excessive log generation on the server.

To configure Windows Server 2008 R2 and Windows Server 2003 R2

1. Click **Start** and browse to **Administrative Tools**→**Group Policy Management**.
2. Browse to **Group Policy Objects** and click **Default Domain Controllers Policy**.
3. Switch to the **Settings** tab.
4. Right-click the tab and select **Edit**.
5. Browse to **Computer Configuration**→**Policies**→**Windows Settings**→**Security Settings**→**Advanced Audit Policy Configuration**→**Audit Policies**→**Account Logon**.
6. Set the following options to Success:
 - Audit Kerberos Authentication Service
 - Audit Kerberos Service Ticket Operations

Collecting Diagnostics

The Diagnostics tool collects User Agent configuration information and logs. The Diagnostics tool is installed during the User Agent Installation.

If you were not able to diagnose and solve the User Agent issue using the tools and information presented in the previous sections of this document, you may need to contact McAfee support. You can use the Diagnostics tool to collect troubleshooting data for support.

Note! Select High as the Diagnostics Log Level in the User Agent interface before collecting Diagnostics.

1. Click **Start**.
2. Browse to **Stonesoft**→**Stonesoft User Agent**→**Diagnostics**. The Collect Diagnostics dialog opens and the Diagnostics tool starts gathering diagnostic information. This process may take several minutes.
3. After all necessary information is collected, click **Save Diagnostics**.
4. Browse to the location where you want to save the diagnostic package and enter a name for the file. A default name is suggested.
5. Click **Save**.
6. When contacting support, deliver the diagnostic package along with an sgInfo package collected from the Security Engine with a clear-text policy installed.

Copyright © 2015 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.