



1.0 **TippingPoint™**

Identity Agent Deployment Guide

Legal and notice information

© Copyright 2017 Trend Micro Incorporated. All rights reserved. TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. TippingPoint Reg. U.S. Pat. & Tm. Off. All other company and/or product names may be trademarks of their respective owners.

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced in any form or by any means, or translated into another language without the prior written consent of Trend Micro Incorporated. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

Contents

Overview.....	1
System requirements.....	2
Installation summary.....	3
Pre-installation steps.....	5
Create a new Active Directory user.....	5
Add the user to the Domain Administrators group.....	6
Assign permissions for the Active Directory user.....	6
Windows Firewall.....	7
Enable predefined Windows Firewall rules.....	8
Create a new Inbound Windows Firewall rule.....	8
Specify the amount of Identity Agent data to retain in the SMS.....	9
Install Identity Agent.....	11
Add logon credentials for the Identity Agent service.....	11
Provide full access for the Identity Agent service account.....	12
Allow port access for Identity Agent user.....	13
Identity Agent.....	14
Identity Agent configuration.....	14
Create the initial Identity Agent configuration.....	15
Manage domain controllers.....	16
Add an IP address to the Mapped IPs list.....	16
Remove an IP address from the Mapped IPs list.....	17
Add an IP address to the Excluded IPs list.....	17
Remove an IP address from the Excluded IPs list.....	17
Manage custom schemas.....	17

Uninstall Identity Agent.....	19
Where to go next.....	20
Identity Agent issues and resolutions.....	21
Agent service not able to query domain controller security log events.....	21
Agent service not able to query domain controller OS information.....	22
OS information resolution.....	23
Agent service is not able to communicate to domain controller.....	26
To enable Windows Firewall rules.....	26
Agent service running but not querying domain controllers for security event logs.....	29
To modify the account.....	29
Agent service is not creating db and logs folders.....	30
To provide full access.....	30
Agent APIs are not listening in agent port.....	32
Agent APIs are not accessible outside agent server.....	33
Groups API call response with no data.....	34
Configuration changes are not reflected in the agent service.....	34
SMS is not able to establish connectivity with the Identity Agent.....	35
Agent not able to establish LDAP connectivity.....	36
Agent not able to establish secure LDAPS connectivity.....	36
To test domain controller connectivity.....	36
To test agent machine connectivity.....	38

Overview

This guide provides information for installing and configuring the Identity Agent in a Windows environment (Windows Server 2008, 2008 R2, 2012, and 2012 R2).

Once configured, the Identity Agent will poll the Active Directory domain controller to collect user account and user group information. The Identity Agent will also poll the domain controller for security login events.

Once the SMS is configured to poll the Identity Agent, the SMS will display the User ID to User IP correlation and security login events.

You can configure the Identity Agent to:

- Connect to one or more domain controllers to poll user login information.
- Change the default user/group and security log connection settings.
- Enable secure LDAP.
- Map or exclude IP addresses.
- If you customized your Active Directory schema, you can match the same schema in the Identity Agent.

System requirements

The tables in this topic provide the hardware, operating system, and software requirements for the Identity Agent.

Hardware requirements

RAM	4 GB
Disk space	40 GB

Supported server operating system

Note the following requirements for the Identity Agent and the Active Directory Server.

Operating system	Supported editions
Windows Server 2012 R2	64-bit
Windows Server 2012 (64-bit edition)	64-bit
Windows Server 2008 R2	64-bit
Windows Server 2008	64-bit

Microsoft Kerberos

Microsoft Kerberos is an integral part of an Active Directory implementation. Kerberos provides secure user authentication that permits interoperability. The Active Directory domain controller maintains user account and log-in information to support the Kerberos service.

The Identity Agent depends on Kerberos protocol being used in the Active Directory authentication process. To make use of Kerberos, you must add Kerberos to your Active Directory Server.

Installation summary

These checklists include cross-reference links to important concepts and tasks about deploying the Identity Agent. Complete the tasks in this checklists in order.

When a reference link takes you to a topic, return to this topic after you complete the tasks so that you can proceed with the remaining tasks in this checklist.

If the Identity Agent Service account will have Administrative permissions

Follow the steps below if the Identity Agent Service account will have administrative permissions.

Step 1	Enable predefined Windows Firewall rules on page 8
Step 2	Create a new Inbound Windows Firewall rule on page 8
Step 3	Add logon credentials for the Identity Agent service on page 11
Step 4	Provide full access for the Identity Agent service account on page 12
Step 5	Specify the amount of Identity Agent data to retain in the SMS on page 9
Step 6	Install Identity Agent on page 11
Step 7	Create the initial Identity Agent configuration on page 15

If the Identity Agent Service account will not have Administrative permissions

Follow the steps below if the Identity Agent Service account will not have administrative permissions.

Step 1	Create a new Active Directory user on page 5
Step 2	Add the user to the Domain Users group on page 11
Step 3	Assign permissions for the Active Directory user on page 6
Step 4	Enable predefined Windows Firewall rules on page 8

Step 5	<i>Create a new Inbound Windows Firewall rule</i> on page 8
Step 6	<i>Add logon credentials for the Identity Agent service</i> on page 11
Step 7	<i>Provide full access for the Identity Agent service account</i> on page 12
Step 8	<i>Specify the amount of Identity Agent data to retain in the SMS</i> on page 9
Step 9	<i>Allow port access for Identity Agent user</i> on page 13
Step 10	<i>Install Identity Agent</i> on page 11
Step 11	<i>Create the initial Identity Agent configuration</i> on page 15

Pre-installation steps

This section describes the items that must be done before installing the Identity Agent. Instructions are included in each topic.

Before you begin, see the [Installation Summary](#) on page 3 and the latest *TippingPoint SMS Release Notes* available on the TMC.

Important: To secure your environment against POODLE, disable SSLv3 in the Windows OS where the Agent will be installed. For assistance, contact Microsoft.

Create a new Active Directory user

Use Active Directory Users and computers to create a new user account. This user account will be used for running the agent service and connecting to the domain controllers.

As a security best practice, consider using **Run as Administrator** to perform this procedure. This procedure must be preformed on the domain controller.

1. Open Active Directory Users and Computers (**Start > Control Panel > Administrative Tools > Active Directory User and Computers**).

To open Active Directory Users and Computers in Windows Server 2012, click **Start**, and then type **dsa.msc**.

2. In the console tree, right-click the folder in which you want to add a user account.
3. Point to **New**, and then click **User**.
4. Enter the following information, and then click **Next**.

Field	Description
First name	Type the user's first name.
Last name	Type the user's last name.
Full name	Modify the user's full name to add initials or reverse the order of the first and last names.
User logon name	Type the user logon name, and then click the user principal name (UPN) suffix in the drop-down list.

5. Enter the following information, and then click **Next**.

Field/check box	Description
Password	Type the user's password.
Confirm password	Type the user's last name.
User cannot change password	Select this check box to prevent the user from changing his or her password and to maintain control over the user account.
Password never expires	Select this checkbox to prevent the user password from expiring. We recommend that service accounts have this option enabled and use strong passwords.

6. Review the user account settings, and then click **Finish**.

Add the user to the Domain Administrators group

If you are going to provide administrative permissions to the Identity Agent service account, you must add the Identity Agent service account to the Domain Administrators group.

As a security best practice, consider using **Run as Administrator** to perform this procedure. This procedure must be preformed on the domain controller.

1. Open Active Directory Users and Computers (**Start > Control Panel > Administrative Tools > Active Directory User and Computers**).

To open Active Directory Users and Computers in Windows Server 2012, click **Start**, and then type **dsa.msc**.

2. In the console tree, click **Users**.
3. Right-click on the user account, and then click **Properties**.
4. On the **Member Of** tab, click the **Domain Admins** group to set as the user's primary group.
5. Click **Set Primary Group**.

Assign permissions for the Active Directory user

If you do not have administrative credentials, you must assign certain permissions to allow the Active Directory user to perform specific actions, such as connecting to the Identity Agent.

If you have administrative credentials, skip this procedure, as the user already has these permissions assigned by default.

As a security best practice, consider using **Run as Administrator** to perform this procedure. This procedure must be performed on the domain controller.

1. Open Computer Management (**Start > Control Panel > System and Security > Administrative Tools > Computer Management**).
2. In the navigation pane, expand **Services and Applications**, right-click **WMI Control**, and then click **Properties**.
3. Expand **Root**, select **CIMV2**, and then click **Security**.
4. Click the **Security** tab.
5. Click **Add**.
6. On the Select Users, Computers, Service Accounts, or Groups dialog box, select the following items, and then click **OK**.
 - (Optional) Click **Locations** to define the root location from which to begin your search for the Identity Agent user.
 - Type the name of the Identity Agent user in the **Enter the object names to select** field.
 - (Optional) Click **Check Names** to locate all matching or similar object names listed in the Enter the object names to select field.
7. Select the Identity Agent user from the Group or user names list, and then select the following check boxes to Allow permissions:
 - Enable Account
 - Remote Enable
 - Read Security
8. Click **Apply**.
9. Repeat this procedure in all domain controllers that are configured in the Identity Agent.

Windows Firewall

Windows Firewall with Advanced Security allows you to require that computers authenticate before communicating with the Identity Agent. From here, you must:

- Enable predefined firewall rules to activate the rule and allow the user to connect to the Identity Agent through Windows Firewall.
- Create a new rule to allow a connection based on the TCP port number over which the computer is trying to connect to the Identity Agent. You can specify more than one port number. The port numbers will display in the Agent Port field in the Identity Agent.

Enable predefined Windows Firewall rules

Use Windows Firewall with Advanced Security to enable predefined rules.

This procedure must be preformed on the domain controller.

1. Open Windows Firewall (**Start > Control Panel > System and Security > Windows Firewall**).
2. In the Control Panel Home navigation pane, click **Advanced Settings**.
3. In the navigation pane, click **Inbound Rules**.
4. Search for the following rules, right-click on the rule, and then click **Enable Rule**.

For this Windows version:	Enable the following rules ...
Windows Server 2008	<ul style="list-style-type: none">• Remote Administration (RPC)• Windows Management Instrumentation (DCOM-In)• Remote Event Log Management (RPC)
Windows Server 2012	<ul style="list-style-type: none">• Remote Service Management (RPC)• Windows Management Instrumentation (DCOM-In)• Remote Event Log Management (RPC)

Create a new Inbound Windows Firewall rule

To perform this procedure, you must be a member of the Domain Administrators group. This procedure must be preformed on the Identity Agent server.

1. Open Windows Firewall (**Start > Control Panel > System and Security > Windows Firewall**).
2. In the Control Panel Home navigation pane, click **Advanced Settings**.
3. In the navigation pane, click **Inbound Rules**.
4. In the Actions navigation pane, click **New Rule**.

The New Inbound Rule Wizard opens.

5. Use the wizard to create a rule to explicitly allow a connection to the Identity Agent through Windows Firewall. Click **Next** to go through each wizard page.

On this wizard step (page):	Select the following ...
Rule Type	Port.
Protocol and Ports	<ul style="list-style-type: none"> • TCP • Specific local ports, and then type the port number (8443). Only the port number listed in this field will be able to communicate with the Identity Agent. You can specify multiple port numbers, separated by commas. You can also include a range of port numbers by separating the low and high values with a hyphen.
Action	Allow the connection.
Profile	<ul style="list-style-type: none"> • Domain • Private • Public
Name	Type a name for the rule in the Name field.

6. Click **Finish**. The rule appears in the Inbound Rules list, and the port for the Identity Agent in the Windows Firewall is open.

Specify the amount of Identity Agent data to retain in the SMS

Use the Database Maintenance table in the SMS (**Admin > Database**) to manage the following maintenance settings for the Identity Agent:

- User ID IP Correlation
- IP User Mapping
- Historical IP User Mapping

By default, the each maintenance settings is set to a default of a maximum of 10 million rows, and the SMS polls the Identity Agent for security login events at a rate of up to 7000 per minute.

When you reach the maximum number of entries, the SMS automatically deletes a percentage of the oldest events and a cleanup is requested/scheduled by the SMS.

You can manage the User ID IP Correlation data maintained by the SMS when you perform Database Maintenance and specify retention parameters for the data. For more information about managing TippingPoint systems, see the *TippingPoint SMS User Guide* or the SMS online Help.

Kerberos events

Use the following Kerberos event IDs in the Identity Agent security logs as a guide for adjusting the maximum number of rows in the Database Maintenance tables:

- 4768
- 4769
- 4770

Install Identity Agent

1. Log in to the TMC.
2. Download the TippingPoint Identity Agent zip file.
3. Log in with the administrator account in the Identity Agent service account and copy the zip file.
4. Unzip the file, right-click on **setup**, and then click **Run as administrator**.

The Identity Agent - InstallShield Wizard opens.

5. Use the wizard to accept the terms of the license agreement, create a user name, and to select or change the location where the application will be installed. Click **Next** to go through each wizard page.

On this wizard step (page):	Do the following ...
License Agreement	Read and accept the terms in the license agreement. You can also print a copy of the agreement.
Customer Information	Type a user name and organization.
Destination Folder	Review and confirm the location or browse to and select a new location to install the Identity Agent.

6. Click **Install**, and then click **Finish**.

The Identity Agent installs the service and configuration tool and creates a desktop icon.

Add logon credentials for the Identity Agent service

Use Services to configure the user account for the Identity Agent. This user account is used for running the agent service to connect to the domain controllers.

As a security best practice, consider using **Run as Administrator** to perform this procedure.

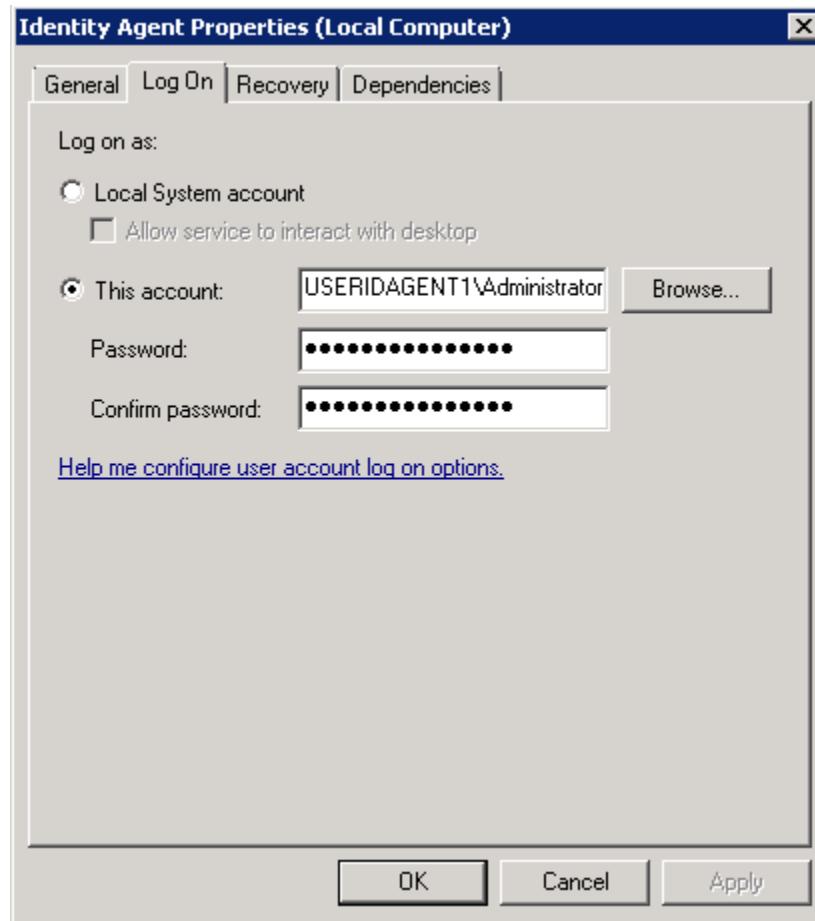
1. Open Services (**Start > Control Panel > Administrative Tools > Services**).
2. In the details pane, right-click the **Identity Agent** service, and then click **Properties**.
3. Click the **Log On** tab.
4. Select **This account**, and then click **Browse**.
5. On the Select User dialog box, select the following items, and then click **OK**.

- Verify that the location listed in the **From this location** field is the name of the machine hosting the agent.

Note: If the location listed is not the domain in which the agent will connect, click the **Locations** button, and then browse to and select the appropriate domain.

- Type the name of the Identity Agent user in the **Enter the object names to select** field.
- (Optional) Click **Check Names** to locate all matching or similar object names listed in the **Enter the object names to select** field.

The Identity Agent user displays in the **This account** field.



- Enter and confirm the password, and then click **OK**.

Provide full access for the Identity Agent service account

After you install the Identity Agent, update the security properties.

- Navigate to the folder in which you installed the Identity Agent.

If you used the default settings, the Identity Agent is located in the Program Files.

2. Right-click **TippingPoint**, and then click **Properties**.
3. Click the **Security** tab.
4. Click **Edit**.
5. On the Permissions for Identity Agent dialog box, click **Add**.
6. On the Select Users, Computers, Service Accounts, or Groups dialog box, select the following items, and then click **OK**.
 - (Optional) Click **Locations** to define the root location from which to begin your search for the Identity Agent user.
 - Type the name of the Identity Agent user in the **Enter the object names to select** field.
 - (Optional) Click **Check Names** to locate all matching or similar object names listed in the **Enter the object names to select** field.
7. Select the Identity Agent user from the Group or user names list, and then select the **Full control** check box under Allow permissions.
8. Click **Apply**.

Allow port access for Identity Agent user

If the Identity Agent user does not have administrative rights, use the command-line to allow port access to the Identity Agent.

```
netsh http add urlacl url=https://*:8443/  
user=USERIDAGENT1\TP_IdentityAgent
```

In the example above:

- 8443 is the Identity Agent port number
- USERIDAGENT is the Identity Agent domain
- TP_IdentityAgent is the Identity Agent service account

Identity Agent

The Identity Agent keeps track of specific groups based on IP address with the goal of maintaining Identity Management and efficiently enforcing user policies.

The Identity Agent adds another layer of network policy refinement by using Active Directory (AD) of users and user groups. Through its interaction with an AD domain controller, the Identity Agent enables SMS administrators to keep track of specific users and groups based on IP address. The Agent constantly polls the security logs of the AD domain controller--at a rate of every four to five seconds for security login events and every 15 minutes for metadata and diagnostics--and communicates this information to the SMS.

With this degree of visibility for the SMS, administrators can target policies according to, for example, an engineering group vs a marketing group. The service is most useful in environments where control and visibility are a higher priority than filter management.

This enables the SMS to determine the IP address of any user/group.

Identity Agent configuration

Identity Agent configuration is the Identity Agent component where you configure the agent, manage domain controllers, set connection settings, and maintain a list of mapped or excluded IP addresses.

The following table describes the main areas of the Identity Agent interface is divided into four main areas.

Field	Description
Agent Host IP	Displays all available IP addresses. Once you select an IP address and click save, this field will be unavailable. If you want to select a different IP address, you must uninstall and reinstall the Identity Agent.
Agent Port	The port in which the Identity Agent will communicate with the SMS. Remember that this port must also be the port that is open in the Windows Firewall.
Domain Name	The domain name that the Identity Agent is connected to.
Base DN	The distinguished name of the node in the active directory under which all users and groups are located.
Domain Controller	

Field	Description
IP Address	The IP address of the domain controller. You can have up to 30 domain controllers, but remember that the first one entered will be the primary domain. If you want to set a different primary domain controller, you must remove all IP addresses from the list, and then reenter the IP address or hostname.
Connection Settings	
User/Group Poll	The amount of time that the Identity Agent will poll the user and group information. The default frequency is every 15 minutes.
Security Log Poll	The amount of time that the Identity Agent will poll the login security events. The default frequency is every four to five seconds.
Secure LDAP	Determines whether the LDAP is secure.
Mapped IPs	Displays a list of correlated, or permitted, IP addresses. You can add an individual IP address, a range, or a CIDR. If the list is blank, the Identity Agent will correlate all IP addresses.
Excluded IPs	Displays a list of values that you do not want to correlate from the Identity Agent.
Custom Schema	If you customized your Active Directory schema, you can match the same schema in the Identity Agent.

Create the initial Identity Agent configuration

1. Double-click the **Identity Agent** desktop icon.
2. Select an IP address from the **Agent Host IP** drop-down list.

Important: The Agent Host IP is only entered one time. The next time you access the configuration, this field will appear unavailable. After you save the initial configuration, you must reinstall the Identity Agent if you want to update the host IP address.

3. Type the Identity Agent domain name in the **Domain Name** field.

Important: The domain name must be the same name listed in the *Permissions for Identity Agent dialog box* on page 12.

4. Type the distinguished name of the node in the Active Directory under which all the users and groups are located in the **Base DN** field.

Important: Separate the CN, OU, and DC with commas.

5. Type an individual IP address, range or CIDR in the **IP Address** field, and then click the + icon.
6. Enter the user/group mapping polling frequency in the **User/Group Poll** field.
7. Enter the security log polling frequency in the **Secuirty Log Poll** field.
8. (Optional) Select the check box to enable secure LDAP.
9. Click **Save**.
10. Click **Yes** to restart the Identity Agent service and to apply the configuration.

Manage domain controllers

You can have up to 30 domain controllers listed for each Identity Agent.

Multi-domain users: Each domain (or subdomain) must have an Identity Agent configured on a server located within that domain (or subdomain).

Load balancing: If your network uses multiple domain controllers for load balancing, then each domain controller (up to 30) must connect to the same Identity Agent.

1. Double-click the **Identity Agent** desktop icon.
2. Select an IP address from the **Domain Controller** list.
3. Click the - icon.
4. Click **Save**.
5. Click **Yes** to overwrite the existing configuration.

Add an IP address to the Mapped IPs list

You can have up to 64 IP addresses listed for each Identity Agent.

1. Double-click the **Identity Agent** desktop icon.
2. Click the **Mapped IPs** tab.
3. Enter an individual IP address, range or CIDR in the **IP Address** field.
4. Click the + icon.
5. Click **Save**.
6. Click **Yes** to overwrite the existing configuration.

Remove an IP address from the Mapped IPs list

1. Double-click the **Identity Agent** desktop icon.
2. Click the **Mapped IPs** tab.
3. Select an individual IP address, range or CIDR from the **IP Address** field.
4. Click the - icon.
5. Click **Save**.
6. Click **Yes** to overwrite the existing configuration.

Add an IP address to the Excluded IPs list

You can have up to 64 IP addresses listed for each Identity Agent.

1. Double-click the **Identity Agent** desktop icon.
2. Click the **Excluded IPs** tab.
3. Enter an individual IP address, range or CIDR in the **IP Address** field.
4. Click the + icon.
5. Click **Save**.
6. Click **Yes** to overwrite the existing configuration.

Remove an IP address from the Excluded IPs list

1. Double-click the **Identity Agent** desktop icon.
2. Click the **Excluded IPs** tab.
3. Select an individual IP address, range or CIDR from the **IP Address** field.
4. Click the - icon.
5. Click **Save**.
6. Click **Yes** to overwrite the existing configuration.

Manage custom schemas

If you customize your Active Directory schema, you can match the same schema in the Identity Agent.

1. Double-click the **Identity Agent** desktop icon.
2. Click the **Custom Schemas** tab.
3. Enter a value in the **User Object Class** field.
4. Enter a value in the **Unique Identifier** field.
5. Enter a value in the **Member Of** field.
6. Enter a value in the **Groups Object Class** field.

7. Enter a value in the **Distinguished Name** field.
8. Click **Save**.
9. Click **Yes** to overwrite the existing configuration.

Uninstall Identity Agent

Follow these steps to uninstall the Identity Agent. Alternatively, you can also uninstall the agent from the Windows Control Panel.

1. Navigate to the folder in which you installed the Identity Agent.

If you used the default settings, the Identity Agent is located in the Program Files.

2. Right-click on **setup**, and then click **Run as administrator**.

The Identity Agent - Install Shield Wizard opens.

3. Use the wizard to remove the Identity Agent from your computer. Click **Next** to go through each wizard page.

On this wizard step (page):	Do the following ...
License Agreement	Read and accept the terms in the license agreement. You can also print a copy of the agreement.
Customer Information	Type a user name and organization.
Destination Folder	Review and confirm the location or browse to and select a new location to install the Identity Agent.

4. Click **Remove**, and then click **Finish**.

The Identity Agent removes all installed files except for the logs and the Config file.

Where to go next

The SMS is a central console where you can manage multiple TippingPoint devices, products, and services. After the initial setup, you can begin monitoring and managing your TippingPoint systems.

Connect the Identity Agent in the SMS from the Admin workspace (**Admin > User Id IP correlation**).

Once the SMS is configured to poll the Identity Agent, the SMS will display the User ID to User IP correlation and security login events. When you first connect the Identity Agent in the SMS, the SMS will automatically poll the domain controller for the last 15 minutes of historical information.

For complete information about managing TippingPoint systems, see the *TippingPoint SMS User Guide* or the SMS online Help.

Identity Agent issues and resolutions

This document covers the agent issues found during pre-installation, installation, and post installation as well as the steps required to resolve these issues.

Agent service not able to query domain controller security log events

Issue

The agent service is not able to query domain controller security log events.

Root cause

The Identity Agent service logon user does not have sufficient privileges in the active directory (AD) to access security log events.

Resolution

To resolve this problem, verify in the AD that the Identity Agent service logon user account has the following group membership:

- Domain Users

(OR)

- Distributed COM Users
- Event Log Readers
- Performance Monitor Users

If it doesn't have the correct membership, then it should be added.

The image below shows an example of adding a group membership to a user account.

Tipping Point Identity Agent Properties

Remote control	Remote Desktop Services Profile			
General	Address	Account	Profile	Telephone
Member Of	Dial-in	Environment		

Member of:

Name	Active Directory Domain Services
Distributed COM Users	w2k12ad02.info/Builtin
Domain Users	w2k12ad02.info/Users
Event Log Readers	w2k12ad02.info/Builtin
Performance Monitor Users	w2k12ad02.info/Builtin

< III

Add... Remove

Note: If you are using the **Domain Admins** approach, only that group will be displayed in the membership tab.

Agent service not able to query domain controller OS information

Issue

The agent service is not able to query domain controller OS information for the meta-data.

Additional info in agent logs

```
[DIAGNOSTICS] WARN ADAgentService.Diagnostics.DiagnosticWorker - 
Encountered unexpected exception trying to obtain directory controller
meta-data:
System.Management.ManagementException: Access denied
```

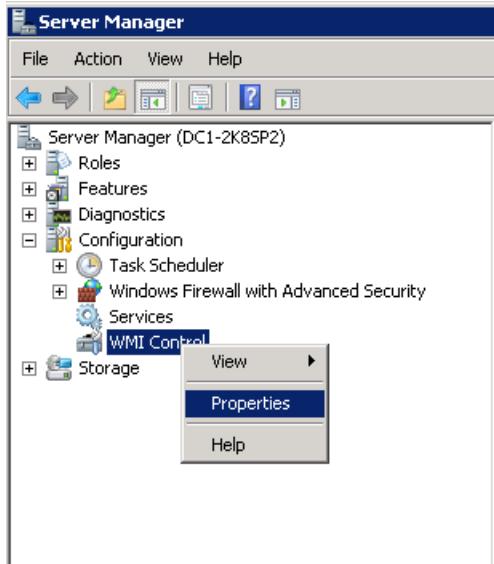
Root cause

The Identity Agent service logon user does not have sufficient WMI privileges in the domain controller to access OS information.

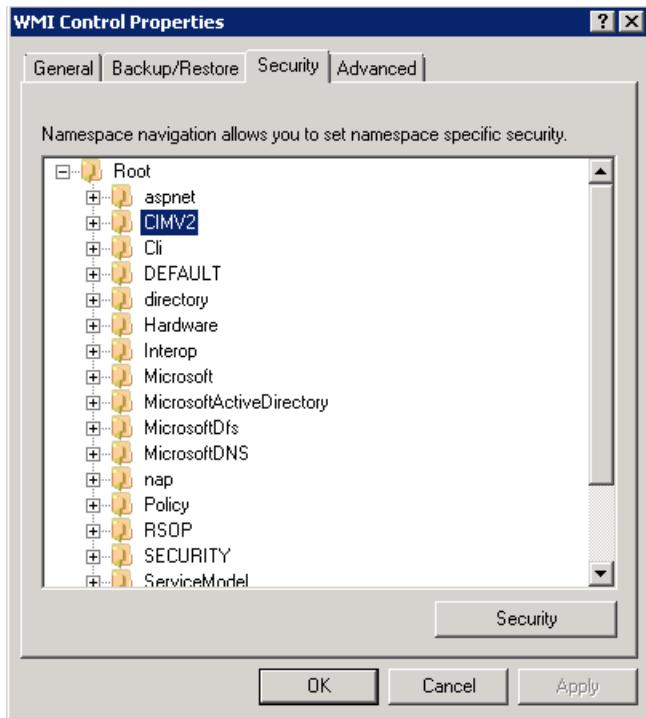
OS information resolution

Follow these steps to allow the Identity Agent Service account to have access to WMI in the domain controller. These steps need to be executed in all domain controllers, which will be configured in the agent.

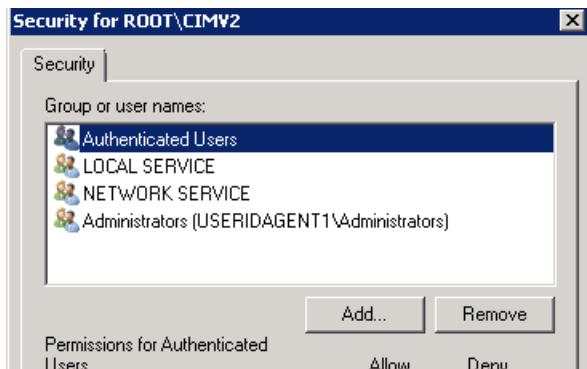
1. In the domain controller, click **Start**, click **Administrative Tools**, and then click **Computer Management**.
2. Within the management console, navigate to **Services and Applications > WMI Control**.
3. Right-click **WMI Control**, and select **Properties**.



4. Navigate to **Security**.
5. Add your Identity Agent service logon user account, and modify the domain controller permissions so that the agent will be able to connect.
6. Expand the namespace to **Root > CIMV2**, and select the **Security** button as shown in the image below.

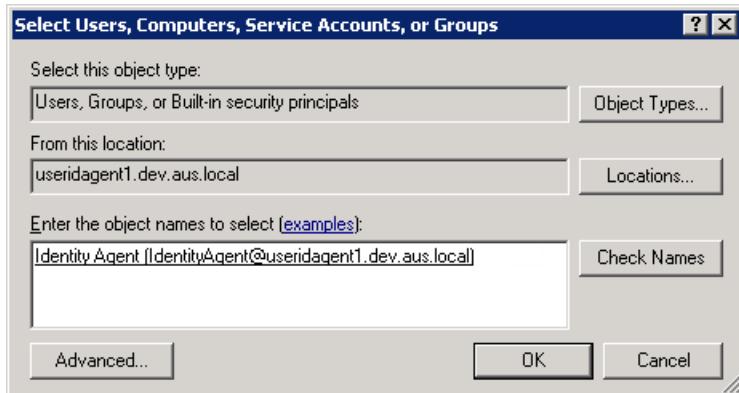


7. Select **Add**, and choose your service account, as described above, to the list of users that will have the specified permissions.



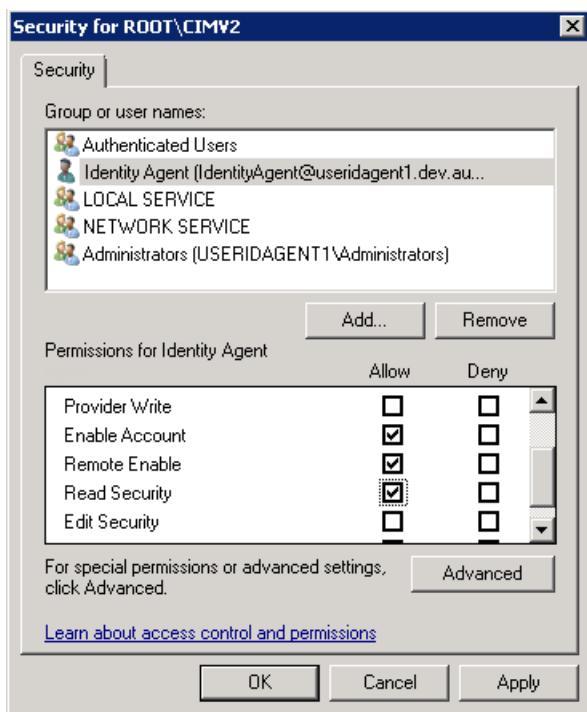
8. Enter the name of the account that you will operate the service under, verifying that the value for **Location** is appropriate.

In the example below, it points to the AD domain.



Note: Select **Check Names** if you are uncertain of the correct location, and the user account will be validated.

9. After adding the user successfully, select the appropriate permissions for the CIMV2 Namespace for the user account as shown below.



The specified permissions that are required are:

- Enable account
- Remote Enable
- Read Security

No other permissions should be necessary.

Agent service is not able to communicate to domain controller

Issue

The agent service is not able to communicate with the domain controller.

Root cause

The domain controllers are protected by a firewall.

Resolution

If your domain controllers are protected by the built-in Windows Firewall with Advanced Security, you will need to enable the following rules on each domain controller to be monitored by the Identity Agent.

In Windows 2008

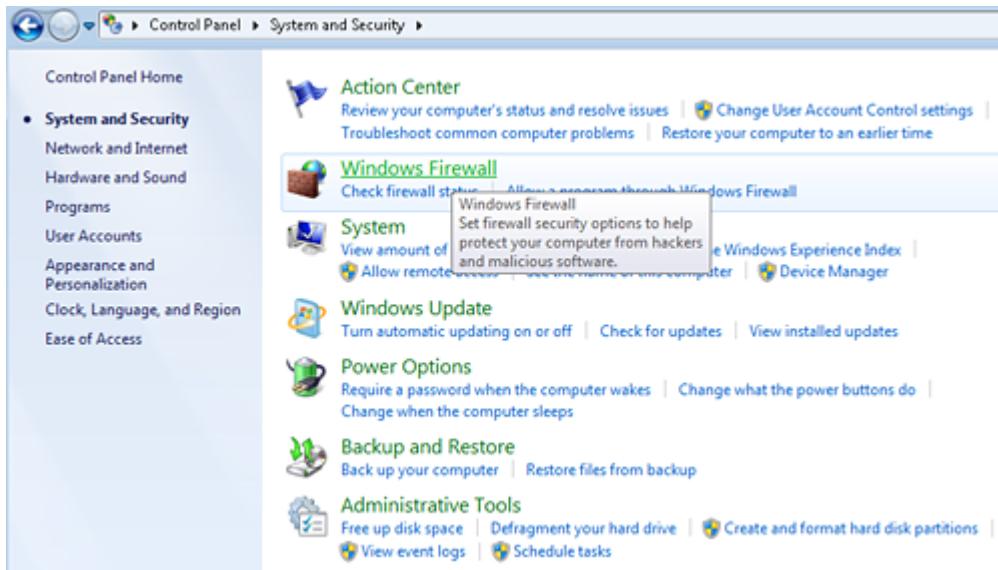
- Remote Administration (RPC)
- Windows Management Instrumentation (DCOM-In)
- Remote Event Log Management (RPC)

In Windows 2012

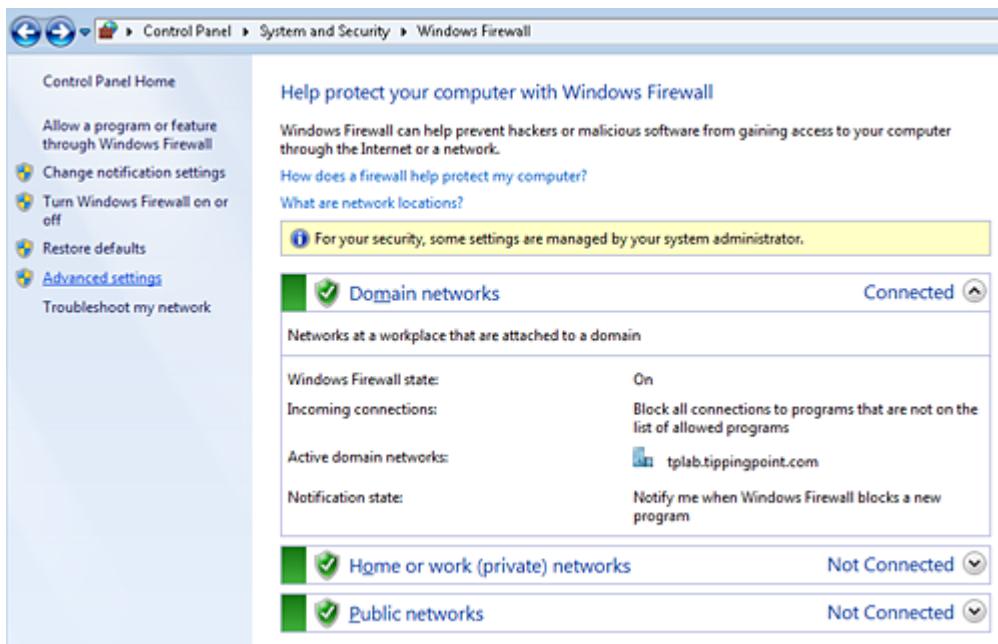
- Remote Service Management (RPC)
- Windows Management Instrumentation (DCOM-In)
- Remote Event Log Management (RPC)

To enable Windows Firewall rules

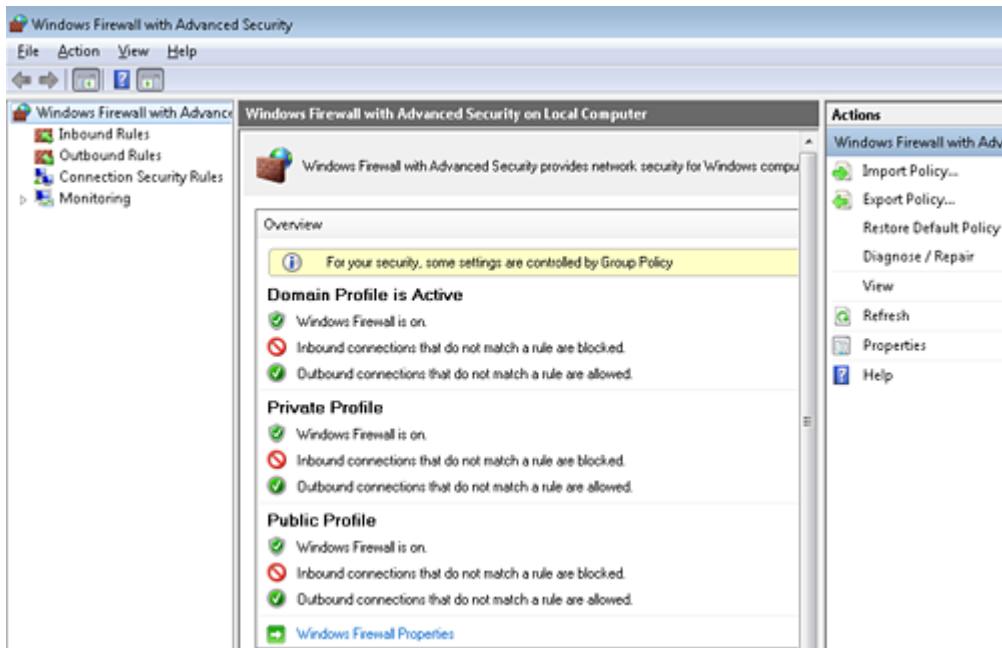
1. Go to **Start > Control Panel**.
2. Click the **System and Security** link, and then click **Windows Firewall**.



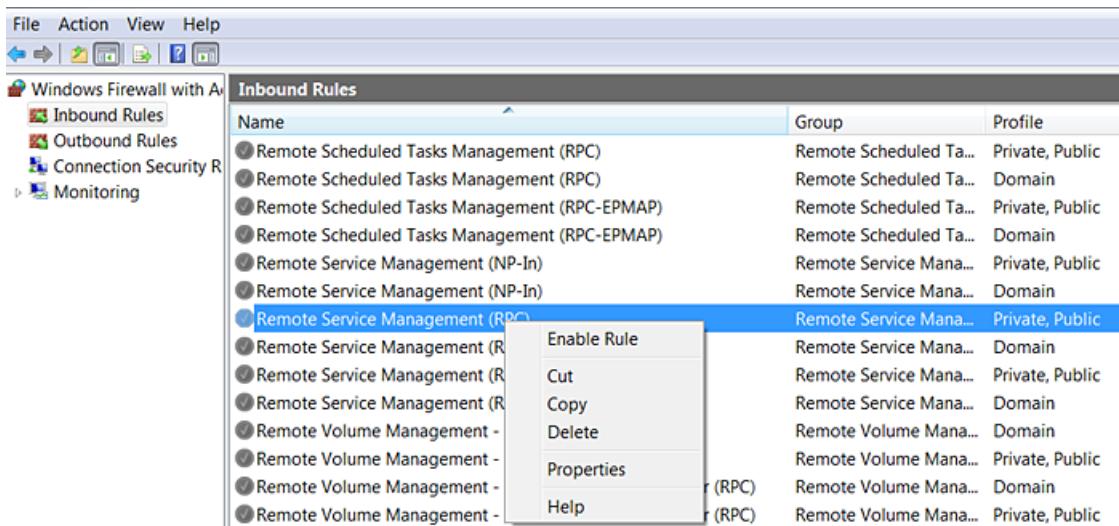
3. In the main Windows Firewall control window, click the **Advanced Settings** link on the left.



You will see the Windows Firewall and Advanced Security window as shown below.



4. On the left, click **Inbound Rules**.
5. Within the list of **Inbound Rules**, search for the correct rule, right click it, and then click **Enable Rule**.



6. Verify that the firewall rule is enabled after completing the above steps.

Agent service running but not querying domain controllers for security event logs

Issue

The agent service is running, but it is not querying domain controllers for the security event logs.

Root cause

A valid domain logon user account is not specified in the Identity Agent service.

Resolution

Follow the steps in [To modify the account](#) on page 29 to resolve this issue.

To modify the account

To modify the account under which the agent will operate, perform the following steps.

1. Open **Control Panel > Administrative Tools > Services**.
2. Navigate to the entry for the **Identity Agent Service**, right click the entry, and select **Properties**.
3. Navigate to the **Log On** tab within the service properties.
4. Select the icon next to **This account**, and click **Browse** as shown in the image below.



5. Search for the correct domain account, click **OK**, and then restart the Identity Agent service.
6. Restart the Identity Agent service after completing the above steps.

Agent service is not creating db and logs folders

Issue

The agent service is not creating the **db** and **logs** folders and files that are needed for agent functioning.

Root cause

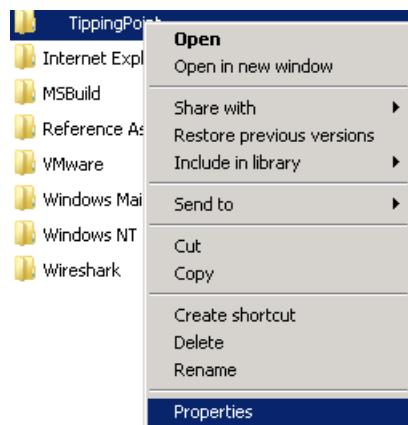
The Identity Agent service logon user does not have sufficient permission to create or modify folders and files in the agent installed folder.

Resolution

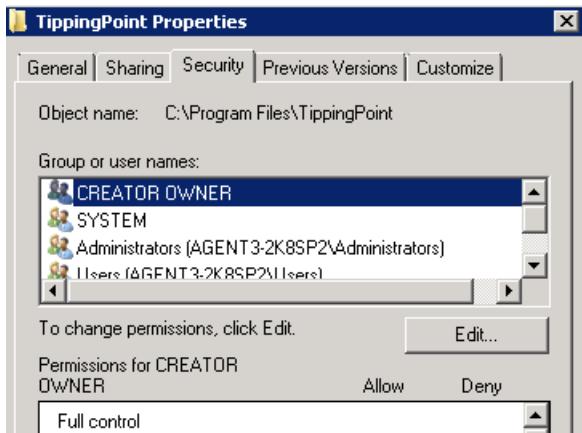
Provide full access for the service account to the Identity Agent installed folders. Follow the steps in [To provide full access](#) on page 30 to resolve this issue.

To provide full access

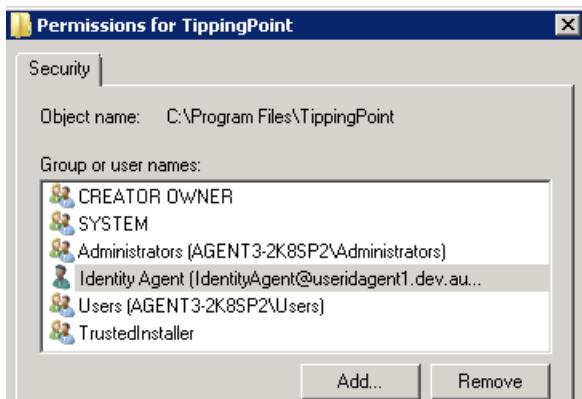
1. Right click the TippingPoint folder in which the agent has been installed, and select the **Properties** action at the bottom of the context menu.



2. Navigate to the **Security** tab, and select the **Edit** button.

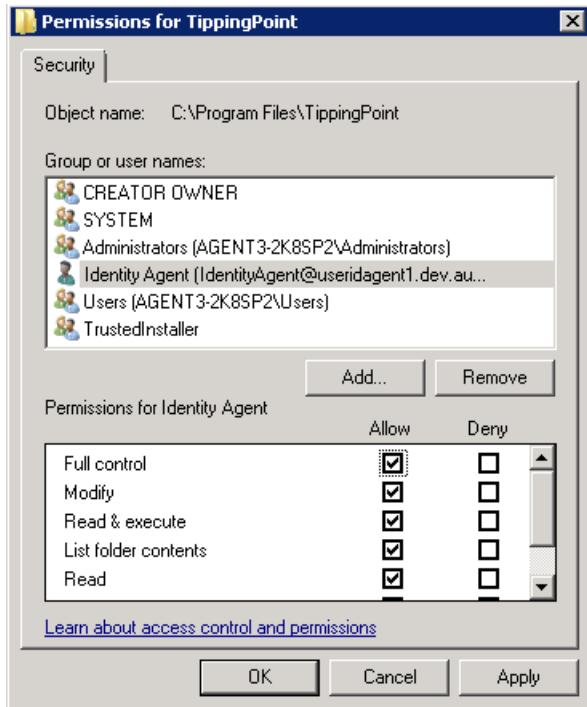


3. Click **Add** to add the appropriate user. Make sure to add the domain user account with which you intend to execute the agent.



4. After adding that account to the list, select the **Allow** check box on the **Full Control** entry with the correct user highlighted.

Ensure that the appropriate check boxes are all selected.



5. Click **OK**.

Agent APIs are not listening in agent port

Issue

The agent APIs are not listening in the agent port. There is no response to API calls.

Additional information in event logs

Description:

The process was terminated due to an unhandled exception.

Exception Info:

```
System.Net.HttpListenerException
Stack: at System.Net.HttpListener.Start() at
ADAgentService.Http.HttpServer..ctor
(System.Collections.Generic.List`1<ADAgentService.Http.PortConfiguration>)
```

Root cause

The following are possible causes:

- The Identity Agent service logon user does not have sufficient permission to register HTTP Listeners.
- The agent port might already be reserved for other services.

Resolution

- Add the Identity Agent service logon user to the local administrator group, and restart the Identity Agent service.

OR

- Verify that any URL reservation is already present for that port. If it is, delete the URL reservation, add the new URL ACL, and restart the Identity Agent service.

Commands

Command to show URL ACL:

```
netsh http show urlacl
```

Command to delete URL ACL:

```
netsh http delete urlacl url=https://*:agentport/
```

Example:

```
netsh http delete urlacl url=https://*:8445/
```

Command to add URL ACL:

```
netsh http add urlacl url=https://*:Agent Port/ user=Domain\agent service account
```

Example:

```
netsh http add urlacl url=https://*:8445/ user=USERIDAGENT1\TP_IdentityAgent
```

Agent APIs are not accessible outside agent server

Issue

The agent APIs are not accessible outside of the agent server.

Root cause

The agent server firewall is restricting access to the agent port.

Resolution

Open the port for the Identity Agent in the Windows Firewall in an agent-installed machine.

Groups API call response with no data

Issue

The groups API call (GET/groups) has a response with no data.

Root cause

The following are possible causes:

- The Identity Agent service logon user does not have sufficient privileges in the AD to query group and user objects.
- An invalid Base DN value is specified in the configuration tool.
- There are invalid user and group object attributes specified in the configuration tool.

Resolution

There are several possible solutions to resolve this problem:

- Verify that the Identity Agent service logon user has sufficient privileges in AD to query group and user objects. If not, add the necessary privileges to the service logon domain user account. Add the user account to the **Domain Users** group.
- Verify that a valid Base DN value is specified in the configuration tool. There is a high probability of a typo error occurrence. Validate that the Base DN value specified in the configuration tool is present in the configured AD.
- Verify that there are valid user and group object attributes specified in the configuration tool. There is a high probability of a typo error occurrence. Validate that the user and group object attributes value specified in the configuration tool is present in the configured AD.

Make sure to restart the service after any changes are made in the configuration tool.

Configuration changes are not reflected in the agent service

Issue

Configuration changes made in the configuration tool are not reflected in the agent service.

Root cause

The agent service is running with stale configuration data, and it was not restarted after configuration changes were made.

Resolution

Restart the Identity Agent service to reflect the latest configuration changes.

SMS is not able to establish connectivity with the Identity Agent

Issue

The SMS is not able to establish connectivity with the Identity Agent.

Root cause

The following are possible causes:

- The agent service is not running.
- The SMS does not connect using the agent configured IP.
- The SMS mandatory certificates are not properly installed in the agent server.
- The agent self-signed certificate was not properly created and installed in the agent server.
- The agent port is not open in the firewall.

Resolution

There are several possible solutions to resolve this problem:

- Verify that the agent service is running in the agent server. If not, restart the Identity Agent service.
- Verify that the SMS is trying to connect using the agent IP, which is present in the agent configuration tool. To validate the agent IP, log in to the agent server and open the configuration tool.
- Verify that the SMS root certificates are properly installed in the agent server.

To do this, go to **run > mmc > File > Add/Remove snap-in > Certificates > Add > Computer account > Finish > OK**.

Verify that the SMS root certificate is present in **Trusted Root Certification Authorities/Certificates**.

- Verify that the self-signed certificates are properly created and installed in the agent server.

To do this, go to **run > mmc > File > Add/Remove snap-in > Certificates > Add > Computer account > Finish > OK**.

Verify that the SMS root certificate is present in **Personal/Certificates**.

- Verify that the IP address is the same on the Identity Agent (on the server) and the SMS. If you receive an error message that the Identity Agent certificate is invalid, uninstall the Identity Agent and then install it again on the server.

Agent not able to establish LDAP connectivity

Issue

The agent is not able to establish LDAP connectivity for user group mapping.

Root cause

- The AD is not configured to listen on LDAP port (389).
- The firewall is blocking the connection that uses the LDAP port (389).

Resolution

Verify that the LDAP port is blocked by the firewall. If the firewall is blocking the LDAP port connectivity between the domain controller and the agent server, then open the port.

Agent not able to establish secure LDAPS connectivity

Issue

The agent is not able to establish LDAPS connectivity for user group mapping.

Root cause

- The AD is not configured to listen on the LDAPS port (636).
- The firewall is blocking the connection that uses the LDAP port (636).

Resolution

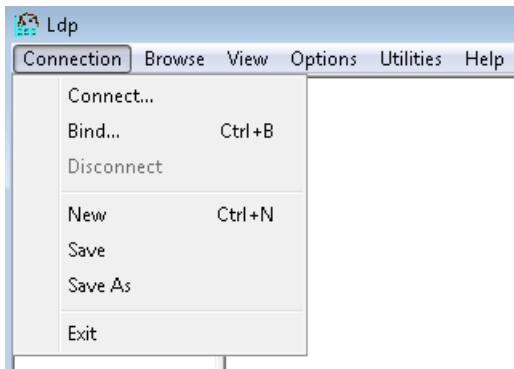
Verify that the domain controller is configured to listen on the LDAPS port (636).

Verify that the LDAPS port is blocked by the firewall. If the firewall is blocking the LDAPS port connectivity between the domain controller and the agent server, then open the port.

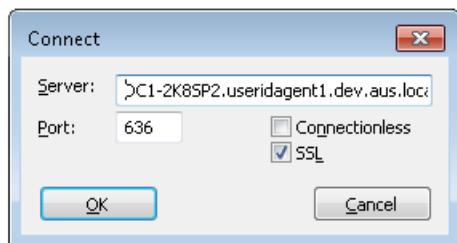
To test domain controller connectivity

To test the LDAPS connectivity in the domain controller using ldp.exe, perform the following steps.

1. Login to the domain controller by going to **Start > Run > type ldp.exe**.
2. Click **Connection**, and then click **Connect** as shown in the image below.



3. Enter the full FQDN of the domain controller for the server, enter 636 for the port, and select the SSL check box, as shown in the image below.



4. Click **OK**.
5. If you receive the domain information, the LDAPS connection was performed successfully, as shown in the image below.

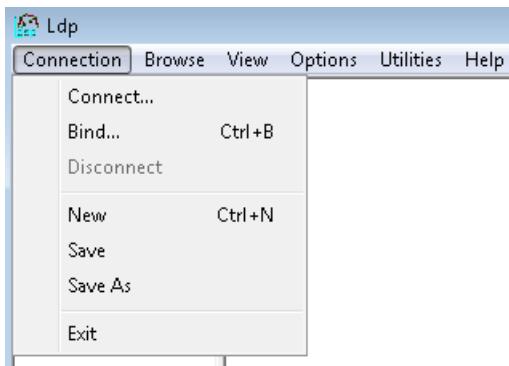
```

Id = ldap_s_sinit("DC1-2K8SP2.useridagent1.dev.aus.local", 636, 1);
Error 0 = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3);
Error 0 = ldap_connect(hLdap, NULL);
Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)81v);
Host supports SSL, SSL cipher strength = 128 bits
Established connection to DC1-2K8SP2.useridagent1.dev.aus.local.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
  configurationNamingContext: CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  currentTime: 7/1/2014 6:19:24 PM Central Daylight Time;
  defaultNamingContext: DC=useridagent1,DC=dev,DC=aus,DC=local;
  dnsHostName: DC1-2K8SP2.useridagent1.dev.aus.local;
  domainControllerFunctionalit: 4 = (WIN2008R2);
  domainFunctionalit: 4 = (WIN2008R2);
  dsServiceName: CN=NTDS Settings,CN=DC1-2K8SP2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  forestFunctionalit: 4 = (WIN2008R2);
  highestCommittedUSN: 258402;
  isGlobalCatalogReady: TRUE;
  isSynchronized: TRUE;
  ldapServiceName: useridagent1.dev.aus.local:dc1-2k8sp2@USERIDAGENT1.DEV.AUS.LOCAL;
  namingContexts (5): DC=useridagent1,DC=dev,DC=aus,DC=local; CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  CN=Schema,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  DC=DomainDnsZones,DC=useridagent1,DC=dev,DC=aus,DC=local; DC=ForestDnsZones,DC=useridagent1,DC=dev,DC=aus,DC=local;
  rootDomainNamingContext: DC=useridagent1,DC=dev,DC=aus,DC=local;
  schemaNamingContext: CN=Schema,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  serverName: CN=DC1-2K8SP2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  supportedCapabilities (5): 1.2.840.113556.1.4.800 = (ACTIVE_DIRECTORY); 1.2.840.113556.1.4.1670 = (ACTIVE_DIRECTORY_V51);
  1.2.840.113556.1.4.1791 = (ACTIVE_DIRECTORY_LDAP_INTEG); 1.2.840.113556.1.4.1935 = (ACTIVE_DIRECTORY_V61);
  1.2.840.113556.1.4.2080;
  supportedControl (29): 1.2.840.113556.1.4.319 = (PAGED_RESULT); 1.2.840.113556.1.4.801 = (SD_FLAGS); 1.2.840.113556.1.4.473 = (SORT);
  1.2.840.113556.1.4.528 = (NOTIFICATION); 1.2.840.113556.1.4.417 = (SHOW_DELETED);
  1.2.840.113556.1.4.619 = (LAZY_COMMIT);
  1.2.840.113556.1.4.841 = (DIRSYNC);
  1.2.840.113556.1.4.529 = (EXTENDED_DN);
  1.2.840.113556.1.4.805 = (TREE_DELETE);
  1.2.840.113556.1.4.521 = (CROSSDOM_MOVE_TARGET);
  1.2.840.113556.1.4.970 = (GET_STATS);
  1.2.840.113556.1.4.1338 = (VERIFY_NAME);
  1.2.840.113556.1.4.474 = (RESP_SORT);
  1.2.840.113556.1.4.1339 = (DOMAIN_SCOPE);
  1.2.840.113556.1.4.1340 = (SEARCH_OPTIONS);
  1.2.840.113556.1.4.1413 = (PERMISSIVE MODIFY);
  2.16.840.1.113730.3.4.10 = (VLVREQUEST);
  2.16.840.1.113730.3.4.10 = (VLVRESPONSE);
  1.2.840.113556.1.4.1504 = (ASQ);
  1.2.840.113556.1.4.1852 = (
```

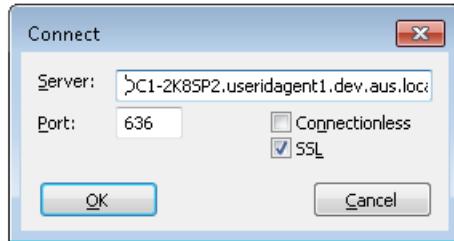
To test agent machine connectivity

To test the LDAPS connectivity in agent machine using ldp.exe, perform the following steps.

1. Login to the agent machine by going to **Start > Run > type ldp.exe**.
2. Click **Connection**, and then click **Connect** as shown in the image below.



3. Enter the full FQDN of the domain controller for the server, enter 636 for the port, and select the SSL check box, as shown in the image below.



4. Click **OK**.
5. If you receive the domain information, the LDAPS connection was performed successfully, as shown in the image below.

ldap://DC1-2K8SP2.useridagent1.dev.aus.local/DC=useridagent1,DC=dev,DC=aus,DC=local

Connection Browse View Options Utilities Help

```

Id = ldap_s_sslinit("DC1-2K8SP2.useridagent1.dev.aus.local", 636, 1);
Error 0 = ldap_s_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3);
Error 0 = ldap_connect(hLdap, NULL);
Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)81v);
Host supports SSL, SSL cipher strength = 128 bits
Established connection to DC1-2K8SP2.useridagent1.dev.aus.local.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
  configurationNamingContext: CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  currentTime: 7/1/2014 6:19:24 PM Central Daylight Time;
  defaultNamingContext: DC=useridagent1,DC=dev,DC=aus,DC=local;
  dnsHostName: DC1-2K8SP2.useridagent1.dev.aus.local;
  domainControllerFunctionality: 4 = (WIN2008R2);
  domainFunctionality: 4 = (WIN2008R2);
  dsServiceName: CN=NTDS Settings,CN=DC1-2K8SP2,CN=Servers,CN=Default-First-Site-
    Name,CN=Sites,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  forestFunctionality: 4 = (WIN2008R2);
  highestCommittedUSN: 258402;
  isGlobalCatalogReady: TRUE;
  isSynchronized: TRUE;
  ldapServiceName: useridagent1.dev.aus.local:dc1-2k8sp2@USERIDAGENT1.DEV.AUS.LOCAL;
  namingContexts (5): DC=useridagent1,DC=dev,DC=aus,DC=local; CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  CN=Schema,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  DC=DomainDnsZones,DC=useridagent1,DC=dev,DC=aus,DC=local; DC=ForestDnsZones,DC=useridagent1,DC=dev,DC=aus,DC=local;
  rootDomainNamingContext: DC=useridagent1,DC=dev,DC=aus,DC=local;
  schemaNamingContext: CN=Schema,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  serverName: CN=DC1-2K8SP2,CN=Servers,CN=Default-First-Site-
    Name,CN=Sites,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=useridagent1,DC=dev,DC=aus,DC=local;
  supportedCapabilities (5): 1.2.840.113556.1.4.800 = (ACTIVE_DIRECTORY); 1.2.840.113556.1.4.1670 = (ACTIVE_DIRECTORY_V51);
    1.2.840.113556.1.4.1791 = (ACTIVE_DIRECTORY_LDAP_INTEG); 1.2.840.113556.1.4.1935 = (ACTIVE_DIRECTORY_V61);
    1.2.840.113556.1.4.2080;
  supportedControl (29): 1.2.840.113556.1.4.319 = (PAGED_RESULT); 1.2.840.113556.1.4.801 = (SD_FLAGS); 1.2.840.113556.1.4.473 = (SORT);
    1.2.840.113556.1.4.528 = (NOTIFICATION); 1.2.840.113556.1.4.417 = (SHOW_DELETED); 1.2.840.113556.1.4.619 = (LAZY_COMMIT);
    1.2.840.113556.1.4.841 = (DIRSYNC); 1.2.840.113556.1.4.529 = (EXTENDED_DN); 1.2.840.113556.1.4.805 = (TREE_DELETE);
    1.2.840.113556.1.4.523 = (CROSSDOM_MOVE_TARGET); 1.2.840.113556.1.4.970 = (GET_STATS);
    1.2.840.113556.1.4.1338 = (VERIFY_NAME); 1.2.840.113556.1.4.474 = (RESP_SORT); 1.2.840.113556.1.4.1339 = (DOMAIN_SCOPE);
    1.2.840.113556.1.4.1340 = (SEARCH_OPTIONS); 1.2.840.113556.1.4.1413 = (PERMISSIVE MODIFY); 2.16.840.1.113730.3.4.10 = (VLVREQUEST);
    2.16.840.1.113730.3.4.10 = (VLVRESPONSE); 1.2.840.113556.1.4.1504 = (ASQ); 1.2.840.113556.1.4.1852 = (VLRREQUEST);
  
```

Ready

**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM17888/170801