Forcepoint

Web Security On-prem

v8.5.x

DC Agent Troubleshooting

Revision A

Contents

Introduction

This collection includes the following articles to help you troubleshoot DC Agent installation and user identification issues.

Click a link below to jump to the topic, or use the arrows at the top of the content pane to browse the troubleshooting articles in the collection.

For information about deploying and configuring DC Agent, see the Using DC Agent for Transparent User Identification technical paper.

Related concepts

DC Agent: ERROR_ACCESS_DENIED - 5 on page 7
DC Agent doesn't see some or all users on page 9
dc_config.txt file is missing or empty on page 13

Related tasks

DC Agent: Error Code 1058 (seen on startup) on page 7
DC Agent: ERROR_BAD_NETPATH - 53 on page 9

Related information

Problems installing DC Agent on page 2
DC Agent initial diagnostic steps on page 5

Problems installing DC Agent

Installation account permissions issue

Before you begin

Error messages can appear when you attempt to install DC Agent using an account that does not have domain and local administrator privileges. As a result, some of the required DC Agent files are not installed properly, and the service cannot run.

Typically, one of the following error messages is displayed:

```
Error Code 997
```

```
Could not configure DC Agent (Code 3)
```

To correct this issue, manually remove the failed installation and reinstall the service:

Steps

1) Log on to the DC Agent machine with **domain** and **local administrator** privileges.

2) Open a command prompt (**Start** > **Run** > **cmd**) or the Windows Powershell.

3) Navigate to the web protection **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default).

4) Use the following command to manually uninstall the DC Agent service:
   `XidDcAgent.exe -u`
   A status message verifies that the service was successfully removed.

5) Use the following command to manually reinstall and register the DC Agent service:
   `XidDcAgent.exe -i`
   A status message verifies that the service was successfully installed.

6) Use the Windows Services tool to start the **Websense DC Agent** service.

Next steps

If the service is running correctly, after a few minutes, a **dc_config.txt** file is created in the **bin** directory.

Manually enable the Computer Browser service

Before you begin

User Service and DC Agent require a Microsoft service, the **Computer Browser** service, to enable user identification.

If the service is not started during installation, enable it manually:

Steps

1) Make sure that Windows Network File Sharing is enabled.
   a) Windows Server 2016:
      i) Go to **Start** > **Windows System** > **Control Panel**.
      ii) In the Control Panel, click **Network and Internet**, then **Network and Sharing Center**.
      iii) Click **Change advanced sharing settings** in the left navigation pane, then select **Turn on file and printer sharing**.
      iv) Click **Save Changes** to save and exit.
   b) Windows Server 2012:
      i) On the desktop, point the mouse to the top, right corner of the screen, then go to **Settings** > **Control Panel**.
      ii) In the Control Panel, click **Network and Internet**, then **Network and Sharing Center**.
      iii) Click **Change advanced sharing settings** in the left navigation pane, then select **Turn on file and printer sharing**.
      iv) Click **Save Changes** to save and exit.
   c) Windows Server 2008:
      i) Go to **Start** > **Network** > **Network and Sharing Center**.
      ii) Click **Advanced Sharing Settings**, then select **Turn on file and print sharing**.
2) Open the Windows Services tool.
   - Windows Server 2016: Go to **Start**, then select **All Programs** > **Windows Administrative Tools** > **Services**.
   - Windows Server 2012: **Server Manager** > **Tools** > **Services**.
   - Windows Server 2008: **Start** > **Administrative Tools** > **Services**.

3) Double-click **Computer Browser** to open the Properties dialog box.

4) Set the Startup type to **Automatic**.

5) Click **Start**.

6) Click **OK** to save your changes and close the Services tool.

Next steps

Repeat these steps on each Windows machine running an affected component.

DC Agent initial diagnostic steps

Locate error messages

To start troubleshooting DC Agent user identification problems, start by assessing the status of the DC Agent service:

1) On the DC Agent machine, open the Windows Services tool and make sure that the **Websense DC Agent** service has started. If the service has stopped, right-click the service name and attempt to start it.

   Regardless of whether the service starts, was already started, or refuses to start, continue with the next step.

2) Open the Windows Event Viewer to look for error messages and warnings from the **Websense DC Agent** service.

The most common DC Agent errors are:

- **ERROR_ACCESS_DENIED**, which indicates a permissions issue. Although they do not make any changes to the domain, both DC Agent and User Service must run with domain administrator privileges. If you suspect a permissions issue, you can enable directory service auditing to find out what user and group information your software is trying to access. See *DC Agent: ERROR_ACCESS_DENIED - 5*.
- **ERROR_BAD_NETPATH**, which indicates a network communication issue. See *DC Agent: ERROR_BAD_NETPATH - 53*.

Related concepts
DC Agent: ERROR_ACCESS_DENIED - 5 on page 7

Related tasks
DC Agent: ERROR_BAD_NETPATH - 53 on page 9

Make sure that users are being identified correctly

To ensure that users are being identified correctly, start with the following procedure:

Steps

1) Log on to a machine whose users do not appear to be getting identified properly.

2) Open a browser and navigate to 4 or 5 distinctive websites.

3) Go to the DC Agent machine and check the Windows Event Viewer for error messages. If error messages appear, see:
   - *DC Agent: Error Code 1058 (seen on startup)*
   - *DC Agent: ERROR_ACCESS_DENIED - 5*
   - *DC Agent: ERROR_BAD_NETPATH - 53*

4) If there are no errors, open the Forcepoint Security Manager and use Real-Time Monitor or investigative reports to see if your Internet activity (in step 2) was logged as the correct user.
   - If the correct user name appears associated with the requests, there may be a policy configuration issue, rather than a user identification issue. Use the Check Policy tool in the Security Manager to troubleshoot the issue.
   - If the user name is incorrect, see *DC Agent doesn't see some or all users*.
   - If no user name information appears, verify that DC Agent and User Service are able to communicate with your directory service, and that the Windows **Computer Browser** service is enabled on the DC Agent machine.

   To enable the Computer Browser service, open the Windows Services tool, right-click **Computer Browser**, and select **Properties**. Change the Startup type selection to **Automatic**, then click **Start**.

Next steps

You can also use either Real-Time Monitor, in the Security Manager, or the command- line TestLogServer utility, located on the Log Server machine, to verify that user names are being associated with Internet requests.

- See Real-Time Monitor for more information.
- For more information about TestLogServer see Using TestLogServer for Troubleshooting.

Related concepts

DC Agent: ERROR_ACCESS_DENIED - 5 on page 7
DC Agent doesn't see some or all users on page 9

Related tasks

DC Agent: Error Code 1058 (seen on startup) on page 7
DC Agent: ERROR_BAD_NETPATH - 53 on page 9

DC Agent: Error Code 1058 (seen on startup)

Before you begin

This issue may be caused by a Local Security Policy on the DC Agent machine that has disabled the service.

Note

For further details about the causes of this error message, refer to Microsoft KB article 241584.

To troubleshoot this issue:

Steps

1) Open the Windows Services tool on the DC Agent machine.
2) Scroll down to locate the **Websense DC Agent** service. If the service is running, no further troubleshooting is necessary.
3) If the service has not started, right-click on the service name, and then select **Properties**.
4) Click the **Log On** tab of the Properties dialog box. The Hardware Profile list shows whether the service is enabled or disabled.

   Typically, this error message appears when the profile is disabled.
5) Click **Enable** to attempt to enable the service, then go to the General tab and click **Start**.
6) Click **OK**, then close the Services tool.

DC Agent: ERROR_ACCESS_DENIED - 5

This error appears when DC Agent does not have sufficient permissions to perform its required tasks.

To a domain controller, an anonymous account is equivalent to a Windows Guest account. If DC Agent is configured to use an anonymous account, and the domain controller has been set not to give the list of user logon sessions to an anonymous user, then DC Agent is unable to retrieve logon information.

- DC Agent uses the **NetSessionEnum** call, which may fail depending on your Local Security Policy or Trust Relationship configuration.
- User Service uses **NetUserGetGroups**, which requires domain administrative rights.

To address this issue, create an account domain controller read privileges for DC Agent to use when requesting user logon information from the directory service.

If DC Agent is configured to perform computer polling, the service must run as an account with **domain** or **enterprise admin** privileges.

Updating DC Agent permissions

Steps

1) On the DC Agent machine, create a user account with a descriptive name, like **WebDcAgent**. This account exists only to provide a security context for DC Agent when it requests information from the directory service.
   - Assign the new account read/write privileges in all domains.
   - Make the account a member of the domain controller's Event Reader group.
   - Assign the same password to this account in all domains.
   - Set the password to never expire. This account exists only to provide a security context for accessing directory objects.

   Make a note of the user name and password so that you have it when you get to step 5.

   

   Note

   Domain administrators are not, by default, part of the Event Log Reader group.

2) Open the Windows Services tool.

3) Scroll to the **Websense DC Agent** service, right-click the service name, and then select **Stop**.

4) Double-click the service name, and then select the **Log On** tab.

5) Select **This account**, and then enter the DC Agent account name and password that you just created. Some domains require that the account name be entered in the format **domain\username**.

6) On the General tab, click **Start** to start the service, then click **OK**.

7) Close the Services tool.

Next steps

You may also need to assign the same set of administrative privileges to User Service.

DC Agent: ERROR_BAD_NETPATH - 53

Before you begin

This error typically indicates that a network problem is preventing DC Agent from contacting a domain controller.

If you encounter this remote access issue:

Steps

1) On the DC Agent machine, use the Windows Services tool to verify that the **Remote Registry Service** is running.

2) If DC Agent is configured to use NetBIOS ("UseNetBIOS=true" appears in the transid.ini file), make sure that NetBIOS is bound to the network adapter on the DC Agent machine:

   a) Navigate to Control **Panel** > **Network and Internet** > **Network and Sharing Center**.

   b) Click **Local Area Connection**, then click **Properties**.

   c) Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.

   d) Click **Advanced**, and then select the **WINS** tab.

   e) Make sure that the NetBIOS setting is **Default** or **Enable**.

   f) If you made a change, click **OK** three times to save your changes and close Properties dialog boxes.

3) Verify that the DC Agent machine and the domain controller machine are using the same network protocol for communication (for example, TCP/IPv4).

4) Use the **net view** command to verify that the DC Agent machine can communicate with client machines in the network, and with the domain controller:

   `net view \\<machineIPaddress>`

   `net view \\<domaincontrollerIPaddress>`

   If the net view command fails, check the DC Agent machine's network connection and placement within the network.

5) Make sure that remote administration is enabled on the domain controller.

DC Agent doesn't see some or all users

If DC Agent is installed, but user and group policies aren't being applied, DC Agent might:

- Not be able to contact the domain controller.
- Be retrieving information from the wrong domain controller.
- Have a corrupted or missing configuration file.

The following error may accompany the problem:

```
WSDCagent : Error reading Config File: dc_config.txt
```

```
Erroneous Entry: <string>
```

To troubleshoot issues of this type, see:

Related concepts

DC Agent is not receiving domain controller information on page 10
dc_config.txt file is missing or empty on page 13

Related tasks

Configure which domain controllers DC Agent polls on page 11
Uncover DC Agent communication issues on page 12
Manually enable the Computer Browser service on page 4

DC Agent is not receiving domain controller information

DC Agent can misidentify users if it is unable to get data from domain controllers, resulting in incorrect filtering behavior. This can happen if:

- DC Agent is not detecting all domain controllers in the network.

  To see which domains and domain controllers DC Agent has identified, go to the **Web** > **Settings** > **General** > **User Identification** page in the Forcepoint Security Manager, and click **View Domain List** (under DC Agent Domains and Controllers). This lists all domains currently being polled by all DC Agent instances in your network. The instances polling each domain are listed in the DC Agent Instances column.

  If one or more domains is missing from the list, or if an instance is not polling the correct domains, see *Configure which domain controllers DC Agent polls*.

- DC Agent may not be able to identify the domain controllers in a particular domain.

  Use the Windows Event Viewer to check for the following error:

  ```
  ERROR_NO_BROWSER_SERVERS_FOUND -6118
  ```

  If your network includes multiple subnets, DC Agent may have problems communicating with Master Browser or domain controller machines in other subnets. As a best practice, install a separate DC Agent in each subnet to avoid problems gathering logon information from domain controllers.

- DC Agent and User Service may be configured to use an anonymous account. To change the account used to run DC Agent or User Service, see *Updating DC Agent permissions*.
- DC Agent may not be able to contact a remote domain controller that has been shut down or restarted. See *DC Agent: ERROR_BAD_NETPATH - 53*.

Related tasks
Configure which domain controllers DC Agent polls on page 11
Updating DC Agent permissions on page 8
DC Agent: ERROR_BAD_NETPATH - 53 on page 9

Configure which domain controllers DC Agent polls

Before you begin

If DC Agent is attempting to poll domain controllers that don't exist, or if you have turned off automatic domain discovery and want to have DC Agent poll a new domain controller, edit the **dc_config.txt** file to configure DC Agent behavior.

Steps

1) Go to the web protection **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default) on the DC Agent machine.

2) Make a backup copy of the **dc_config.txt** file in another location.

3) Open the original **dc_config.txt** file in a text editor (like Notepad).

4) Confirm that all of your domains and domain controllers are listed. For example:

```
[WEST_DOMAIN]
dcWEST1.forcepoint.com=on
dcWEST2.forcepoint.com=on
EAST_DOMAIN]
dcEAST1.forcepoint.com=on
dcEAST2.forcepoint.com=on
```

If there are domain or domain controller entries missing from the list, you can add them manually. Before adding entries, run the `net view /domain` command on the DC Agent machine to make sure that the agent can see the new domain.

5) If there are entries in the list that DC Agent should not poll, change the entry value from on to off. For example:

`dcEAST2.forcepoint.com=off`

- If you configure DC Agent to avoid polling an active domain controller, the agent cannot transparently identify users logging on to that domain controller.
- If DC Agent's automatic domain discovery has detected a domain controller that should not be used to authenticate users, set the entry to off, rather than removing it. Otherwise, the next discovery process will re-add the controller.

6) Save your changes and close the file.

7) Use the Windows Services tool to restart the **Websense DC Agent** service.

Uncover DC Agent communication issues

Before you begin

In order to identify users, DC Agent uses DNS or NetBIOS to identify domains and domain controllers in the network. DC Agent may be unable to identify domain controllers if there are network communication problems, or DNS or NetBIOS configuration problems.

To identify these issues:

Steps

1) Open a command prompt or Windows Powershell on the DC Agent machine.

2) To verify that the DC Agent machine can see all required domains, use the **net view** command:

```
net view /network
```

3) To check for DNS issues, use the **nslookup** command.

For example, to find out if DNS resolves the hostname “testmachine1”:

```
nslookup testmachine1
```

If the DNS lookup succeeds, the result looks something like this:

```
Server: testdns.test.example.com
Address: 10.56.1.4
Name: testmachine1.test.example.com
Address: 10.56.100.15
```

Use a similar command to verify that a reverse DNS lookup will succeed for a dual-stack (IPv4 and IPv6) client with IPv6 address “::ffff:A.B.C.D”:

```
nslookup ::ffff:A.B.C.C
```

If the DNS lookup succeeds, the result looks something like this:

```
Server: testdns.test.example.com
Address: ::ffff:A.B.C.C
```

If lookup does not succeed, make sure you have a reverse lookup zone for IPv6 in your DNS.

4) If DC Agent is configured to use NetBIOS, attempt to telnet to a domain controller on port **139**. If the telnet command is successful, you will see a blank screen. If unsuccessful:

- A router, firewall, or other device may be blocking NetBIOS traffic.
- NetBIOS may not be enabled, and the domain controller may not be listening on port 139. To check the status of the port, use the **netstat** command:

  Windows:

  ```
  netstat -na | find "139"
  ```

  Linux:

  ```
  netstat -na | grep 139
  ```

Configure DC Agent to use only NetBIOS for user identification

Steps

1) Navigate to the web protection **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default) and open the **transid.ini** file in a text editor.
   If the file does not exist, use a text editor to create a file called **transid.ini**, and add the following line to the top of the file:
   ```
   [DCAgent]
   ```

2) Locate the or add the **UseNetBIOS** parameter, then set its value to **True**. For example:
   ```
   [DCAgent]
   UseNetBIOS=True
   ```

3) Save and close the INI file.

4) Use the Windows Services tool to stop the **Websense DC Agent** service.

5) Remove the **XidDcAgent.bak** file from the **bin** directory.
   The file is recreated when you start DC Agent.

6) Start the **Websense DC Agent** service.

dc_config.txt file is missing or empty

If DC Agent does not create a **dc_config.txt** file, this indicates that it is either unable to see any domain controllers, or the service does not have read and write privileges to the web protection **bin** directory.

If the DC Agent Service has read and write permissions to the bin directory, the most typical reasons it cannot create the file, or the file is empty, are:

1) DC Agent is not joined to the specific domain.

2) DC Agent cannot locate the domain controllers when doing an nslookup on the Fully Qualified Domain Name (FQDN).

If you are unable to resolve the issue preventing DC Agent from creating the file, it is possible to create the file manually (see *Create the dc_config.txt file manually*). When you do this, however, if the underlying problem is not resolved, DC Agent cannot detect changes to your network structure. You must maintain the list of domains and domain controllers in the dc_config.txt file manually.

Related tasks
Create the dc_config.txt file manually on page 14

Use DC Agent for domain discovery

Steps

1) Log on to the Forcepoint Security Manager and go to the **Web** > **Settings** > **General** > **User Identification** page.

2) Click the DC Agent instance hostname or IP address in the Transparent Identification Agents list.

3) Under Domain Discovery, make sure **Enable automatic domain discovery** is selected. If you are using v8.5, then select **DC Agent** as the service to use for domain discovery. With v8.5.3 and later, domain discovery will always be done by DC Agent.

   DC Agent must run with **domain** or **enterprise admin** permissions to perform automatic domain discovery.

4) Click **OK** to cache the change, then click **Save and Deploy**.

Next steps

After about 2 minutes, the **dc_config.txt** file should be created automatically.

Create the dc_config.txt file manually

Steps

1) Open a text editor on the DC Agent machine.

2) Use the following format to list each domain that DC Agent should poll, followed by its domain controllers, as shown below. The square brackets ([]) around the domain name are required.

```
[WEST_DOMAIN]
dcWEST1.forcepoint.com=on
dcWEST2.forcepoint.com=on
[EAST_DOMAIN]
dcEAST1.forcepoint.com=on
dcEAST2.forcepoint.com=on
```

3) Enter a carriage return after the last line in the new file.

   If this hard return is not included (creating a blank line at the end of the file), the last entry in the file gets improperly truncated, and an error message like the following appears in the **websense.log** file:

   `WSDCagent : Error`

   `reading Config File: dc_config.txt`

   `Erroneous Entry: dcEAST2=o`

4) Save the file in the web protection **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default) with the name **dc_config.txt**.

5) Use the Windows Services tool to restart the **Websense DC Agent** service.

Published 21 August 2024