Using DC Agent for Transparent User Identification

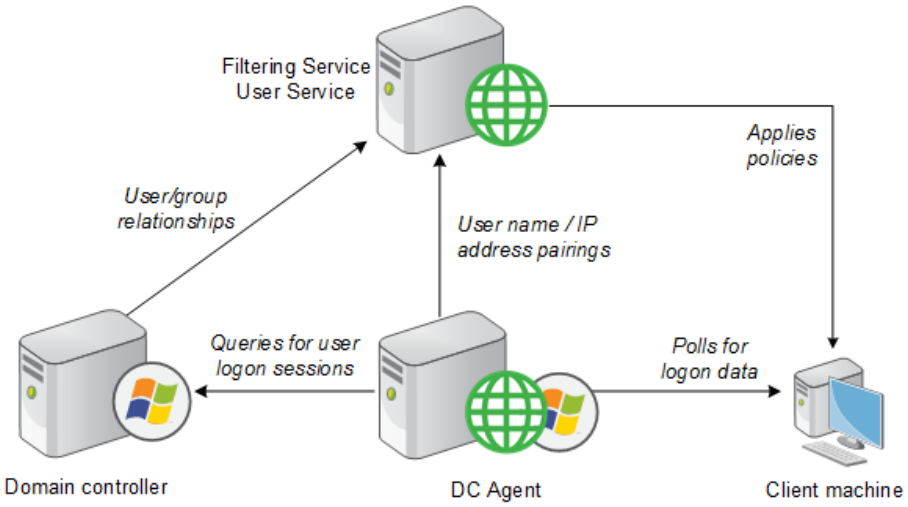
Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

If you have an on-premises installation of TRITON AP-WEB or Web Filter & Security, and your organization uses Microsoft Windows Active Directory, you can use **DC Agent** to identify users transparently. The agent periodically queries domain controllers for logon session information, and can be configured to poll client machines to verify logon status.

This collection includes the following articles to help you understand how to deploy, configure, and use DC Agent. Click a link below to jump to the topic, or use the arrows at the top of the content pane to browse the articles.

For DC Agent troubleshooting help, see the DC Agent Troubleshooting, available from support.forcepoint.com.

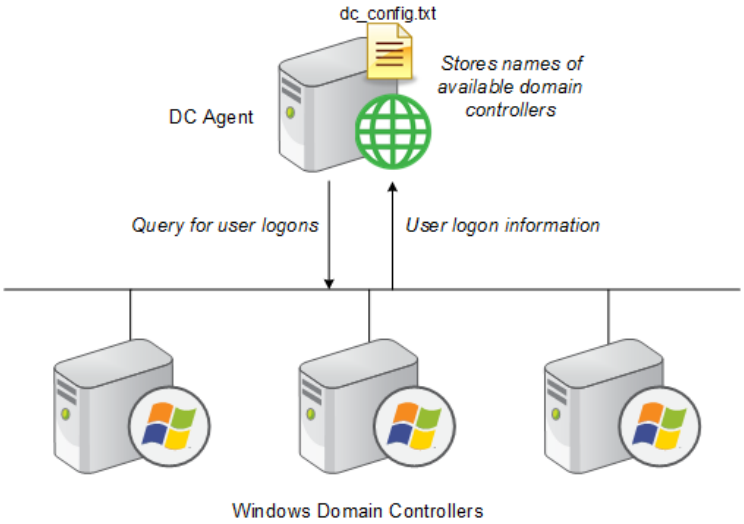
How DC Agent identifies users



- **DC Agent detects domain controllers:** At startup, and (by default) every 24 hours thereafter, DC Agent identifies available domains and domain controllers in the network and saves the information to its **dc_config.txt** file.

  In order to perform domain discovery, DC Agent requires **domain** or **enterprise admin** permissions. If you do not want to grant DC Agent these permissions, you can maintain the DC Agent list of domains and domain controllers manually.

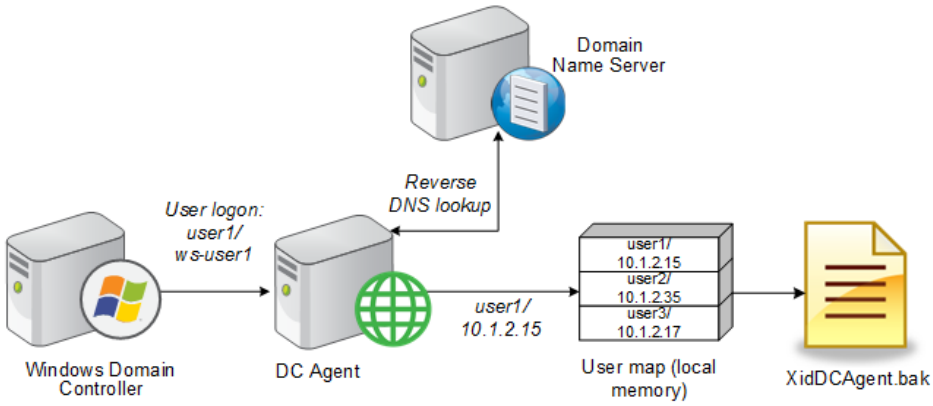
- **DC Agent obtains logon session information:** DC Agent queries each domain controller for user logon sessions, obtaining the user and computer name.



By default, the query occurs every 10 seconds. This interval can be configured in the TRITON console (go to **Web > Settings > General > User Identification**, and then click a DC Agent instance in the Transparent Identification Agents list).

> **Note**
> If DC Agent is not running when a user logs on to a domain controller (because the DC Agent machine was restarted, for example), the logon session is not recorded. In this case, the computer or network policy (if it exists), or the Default policy, is used to manage user requests.

- **DC Agent records user name/IP address pairs:** For each logon session, DC Agent performs a DNS lookup to resolve the computer name to an IP address, and then stores the user name/IP address pair in its user map in local memory. It periodically writes a copy of the user map to **XidDcAgent.bak**.



- **DC Agent sends user information to Filtering Service:** DC Agent provides user names and IP addresses to Filtering Service each time its user map is updated.
  - The agent sends only those new user name/IP address pairs recorded since the last query.
  - Filtering Service adds new user name/IP address pairs to its copy of the user map in local memory.

  No confidential information (such as user passwords) is transmitted.
- **Filtering Service gets group information for logged-on users:** Filtering Service queries User Service to get group information for users in its copy of the user map. User Service queries the directory service for this group information, and sends the information to Filtering Service.
- **Policies are applied to logged-on users:** Filtering Service uses the information from DC Agent and User Service to ensure that the correct policies are applied to directory clients (users, groups, and OUs).

  Filtering Service does not check the policy every time an Internet request is made; policy data is cached for 3 hours by the server, unless the user cache is explicitly cleared in the TRITON Manager.

DC Agent can be used in conjunction with Logon Agent. In this configuration, user logon information provided by Logon Agent takes precedence over information from DC Agent. DC Agent communicates a logon session to Filtering Service only in the unlikely event that Logon Agent has missed one. For more information about Logon Agent, see Using Logon Agent for Transparent User Identification.

DC Agent computer polling

In addition to polling domain controllers for logon information, DC Agent also polls client machines (computers or workstations), by default. This helps to verify which user is logged on to a machine.

When Filtering Service receives a request from a client machine, Filtering Service prompts DC Agent to poll the client machine, unless the machine was already polled more recently than the configured query interval (15 minutes, by default).

DC Agent uses WMI (Windows Management Instruction) for computer polling. If you use computer polling, configure the Windows Firewall on client machines to allow communication on port 135.

Note

Computer polling is not effective for client machines that users access via remote desktop.

DC Agent stores the resulting user name/IP address pair in its user map and provides the information to Filtering Service. At a pre-defined interval, DC Agent uses computer polling to verify that users are still logged on.

You can configure how often DC Agent attempts to verify that users are still logged on, and how long an entry remains in the user map. See *Configure DC Agent settings*, page 7.

In order to use computer polling, DC Agent must run with **domain** or **enterprise admin** permissions.

Components used for DC Agent user identification

Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

- **DC Agent** monitors domain controllers and client machines for user logon information, and then provides the information to Filtering Service for use in applying policies.

  You can configure DC Agent and Filtering Service to use an authenticated connection for communication (see *Configure DC Agent settings*, page 7).

A DC Agent installation includes the following files, all located in the **Websense\Web Security\bin** folder:

Name	Functionality
XidDcAgent.exe	The DC Agent executable: • Automatically discovers domains at startup and at 24-hour intervals, by default. • Sends new entries to Filtering Service, when queried. • Uses port 30600 by default. • Runs as a Windows service named Websense DC Agent.
dc_config.txt	• Lists the domains and domain controllers in the network • Indicates whether DC Agent monitors each domain controller. New domain information is written to the file at agent startup, and every 24 hours thereafter (by default).
XidDcAgent.bak	Serves as a backup copy of the DC Agent user map. Read on agent startup.
ignore.txt	Contains list of user names, machines, and user/machine pairs for DC Agent to ignore.

- **User Service** works with DC Agent to provide an up-to-date list of domains in the network and users in each domain. User Service interacts with the directory service to get group and OU information for logged-on users.
- **Filtering Service** receives user logon session information from DC Agent in the form of user name/IP address pairs. When Filtering Service receives the IP address of a machine making an Internet request, it matches the address with the user name provided by DC Agent and applies the appropriate policy to the request.

  Filtering Service and DC Agent can be installed on the same machine, or on different machines.

DC Agent and user machines

In order for DC Agent to identify users, the users must log on to a Windows domains. Client machines do not necessarily need to be running a Windows operating system.

The IP address of each computer is a key element in applying policies. If DC Agent cannot identify a machine by IP address, the Default policy is applied to Internet requests made from that machine.

For each logon session detected by a domain controller, DC Agent performs a DNS lookup to convert the user's machine name to an IP address, and then stores the IP address in its user map.

DC Agent deployment overview

Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

To enable transparent user identification with DC Agent:

1. Install DC Agent and User Service. To ensure a smooth DC Agent installation:
   - Make sure the Windows **Computer Browser** service is running on the server. (The installer attempts to enable the service if it is not running.)
   - Run the installer with an account that has both **local** and **domain** administrator privileges.
2. Use the TRITON Manager to configure your product to communicate with DC Agent (see *Configure DC Agent settings*, page 7).
   - If User Service is running on a Linux machine, be sure to complete the WINS setup steps included in the configuration instructions.
   - Optionally, also configure your software to prompt users for logon information if transparent identification fails or is not available. See the *Administrator Help* for your version (v8.2.x or v8.3.x) for details.
3. Use the TRITON Manager to identify directory clients for policy enforcement.

If your network is very large (10,000+ users or 30+ domain controllers), you may benefit from installing DC Agent on multiple machines, particularly if you have different domains in separate subnets. This way, you have ample space for files that are continually populated with user information, and the user identification process is faster.

In most cases, you need only 1 Filtering Service that communicates with every instance of DC Agent in your network. If you have installed multiple Filtering Services for load-balancing purposes, each Filtering Service must be able to communicate with every DC Agent.

Typically, User Service is installed on the same machine as Policy Server. User Service can be installed separately, as long as there is 1 instance of User Service for each instance of Policy Server.

DC Agent uses TCP (Transmission Control Protocol) to transmit data. When user data is sent to Filtering Service, roughly 80 bytes is transmitted per user name/IP address pair. The table below shows average quantities of data transferred per day, by number of users.

250 users	30 KB
2000 users	240 KB
10,000 users	1200 KB

Configure DC Agent settings

Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

In the Web module of the TRITON Manager, use the **Settings > General > User Identification** page to review and edit DC Agent configuration information.

To edit DC Agent settings:

1. Use the Transparent Identification Agents table to select the IP address or hostname of the DC Agent instance that you want to configure.

   If you have installed a new DC Agent instance that does not appear in the list, click **Add Agent**, then select **DC Agent** from the drop-down list.
2. Under Basic Agent Configuration, enter or verify the **IPv4 address or hostname** of the machine on which the agent is installed.

   Note

   Hostnames must start with an alphabetical character (a-z), not a numeric or special character.

   Hostnames containing certain extended ASCII characters may not resolve properly. To avoid this issue, enter an IP address instead of a hostname.
3. Enter or verify the **Port** that DC Agent should use to communicate with other web protection components. The default is 30600.
4. To establish an authenticated connection between Filtering Service and DC Agent, select **Enable authentication**, and then enter a **Password** for the connection.

Next, customize global DC Agent communication and troubleshooting, domain controller polling, and computer polling settings. By default, changes that you make here affect all DC Agent instances associated with a Policy Server instance.

Some of these settings can, however, be overridden in a configuration file. See *Custom configuration for a DC Agent instance*, page 11.

1. Under Domain Discovery, mark or clear **Enable automatic domain discovery** to determine whether DC Agent automatically finds domains and domain controllers in your network.
2. If domain discovery is enabled, also specify:
   - How often to discover domains (**Identify domains every** setting). Domain discovery occurs at 24-hour intervals, by default.
   - Whether **DC Agent** or **User Service** is responsible for performing domain discovery.

     In many environments, it is preferable to use User Service for domain discovery.

     If DC Agent is used for domain discovery, the service must run with **domain** or **enterprise admin** privileges.

3. When User Service is installed on a Linux machine, the page includes a **Linux WINS Server Information** section. Configure a WINS server if both of the following are true:
   - You selected User Service as the component to use for domain discovery.
   - User Service is installed on Linux.

   This is required to resolve domain names to domain controller IP addresses.

   To configure WINS server communication, enter:

   a. The account name of an **Administrative user** that can access the directory service.

   b. The **Password** for the account.

   c. **Domain** information for the account.

   d. The IP address or hostname of a WINS server in your network.
4. In the Domain Controller Polling section of the DC Agent Communication box, mark **Enable domain controller polling** to enable DC Agent to query domain controllers for user logon sessions.

   You can specify which domain controllers each instance of DC Agent polls in the agent's configuration file. See *Configure domain controller polling in dc_config.txt*, page 9.

   To perform domain controller polling, the DC Agent service needs only read privileges on the domain controller. Automatic domain discovery (steps 1 and 2) and computer polling (step 7) require that the service run with elevated permissions.
5. Use the **Query interval** field to specify how often (in seconds) DC Agent queries domain controllers.

   Decreasing the query interval may provide greater accuracy in capturing logon sessions, but also increases overall network traffic. Increasing the query interval decreases network traffic, but may also delay or prevent the capture of some logon sessions. The default is 10 seconds.
6. Use the **User entry timeout** field to specify how frequently (in hours) DC Agent refreshes the user entries in its map. The default is 24 hours.
7. Under Computer Polling, check **Enable computer polling** to enable DC Agent to query computers for user logon sessions. This may include computers that are outside the domains that the agent already queries.

   DC Agent uses WMI (Windows Management Instruction) for computer polling. If you enable computer polling, configure the Windows Firewall on client machines to allow communication on port **135**.

   If DC Agent performs computer polling, the service must run with **domain** or **enterprise admin** privileges.
8. Enter a **User map verification interval** to specify how often DC Agent contacts client machines to verify which users are logged on. The default is 15 minutes.

   DC Agent compares the query results with the user name/IP address pairs in the user map it sends to Filtering Service. Decreasing this interval may provide greater user map accuracy, but increases network traffic. Increasing the interval decreases network traffic, but also may decrease accuracy.

9. Enter a **User entry timeout** period to specify how often DC Agent refreshes entries obtained through computer polling in its user map. The default is 1 hour.

   DC Agent removes any user name/IP address entries that are older than this timeout period, and that DC Agent cannot verify as currently logged on. Increasing this interval may lessen user map accuracy, because the map potentially retains old user names for a longer time.

   > **Note**
   > Do not make the user entry timeout interval shorter than the user map verification interval. This could cause user names to be removed from the user map before they can be verified.

10. Click **OK** to return to the User Identification page, then click **OK** again to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Configure domain controller polling in dc_config.txt

Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

By default, DC Agent automatically identifies domains and domain controllers at startup, then detects when domains or domain controllers are added or removed from the network. This process is called domain discovery (see *Configure DC Agent settings*, page 7).

DC Agent stores domain and domain controller information in a file called **dc_config.txt** (located, by default, in the C:\Program Files\Websense\Web Security\bin\ directory on each DC Agent machine).

- You can edit the dc_config.txt file to change which domain controllers a DC Agent instance polls. Do this, for example, to:
  - Enable load balancing across multiple DC Agent instances.
  - Stop DC Agent from polling domain controllers that don't exist.
- If you do not want DC Agent or User Service to perform domain discovery, you can create and maintain the dc_config.txt file manually.
- You can review domain and domain controller information from dc_config.txt in the TRITON Manager. Go to the **Web > Settings > General > User Identification** page and click **View Domain List**.

  Note that the DC Agent Domains and Controllers page lists information for the DC Agent instances associated with a specific Policy Server. You may need to use the Policy Server **Switch** button in the Web toolbar to select the Policy Server associated with the DC Agent instances you want to review.

To edit or create the dc_config.txt file:

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

2. If the **dc_config.txt** file already exists, make a backup copy in another location.
3. Create or open the **dc_config.txt** file using a text editor.
4. List all of your domains and domain controllers, or verify that all of your domains and controllers are listed. For example:

   ```
   [WEST_DOMAIN]
   dcWEST1=on
   dcWEST2=on
   [EAST_DOMAIN]
   dcEAST1=on
   dcEAST2=on
   ```

   If you are editing a file, and domains or domain controllers are missing, you can add them. 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 domain controllers in the list that DC Agent should not poll, change the entry value from **on** to **off**. For example:

   ```
   dcEAST2=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 identify users, set the entry to **off**, rather than removing it. Otherwise, the next discovery process will re-add the controller.
6. Make sure that the file includes a carriage return after the last entry.

   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 appears in the **websense.log** file.
7. Save your changes and close the file.
8. Use the Windows Services tool to restart the **Websense DC Agent** service.

Configure DC Agent to ignore certain user names

Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

The method that some Windows services use to contact domain controllers from user machines can cause the users logged on to those machines to be misidentified. For example, problems can be caused by:

- The internal user names (Local Service and Network Service) that Windows XP assigns for processes to use for communication with domain controllers
- Running Systems Management Server (SMS) on a client machine.

To prevent or work around possible misidentification, configure your transparent identification agent to ignore logon names that are not associated with actual users.

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

2. Navigate to the web protection **bin** directory (C:\Program Files\Websense\Web Security\bin, by default).
3. Use a text editor to either create or open **ignore.txt**.

> **Note**
> To set a size limit for the ignore list, use the *MaxIgnoreListSize* initialization parameter.

4. Populate the file as follows. Place each entry on a separate line.
   - Add each **user name** that should be ignored on its own line. Web protection software ignores these users, regardless of which machine they use.
   - To add a **user name/machine pair**, enter the user name, followed by a comma, and then the machine host name or IP address (ypark,YPARK-WS1). In this case, web protection software ignores the specified user only on the specified machine.
   - To add a **machine**, enter an asterisk (*), followed by a comma, followed by the machine host name, IP address, or IP address range.

   The following example shows correctly formatted entries:

   ```
   anonymous logon
   admin,WKSTA-NAME
   *, WKSTB-NAME
   *, 10.209.34.56
   *, 10.203.34.1-10.203.34.255
   ```

   In this example, the Windows 7 service account **anonymous logon** is ignored on all machines, the user name **admin** is ignored only when associated with machine **WKSTA-NAME**, and logons for **WKSTB-NAME**, **10.209.34.56**, and the network range **10.203.34.1** to **10.203.34.255** are ignored.
5. When you are finished making changes, save and close the file.
6. Start the **Websense DC Agent** service.

Custom configuration for a DC Agent instance

Using DC Agent | Web Protection Solutions | v8.2.x, v8.3.x | 10-Dec-2016

Many of the DC Agent settings configured in the TRITON console apply to all agent instances in your deployment. You can, however, configure settings unique to a DC Agent instance by creating a configuration file called **transid.ini**.

1. Use a text editor to create a file called **transid.ini**, then save the file in the web protection **bin** directory (C:\Program Files\Websense\Web Security\bin, by default).
2. Add the following heading to the beginning of the file:

   ```
   [DCAgent]
   ```

3. Under the heading, enter the parameter to customize for this agent instance. For example, configure the agent to ignore user names that contain a dollar sign:

   ```
   AllDollarSign=True
   ```

4. Add other values as desired.
5. Save and close the INI file.
6. Use the Windows Services tool to stop the **Websense DC Agent** service.
7. Delete the **XidDcAgent.back** file from the web protection **bin** directory.

   The file is recreated when you start DC Agent.
8. Start the **Websense DC Agent** service.

Note that not all user identification settings can be overridden, and that all parameters and values described in this document are case-sensitive.

Before creating or updating the **transid.ini** file, please consider that the default values are designed to maximize accuracy and efficiency in most environments. In most cases, it is best to leave the default values as they are.

AllDollarSign

Prompts DC Agent to ignore logon sessions from any user names that contain a dollar sign character ($).

Default	True
Options	True, False
Synopsis	Ensures that DC Agent drops all entries containing dollar signs from its user map, without performing any additional verification. This option is a more powerful version of *IgnoreDollarSign*.

DiscoverInterval

Interval at which the domain auto-discovery process runs, in seconds (equivalent to the **Identify domains every** value under Domain Discovery in the TRITON Manager). The default is 86400 seconds, or 24 hours.

Default	86400
Options	Integer greater than 3600, or 0 to disable
Synopsis	DC Agent automatically detects new domains or domain controllers added to the network. By default, detected domain names are recorded to the **dc_config.txt** file at startup, and every 24 hours thereafter. Increasing the domain discovery interval may delay discovery of a new domain or domain controller. Decreasing the interval increases network traffic, because the process runs more frequently.

IgnoreDollarSign

Enables DC Agent to ignore logons from user names containing dollar signs ($).

Default	True
Options	True, False
Synopsis	Used to prevent a problem involving Windows 2000 services that use a machine name followed by a dollar sign (**wkstn$**) as a user name when contacting the domain controller. DC Agent interprets the service as a new user to whom no policy has been assigned. When this parameter is set to **True**, if DC Agent detects a **user$** entry in its map, it compares the name to the source machine's name. If these match, DC Agent ignores the logon session entirely, because it knows the logon did not originate from an actual user. If the logon name and machine name do not match, DC Agent attempts to get the name of the actual user logged on from the source machine. If it obtains a user name, DC Agent pairs that with the IP address of the source machine, and records these together in its map. If DC Agent cannot obtain an actual user name, it simply records the **user$** entry in its map. This process minimizes the number of false user names DC Agent stores in its map and sends to Filtering Service. When the parameter is set to **False**, if DC Agent detects a **user$** entry in its map, the agent attempts to replace it with an actual user name from the source machine. If DC Agent does not obtain an actual user name, it records the **user$** entry in its map.

IgnoreLocalLogins

Determines whether DC Agent registers local (non-domain) user logons to local client machines.

Default	False
Options	True, False
Synopsis	By default, DC Agent detects users logging on to domains and to local machines. If for some reason you want DC Agent to register logons only to domain controllers, and ignore local logons, set this value to True. See also *AllDollarSign*.

IgnoreRepeats

Determines whether DC Agent re-records user logon sessions that it already recorded at the time of the previous query.

Default	True
Options	True, False
Synopsis	By default, DC Agent ignores a user logon to a domain controller, if it already registered that logon after the previous domain controller query. As a best practice, leave this default setting as is. In most cases, there is no benefit to duplicating recognition of an earlier logon session.

IPCleanInterval

Interval at which DC Agent checks its cache for stale machine name/IP address pairs, in seconds.

Default	600 [seconds = 10 minutes]
Options	Between 300 and 3600 seconds.
Synopsis	Determines how often DC Agent checks the machine name/IP address pairs in its cache for entries older than the *IPCleanLifetime* period. Entries older than this time period are removed from the cache. This parameter typically does not need to be changed.

IPCleanLifetime

The amount of time a machine name/IP address pair remains in DC Agent's cache before it is removed, in seconds.

Default	7200 [seconds = 2 hours]
Options	Integer greater than 3600, or 0 to disable
Synopsis	As DC Agent receives logon session information, it stores machine name/IP address pairs in its local memory cache. This reduces the number of times DC Agent must perform DNS lookups for each active client machine, because it already has the IP address.

MaxIgnoreListSize

The maximum number of entries (user names, user name/machine name pairs, and machine names) in DC Agent's **ignore.txt** file.

Default	70000
Options	Integer 5000 or greater
Synopsis	If you use an **ignore.txt** file to configure DC Agent to ignore particular users or client machines, this parameter sets an upper limit on the number of entries in the file. See *Configure DC Agent to ignore certain user names*, page 10.

StartDelay

Time period by which to delay DC Agent service initialization to allow diagnostic routines to start first.

Default	0 [seconds]
Options	Between 0 and 120 seconds
Synopsis	Used primarily by Forcepoint Technical Support. Allows the ConsoleClient diagnostic tool to connect to DC Agent while the service is running, but before its processes are activated. Use extreme caution when modifying this parameter.

UseDNSReverse

Determines whether DC Agent identifies the client hostname in the process of retrieving client IP address information.

Default	True
Options	True, False
Synopsis	By default, DC Agent uses the workstation entry in the session information it receives from the domain controller to first find the client hostname, then find the associated IP address. When UseDNSReverse is set to False, DC Agent uses the workstation entry to retrieve IP address information without first looking up the client hostname. Note: When UseDNSReverse is set to True and you have dual-stack (Ipv4 and IPv6) clients, you must have a reverse lookup zone in your DNS.

UseNetBIOS

Whether to use NetBIOS to perform domain controller machine name lookups.

Default	False
Options	True, False
Synopsis	By default, DC Agent uses DNS lookup to identify domain controllers by name and IP address. If the DNS lookup fails, the agent uses NetBIOS calls. Set this parameter to **True** to cause DC Agent to use only NetBIOS to identify domain controllers.

UseUserService

Whether to use User Service or Windows networking calls to communicate with domain controllers. (Equivalent to selecting **User Service** as the component to use for domain discovery in the TRITON Manager.)

Default	True
Options	True, False
Synopsis	By default, DC Agent uses User Service for communications with domain controllers in the network. To close the ports required for User Service to facilitate communications between DC Agent and domain controllers, set this value to **False**. In this case, DC Agent uses Windows networking calls for communications instead.

VerifyUserDomain

Whether to make sure that a user exists in a particular domain as indicated by domain controller polling results.

Default	True
Options	True, False
Synopsis	When this parameter is enabled, DC Agent checks the existence of a user account against the domain where a user logon session is detected. When this parameter is set to **False**, DC Agent may not update its user map right away if a user account is moved from one domain to another.