



Web Security On-prem

v8.5.x

Using eDirectory Agent for Transparent User
Identification

Contents

- [Introduction on page 2](#)
- [How eDirectory Agent works on page 2](#)
- [Novell eDirectory server replication on page 3](#)
- [eDirectory Agent user identification process on page 4](#)
- [Components used for transparent identification with eDirectory Agent on page 5](#)
- [Deploying and configuring eDirectory Agent on page 7](#)
- [eDirectory Agent troubleshooting on page 17](#)

Introduction

eDirectory Agent works with Novell eDirectory to transparently identify users so that Filtering Service can apply policies to users and groups.

This collection includes the following articles to help you understand how eDirectory Agent works, configure eDirectory Agent, and troubleshoot user identification issues.

Related concepts

- [How eDirectory Agent works on page 2](#)
- [Novell eDirectory server replication on page 3](#)
- [Components used for transparent identification with eDirectory Agent on page 5](#)
- [Deploying and configuring eDirectory Agent on page 7](#)
- [eDirectory Agent troubleshooting on page 17](#)

Related tasks

- [eDirectory Agent user identification process on page 4](#)

How eDirectory Agent works

eDirectory Agent does not authenticate users directly. Instead, the agent uses Netware Core Protocol (NCP) to gather user logon session information from Novell eDirectory, which authenticates users logging on to the network. (The query protocol can be changed; see *Configuring the default directory protocol.*)

eDirectory Agent associates each authenticated user with an IP address and records user name-to-IP-address pairings in its user map, then supplies the information to Filtering Service.

- **User name:** The name by which the user is identified and authenticated in the network. eDirectory Agent correlates the Novell eDirectory Common Name (cn) attribute to a user logging in. The cn acts as a unique identifier of an object within the Novell eDirectory structure.

- **IP address:** The IP address of a logged-on user. eDirectory correlates the Novell attribute “networkAddress” with the user.

It is possible for each user to have zero, 1, or more attributes with this name. For each successful logon, Novell eDirectory server adds 1 networkAddress entry to a user’s attribute profile. If the networkAddress attribute is not present for a user, it means the user is not logged on to Novell eDirectory. eDirectory Agent scans all the networkAddress attributes of a user and adds corresponding user name/IP address entries to its user map.



Note

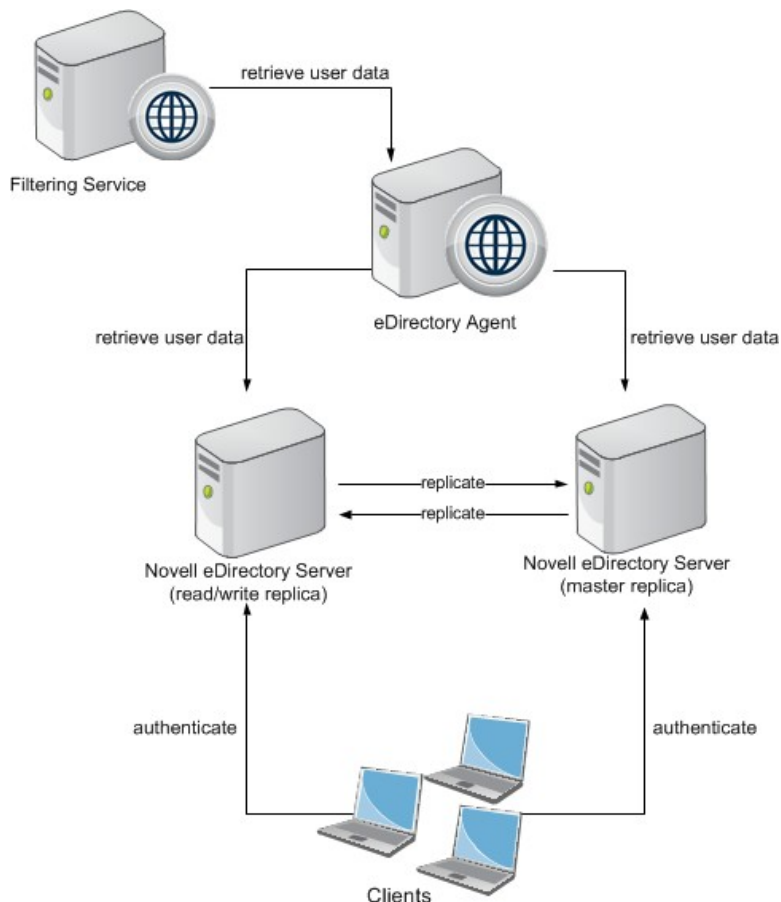
From a Novell client running Windows, multiple users can log on to a single Novell eDirectory server. This associates one IP address with multiple users. In this scenario, eDirectory Agent’s user map only retains the user name/IP address pairing for the last user logged on from a given IP address.

Related tasks

[Configuring the default directory protocol on page 10](#)

Novell eDirectory server replication

Novell eDirectory server can be configured to support several replicas of the directory service on separate machines.



There are two schemes by which Novell server performs replication between machines running eDirectory server replicas: fast and slow. Fast replication occurs every 10 seconds, and slow replication every five minutes. When a user logs on to a particular eDirectory replica, the data for this user is first updated on the machine running this replica. It takes time for user logon data to propagate to all replicas.

eDirectory Agent uses the “networkAddress” property of a user object to associate IP addresses with logged-on users. Because the networkAddress property is synchronized during the slow replication process, there is potentially a five-minute gap between the logon event and the update of user data on all machines containing replicas.

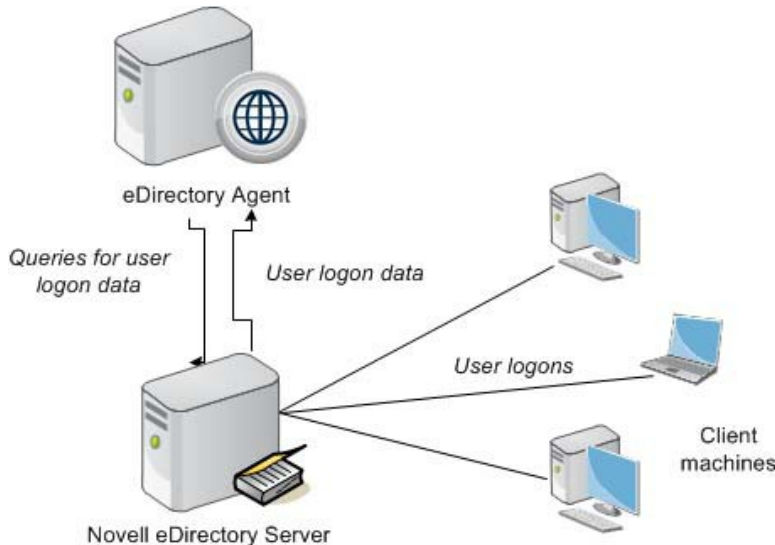
eDirectory Agent must be configured to connect to each machine running a Novell eDirectory replica.

eDirectory Agent user identification process

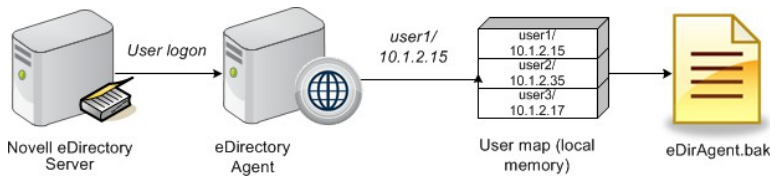
The transparent identification process with eDirectory Agent is as follows:

Steps

- 1) Novell eDirectory authenticates users as they log on.
- 2) eDirectory Agent retrieves information from Novell eDirectory about logged-on users. The agent queries the directory service or user logons at regular intervals (30,000 milliseconds, or 30 seconds, by default). The agent detects only users logging on directly to Novell eDirectory server.



- 3) eDirectory Agent stores the user name, domain name, and originating IP address from each logon session in a user name-to-IP-address map in local memory, and in the **eDirAgent.bak** file.



Note

Due to a Novell limitation, user names that exceed 39 characters cannot be successfully stored in the user map.

If eDirectory Agent receives a new request from an IP address already included in its map, it **replaces** the existing pairing with the new pair

- 4) eDirectory Agent sends user names and IP addresses to Filtering Service using port 30700. Filtering Service records user name/IP address pairs to its own copy of the user map in local memory. No confidential information (such as user passwords) is transmitted.
- 5) Filtering Service queries User Service for group information for user names in its user map. User Service queries Novell eDirectory for group information corresponding to those users, and sends the information to Filtering Service.
- 6) Filtering Service applies policies to the logged-on users. For more information about applying policies to directory clients, see the [Administrator Help](#) for details.

Components used for transparent identification with eDirectory Agent

Transparent user identification with eDirectory Agent involves the following components.

eDirectory Agent

eDirectory Agent queries Novell eDirectory for user logon session information at a given interval. eDirectory Agent associates each authenticated user with an IP address, and records user name-to-IP-address pairings to a local user map. This user map is also written to a backup file named **eDirAgent.bak**.

eDirectory Agent supplies this information to Filtering Service for use in applying policies to requests.

eDirectory Agent uses the following files.

| File name | Location | Functionality |
|---------------------------------|--|---|
| eDirectoryAgent.exe | websense\Web Security\bin\ or / opt/Websense/ | The eDirectory Agent executable. Collects user logon information from Novell eDirectory Server. Sends user logon data to Filtering Service. |
| wsedir.ini | websense\Web Security\bin\ or opt/Websense/ | Contains eDirectory Agent initialization parameters. |
| eDirAgent.bak | websense\Web Security\bin\ or / opt/Websense/ | Backup copy of eDirectory Agent's user name-to-IP address map. Read at startup. |
| ignore.txt (optional) | websense\Web Security\bin\ or / opt/Websense | Contains list of user names, machines, and user/machine pairs for eDirectory Agent to ignore. |

Novell eDirectory

Novell eDirectory houses your organization's user accounts, and provides user authentication.

One instance of eDirectory Agent can support one Novell eDirectory master, plus any number of Novell eDirectory replicas. eDirectory Agent must be able to communicate with each machine running a replica of the directory service. This ensures that the agent gets the latest logon information as quickly as possible, and does not need to wait for eDirectory replication to occur.

User Service

Filtering Service queries User Service to get group information for user names in its copy of the user map. User Service queries Novell eDirectory for group information corresponding to those users, and sends the information to Filtering Service. Directory clients (users and groups) are then made available to the Forcepoint Security Manager so that policies can be assigned to those users and groups.

Filtering Service

Filtering Service receives user logon information from eDirectory Agent as users log on to the network. At each transmission, only the record of logon sessions established since the last transmission is sent back to the server. This includes new users logged on to existing machines and new users logged on to new machines.

Filtering Service receives user data in the form of user name/IP address pairs (originating from eDirectory Agent's map in local memory). When Filtering Service gets the IP address of a machine making an Internet request, it matches the address with the corresponding user name provided by eDirectory Agent, allowing users to be identified transparently whenever they make Internet requests. Filtering Service then applies the policies assigned to those users or groups.

When you are troubleshooting user identification problems, be sure to determine whether Filtering Service is getting the latest and most accurate user data from eDirectory Agent.

Filtering Service can be configured to prompt users to manually authenticate if they cannot be identified transparently. With manual authentication, users that do not provide a valid user name and password are blocked from Internet access.

If a user cannot be identified transparently and manual authentication is not enabled, Filtering Services applies a computer or network (IP address-based) policy, or on the Default policy.

Deploying and configuring eDirectory Agent

eDirectory Agent needs to be installed on only 1 machine in the network. However, if your network is very large, you may benefit from installing the agent on multiple machines. 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 eDirectory Agent. If you have installed multiple Filtering Services for load-balancing purposes, each Filtering Service must be able to communicate with every eDirectory Agent.



Note

eDirectory Agent can **not** be used in combination with DC Agent.

Special deployment considerations

Your web protection software supports using NMAS with eDirectory Agent. To use eDirectory Agent with NMAS enabled, eDirectory Agent must be installed on a machine that is also running the Novell client.

Configuration instructions

After installation, use the following articles to configure eDirectory Agent:

Related concepts

[Adding an eDirectory server replica on page 9](#)

[Enabling full queries on page 11](#)

Related tasks

[Configuring eDirectory Agent settings on page 8](#)

[Configuring the default directory protocol on page 10](#)

[Configuring eDirectory Agent to ignore certain user names on page 12](#)

[Custom configuration for an eDirectory Agent instance on page 13](#)

Configuring eDirectory Agent settings

Use the **Settings > General > User Identification** page in the Web Security module of the Forcepoint Security Manager to review and edit eDirectory Agent configuration information.

To edit settings for an eDirectory Agent instance:

Steps

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

If you have installed a new eDirectory Agent instance that does not appear in the list, click **Add Agent**, then select **eDirectory Agent** from the drop-down list.

- 2) Under Basic Agent Configuration, enter or verify the **IPv4 address or hostname** of the eDirectory Agent machine.



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 host name.

- 3) Enter the **Port** that eDirectory Agent should use to communicate with other web protection components. (30700, by default).
- 4) To establish an authenticated connection between Filtering Service and eDirectory Agent, select **Enable authentication**, and then enter a **Password** for the connection.

Next steps

Next, customize global eDirectory Agent communication settings. By default, changes that you make here affect all eDirectory Agent instances. Settings marked with an asterisk (*), however, can be overridden in an agent's configuration file to customize the behavior of that agent instance (see *Custom configuration for an eDirectory Agent instance*).

Related tasks

[Custom configuration for an eDirectory Agent instance on page 13](#)

title need to give

Steps

- 1) Under eDirectory Server, specify a **Search base** (root context) for eDirectory Agent to use as a starting point when searching for user information in the directory.

- 2) Provide the administrative user account information that eDirectory Agent should use to communicate with the directory:
 - a) Enter the **Administrator distinguished name** for a Novell eDirectory administrative user account.
 - b) Enter the **Password** used by that account.
 - c) Specify a **User entry timeout** interval to indicate how long entries remain in the agent's user map. This interval should be approximately 30% longer than a typical user logon session. This helps prevent user entries from being removed from the map before the users are done browsing.
Typically, the default value (24 hours) is recommended.

**Note**

In some environments, instead of using the User entry timeout interval to determine how frequently eDirectory Agent updates its user map, it may be appropriate to query the eDirectory Server at regular intervals for user logon updates. See *Enabling full queries*.

- 3) Add the eDirectory Server master, as well as any replicas, to the **eDirectory Replicas** list. To add an eDirectory Server master or replica to the list, click **Add**, and then follow the instructions in *Adding an eDirectory server replica*.

Next steps

When you are finished making configuration changes, click **OK** to return to the User Identification page, then click **OK** again to cache your changes. Changes are not saved until you click **Save and Deploy**.

Related concepts

[Enabling full queries](#) on page 11

[Adding an eDirectory server replica](#) on page 9

Adding an eDirectory server replica

One instance of the eDirectory Agent can support one Novell eDirectory master, plus any number of Novell eDirectory replicas running on separate machines.


eDirectory Agent must be able to communicate with each machine running a replica of the directory service. This ensures that the agent gets the latest logon information as quickly as possible, and does not wait for eDirectory replication to occur.

Novell eDirectory replicates the attribute that uniquely identifies logged-on users only every 5 minutes. Despite this replication time lag, eDirectory Agent picks up new logon sessions as soon as a user logs on to any eDirectory replica.

Procedure to configure eDirectory Agent

To configure eDirectory Agent installation to communicate with eDirectory:

Steps

- 1) In the Add eDirectory replica screen, enter the **Server IP address** or name for eDirectory Server (master or replica).
- 2) Enter the **Port** that eDirectory Agent uses to communicate with the eDirectory machine. The valid values are **389** (standard port) and **636** (SSL port).
- 3) Click  to return to the eDirectory Agent page. The new entry appears in the eDirectory Replicas list.
- 4) Repeat the process for any additional eDirectory server machines.
- 5) Click **OK** to cache changes, and then click **Save and Deploy**.
- 6) Stop and start eDirectory Agent so that the agent can begin communicating with the new replica.

Configuring the default directory protocol

eDirectory Agent can use Netware Core Protocol (NCP)—the Windows default—or Lightweight Directory Access Protocol (LDAP)—required on Linux—to retrieve user logon information from Novell eDirectory.

In Windows environments, NCP generally provides a more efficient query method. If your network supports LDAP, however, you can configure eDirectory Agent to use LDAP:

Steps

- 1) Ensure that you have at least 1 Novell eDirectory replica containing all directory objects to which you want to apply policies.
- 2) Stop the eDirectory Agent service.
- 3) Go to the eDirectory Agent directory (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin/, by default).
- 4) Locate the file **wsedir.ini** and make a backup copy in another directory.
- 5) Open the original file in a text editor.
- 6) Modify this **QueryMethod** entry as follows:

```
QueryMethod=0
```

Here, **0** enables LDAP queries. (1, the default, enables **NCP** queries.)
- 7) Save and close the file.
- 8) Restart the eDirectory Agent service.

Next steps

eDirectory Agent now uses LDAP to query the directory service.

Enabling full queries

In small networks, you can configure the eDirectory Agent to query the eDirectory Server for all logged-on users at regular intervals. This allows the agent to detect both newly logged-on users and users who have logged off since the last query, and to update its local user map accordingly.



Important

Configuring eDirectory Agent to use full queries is not recommended for larger networks, because the length of time required to return query results depends on the number of logged on users. The more logged-on users there are, the higher the performance impact.

When you enable full queries for eDirectory Agent, the **User entry timeout** interval is not used, because users who have logged off are identified by the query. By default, the query is performed every 30 seconds.

Enabling this feature increases eDirectory Agent processing time in 2 ways:

- Time needed to retrieve the names of logged-on users each time a query is performed
- Time required to process user name information, remove obsolete entries from the local user map, and add new entries based on the most recent query

eDirectory Agent examines the entire local user map after each query, rather than identifying only new logons. The time required for this process depends on the number of users returned by each query. The query process can therefore affect both eDirectory Agent and Novell eDirectory Server response times.

Procedure to enable full queries

Steps

- 1) On the eDirectory Agent machine, navigate to the **bin** directory (`C:\Program Files\WebSense\Web Security\bin` or `/opt/WebSense/bin`, by default).
- 2) Locate the file **wsedir.ini** and make a backup copy in another directory.
- 3) Open the original file in a text editor.
- 4) Locate the following entry:


```
QueryMethod=<N>
```
- 5) Update the **QueryMethod** value as follows:
 - If the current value is **0** (communicate with the directory via LDAP), change the value to **2**.
 - If the current value is **1** (communicate with the directory via NCP), change the value to **3**.



Note

If changing this query value slows system performance, return the QueryMethod entry to its previous value.

- 6) If the default query interval (30 seconds) is not appropriate for your environment, edit the *PollInterval* value appropriately.
Note that the interval time is set in milliseconds.

- 7) Save and close the file.
- 8) Restart the eDirectory Agent service.

Related reference

PollInterval on page 15

Configuring eDirectory Agent to ignore certain user names

Before you begin

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.

Steps

- 1) Use the Windows Services tool or `/opt/Websense/WebsenseDaemonControl` command to stop **eDirectory Agent**.
- 2) Navigate to the **bin** directory (`C:\Program Files\Websense\Web Security\bin` or `/opt/Websense/bin/`, by default).
- 3) Use a text editor to either create or open **ignore.txt**.

- 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. Your 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, your 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.

With v8.5.3f and later, regular expressions are also supported as part of each of these entries.

- 5) When you are finished making changes, save and close the file.
- 6) Start eDirectory Agent.

Custom configuration for an eDirectory Agent instance

Before you begin

After configuring eDirectory Agent behavior in the Forcepoint Security Manager, you can customize the behavior of a specific eDirectory Agent instance in **wsedir.ini**, the agent's initialization file.

- Some eDirectory Agent settings can only be configured via the Security Manager.
- Some settings can only be configured via the initialization file.
- Parameters that can be modified via either method are marked with an asterisk (*).

To use **wsedir.ini** to configure an agent instance:

Steps

- 1) Use the Windows Services tool or `/opt/Websense/WebsenseDaemonControl` command to stop **eDirectory Agent**.
- 2) Navigate to the **bin** directory (`C:\Program Files\Websense\Web Security\bin` or `/opt/Websense/bin/`, by default) and open **wsedir.ini** in a text editor.

- 3) Modify or add parameters and their values as described below.
- 4) Save and close the INI file.
- 5) Restart eDirectory Agent.

Next steps

The parameters and values described in this document are case-sensitive.

Before making changes to the initialization files, please consider that the default values are designed to maximize accuracy and efficiency in most environments. In most cases, Forcepoint recommends leaving the default values as they are.

DebugLevel

Determines the detail level of the eDirectory Agent diagnostic activity. (See definition for *DebugMode*.)

| | |
|-----------------|--|
| Default | 0 |
| Options | 0, 1, 2, 3 |
| Required | No |
| Synopsis | Specifies the level of log file detail provided for debugging purposes, from none (0) to high (3). Any value outside the range of 0-3 is interpreted as 0. |

Related reference

[DebugMode](#) on page 14

DebugMode

Controls the eDirectory Agent diagnostic activity.

| | |
|-----------------|---|
| Default | Off |
| Options | On, Off |
| Required | No |
| Synopsis | Enables or disables eDirectory Agent's built-in diagnostic (logging and debugging) capabilities. This can be a valuable tool for troubleshooting user identification problems, and determining whether eDirectory Agent is identifying Novell eDirectory users correctly. |

DN*

Novell eDirectory server administrator name.

| | |
|----------------|------|
| Default | None |
|----------------|------|

| | |
|-----------------|---|
| Options | Any valid distinguished user name |
| Required | Yes |
| Synopsis | The distinguished name of a user with administrative rights in Novell eDirectory server. Novell eDirectory requires an authenticated name to issue LDAP requests. Should match the account specified on the Web > Settings > General > Directory Services page in the Forcepoint Security Manager. |

LogFile

Output file for eDirectory Agent diagnostic messages.

| | |
|-----------------|---|
| Default | N/A |
| Options | Any string of characters valid for your operating system |
| Required | No |
| Synopsis | If you have enabled <i>DebugMode</i> , specify a name for the text file where eDirectory Agent sends diagnostic (log) output. |

Related reference

[DebugMode](#) on page 14

password*

Novell eDirectory server administrator password.

| | |
|-----------------|--|
| Default | N/A |
| Options | Any string of characters |
| Required | Yes |
| Synopsis | The password for the Novell eDirectory server administrator account specified via <i>DN*</i> . Should match the password specified on the Web > Settings > General > Directory Services page in the Forcepoint Security Manager. |

Related reference

[DN*](#) on page 14

PollInterval

Interval at which to query Novell eDirectory for user logon sessions.

| | |
|-----------------|---|
| Default | 30000 [milliseconds = 30 seconds] |
| Options | Any number of milliseconds |
| Required | Yes |
| Synopsis | <p>Determines how long eDirectory Agent waits between Novell eDirectory server queries.</p> <ul style="list-style-type: none"> ■ A higher query frequency increases accuracy in identifying users but increases network traffic. ■ A lower frequency may decrease immediacy in identifying users, but also decreases network traffic. |

QueryMethod

Method (NCP or LDAP) used to query Novell eDirectory for user logon sessions, and whether each query is a full query are enabled (see *Enabling full queries*).

| | |
|-----------------|--|
| Default | 1 [NCP] |
| Options | 0, 1, 2, 3 [LDAP, NCP, LDAP + full queries, NCP + full queries] |
| Required | Yes |
| Synopsis | <p>Determines whether eDirectory Agent uses NCP or LDAP to communicate with Novell eDirectory servers.</p> <p>Also determines whether eDirectory Agent performs a full query each time it polls the Novell eDirectory server. Enabling full queries is not recommended in larger networks, because the length of time required to return query results depends on the number of logged on users. The more logged-on users there are, the higher the performance impact.</p> |

Related concepts

[Enabling full queries on page 11](#)

SearchBase*

Novell eDirectory server root context.

| | |
|-----------------|---|
| Default | N/A |
| Options | Any string of characters |
| Required | Yes |
| Synopsis | <p>The DN (distinguished name) of your Novell eDirectory root context. This value should match the root context specified on the Web > Settings > General > Directory Services page in the Forcepoint Security Manager.</p> |

Server

IP addresses or names of machines running Novell eDirectory.

| | |
|-----------------|---|
| Default | N/A |
| Options | A valid IP address or host name |
| Required | Yes |
| Synopsis | Specify the identity of any machine running Novell eDirectory so that eDirectory Agent can query the directory service. If you are running multiple instances of Novell eDirectory, place each server entry on a separate line. |

eDirectory Agent troubleshooting

Use the following articles to identify and resolve user identification issues with eDirectory Agent:

Related concepts

[eDirectory Agent: An incorrect policy is being assigned to users](#) on page 17

Related tasks

[eDirectory Agent miscounts eDirectory Server connections](#) on page 19

[Enabling eDirectory Agent diagnostics](#) on page 20

eDirectory Agent: An incorrect policy is being assigned to users

This issue can occur when:

Related concepts

[eDirectory Agent is not receiving the user name](#) on page 17

[The eDirectory root context is defined incorrectly](#) on page 18

[eDirectory Agent is running on Linux, and NMAP is enabled](#) on page 19

eDirectory Agent is not receiving the user name

User requests may not be handled by the correct policy if the user name is not being passed to eDirectory Agent. If a user does not log on to Novell eDirectory server, eDirectory Agent cannot detect the logon. This happens because:

- A user logs on to a domain that is not included in the default root context for eDirectory user logon sessions. This root context is specified during installation, and should match the root context specified for Novell eDirectory on the **Settings > Directory Services** page.
- A user tries to bypass a logon prompt to circumvent Forcepoint policy enforcement.
- A user does not have an account set up in eDirectory server.

If a user does not log on to eDirectory server, user-specific policies cannot be applied to that user. Instead, the **Default** policy takes effect. If there are shared workstations in your network where users log on anonymously, apply a computer or network policy to those particular machines.

Procedure to determine the eDirectory Agent

To determine whether eDirectory Agent is receiving a user name and identifying that user:

Steps

- 1) Activate eDirectory Agent logging (see *Enabling eDirectory Agent diagnostics*).
- 2) Open the log file you have specified in a text editor.
- 3) Search for an entry corresponding to the user who is receiving the incorrect policy.
- 4) An entry like the following indicates that eDirectory Agent has identified a user:

```
WsUserData:WsUserData()  
User: cn=Admin,o=novell (10.202.4.78)  
WsUserData::~WsUserData()
```

In the example above, the user **Admin** logged on to eDirectory server, and was identified successfully.

- 5) If a user is being identified, but is still receiving the expected policy, check your policy configuration to verify that the appropriate policy is applied to that user, and that the user name in the Forcepoint Security Manager corresponds to the user name in Novell eDirectory.
If the user is not being identified, verify that:
 - The user has a Novell eDirectory account.
 - The user is logging on to a domain that is included in the default root context for eDirectory user logons.
 - The user is not bypassing a logon prompt.

Related tasks

[Enabling eDirectory Agent diagnostics](#) on page 20

The eDirectory root context is defined incorrectly

The root context set in the **wseidir.ini** file is different from the one set for eDirectory Agent in the Forcepoint Security Manager. In this case, although the user can be identified, your web protection software may not be able to apply the correct policy.

The user's requests may be handled by a computer or network policy (if applicable), or by the Default policy.

If these root context values are different, a user can log on to two different trees or branches in Novell eDirectory server, and still be identified by eDirectory Agent. However, when Filtering Service determines the policy for this user, it uses the root context specified in the Forcepoint Security Manager to retrieve information. Filtering Service cannot determine the appropriate policy for a user logging into a Novell eDirectory tree or branch outside the specified root context.

Ensure that you are using the same user and the same root context in both the INI file and the Security Manager.

Procedure to verify the root context value

To verify the root context value in **wsedir.ini**:

Steps

- 1) On the eDirectory Agent machine, go to the **bin** directory (`C:\Program Files\WebSense\Web Security\bin` or `/opt/WebSense/bin/`, by default).
- 2) Open the **wsedir.ini** file in a text editor.
- 3) Verify the line
`SearchBase=[DN]`
Here, **DN** is the distinguished name of the eDirectory root context.
- 4) Save the file, and then restart eDirectory Agent to activate the changes.

eDirectory Agent is running on Linux, and NMAS is enabled

eDirectory Agent is running on Linux, and the Novell Modular Authentication Service (NMAS) is running when it should not be.

In order for eDirectory Agent to work properly on Linux, NMAS must be disabled in Novell eDirectory server. See your Novell documentation for instructions.

eDirectory Agent miscounts eDirectory Server connections

If eDirectory Agent is monitoring more than 1000 users in your network, but shows only 1000 connections to the Novell eDirectory server, it may be due to a limitation of the Windows API that conveys information from the eDirectory server to the eDirectory Agent. This occurs very rarely.

To work around this limitation, add a parameter to the **wsedir.ini** file that counts server connections accurately (Windows only):

Steps

- 1) Use the Windows Services tool to stop **eDirectory Agent**.

- 2) Navigate to the **bin** directory (`C:\Program Files\WebSense\Web Security\bin`, by default) on the eDirectory Agent machine.
- 3) Open the **wsedir.ini** file in a text editor.
- 4) Insert a blank line, and then enter:
`MaxConnNumber = <NNNN>`
Here, **NNNN** is the maximum number of possible connections to the Novell eDirectory server. For example, if your network has 1,950 users, you might enter 2000 as the maximum number.
- 5) Save the file.
- 6) Restart eDirectory Agent.

Enabling eDirectory Agent diagnostics

eDirectory Agent has built-in diagnostic capabilities, but these are not activated by default. You can enable logging and debugging during installation, or at any other time.

Steps

- 1) Use the Windows Services tool or `/opt/WebSense/WebSenseDaemonControl` command to stop **eDirectory Agent**.
- 2) Navigate to the **bin** directory (`C:\Program Files\WebSense\Web Security\bin` or `/opt/WebSense/bin/`, by default) on the eDirectory Agent machine.
- 3) Open the file **wsedir.ini** in a text editor.
- 4) Locate the **[eDirAgent]** section.
- 5) To enable logging and debugging, change the value of **DebugMode** to **On**:
`DebugMode=On`
- 6) To specify the log detail level, modify the following line:
`DebugLevel=<N>`
N can be a value from 0-3, where 3 indicates the most detail.
- 7) Modify the **LogFile** line to specify the name of the log output file:
`LogFile=filename.txt`
By default, log output is sent to the eDirectory Agent console. If you are running the agent in console mode (see *Running eDirectory Agent in console mode*), you can keep the default value.
- 8) Save and close the **wsedir.ini** file.
- 9) Start eDirectory Agent.

Related concepts

[Running eDirectory Agent in console mode](#) on page 21

Running eDirectory Agent in console mode

Do one of the following:

- At the Windows command prompt or PowerShell, enter the command:
`eDirectoryAgent.exe -c`
- At the Linux command shell, enter the command:
`eDirectoryAgent -c`

When you are ready to stop the agent, press **Enter**. It may take a few seconds for the agent to stop running.

