

# Working with User Agent

Enabling the **Perform User Agent lookup** option on the **Advanced Network Monitor Properties** dialog activates the query function for the existence of User Agent on a user's system. Before implementing this special feature, certain conditions must be carefully evaluated so that the correct solution for your work environment is put into place.

## Initial Request Scenario

1. User logs on and sends first Internet request.
2. Internet request is routed through the network which is seen by the Network Monitor.
3. As the request is sent on to the Internet, the Network Monitor queries the requesting system via UDP port 52525 for the existence of User Agent:
  - If found, User Agent returns the logon name to the Network Monitor.
  - If not found, system identification is returned (NetBIOS name, DNS name, etc.)
4. The returned information is placed in cache memory of the Network Monitor.
5. After 10 minutes of inactivity, the logon information expires from the cache.

**Note:** The inactivity time length can be changed. See the DynaComm i:filter Online Reference: User Agent Caching for details.

## Request Identification

Identification of a user request occurs when the Network Monitor queries the sending machine for:

- 1) existence of the User Agent, or
- 2) machine identification which could include reverse DNS lookup, etc.

When request identification is complete, the Monitor log file is updated.

All requests are associated with the "Everyone" user until the requesting source is identified (associated with a logon name or system identification). The request is evaluated with the active rule set. Any rules that include the User property of "Everyone" take effect on the unidentified request.

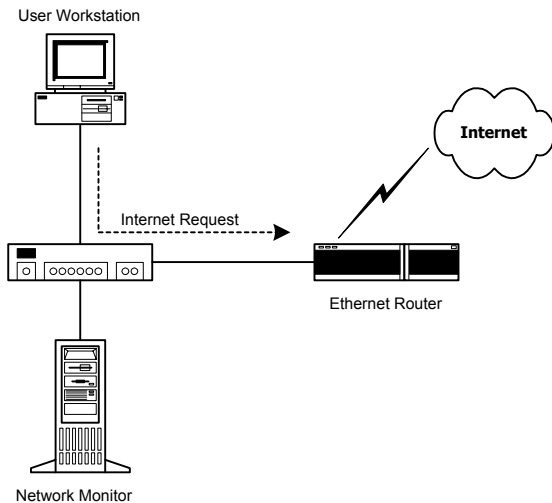


Figure 1 User Agent Functions

# Deploying User Agent

Deploying User Agent can be accomplished through a variety of methods. Two possible methods follow including the method advantages and steps to complete the deployment.

## Method One: Logon Script Deployment

This method deploys User Agent at the discretion of the administrator through a logon batch file. The advantages of using this method include:

- ▼ Transparent to the user; no response or action by the user is required
- ▼ Centralized control; Internet access is not allowed until set up of the logon script.
- ▼ Requires minimal set up by the administrator.
- ▼ No Internet access is allowed until User Agent is installed.

For this method, use these steps:

- 1 Create a logon batch file and include the following entries:

```
@echo off
rem Sample Logon Script

IF EXIST "%USERPROFILE%\Start Menu\Programs\ifagent.exe" exit
IF EXIST "c:\windows\start menu\programs\startup\ifagent.exe" exit
\\fileservname\netlogon\ifagent.exe /s
```

**Note:** These commands must be placed at the end of the logon script to ensure that they execute unimpeded.

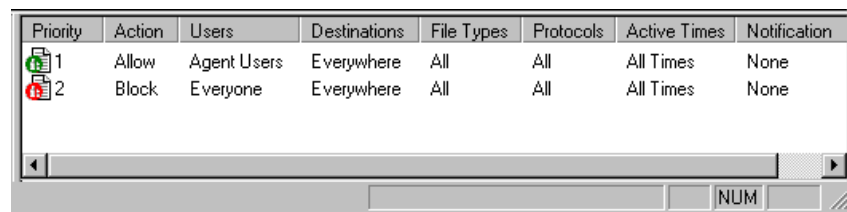
The path in the last statement must be modified to reflect the path to the User Agent file on your network.

Explanation: The first IF statement is for Windows NT or Windows 2000 users. The second IF statement is for Windows 9.x users. These statements determine if the User Agent client is present on the users system.

The last statement performs the installation if the User Agent client is not found.

2. Deploy batch file to users. This can be accomplished via user profile settings from your server.
3. Optional: The following is not required for deployment. However, to ensure that users who do not logon on to a domain are forced to install User Agent include the following rules in either the Default rule set or a new rule set. Including these rules ensures that all Internet users have activity recorded in the log file.

Figure 2  
User Agent  
Deployment



Priority	Action	Users	Destinations	File Types	Protocols	Active Times	Notification
1	Allow	Agent Users	Everywhere	All	All	All Times	None
2	Block	Everyone	Everywhere	All	All	All Times	None

The two rules shown in Figure 2 force the installation of the User Agent by:

- ▼ Blocking all Internet activity (rule 1 always results in a False condition thus sending the evaluation to rule 2) until
- ▼ All users become “Agent Users” (at which point Internet access is allowed).

## Method Two: Rule Deployment

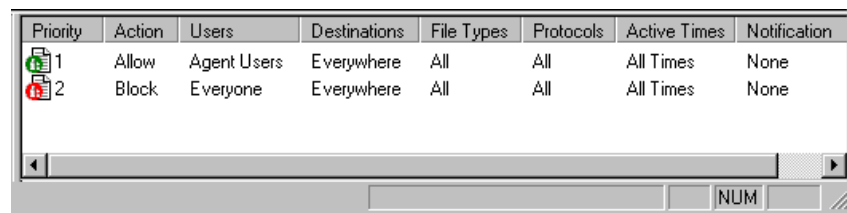
This method deploys User Agent at the discretion of the user. The advantages of using this method include:

- ▼ Centralized control.
- ▼ Requires minimal set up by the administrator.
- ▼ Updates to the User Agent client also require minimal set up.
- ▼ No Internet access is allowed until User Agent is installed.

For this method, use these steps:

1. Set up a blocking message that provides a link to the User Agent client along with instructions on how to perform the installation (see the DynaComm i:filter Online Reference, keyword: blocking messages, user agent for detailed examples).
2. Include the following rules in either the Default rule set or a new rule set:

Figure 3  
User Agent  
Deployment



Priority	Action	Users	Destinations	File Types	Protocols	Active Times	Notification
1	Allow	Agent Users	Everywhere	All	All	All Times	None
2	Block	Everyone	Everywhere	All	All	All Times	None

3. Assign the rule set to the Network Monitor through the **Network Monitor Properties** dialog.
4. Update the Central Admin database with the configuration changes.

## Method Three: Implementing Login Script via Active Directory through Group Policy

For this method, use these steps:

1.
  - ▼ Create a batch file by pasting the following information into a text file and saving it as 'ifagent.bat':

```
@echo off
rem Sample Logon Script

IF EXIST "C:\WINNT\Profiles\All Users\Start Menu\Programs\Startup\ifagent.exe" exit
IF EXIST "C:\Documents and Settings\All Users\Start Menu\Programs\Startup\ifagent.exe" exit
IF EXIST "%USERPROFILE%\Start Menu\Programs\Startup\ifagent.exe" exit
IF EXIST "c:\windows\start menu\programs\startup\ifagent.exe" exit

\\fileserver\downloads\ifagent.exe \s
```

- ▼ Place the file 'ifagent.exe' (located in a subfolder of the Dynacomm ifilter directory called 'user agent') in a shared directory on one of your file servers
- ▼ Change the last line of the batch file (beginning with "\\fsfileserver...") to reflect the location of the shared directory where 'ifagent.exe' resides

2.

- ▼ In Start Menu of your Active Directory Server, choose Administrative Tools > Active Directory Users & Computers
- ▼ Right click on your Active Directory server's name > Properties
- ▼ Go to the Group Policy tab
- ▼ Choose the "Default Domain Policy", click Edit
- ▼ Under User Configuration, choose Windows Settings > Scripts (Logon/Logoff)
- ▼ On right side of window, right click on "Logon" > Properties
- ▼ Click "Show Files", paste the attached file 'ifagent.bat' into this folder and close the folder
- ▼ Click "Add", Browse, then choose 'ifagent.bat' and click OK all the way out of the Group Policy's properties

## Troubleshooting User Agent

In the two installation methods described on the previous pages, a "Block Everyone" rule (Rule 2) is placed in the active rule set. The use of this rule in combination with network load could result in the following situations:

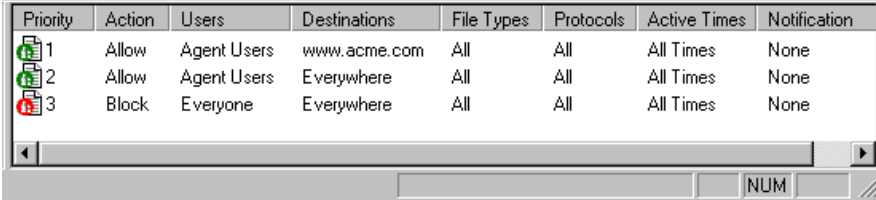
### Situation One

User accesses a blocked web site.

Reason: User has received a response from the Internet before the activities described in steps three and four of the Initial Request Scenario (page 1) were completed.

Solution: Create a rule that specifically blocks the user from the denied location. For example:

Figure 4  
Situation One  
Rules



Priority	Action	Users	Destinations	File Types	Protocols	Active Times	Notification
1	Allow	Agent Users	www.acme.com	All	All	All Times	None
2	Allow	Agent Users	Everywhere	All	All	All Times	None
3	Block	Everyone	Everywhere	All	All	All Times	None

Note: Due to network traffic load, it is possible for any user to be blocked from an allowed site with the "Block Everyone" rule in place. However, this rule ensures that users will not receive blocked web pages.

### Situation Two

User receives a block message with first request, even though the request is for an allowed site.

- Reason:
1. A "Block Everyone" rule exists in the active Rule Set.
  2. User request has not been identified and is, therefore, seen as "Everyone".
  3. "Block Everyone" rule has been applied to user request.

- Solution:
1. In each user's browser properties, set the home page to an external web page.
  2. Include as Rule 1 in the active rule set, a rule that Allows access to the external home web page.

Figure 5  
Situation Two  
Rules

Priority	Action	Users	Destinations	File Types	Protocols	Active Times	Notification
1	Block	Mary Smith	www.financeworld.com	All	All	All Times	None
2	Allow	FINANCE	www.financeworld.com	All	FTP - File Tra...	All Times	None
3	Block	Everyone	Everywhere	All	All	All Times	None

### Situation Three

User receives a block message after 10 minutes of inactivity.

Reason: Logon information for the user remains in the Network Monitor cache for 10 minutes. If the user does not make any requests during this time frame, the logon information expires from the Network Monitor cache. Therefore, the next request will be blocked. All succeeding requests will be allowed.

- Solution:
1. User presses Refresh (receives blocking message).
  2. User presses Refresh a second time (request is allowed and page is displayed).

### Situation Four:

A non-monitored user receives a block message that denies access to a requested Internet site.

- Reason:
1. A “Block Everyone” rule exists in the active Rule Set.
  2. User request has not been identified and is, therefore, seen as “Everyone”.
  3. “Block Everyone” rule has been applied to user request.

Note: This activity does not appear in the log files because logging takes place after identification. Identification can occur after blocking has taken place, therefore no logging is performed.

- Solution:
1. In each user’s browser properties, set the home page to an external web page.
  2. Include a first Allow rule that permits access to the external web page set as the home page.

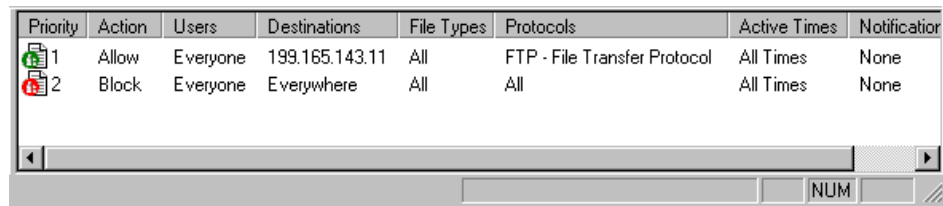
### Situation Five

A scheduled incremental update of the Destinations database has failed.

- Reason:
1. A “Block Everyone” rule that includes the FTP protocol exists in the active Rule Set.
  2. User information has expired from the Network Monitor cache.
  3. User request is seen as an “Everyone” request and is blocked.

Solution: Include a rule at the top of the rule list that allows access to the FutureSoft FTP site. This rule would look like this:

Figure 6  
Situation Five  
Rules



Priority	Action	Users	Destinations	File Types	Protocols	Active Times	Notification
1	Allow	Everyone	199.165.143.11	All	FTP - File Transfer Protocol	All Times	None
2	Block	Everyone	Everywhere	All	All	All Times	None