EaseGate™ Guide

Date : June 16, 2011
Version : 1

PatronSoft

EaseGate™ Guide

Table of Contents

1. Terminologies

Active Directory (AD) - Windows Directory system to store user credential information. EaseGate can use build-in user database or AD for user credential (can be selected under Configuration Manager -> Authentication Server).

Administrator - The “superuser” (user with the highest authority) of EaseGate administration

Authentication Server - the EaseGate component that serves login page and other web page to the client device. It also handles username/password lookup and other authentication services.

Automatic Login - for this type of user, the client device does not need to go through the web-based authentication page. Instead, EaseGate will let the client device log in automatically when the first time it accesses the Internet.

Client Device (or Client PC) - term to describe the client side machine in the network.

Configuration Manager - web-based tools to configure EaseGate (Windows shortcut located in the EaseGate program group).

External Network Interface - the network interface card (NIC) that connects to the public Internet side.

Internal Network Interface - the network interface card (NIC) that connects to the internal network side (e.g. Intranet, internal corporate network)

Multiple Network Segments - the internal network topology which contains more than one network segment. As there are multiple network segments, there will be routers between the client devices and EaseGate.

ODBC datasource - source of data and the connection information needed to access that data. You can define the ODBC datasource through ODBC Data Source Administrator.

Operator - created by EaseGate Administrator, this account will have partial administrative rights

Session Handling - the method which EaseGate uses to identify client device. IP-based session handling will use IP address to identify the client device while MAC-based session handling will use MAC address. EaseGate can also recognize client device by computer name (automatic login only)

2. Running EaseGate™ for the first time

EaseGate installation is designed to be simple to use. Keep in mind that you need to put EaseGate between the client PC and Internet connection. After the installation, you can test EaseGate in the following ways:

i) Test (without Internet connection, and with only 1 physical network adapter) - To achieve this, connect a second PC (i.e. client PC) to EaseGate's Internal Network Interface (see Terminologies chapter) with a crossover cable. For External Network Interface, you can use the "virtual" adapter Microsoft Loopback Adapter as the External Network Interface if you have only one physical Network adapter in the computer that installed EaseGate. If you use a physical adapter for External Network Interface, make sure it is plugged in before starting EeasGate. Then do the following steps:

   a. Start your client PC first since EaseGate needs to detect a connection in the Internet Network Interface.
   (Note that even if you somehow force EaseGate to start, it may not function correctly. Keep in mind that in the real deployment situation, the EaseGate Network Connection will almost certain to have a connection first since it should connect to a switch or a AP instead of a PC via crossover cable.)

   b. Start EaseGate through the web-based Configuration Manager. (The shortcut is in your EaseGate program group, username is "easegate" and password is "password").

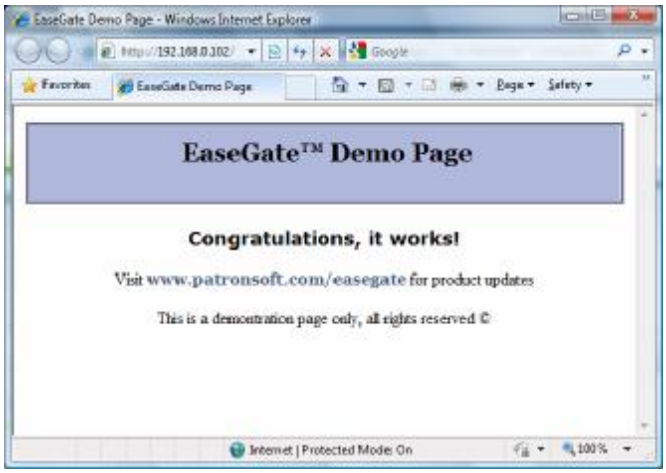
After you start EaseGate successfully (you should see the word "STARTED"), you need to obtain a new IP address for the client PC. (Make sure you set the TCP/IP setting to "Obtain an IP address automatically" in the client PC)

In Windows Command Prompt, issue commands:

ipconfig/release
ipconfig/renew

c. Launch the web browser in the client PC. Type http://externalnic_ip where “externalnic_ip" is the IP address of the External Network Interface.

d. Enter username as “sample” and password as “password”, you should be able to login and after a short delay, see the below screen:



ii) Normal – For more in-depth testing, in additional to i) above, you need to setup the Internet connection. For Internet connection (connects to External Network Interface side), EaseGate can be placed behind NAT, or connect directly to the Internet (either DHCP or fixed IP). For the internal side (connects to the Internet Network Interface), you can connect to switch (or a switch plus router combo). Also, please disable DHCP Server within the switch since EaseGate will handle it. If you use switch plus

router combo, make sure the WAN port is not used (so that it will act as a switch instead of router). Note that EaseGate supports a router between client devices the EaseGate (i.e. Multiple Network Segments), but for this test, we will keep the case simple so please make sure there are no routers between client devices and EaseGate.

After you setup the Internet connection and internal network side correctly, start EaseGate through the web-based Configuration Manager. Then do the following steps:

a. Make sure you set the TCP/IP setting to “Obtain an IP address automatically” in the client PC. This will ensure the client device obtains an IP from EaseGate DHCP server directly.
b. Connect the client device to the internet network. Most of the case, you can just plug in the port of your switch. For wireless network, you need to attach to your AP (access point) correct.
c. If the connection is okay, the client obtain an IP from EaseGate DHCP server. By default, the IP should look like 10.20.7.x.
d. Now, go to Configuration Manger -> Access Rules, click New, type “TestRule” in the “Rule Name” text box, click “Add” and then click “Save”. This will set up an access rule that give unrestricted access to all client devices.
e. The client device should be able to access any site in an unrestricted way due to the above rule. The above “TestRule” may not be very useful for your actual deployment, but it provides a good starting point for you to get familiar with the Access Rule structure. You can now experiment with different access rules by changing the above “TestRule”.

3. Parameters in the Configuration Manager

Access Rules:
Access rules is the center control of EaseGate. Administrator can use access rules to define different user access pattern.

Authentication Server:
Authentication Mode - By default EaseGate has its own built-in user database. Alternatively, administrator can use Active Directory (AD) users if their organization already have the AD built. EaseGate provides a synchronize button which provides a one-way synchronization from AD to EaseGate built-in user database. EaseGate will only synchronize (copy) "authentication related" AD fields to the built-in user database : [objectCategory=user] sAMAccountName, distinguishedName, description, memberOf; [objectCategory=group] sAMAccountName, distinguishedName, description. For EaseGate specific attributes (e.g. Data Transfer Quota), EaseGate will access directly from the built-in user database.

EaseGate will use LDAP to communicate with AD (e.g. during synchronization above, non-single sign-on user login). For single sign-on situation (clients need to set proxy server explicitly in the browser), browser will uses NTLM to communicate with EaseGate.

Bandwidth Throttling Rules:
Use Bandwidth Throttling Rules to define Bandwidth Throttling for different client devices. Note that the Bandwidth Rules do not depend on the Access Rules. You can pick the particular IP Bundles that apply to the Bandwidth Rules.

Client Filters:
Administrator can use Client Filters to block a particular client device. Whether to use client MAC or IP to identify the client device is depend on the Session Handling setting (see below).

Configuration Manager:
Username – the username of the Configuration Manager login. Default is "easegate".

Password – the password of the Configuration Manager login. Default is "password".

Allow configuration manager access from Internal Network - By default,
EaseGate Configuration Manager can only be accessed locally. By selecting this option, one

can also access the Configuration Manager from the Internal Network side.

Allow configuration manager access from the External Network - Similar to the setting above. Allow administrator to access Configuration Manager from the External Network side.

Operator accounts - you can define operator accounts (in addition to the Administrator account, which is really the account with the highest authority). You can assign each operator account to be able to access specific category(s) within Configuration Manager. E.g. you can create an operator “operater1” to be able to access the “Administration” and “Status” categories only.

DHCP:
By default, EaseGate will enable its own DHCP server. Administrator are free to use other DHCP server (e.g. Microsoft DHCP) and disable EaseGate’s DHCP server. The only exception is that if you enable “use Computer Name as identifier” under Session Handling, you need to use EaseGate’s DHCP server as EaseGate uses the DHCP request to determine the relationship between the client “Computer Name” and the IP/MAC address.

IP Bundles:
Administrator can define a range of client device IP (e.g. you can define one IP Bundle for each department). The IP Bundles defined here can be used in Access Rules and Bandwidth Rules.

Main:
Internal Network Interface IP - the IP address that Internal Network Interface. Normally, it is set to a private IP address such as 10.20.7.1 . Please note that you should NOT change the IP for the network interface card directly in Windows. Also, the internal network IP address space (for local network segment) delivered by EaseGate DHCP server is derived from this value.

Internal Network subnet mask - the subnet mask of the above IP address

External Network Interface IP - this IP address needed to be configured in Windows directly before starting EaseGate. EaseGate will query the External Network Interface to obtain this IP address.

Bandwidth Throttling (global setting) - to limit (i.e. throttle) the bandwidth consumed by

users. This is used to prevent any particular user to monopolize the bandwidth (which will affect other users' performance). EaseGate will use this global setting unless it is overridden by user bandwidth throttling setting. *Please note that there will be some variations on the actual bandwidth the client device gets and this value is an approximation only (Please use NetMeter as a measuring tool).* Also, the minimum custom bandwidth throttling value should be 2.

Download Data Transfer (Global Setting), Upload Data Transfer (Global Setting) - When enabled, EaseGate will track the total data transfer in one login session. EaseGate will use this global setting unless it is overridden by user data transfer counting setting.

Path & filename for post-startup batch file - Specify a batch file that EaseGate will run as the last step of EaseGate startup sequence. Usually used to change IP or Routing setting. The format should be "[drive]:\[path]\[filename]"

Multiple Network Segments:
This setting allows EaseGate administrator to setup multiple network segments within the internal network (see http://patronsoft.com/easegate/topology.html) . The information provided in this setting will enable EaseGate to setup return-path routing and DHCP server correctly. Below is the explanation of each field:

Router IP - This is the IP address of the router within the network segments. This setting is used by the EaseGate DHCP Server to make sure it delivers the right setting to the client device.

Subnet Mask - This is the subnet mask of the corresponding Router IP.

Gateway (for return-path) - This is the gateway IP that facing EaseGate Internal Network Interface. This setting is used to setup return path to the corresponding network segment (via the corresponding router). The Gateway IP needed to be accessible from Internal Network Interface (i.e. you can ping the Gateway IP from the Internal Network Interface)

NAT:
By default, NAT is enabled within EaseGate. Note that if NAT is disabled, you have to add a return route correctly in your next-hop router. For example:

Client PC → EaseGate → Router (add the return route here) -> Internet

** client PC IP - 10.20.7.x*

Internal Network Interface IP - 10.20.7.1
External Network Interface IP - 192.168.0.4

Disabling NAT will reveal the client IP (i.e. 10.20.7.x) to the router. When the returning traffic arrives from the Internet, your router need to know where the packet should send to. You need to inform your router that all returning traffic which is destined to 10.20.7.x should be forwarded 192.168.0.4. Using the above example, the return route will be:

10.20.7.0, 255.255.255.0, 192.168.0.4

Note that for forward traffic, it is determined by "default gateway" so there is no need to do anything in your network (whether NAT is enabled or not). Also, if your NAT is on (default setting), there is no need to set the return route in the router as all client traffic will be looked as if it is coming from 192.168.0.4 from the router point of view. In that case the router will know where to send the return traffic to (since it belongs to the same subnet, it will just use ARP).

Session Handling:
Specify the way EaseGate client login (for normal user / automatic login user). Administrator can use either IP or MAC to identify the client. The advantage of using MAC is that it is static for a particular client device (MAC is fixed for a particular network card). For IP, EaseGate DHCP server will try keep the IP (if available) for a particular client during IP lease renewal, but the only sure way to keep define a static IP-MAC mapping. Note that if there are router(s) between the client and EeasGate machine, (i.e. Multiple Network Segments), MAC address is not visible from EaseGate. Alternatively, IP-based session handling should be used instead.

EaseGate also allows administrator to identify client using “Computer Name” as an identifier. You can use command “hostname” to display the “Computer Name” in a Windows-based PC. Note that EaseGate only allows administrator to use “Computer Name” as an identifier for “Automatic Login Users”.

Web Filters:
Administrator can define multiple web filters in EaseGate. Each web filter can be attached to a Access Rule. When defining each Web Filter, administrator can define either Black List or White List (but not both). For Black List, user can access all web sites except those defined in the Black List. For White List, user can only access the web sites defined in the White List and nothing else. Organization that has more stringent web access requirements may prefer White List. The downside is that it takes more effort to maintain a White List.