

LogTunnel Deployment Guide



This guide describes the deployment process when using the SiteManager LogTunnel functions for pushing and/or pulling log data from devices to a central server.

Version: 1.3, August 2017

Applicable to GateManager and SiteManager version 7.3 or newer

Table of Contents

Version history	3
1. Introduction	3
1.1. Advantages of LogTunnel over other solutions	3
1.2. Ordering (Enabling) LogTunnel	4
2. SiteManager connection methods	4
3. Configuring LogTunnel PULL mode	5
3.1. LogTunnel Client Pull mode enabling	6
3.1.1. LogTunnel enabling for an existing Ethernet agent	6
3.1.2. LogTunnel enabled by dedicated LogTunnel agent.	6
3.2. Configuring the LogTunnel Master (Pull) Agent	7
3.3. Linking LogTunnel Device addresses to LogTunnel Clients	9
3.3.1. Method 1: Auto assigning LogTunnel Device addresses	9
3.3.2. Method 2: Assign specific LogTunnel Device Address	10
3.3.3. Method 3: Linking from LogTunnel Client view	12
3.3.4. Method 4: List selection from LogTunnel Client view	13
4. Configuring LogTunnel PUSH mode	15
4.1. LogTunnel Client Push mode enabling	16
4.2. Configuring the LogTunnel Master (Push) Agent	18
4.3. Linking LogTunnel Clients to LogTunnel Master	20
4.3.1. Drag-and-drop Clients onto LogTunnel Master	20
5. Push and Pull for the same devices	22
5.1. Configuration on SiteManagers	22
5.2. Configuration on GateManager	23
APPENDIX A. Tech Hints and Known Limitations	25
Larger LogTunnel Device address ranges (Pull mode)	25
Address range entry formats	25
Port range formats	25
Limitations of Listening port and connections	25
Hardware SiteManager	25
SiteManager Embedded	25
Devices requiring the “real” log server address as destination	26
FTP data connections	26
Notices	27

Version history

- 1.0 First release
- 1.1. Added section about ordering/enabling section 1.2
- 1.2. Port range corrected in Appendix A
- 1.3. References to “EasyLogging” changed to “LogTunnel”

1. Introduction

With distributed industrial equipment, there is often a requirement for persistent connections to the remote devices from a central log server or SCADA system.

LogTunnel enables you to establish such persistent connections to the same or other SiteManager controlled devices using simple drag-and-drop operations in the GateManager portal. This function works concurrently and independent of the standard LinkManager “on-demand” access.

LogTunnel is built upon the existing Static Server and Device Relay mechanisms using the same secure data transport mechanism and suiting the same purposes. LogTunnel is, however, considerably easier to configure, and can be used on both Cloud based and own/private GateManagers.

On the SCADA or log server side, you must install a SiteManager as a *LogTunnel Master*, while on the device side, you simply use your existing SiteManagers to setup *LogTunnel Clients* for each device.

The remote log components, the **LogTunnel Clients**, can be either SiteManager hardware or software (SiteManager Embedded with an Extended license).

The solution requires a central **LogTunnel Pull Master** to be a hardware SiteManager, while a **LogTunnel Push Master**, can be either a hardware or software based SiteManager Embedded with an Extended license.

NOTE: *LogTunnel will require both the GateManager and the SiteManagers to be using release 7.2 or later. For Cloud based GateManagers, there may be special terms for your use of this feature based on potential server load when using LogTunnel for constant transmissions of large amounts of data, such as video streams. Consult your GateManager hosting provider for details.*

1.1. Advantages of LogTunnel over other solutions

- Setup is done by simple drag-and-drop in the central GateManager portal. No routing, firewall or tunnel configuration is required.
- Logging and Programming access (by LinkManager) is supported concurrently and independently of each other.
- No need for public addresses exposed on the Internet. Both Master and Client devices can be installed behind corporate firewalls.
- No dependency of static IP addresses. Both Master and Client devices can have dynamically assigned IP addresses.
- No problem with conflicting IP subnets at remote sites, which is a common problem with VPN based solutions (even the central site can have same subnet as the remote sites)
- All data usage is logged centrally on the GateManager (Enabled with the LogTunnel/Usage Statistics activation license).
- An operator on the SiteManager can locally control disabling of LinkManager on-demand access, while retaining the static LogTunnel connections for uninterrupted surveillance.

- Easy setup of logging direction (Pull and/or Push) and port/IP restrictions, for maintaining a high level of security.
- LogTunnel allows full data tunneling for optimum freedom, where most non-VPN logging solutions rely on predefined values to be collected and submitted (web post)
- On hardware SiteManagers, LogTunnel can access devices on both the SiteManager Uplink and DEV side. Typically, VPN solutions would only allow access to the DEV side (aka the LAN interface).
- SiteManager Embedded allows both logging on the device on which SiteManager Embedded is installed, and on devices in the same network (Note that LogTunnel requires a SM-E Extended license)

1.2. Ordering (Enabling) LogTunnel

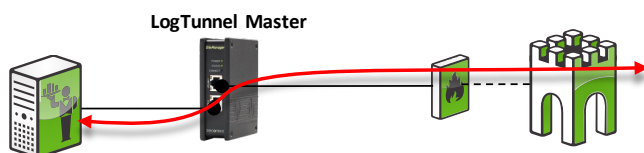
LogTunnel is enabled by ordering the **LogTunnel/Usage Statistics** upgrade from your point of purchase. Refer to the [Enabling and working with Usage Statistics Guide](#) for details on ordering the upgrade. The same guide gives details on the benefits of Usage Statistics in general.

Note that even without the license, you can still configure your entire LogTunnel setup per the following, but no traffic will be forwarded until upgrade is active.

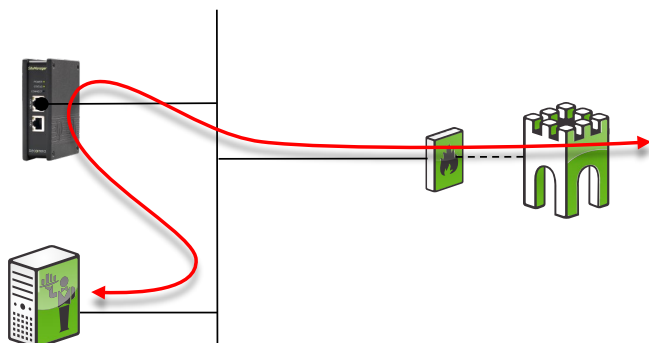
2. SiteManager connection methods

A Hardware SiteManager can be installed in two ways:

1. **Separation**, where the log server accesses the DEV side of the SiteManager and the SiteManager's Uplink side is connected to the Internet (either via a corporate network, or directly via the SiteManager's Uplink2 broadband connection)



2. **Uplink only**, where the Log Server just accesses the Uplink side of the SiteManager, and the SiteManager uses the corporate network to access the Internet. In this case the SiteManager DEV port is not used.

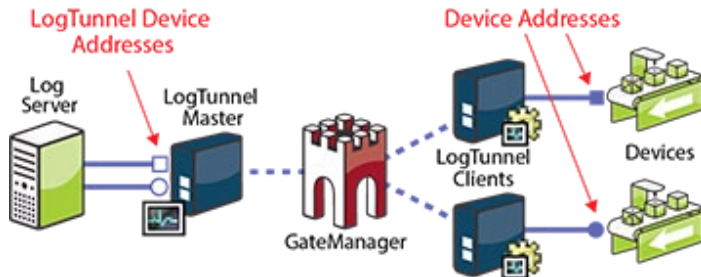


This would be the same setup for a SiteManager Embedded working in **LogTunnel PUSH** mode.

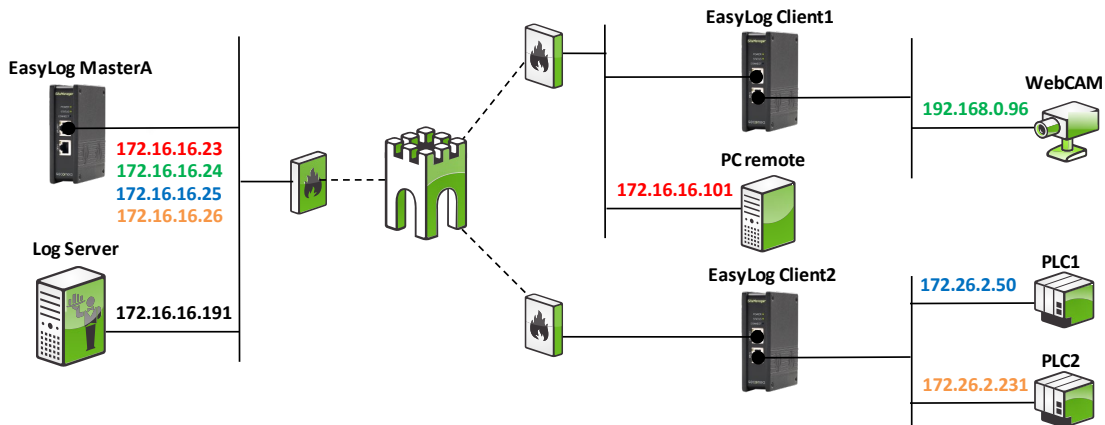
3. Configuring LogTunnel PULL mode

The PULL scenario is based on a central log server or SCADA system, actively collecting data from remote devices.

The principle is that the LogTunnel Master agent creates alias Device addresses on either the DEV or Uplink port that represents the remote devices, and the log server just connects to these addresses locally.



Example: The agents and values in the following will establish this scenario that you can return to for better understand the principles:



A pair of IP addresses with the same colour depict the LogTunnel Device address (the alias) and the corresponding (real) Device address at the remote site.

For instance: The log server connects to **172.16.16.23** (aka the LogTunnel Device Address) and the connection is forwarded to address **172.16.16.101** (aka the Device Target address)

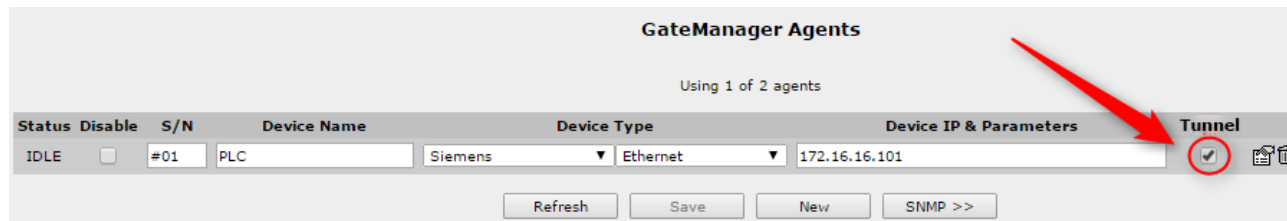
3.1. LogTunnel Client Pull mode enabling

LogTunnel Clients for PULL mode can be enabled on both SiteManager hardware and software models (SiteManager Embedded with Extended license).

There are two methods for enabling LogTunnel Client mode in the SiteManager:

3.1.1. LogTunnel enabling for an existing Ethernet agent

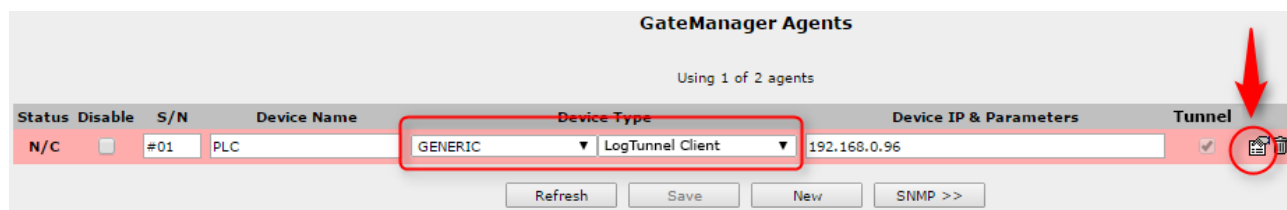
This type of agent could be used for LinkManager access also:



3.1.2. LogTunnel enabled by dedicated LogTunnel agent.

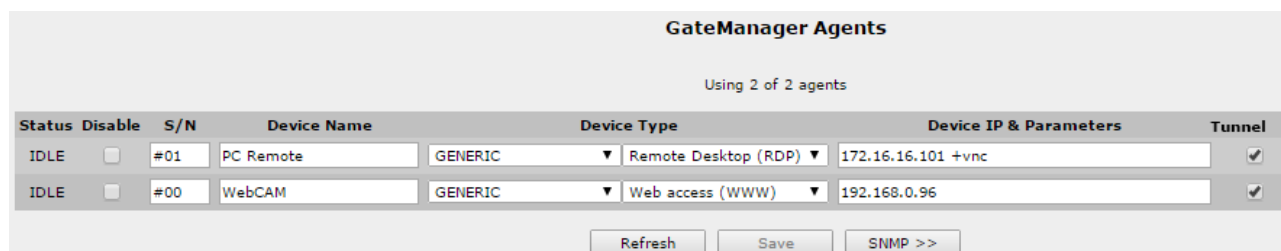
This type of agent is used solely for logging, and cannot be accessed by Linkmanager clients.

Note that the agent will stay “not connected” (N/C) until it is eventually linked to a LogTunnel Master on the GateManager, after which it will go IDLE.

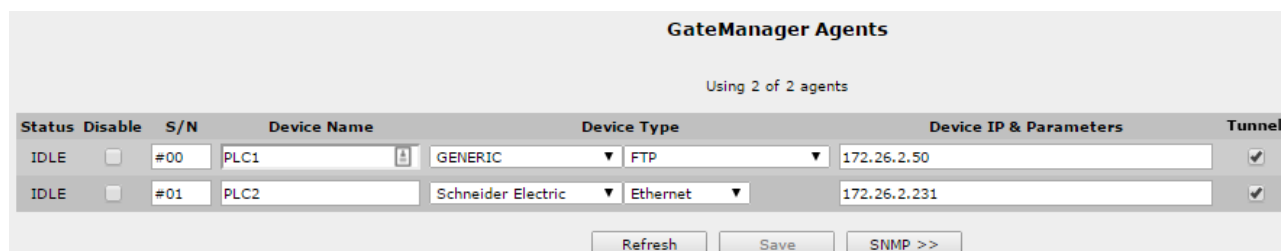


In the examples in the following, we will be working with two SiteManagers named “EasyLog Client1 and Client2” respectively, with the following agents configured:

SiteManager: “EasyLog Client1”

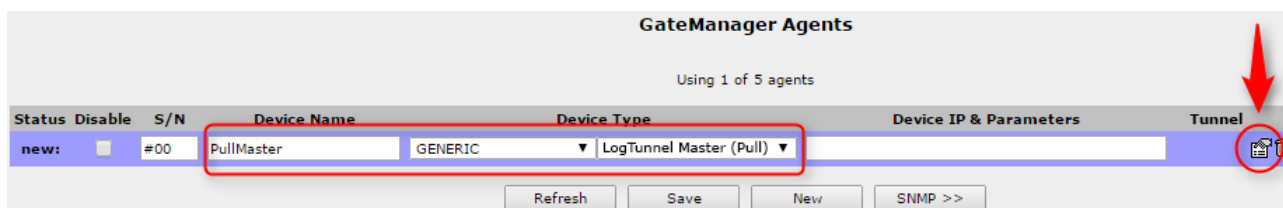


SiteManager: “EasyLog Client2”



3.2. Configuring the LogTunnel Master (Pull) Agent

1. Enter the SiteManager Agents menu and create a **Generic > LogTunnel Master (Pull)** agent; give it a meaning full Device Name (in this case called "PullMaster") and select the Parameter details icon:



2. Complete the configuration:

Log Server Address: * 172.16.16.191 1

Always On:

LogTunnel Device Address range: * 172.16.16.23-26 2

Forwarded TCP ports: * 8000-8010 3

Forwarded UDP ports: * 162 3

Interface: UPLINK 4

Idle Timeout: 5

Custom Settings:

Save Back Ping

* = Mandatory field

1 Enter the IP address of the log server. This must be a static IP address. DNS names cannot be used.

Only the specified Log Server Address will be allowed access to the remote devices, and is a security precaution for preventing unauthorized access.

2 Configure the range of "alias" addresses that should represent the remote devices.

Make sure that no other equipment is using any of the IP addresses in the range, as it may result in unpredictable network behaviour.

In case you do not have enough free addresses in the local network of the server, you may have to ask your IT department to create a VLAN or via a router place the SiteManager in a different subnet, and ensure that the log server has a route to that network.

3 You will need to configure the specific ports or port range for TCP ports and/or UDP ports for the LogTunnel Master to listen on. You can combine single ports with ranges like this: **23,80,5000-5010**. The mandatory indicator * just means that values must be filled in at least one of the fields UDP or TCP.

4 You can specify whether the address range should be created on the **Uplink** or the **DEV** port. (See section 2. **SiteManager connection methods**). Note that device address range you define must match a valid subnet on the selected port.

5 Idle timeout value in seconds. If left blank the default values will be 120 seconds for TCP connections and 30 seconds for UDP connections. Note that if entering a value, this value will apply for both UDP and TCP.

3. When clicking Save, Back and Refresh a couple of times you will notice that a warning informs you to attach it on the GateManager. This is a Security precaution to avoid accidental activation of undesired LogTunnel Device addresses.

Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
ATTACH	<input type="checkbox"/>	#01	PullMaster	GENERIC	LogTunnel Master (Pull)	172.16.16.191 ip=172.16.16.23-26 tcp=8000-8010

Must be attached to a domain in GateManager.

Refresh Save New SNMP >>

4. Login to the GateManager Portal and locate the LogTunnel Master agent (here named "PullMaster"):

The screenshot shows the GateManager Portal interface. On the left, a tree view shows the hierarchy: EasyLog Test (BRONZE) > EasyLog Client1, EasyLog Client2, EasyLog MasterA, and PullMaster (EasyLog MasterA) - 172.16.16.191. A red arrow points from the PullMaster agent in the tree to the 'Attach here' button in the Domain Token section of the main configuration panel. The main panel displays details for the PullMaster agent, including Name, Product, Serial, Master, Created, Source IP, and Firmware. A diagram on the right illustrates the LogTunnel architecture, showing a Log Server, LogTunnel Master, GateManager, LogTunnel Clients, and Devices. The Domain Token section includes a red 'Attach here' button and a warning: 'Agents must be attached to a domain to enable remote access.'

3.3. Linking LogTunnel Device addresses to LogTunnel Clients

You have different methods for linking the LogTunnel Master (Pull) Device Addresses to the LogTunnel Client agents. Try them out and use your preferred method.

3.3.1. Method 1: Auto assigning LogTunnel Device addresses

1. Drag and drop the LogTunnel Client agent to the LogTunnel Master in the tree view. It will automatically assign the first free address in the LogTunnel Device Address range:


The screenshot shows the EasyLog Test interface. On the left, a tree view displays the hierarchy: EasyLog Test (BRONZE) > EasyLog Client1 > PC Remote (EasyLog Client1) - 172.16.16.101. A red arrow points from this client to the PullMaster (EasyLog MasterA) - 172.16.16.191 in the tree view.

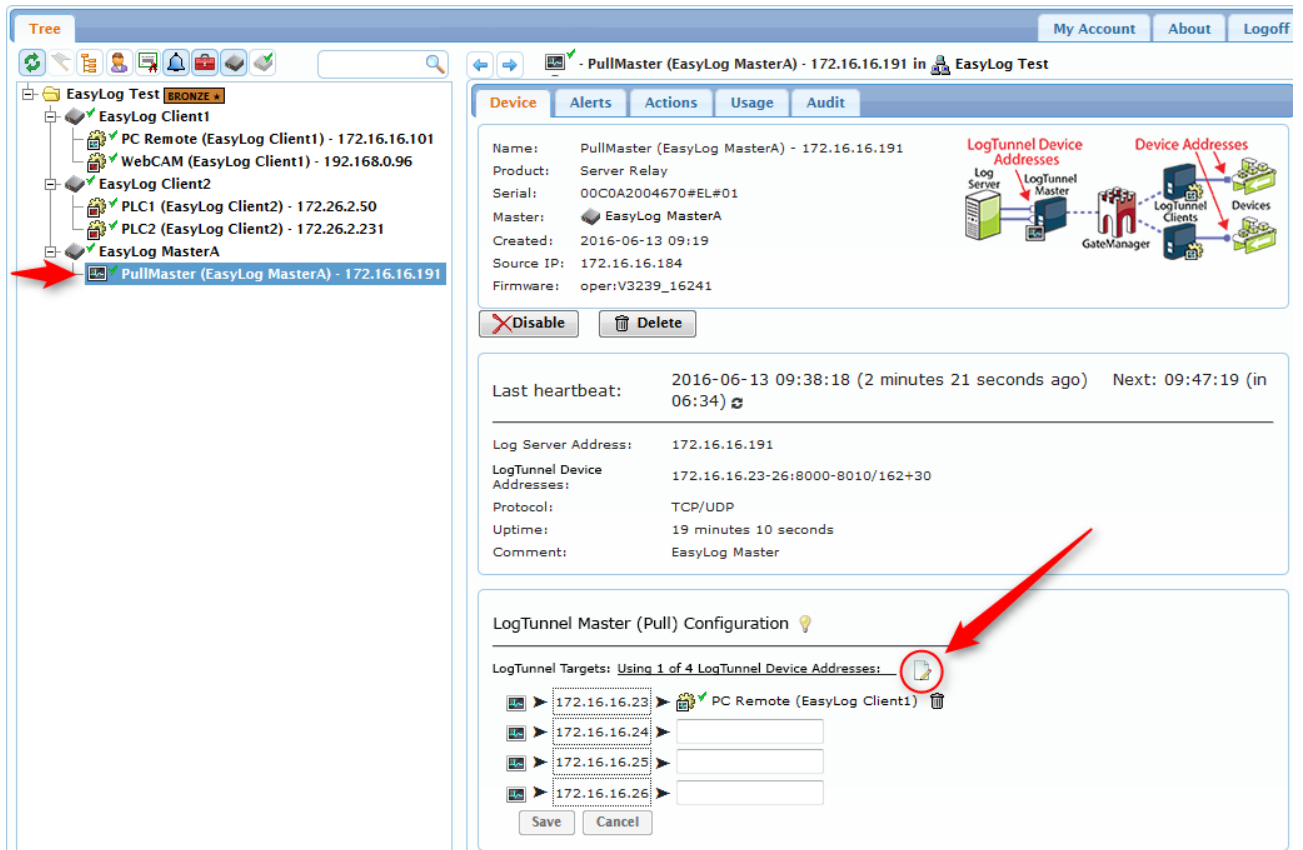
The main configuration panel for the PullMaster (EasyLog MasterA) - 172.16.16.191 is shown. It includes fields for Name, Product, Serial, Master, Created, Source IP, and Firmware. Below these are buttons for Disable and Delete. The Last heartbeat is 2016-06-13 09:38:18 (1 minute 27 seconds ago) and the Next is 09:47:19 (in 07:30). The Log Server Address is 172.16.16.191, and the LogTunnel Device Addresses are 172.16.16.23-26:8000-8010/162+30. The Protocol is TCP/UDP, Uptime is 19 minutes 10 seconds, and the Comment is EasyLog Master.

The LogTunnel Master (Pull) Configuration section shows LogTunnel Targets: Using 1 of 4 LogTunnel Device Addresses. Below this is a table with columns: Log Server, LogTunnel Dev. Addr, LogTunnel Client, and Device Address. A red arrow points to the first row of the table.

Log Server	LogTunnel Dev. Addr	LogTunnel Client	Device Address
172.16.16.191	172.16.16.23	PC Remote (EasyLog Client1)	172.16.16.101


3.3.2. Method 2: Assign specific LogTunnel Device Address

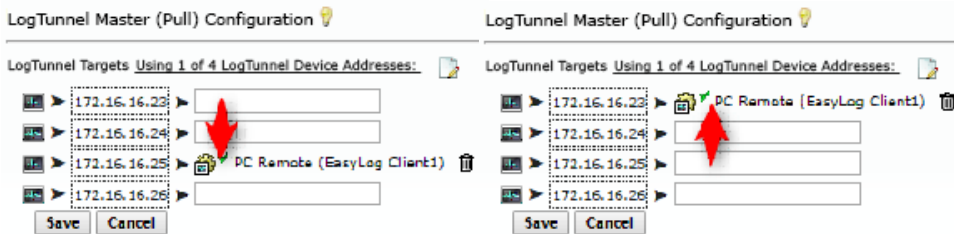
- Stand on the LogTunnel Master and expand the list of available LogTunnel Device addresses, by clicking the  symbol:



The screenshot displays the EasyLog Test web interface. On the left, a tree view shows the hierarchy: EasyLog Test (BRONZE) > EasyLog Client1 > PC Remote (EasyLog Client1) - 172.16.16.101, EasyLog Client2 > PLC1 (EasyLog Client2) - 172.26.2.50, PLC2 (EasyLog Client2) - 172.26.2.231, EasyLog MasterA > PullMaster (EasyLog MasterA) - 172.16.16.191. The main panel shows the configuration for the selected PullMaster device. The 'LogTunnel Master (Pull) Configuration' section is expanded, showing 'LogTunnel Targets: Using 1 of 4 LogTunnel Device Addresses:'. A red circle highlights a document icon next to this text, with a red arrow pointing to it from the right. Below, a table lists four LogTunnel Device Addresses and their corresponding clients:

LogTunnel Device Address	Client
172.16.16.23	PC Remote (EasyLog Client1)
172.16.16.24	
172.16.16.25	
172.16.16.26	

Hint: If you have linked a client to a wrong LogTunnel Device Address, you can either delete the link with the  icon and start over, or you can simply drag-and-drop the client to another free address.



The image shows two side-by-side screenshots of the 'LogTunnel Master (Pull) Configuration' section. The left screenshot shows the configuration table with a red arrow pointing to the 'PC Remote (EasyLog Client1)' entry. The right screenshot shows the same configuration table with a red arrow pointing to the 'PC Remote (EasyLog Client1)' entry, which is now linked to the address 172.16.16.24.

Drag and drop the LogTunnel Client agent onto the field next to the IP address you want to assign as LogTunnel Device address for this agent:

The screenshot shows the EasyLog interface with the following details:

- Tree View:** EasyLog Test (BRONZE)
 - EasyLog Client1
 - PC Remote (EasyLog Client1) - 172.16.16.101
 - WebCAM (EasyLog Client1) - 192.168.0.96
 - EasyLog Client2
 - PLC1 (EasyLog Client2) - 172.26.2.50
 - PLC2 (EasyLog Client2) - 172.26.2.231
 - EasyLog MasterA
 - PullMaster (EasyLog MasterA) - 172.16.16.191



- Device Configuration Panel:**
- Name: PullMaster (EasyLog MasterA) - 172.16.16.191
- Product: Server Relay
- Serial: 00C0A2004670#EL#01
- Master: EasyLog MasterA
- Created: 2016-06-13 09:19
- Source IP: 172.16.16.184
- Firmware: oper:V3239_16241
- Last heartbeat: 2016-06-13 09:38:18 (2 minutes 21 seconds ago) Next: 09:47:19 (in 06:34)
- Log Server Address: 172.16.16.191
- LogTunnel Device Addresses: 172.16.16.23-26:8000-8010/162+30
- Protocol: TCP/UDP
- Uptime: 19 minutes 10 seconds
- Comment: EasyLog Master
- LogTunnel Master (Pull) Configuration:**
- LogTunnel Targets: Using 1 of 4 LogTunnel Device Addresses
- 172.16.16.23 PC Remote (EasyLog Client1)
- 172.16.16.24 WebCAM (EasyLog Client1) - 192.168.0.96
- 172.16.16.25
- 172.16.16.26

3. Finally click **Save**, and you will see the complete list of linked agents:

The screenshot shows the EasyLog interface with the following details:

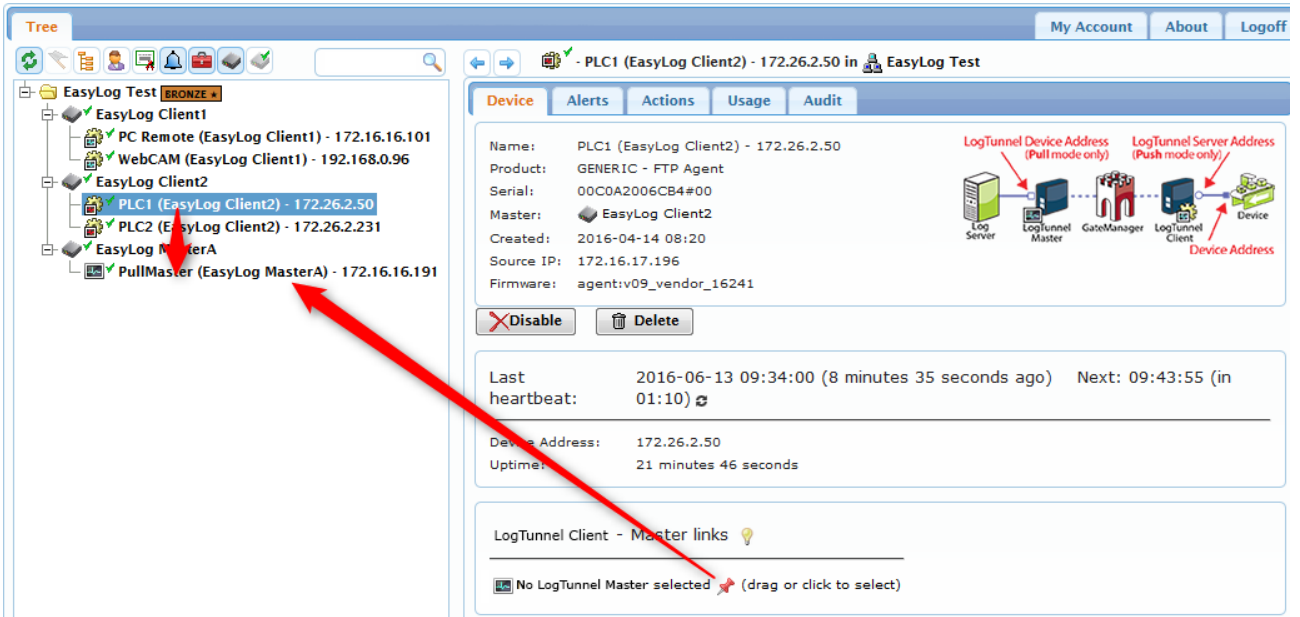
- Tree View:** EasyLog Test (BRONZE)
 - EasyLog Client1
 - PC Remote (EasyLog Client1) - 172.16.16.101
 - WebCAM (EasyLog Client1) - 192.168.0.96
 - EasyLog Client2
 - PLC1 (EasyLog Client2) - 172.26.2.50
 - PLC2 (EasyLog Client2) - 172.26.2.231
 - EasyLog MasterA
 - PullMaster (EasyLog MasterA) - 172.16.16.191

- Device Configuration Panel:**
- Name: PullMaster (EasyLog MasterA) - 172.16.16.191
- Product: Server Relay
- Serial: 00C0A2004670#EL#01
- Master: EasyLog MasterA
- Created: 2016-06-13 09:19
- Source IP: 172.16.16.184
- Firmware: oper:V3239_16241
- Last heartbeat: 2016-06-13 09:38:18 (5 minutes 3 seconds ago) Next: 09:47:19 (in 03:56)
- Log Server Address: 172.16.16.191
- LogTunnel Device Addresses: 172.16.16.23-26:8000-8010/162+30
- Protocol: TCP/UDP
- Uptime: 19 minutes 10 seconds
- Comment: EasyLog Master
- LogTunnel Master (Pull) Configuration:**
- LogTunnel Targets: Using 2 of 4 LogTunnel Device Addresses
- 172.16.16.191 172.16.16.23 PC Remote (EasyLog Client1) 172.16.16.101
- 172.16.16.24 WebCAM (EasyLog Client1) 192.168.0.96

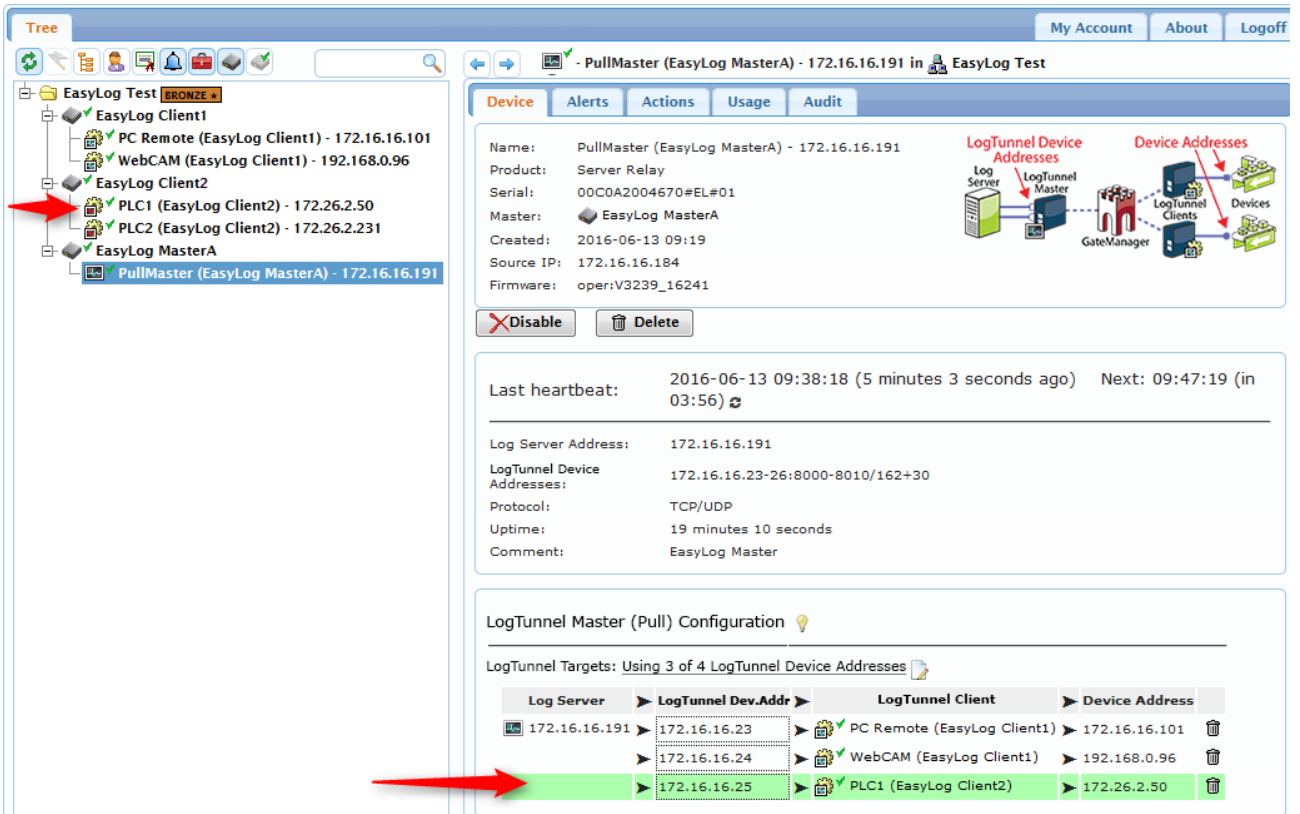
Hint: Notice that the icons for linked agents change colour from  to .

3.3.3. Method 3: Linking from LogTunnel Client view

- While standing on the LogTunnel Client, drag and drop the pin onto the LogTunnel Master (Pull) agent, or simply drag and drop the client agent onto the LogTunnel Master in the tree:

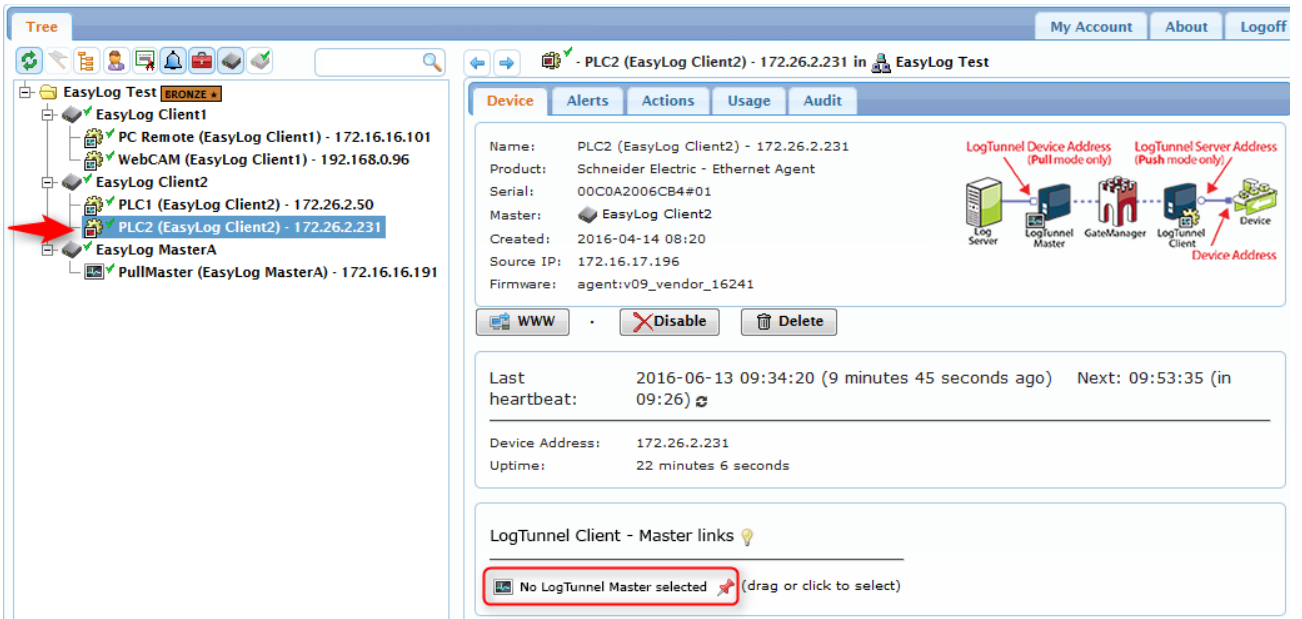


- The LogTunnel Master agent configuration view will automatically expand and indicate the linked client:

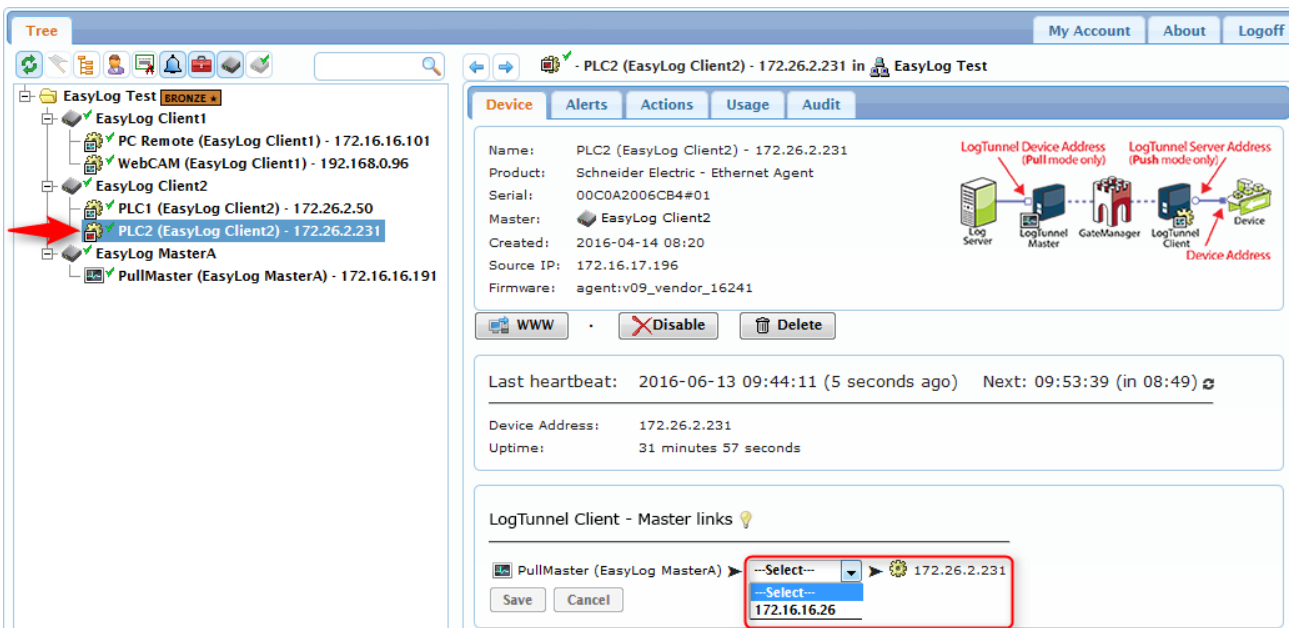


3.3.4. Method 4: List selection from LogTunnel Client view

- As above, while standing on the LogTunnel Client agent, select the available LogTunnel Master:



- A list of unassigned LogTunnel Device IP addresses will appear to select from:



8. With all clients linked, the final view on the LogTunnel Master agent will look like this. You can always edit the IP assigning by editing the fields directly.

The screenshot shows the LogTunnel Master agent interface. On the left is a tree view under 'EasyLog Test' containing:

- EasyLog Client1
 - PC Remote (EasyLog Client1) - 172.16.16.101
 - WebCAM (EasyLog Client1) - 192.168.0.96
- EasyLog Client2
 - PLC1 (EasyLog Client2) - 172.26.2.50
 - PLC2 (EasyLog Client2) - 172.26.2.231
- EasyLog MasterA
 - PullMaster (EasyLog MasterA) - 172.16.16.191

The main panel displays details for the selected 'PullMaster (EasyLog MasterA) - 172.16.16.191' device:

- Device** tab selected.
- Name: PullMaster (EasyLog MasterA) - 172.16.16.191
- Product: Server Relay
- Serial: 00C0A2004670#EL#01
- Master: EasyLog MasterA
- Created: 2016-06-13 09:19
- Source IP: 172.16.16.184
- Firmware: oper:v3239_16241
- Buttons: Disable, Delete
- Last heartbeat: 2016-06-13 09:38:18 (7 minutes 14 seconds ago) Next: 09:47:19 (in 01:41)
- Log Server Address: 172.16.16.191
- LogTunnel Device Addresses: 172.16.16.23-26:8000-8010/162+30
- Protocol: TCP/UDP
- Uptime: 19 minutes 10 seconds
- Comment: EasyLog Master

Below this is the 'LogTunnel Master (Pull) Configuration' section, which includes a table of targets:

LogTunnel Targets: Using 4 of 4 LogTunnel Device Addresses

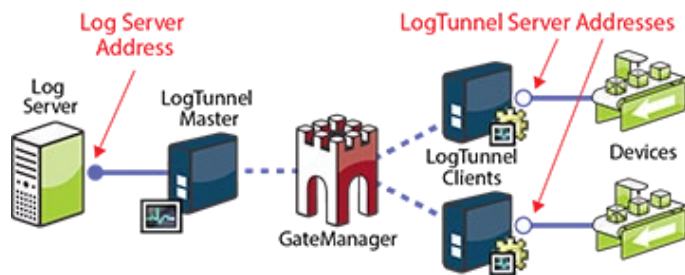
Log Server	LogTunnel Dev. Addr	LogTunnel Client	Device Address
172.16.16.191	172.16.16.23	PC Remote (EasyLog Client1)	172.16.16.101
	172.16.16.24	WebCAM (EasyLog Client1)	192.168.0.96
	172.16.16.25	PLC1 (EasyLog Client2)	172.26.2.50
	172.16.16.26	PLC2 (EasyLog Client2)	172.26.2.231

4. Configuring LogTunnel PUSH mode

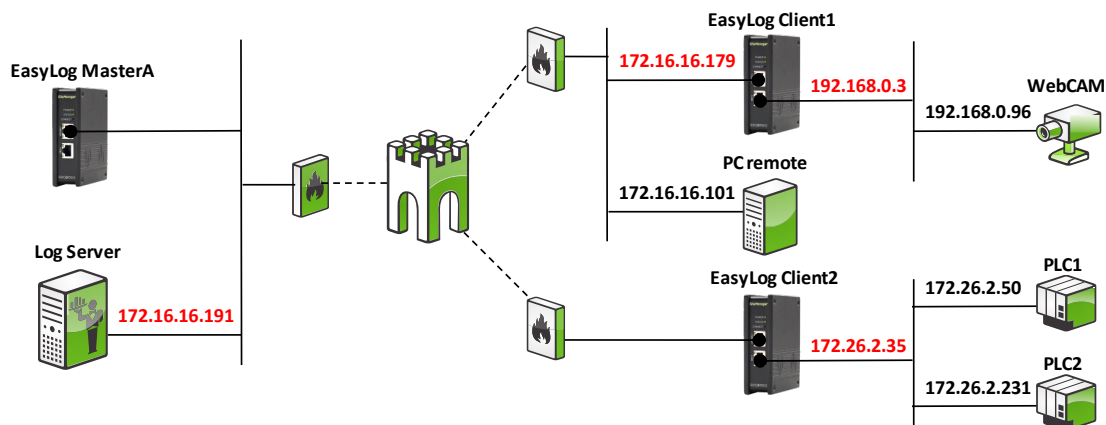
The PUSH scenario is based on remote devices connecting to a central log server or SCADA system for delivering log data. An example of such data is SNMP traps.

A LogTunnel Master for Push mode can be either a hardware SiteManager, or a SiteManager Embedded activated by an Extended license.

The principle is that the LogTunnel Master instructs the LogTunnel Clients to establish IP aliases (aka LogTunnel Server Addresses) and listening ports on the DEV and/or Uplink ports on the SiteManager (or the IP address of a host device having SiteManager Embedded installed), which the industrial devices will regard as the log server destination.



Example: The agents and values in the following will establish this scenario that you can return to for better understand the principles:



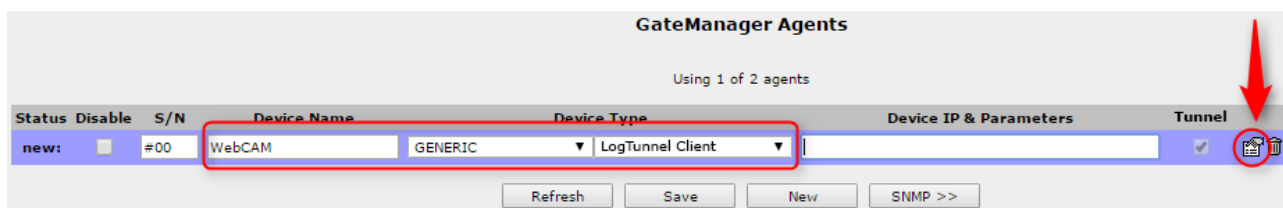
The red coloured IP addresses on the right side depict the log server IP aliases (aka LogTunnel Server addresses) and the corresponding (real) server address (aka Log Server address) at the remote site on the left side.

For instance: PLC1 connects to **172.26.2.35**, and the connection is forwarded to address **172.16.16.191** (aka Log Server Address)

4.1. LogTunnel Client Push mode enabling

LogTunnel Clients for Push mode can be enabled on both SiteManager hardware and software models (SiteManager Embedded with Extended license).

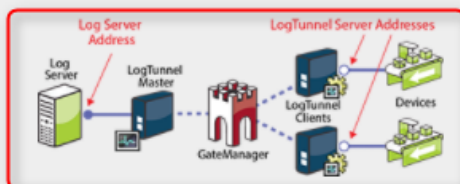
1. Create a unique LogTunnel Agent (Generic > LogTunnel Client); give it a meaning full Device Name and select the Parameter details icon.



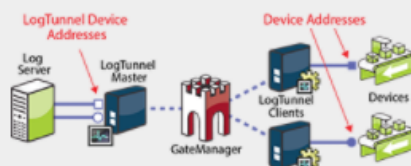
2. Complete the configuration

In Push mode, a device specified by the Device Address below can send (push) data to a central Log Server (typically a SCADA system), by connecting to the LogTunnel Server Address specified below. If left blank, the SiteManager's DEV1 address is used by default. If you specify a different address, an IP alias for that address will automatically be created on the SiteManager.

Note: You should specify a free address matching either the Uplink1 or a DEV subnet of the SiteManager. The SiteManager does not support VLAN.



In Pull mode, a central Log Server can get access to the device specified with the Device Address below, by connecting to a LogTunnel Devices address configured in the LogTunnel Master agent. In this mode, the LogTunnel Server Address is not used.



Device Address: * 192.168.0.96 1

Always On:

LogTunnel Server Address: 2

Custom Settings:

* = Mandatory field

1 Enter the IP address of the device that should access the log server to deliver data. Only one address is allowed per LogTunnel Agent, so you have to create an agent per device.

2 Configure the LogTunnel Server Address that the devices should access for being forwarded to the real log server address.

If left blank the DEV address will be assumed as default, but you can configure any address in the same subnet as the DEV or Uplink port, and the SiteManager will create that "IP alias" as LogTunnel Server Address. You can also specify the Uplink address, and then this will be used as LogTunnel Server Address.

Note that this field is only available on hardware SiteManagers. SiteManager Embedded uses the socket interface of the host platform and it would be the IP address of the host platforms network adapter matching the subnet of the entered Device Address that should be used as LogTunnel Server Address.

- When pressing Save, note that the agent will stay “not connected” (N/C) until it is eventually linked to a LogTunnel Master on the GateManager, after which it will go IDLE.

GateManager Agents						
Using 1 of 2 agents						
Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
N/C	<input type="checkbox"/>	#00	WebCAM	GENERIC	LogTunnel Client	192.168.0.96

Refresh Save New SNMP >>

In the examples in the following, we will be working with two SiteManagers named “EasyLog Client1 and Client2” respectively, with the following named agents:

SiteManager: “EasyLog Client1”

GateManager Agents						
Using 2 of 2 agents						
Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
N/C	<input type="checkbox"/>	#01	PC Remote	GENERIC	LogTunnel Client	172.16.16.101 ip=172.16.16.179
N/C	<input type="checkbox"/>	#00	WebCAM	GENERIC	LogTunnel Client	192.168.0.96

Refresh Save SNMP >>

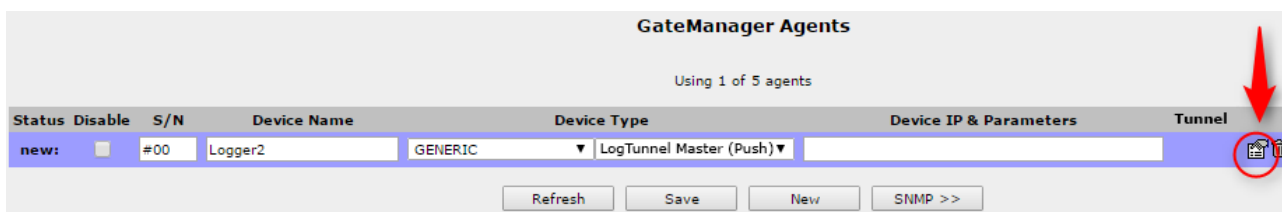
SiteManager: “EasyLog Client2”

GateManager Agents						
Using 2 of 2 agents						
Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
N/C	<input type="checkbox"/>	#00	PLC1	GENERIC	LogTunnel Client	172.26.2.50
N/C	<input type="checkbox"/>	#01	PLC2	GENERIC	LogTunnel Client	172.26.2.231

Refresh Save SNMP >>

4.2. Configuring the LogTunnel Master (Push) Agent

1. Enter the SiteManager Agents menu and create a Generic > LogTunnel Master (PUSH) agent; give it a meaning full Device Name and select the Parameter details icon:



2. Complete the configuration:

Log Server Address: * 172.16.16.191 **1**

Always On:

Listening TCP ports: * 21 **2**

Listening UDP ports: * 162 **2**

Idle Timeout: **3**

Custom Settings:

Save Back Ping

* = Mandatory field

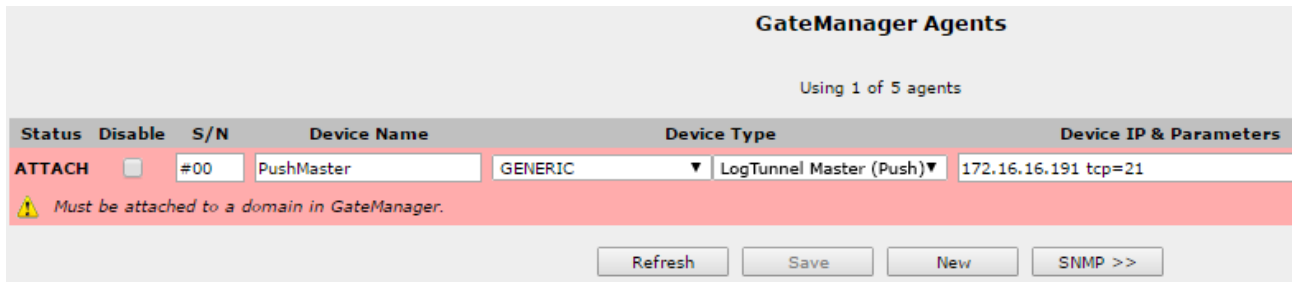
- 1** Enter the IP address of the log server. DNS names are not supported.

Only the specified Master Address will be allowed access to, by the remote devices. This is security precaution for preventing unauthorized access to the network of the log server.

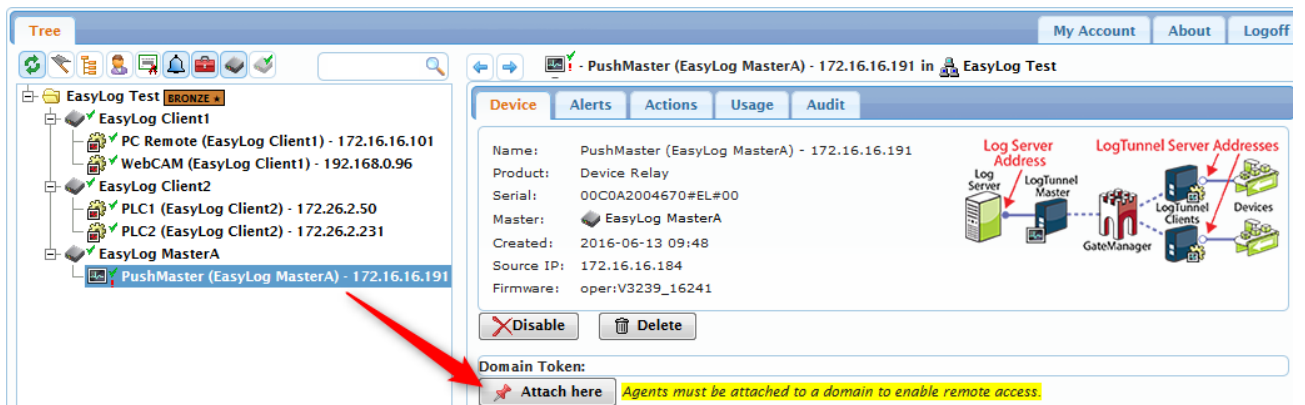
- 2** You will need to configure the specific ports or port range for TCP ports and/or UDP ports to listen on. You can combine single ports with ranges like this "23,80,5000-5010". Note that the mandatory indicator * just means that values must be filled in at least one of the fields UDP or TCP.

- 3** Idle timeout value in seconds. If left blank the default values will be 120 seconds for TCP connections and 30 seconds for UDP connections. Note that if entering a value, this value will apply for both UDP and TCP.

3. When clicking Save, Back and Refresh a couple of times, you will notice that the agent informs you to attach it on the GateManager. This is a Security precaution to avoid accidental access by remote devices.



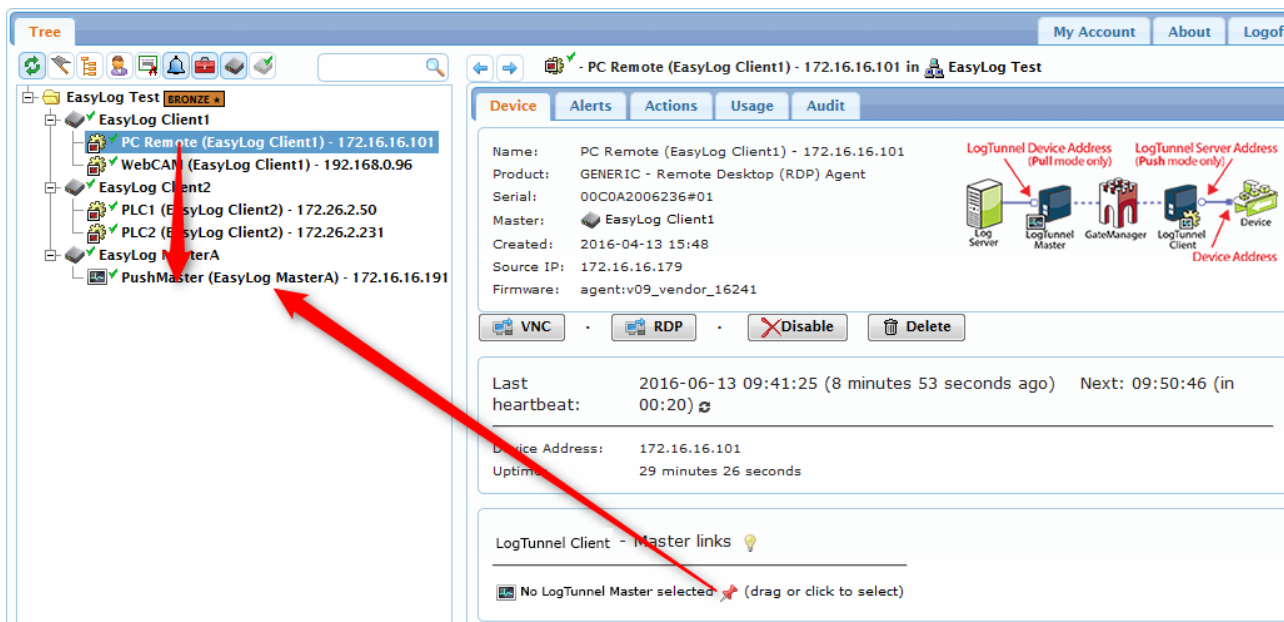
4. Login to the GateManager Portal and locate the LogTunnel Master (Push) agent, and attach it:



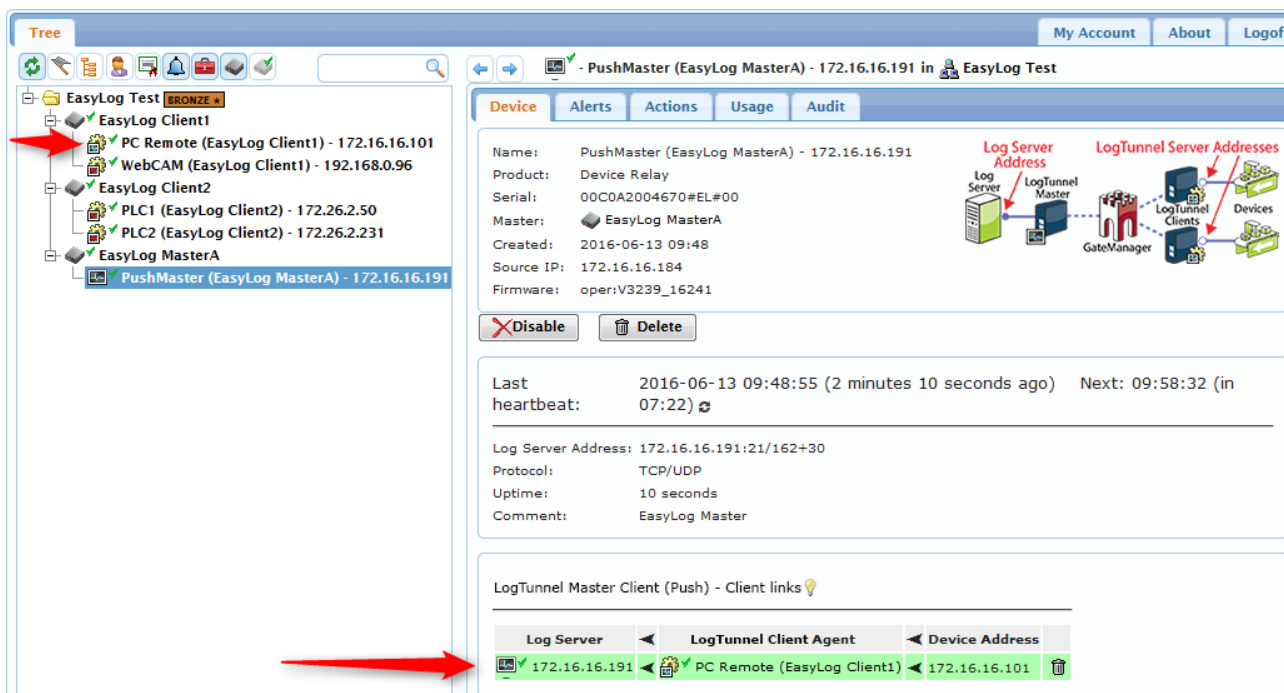
4.3. Linking LogTunnel Clients to LogTunnel Master



4.3.1. Drag-and-drop Clients onto LogTunnel Master

1. While standing on the LogTunnel Client agent, either drag the pin onto the LogTunnel Master Agent, or simply drag the client agent in the tree onto the LogTunnel Master.



2. The LogTunnel Master will automatically indicate the newly linked client:



Hint: Notice that the icons for linked agents change colour from  to .

3. Continue doing step 1 for all LogTunnel Clients that should access the server. The last linked agent is highlighted with green.

The screenshot displays the EasyLog Manager web interface. On the left, a tree view shows the hierarchy: EasyLog Test (BRONZE) > EasyLog Client1 > PC Remote (EasyLog Client1) - 172.16.16.101 > WebCAM (EasyLog Client1) - 192.168.0.96 > EasyLog Client2 > PLC1 (EasyLog Client2) - 172.26.2.50 > PLC2 (EasyLog Client2) - 172.26.2.231 > EasyLog MasterA > PushMaster (EasyLog MasterA) - 172.16.16.191. A red arrow points to the PLC2 entry.

The main panel shows details for the selected device: PushMaster (EasyLog MasterA) - 172.16.16.191. Fields include Product (Device Relay), Serial (00C0A2004670#EL#00), Master (EasyLog MasterA), Created (2016-06-13 09:48), Source IP (172.16.16.184), and Firmware (oper:V3239_16241). There are Disable and Delete buttons.

Below the device details, a section titled "LogTunnel Master Client (Push) - Client links" contains a table:

Log Server	LogTunnel Client Agent	Device Address
172.16.16.191	PLC2 (EasyLog Client2)	172.26.2.231
	PLC1 (EasyLog Client2)	172.26.2.50
	WebCAM (EasyLog Client1)	192.168.0.96
	PC Remote (EasyLog Client1)	172.16.16.101

A red arrow points to the first row of the table, where the PLC2 agent is highlighted in green.

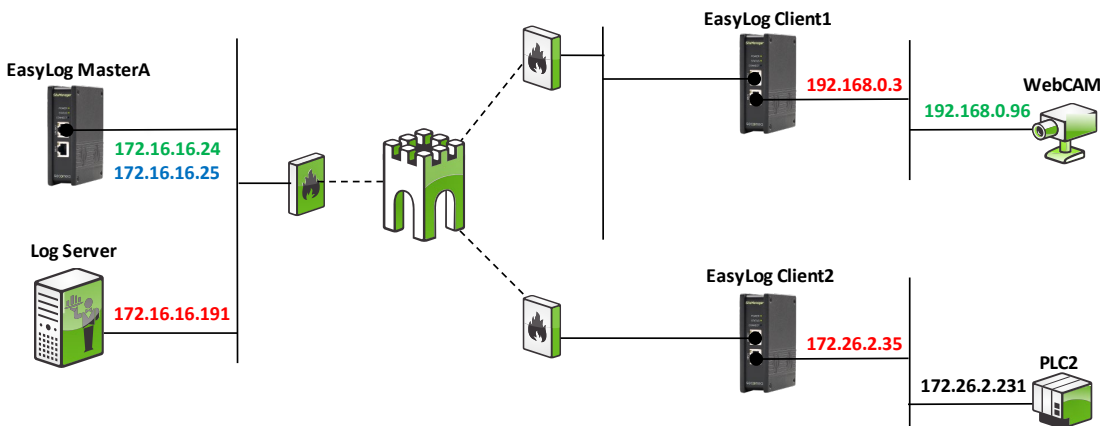
5. Push and Pull for the same devices

The fundamental principle and use case for LogTunnel is that either the server end, or the device is initiator for the connection.

The LogTunnel concept does, however, allow both Pull and Push connections for the same devices. It will just require:

- The central SiteManager to have both a Push and a Pull LogTunnel Master agent configured,
- The Remote SiteManagers having two LogTunnel enabled agents for each device needing both Push and Pull.

For instance, this setup has both Push and Pull enabled for the WebCAM and PLC2 respectively (Red indicates **Push** specific information, and Blue/Green indicates **Pull** specific information)



5.1. Configuration on SiteManagers

Configuration on “LogTunnel Client 1”:

Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
IDLE	<input type="checkbox"/>	#01	WebCAM Pull	GENERIC	Web access (WWW) 192.168.0.96	<input checked="" type="checkbox"/>
N/C	<input type="checkbox"/>	#00	WebCAM Push	GENERIC	LogTunnel Client 192.168.0.96	<input checked="" type="checkbox"/>

Configuration on “LogTunnel Client 2”:

Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
IDLE	<input type="checkbox"/>	#01	PLC2 Pull	Schneider Electric	Ethernet 172.26.2.231	<input checked="" type="checkbox"/>
N/C	<input type="checkbox"/>	#00	PLC2 Push	GENERIC	LogTunnel Client 172.26.2.231	<input checked="" type="checkbox"/>

Configuration on “EasyLog MasterA” (after agents are attached):

Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel
IDLE	<input type="checkbox"/>	#01	PullMaster	GENERIC	LogTunnel Master (Pull) 172.16.16.191 ip=172.16.16.24-25 tcp=80,443,80	<input checked="" type="checkbox"/>
IDLE	<input type="checkbox"/>	#00	PushMaster	GENERIC	LogTunnel Master (Push) 172.16.16.191 tcp=21 udp=162	<input checked="" type="checkbox"/>

5.2. Configuration on GateManager

Before linking agents on the GateManager the setup looks like this:

The screenshot shows the GateManager interface for a PullMaster agent. The left sidebar shows a tree view with the following items:

- EasyLog Test (BRONZE)
- EasyLog Client1
 - WebCAM Pull (EasyLog Client1) - 192.168.0.96
 - WebCAM Push (EasyLog Client1) - 192.168.0.96
- EasyLog Client2
 - PLC2 Pull (EasyLog Client2) - 172.26.2.231
 - PLC2 Push (EasyLog Client2) - 172.26.2.231
- EasyLog MasterA
 - PullMaster (EasyLog MasterA) - 172.16.16.191 (selected)
 - PushMaster (EasyLog MasterA) - 172.16.16.191

The main panel shows the configuration for the selected PullMaster agent:

- Name: PullMaster (EasyLog MasterA) - 172.16.16.191
- Product: Server Relay
- Serial: 00C0A2004670#EL#01
- Master: EasyLog MasterA
- Created: 2016-06-13 09:58
- Source IP: 172.16.16.184
- Firmware: oper:V3239_16241

Buttons: Disable, Delete

Last heartbeat: 2016-06-13 14:50:18 (9 seconds ago) Next: 14:59:36 (in 08:28)

Log Server Address: 172.16.16.191

LogTunnel Device Addresses: 172.16.16.24-25:80,443,8000-8010/162+30

Protocol: TCP/UDP

Uptime: 10 seconds

Comment: EasyLog Master

LogTunnel Master (Pull) Configuration

LogTunnel Targets: Using 0 of 2 LogTunnel Device Addresses:

172.16.16.24	
172.16.16.25	

Buttons: Save, Cancel

When the “Pull” client agents have been linked to the “PullMaster” ref. the descriptions in section 3.3 **Linking LogTunnel Device addresses to LogTunnel Clients**, it looks like this.

The screenshot shows the GateManager interface for the same PullMaster agent, but now with the LogTunnel Device addresses linked to LogTunnel Clients. The left sidebar is the same as in the previous screenshot.

The main panel shows the configuration for the selected PullMaster agent:

- Name: PullMaster (EasyLog MasterA) - 172.16.16.191
- Product: Server Relay
- Serial: 00C0A2004670#EL#01
- Master: EasyLog MasterA
- Created: 2016-06-13 09:58
- Source IP: 172.16.16.184
- Firmware: oper:V3239_16241

Buttons: Disable, Delete

Last heartbeat: 2016-06-13 14:50:18 (1 minute 26 seconds ago) Next: 14:59:36 (in 07:49)

Log Server Address: 172.16.16.191

LogTunnel Device Addresses: 172.16.16.24-25:80,443,8000-8010/162+30

Protocol: TCP/UDP



Uptime: 10 seconds

Comment: EasyLog Master

LogTunnel Master (Pull) Configuration

LogTunnel Targets: Using 2 of 2 LogTunnel Device Addresses:

Log Server	LogTunnel Dev. Addr	LogTunnel Client	Device Address
172.16.16.191	172.16.16.24	WebCAM Pull (EasyLog Client1)	192.168.0.96
	172.16.16.25	PLC2 Pull (EasyLog Client2)	172.26.2.231

Notice that the icons for the agent have changed colour from  to 

When the “Push” client agents have been linked to the “PushMaster” ref. the descriptions in section 4.3 Linking LogTunnel Clients to LogTunnel Master it looks like this:

The screenshot shows the EasyLog Test web interface. On the left, a tree view shows the hierarchy: EasyLog Test (BRONZE) > EasyLog Client1 > WebCAM Pull (EasyLog Client1) - 192.168.0.96, WebCAM Push (EasyLog Client1) - 192.168.0.96, EasyLog Client2 > PLC2 Pull (EasyLog Client2) - 172.26.2.231, PLC2 Push (EasyLog Client2) - 172.26.2.231, EasyLog MasterA > PullMaster (EasyLog MasterA) - 172.16.16.191, PushMaster (EasyLog MasterA) - 172.16.16.191. The main area shows the configuration for the selected device: PushMaster (EasyLog MasterA) - 172.16.16.191. The configuration includes fields for Name, Product (Device Relay), Serial (00C0A2004670#EL#00), Master (EasyLog MasterA), Created (2016-06-13 09:48), Source IP (172.16.16.184), and Firmware (oper:V3239_16241). There are Disable and Delete buttons. Below this, the heartbeat information is shown: Last heartbeat: 2016-06-13 14:43:47 (8 minutes 49 seconds ago), Next: 14:53:34 (in 00:55). The Log Server Address is 172.16.16.191:21/162+30, Protocol is TCP/UDP, Uptime is 9 minutes 21 seconds, and Comment is EasyLog Master. At the bottom, a table titled "LogTunnel Master (Push) - Client links" shows the following data:

Log Server	LogTunnel Client Agent	Device Address
172.16.16.191	PLC2 Push (EasyLog Client2)	172.26.2.231
	WebCAM Push (EasyLog Client1)	192.168.0.96

APPENDIX A. Tech Hints and Known Limitations

Generally, you should consider the LogTunnel connections being connections for specific ports or limited port ranges. Do NOT expect simulating a traditional VPN connection using EasyLog.

Larger LogTunnel Device address ranges (Pull mode)

A LogTunnel Device address range (IP aliases) will always support the last octet regardless of the class. E.g. a class B subnet range of 192.168.1.100 - 192.168.2.250 / 255.255.0.0 would consist of 404 available addresses, but the SiteManager will only create 254 addresses. If the full range should be supported, you must create two LogTunnel Master (Pull) agents; one with the IP range 192.168.1.100-254 and the other with IP range 192.168.2.1-250.

Address range entry formats

Address ranges can be entered in three different formats:

1. 192.168.200.11 (single address)
2. 192.168.200.11-75 (65 IP addresses starting from .11)
3. .11-75 (same as above but will always match DEV1 subnet)

Port range formats

Port range can be entered in three different formats:

1. 8001-8100 (100 ports starting from 8001)
2. 8001-100 (100 ports starting from 8001)
3. 0-65536 (all ports)

Limitations of Listening port and connections

Hardware SiteManager

For SiteManager Hardware models there is a limit of max. 16 single ports and/or port ranges. If wanting to open for all ports, enter 0-65536.

SiteManager Embedded

On SiteManager Embedded there is a limit to a total of 16 ports. If e.g. specifying TCP ports **23,80,5000-5100** effectively only the ports 23,80,5000-5013 will be opened only.

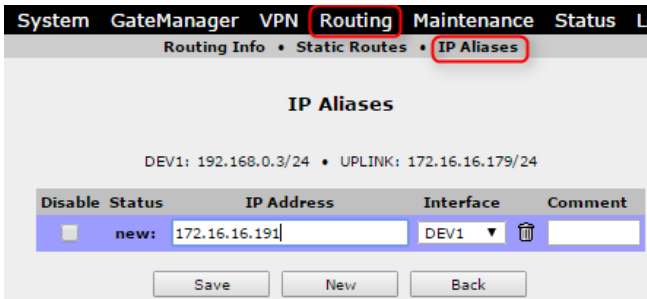
Also, note that TCP ports have preference over UDP ports. So, if TCP ports **23,80,5000-5010** is configured together with UDP port **8000-8010**, then all the TCP ports will be opened but only UDP port **8000-8003**.

As SiteManager Embedded relies on the native socket API of the OS on which it is installed, SiteManager Embedded is limited with regards to the number of concurrent connections. There is a hard limit of max 20 connections per agent (e.g. a web browser would create multiple connections on the same port 80/443). The total number of connections (agents x 20 connections) may also be limited of the hosting OS. For instance, on Microsoft Windows, the current limit is 256.

You can check the log of the SiteManager to troubleshoot if you encounter issues that you suspect may be caused by these limitations.

Devices requiring the “real” log server address as destination

In case a PLC would require (or is programmed for) accessing the genuine IP address of the log server (e.g. 172.16.16.191) but its own address is in another subnet (e.g. 192.168.0.96), you will need to configure the log server address as **LogTunnel Server** address on the LogTunnel Client agent of the remote SiteManager. For the SiteManager to create the LogTunnel Server alias with another subnet than the SiteManager’s DEV port, you will need to manually create the Alias in the SiteManager:



Note that this is only support on a hardware SiteManager. Also note that the device connecting to the log server must have the SiteManagers DEV1 IP address as default gateway.

FTP data connections

SiteManager and SiteManager Embedded support both Active and Passive mode as long as the initial FTP control connection is on port 21. SiteManager is “FTP aware”, which means you do not have to configure additional ports associated with the FTP protocol (such as port 20 or > 1023).

Notices

Publication and copyright

© **Copyright Secomea A/S 2016-2017**. All rights reserved. You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

SiteManager™, LinkManager™ and GateManager™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we cannot guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com