



# Networking Multiple OAISYS Recording Systems Guide

2/29/2012

**Americas Headquarters**

OAISYS

7965 South Priest Drive, Suite 105

Tempe, AZ 85284

USA

[www.oaisys.com](http://www.oaisys.com)

(480) 496-9040



## OVERVIEW

The purpose of this document is to guide a technical administrator through configuration of OAISYS recording solution in a networking environment. A network environment in the context of this document may refer to any of the following configurations:

- Multiple Tracers
- Screen Recording Servers
- Network access for Network Printing
- Network access for Network Staging

## SECTION 1

### ACCESS TO WINDOWS NETWORK RESOURCES

Any OAISYS Service that needs access to Network Resources must be run under an account that has access rights enabled for those resources. This will typically be a domain user account.

**NOTE:** For services to start, the user account must have local admin rights on the server. By default, OAISYS Services run under the local System Account.

#### TO CHANGE THE LOG ON FOR A SERVICE

From the Services applet → double-click on a service → select the Log On tab

See Screenshot below:





EXAMPLES ARE AS FOLLOWS:

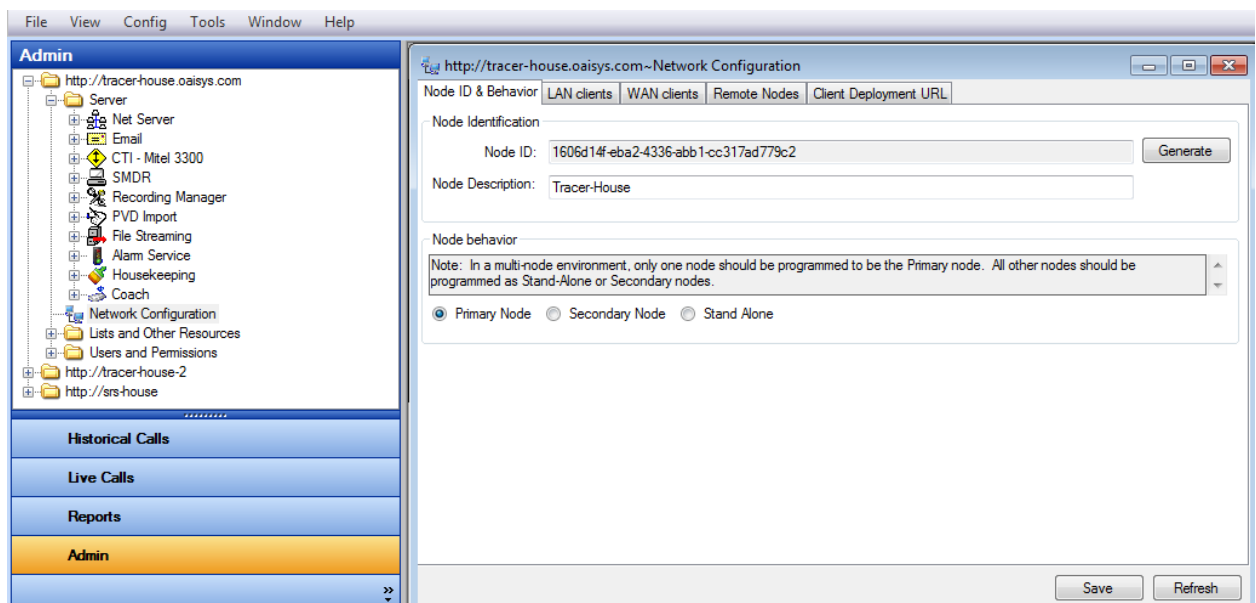
- For automated printing, the OAISYS Report Engine Service must run using an account with the network printer set as the default printer on the OAISYS server.
- OAISYS Triton Recording Manager (TRM) needs access to the file systems of remote computers if you are in OAISYS Multi-node or Screen Recording Server configurations.
- When OAISYS Clients login to the main system and access records which contain a PVD or Screen Recording contained on the remote system, the main system's TRM accesses those files directly and then streams them to the client.
- TRM is also used for Staging to network devices.
- OAISYS Housekeeping service on remote nodes requires access to the file system on the main node so it can do database drive usage calculations for maintenance purposes, orphan recovery, or for Staging to network devices/location.
- See Section 3 of this document for other requirements of the Housekeeping Service.
- OAISYS Historian service needs to have access to the SQL database.

## SECTION 2

### MULTIPLE TRACERS (ALSO SCREEN RECORDING SERVERS)

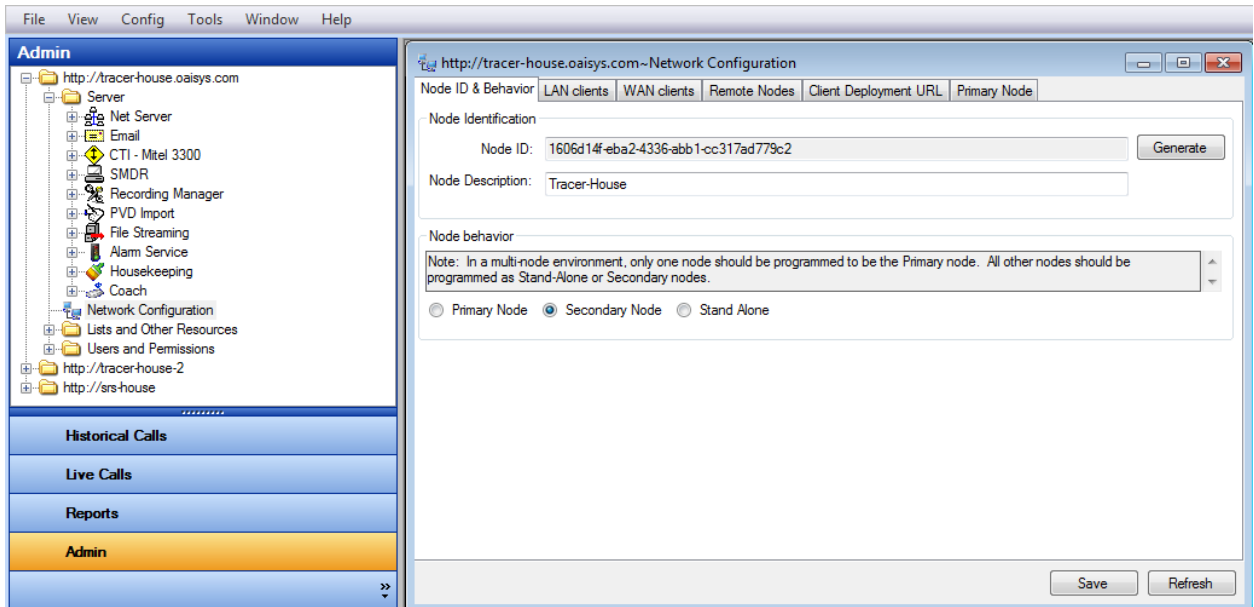
1. When logged into the primary Tracer, from Network Configuration → Node ID & Behavior Tab → select **Primary Node**

**NOTE:** When switching node behavior, the client will be disconnected and will require the user to login again.





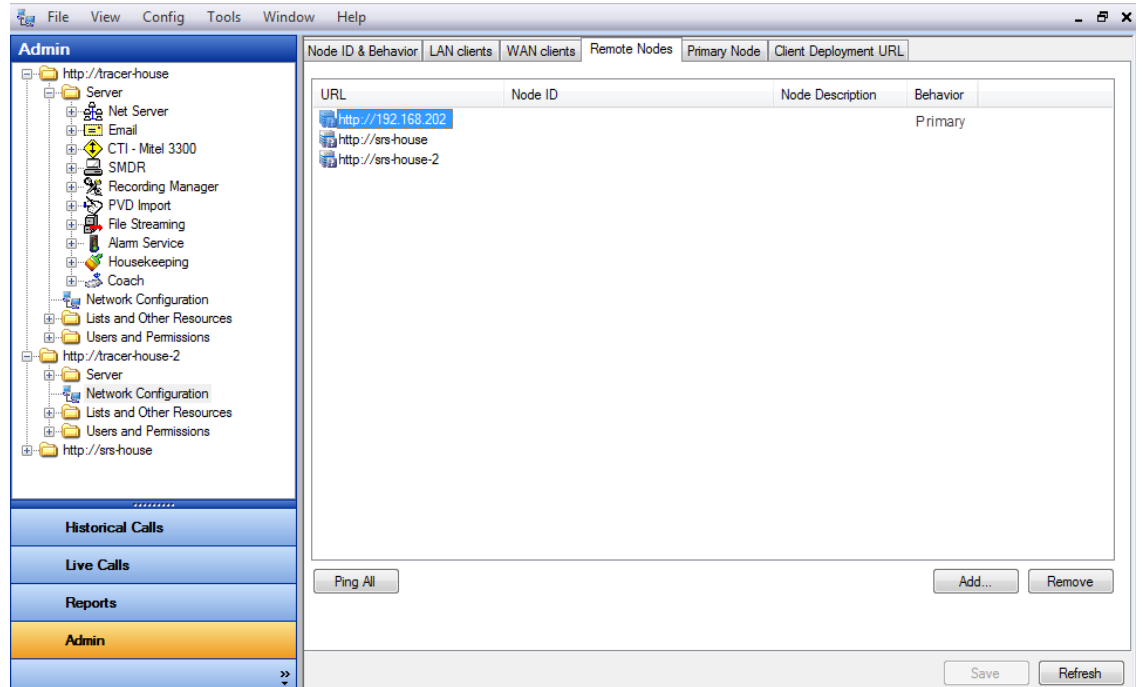
2. When logged into the secondary Tracer, from Network Configuration → Node ID & Behavior Tab → select **Secondary Node**





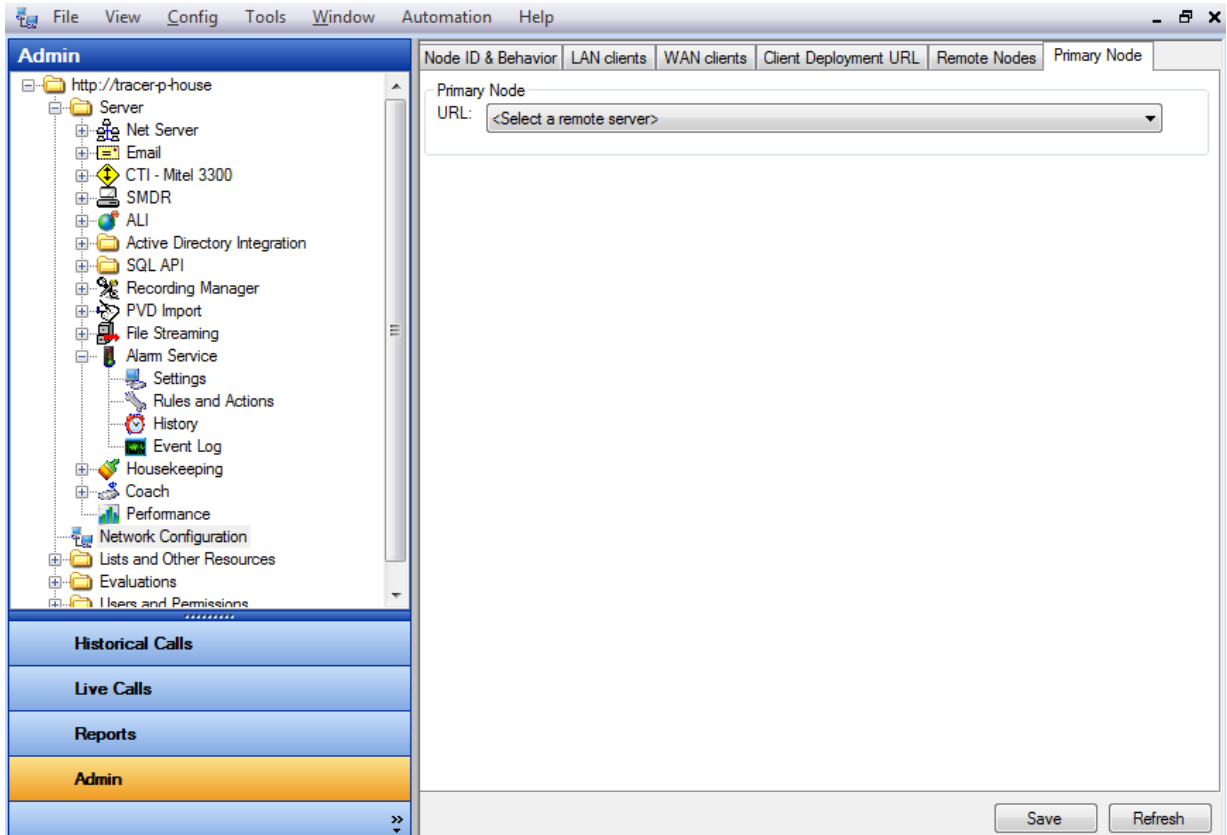
3. Next, on the secondary system: from the Remote Nodes Tab → click **Add** → enter the address of the Primary Tracer/Node → click **Ping All**

a. This should show a green check indicating communication is enabled, and the Behavior column should be filled out with Primary as shown below:





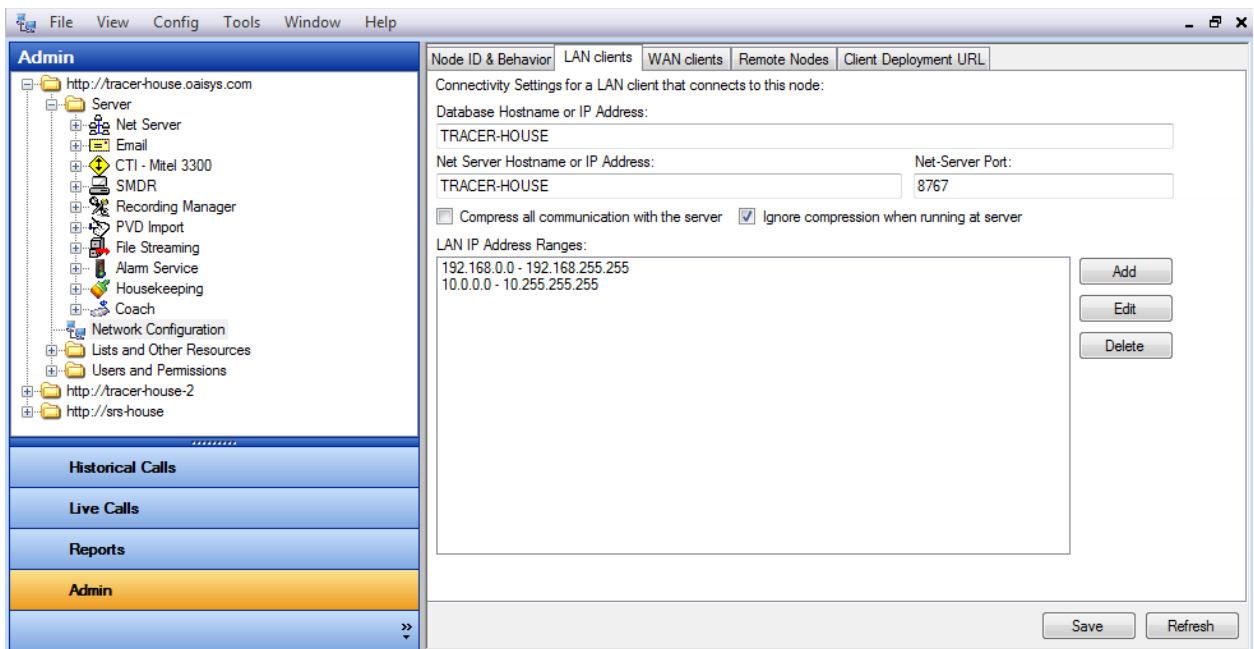
4. Go to the Primary Node Tab → select the Primary Node from the drop down list → click **Save**

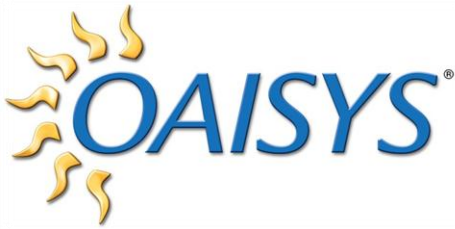




- Return to the main Tracer → add the remote Tracer/Node(s) on the Remote Node Tab → click **Ping All** → verify the Behavior column indicates Secondary

**NOTE:** From the Network Configuration screen, under LAN Clients Tab, both the main Tracer and secondary Tracer should show their own local name or IP address for the Database and Net Server fields. You do not need to change this.





## SECTION 3

### HOUSEKEEPING AND HISTORIAN REQUIREMENTS

The Housekeeping and Historian Service account must have permissions enabled to query the shares on SQL Server (using level 502).

- Level 502 is the lowest level providing the share name and its local path, and specifies the type of information required.

For the remote databases to be backed up, please create a share for the TritonBackup folder on the Primary Tracer server. The default is typically on the C: drive.

Regardless of the level of permissions, services CANNOT use drive mappings.

- For example, "Z:" cannot be mapped to a share because the Services run in a different session than the user login session, and drive mappings are not shared between sessions.
- Services must use a full UNC to access a share (e.g., `\\computername\sharename\subfolder`).

The following configurations require this setup:

- Multiple Tracers
- The secondary node must have access to the share on the primary node where the database is held.
- SQL Server database being hosted on a customer provided PC.

**NOTE:** This requires Administrator, Power User, Print Operator, or Server Operator group membership to successfully execute the NetShareEnum function at levels 2 and 502 (Windows Server 2003, Windows XP). The Windows user account must belong to one of these groups to gain network access.