

User Perspectives: Maximizing Your Network

The current DDMS software applications are optimized to allow you to better utilize your network infrastructure for your business needs. For example, rather than printing to complex, unreliable serial printers, you may now utilize network printers for managing your hardcopy output such as reports, invoices, and tickets. In addition, eNsite Pro, DDMS' graphical distribution system, runs on Windows clients, and operates via your internal network. See the headings below for more information on preparing a network for use with DDMS software.

Basic Requirements

eNsite Pro is a true client/server application. This means that some information is processed on the server, and the remainder is processed on the client. This helps to alleviate performance bottlenecks caused by the server having to process all of the information and business logic that occurs when utilizing the system. Conversely, systems configured with only text-based DDMS software utilize the server to do 100% of the data processing.

eNsite Pro utilizes COM+ and DCOM for moving data records between the client and server over the network for the clients to process some of the information. These are standard Microsoft protocols designed for this purpose. In order for this to function, there are several basic requirements for the network, client, and server:

Network

- Network must be an Ethernet network (not token ring or other variations)
- Must utilize TCP/IP as the communications protocol
- Must have at least a 10Mbps connection speed (100Mbps is preferable)

Server

- Requires DCOM to be installed
- Requires necessary client credentials
 - User accounts must be able to access DCOM on the server
 - User accounts must be able to access necessary data files
- Must have TBL Server installed/configured

Client

- Requires DCOM to be installed
- Requires necessary credentials to the server

Security

Windows security can be quite complex. In fact, an entire course could be created simply to cover the intricacies of the Microsoft Windows security model. This document only discusses what is pertinent to effectively setting up and utilizing eNsite Pro. To get started, there are two different types of security discussed in this handout:

- Share Level Security
- File/Directory Level Security

File and directory level security could easily be split further, but that information is not necessary for this application.

Share-Level Security

When browsing a Microsoft Windows network, it is possible to pull up a machine and see the various folders that the user of that machine has chosen to “share.” This means that the files are available to have their contents browsed, copied, edited, executed, etc. across the network.

In this example, there is a share on the folder named support. Clearly, there are two different ways to access security. The first way is by clicking the button labeled “Permissions” on this form, and the second method is to select the tab labeled “Security.” Share level permissions are set via the button.

Clicking on this button allows the user to specify a list of users on the network that can access the share. This allows them to set three types of permissions:

- Full Control
- Change
- Read



Full Control is the most permissive change. It allows the user to do anything that is possible to the file or directory in question from across the network. Change allows the user to edit the contents of the file from across the network. Finally, Read is the least permissive. It allows the user to copy or view the file as a read-only file. All three of these permission types are specific to each user specified in this share permissions dialog

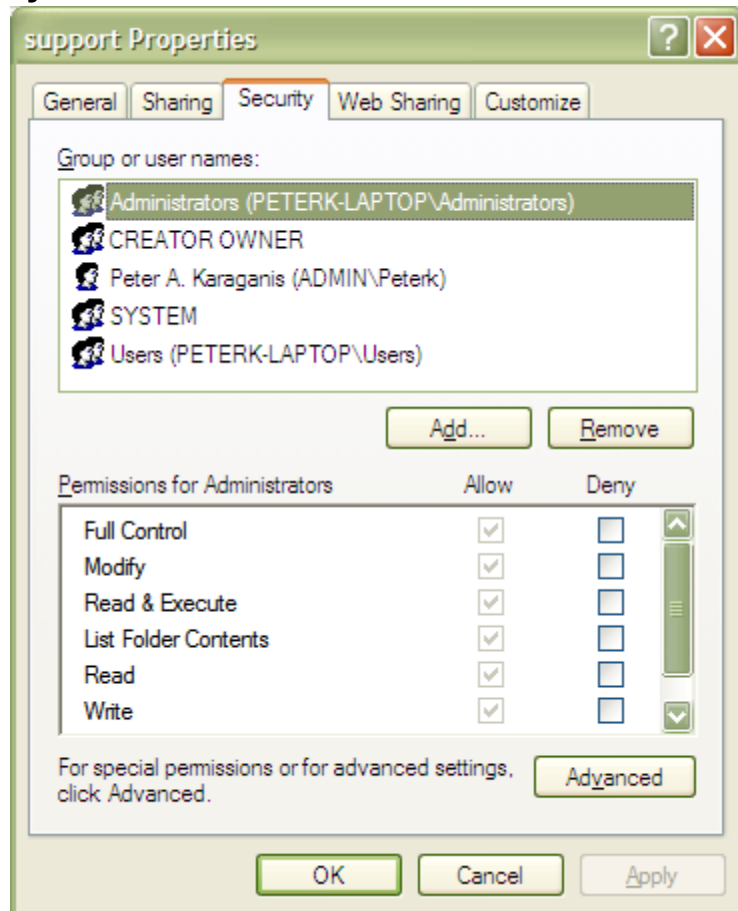
box. It is possible to set all three attributes for one user, and a completely different set of attributes for another user. *The most important thing to remember about share-level permissions is that they only apply when a folder is accessed from across the network.* In other words, a user would be bound by the requirements listed here when accessing this resource from a different machine on the network; however, if they logged on locally to the server, they would not be bound by the permissions listed here. Also, if a user is not included in the list of users to whom permission is granted (by inclusion in a specific group or by being listed specifically) then they won't have access to the directory.

File/Directory-Level Security

While share-level security applies to access of files and folders via the network, File and directory level security pertains to all aspects of file access. In other words, if a user logs onto a machine locally, he is bound by the ACL, Access Control List. The ACL controls all of the file and directory level permissions for folder and files. ACL security settings can be reached by selecting the "Security" tab in the properties dialog box of a file or folder.

As with share-level permissions, these permissions can be setup by user or group. The list of applicable permissions for ACL Security is significantly longer than for share-level security:

- Full-Control
- Modify
- Read & Execute
- List Folder Contents
- Read
- Write
- Special Permissions



Omission of a user from this list (by group or specific listing) makes the user unable to access the resource. It is important to note, that by default, sub-folders will always inherit permissions from the parent folder (the folder in which this folder resides). These settings

are designed for ease of administration. While it is possible to break this model, it is not recommended.

Permission Level Conflicts

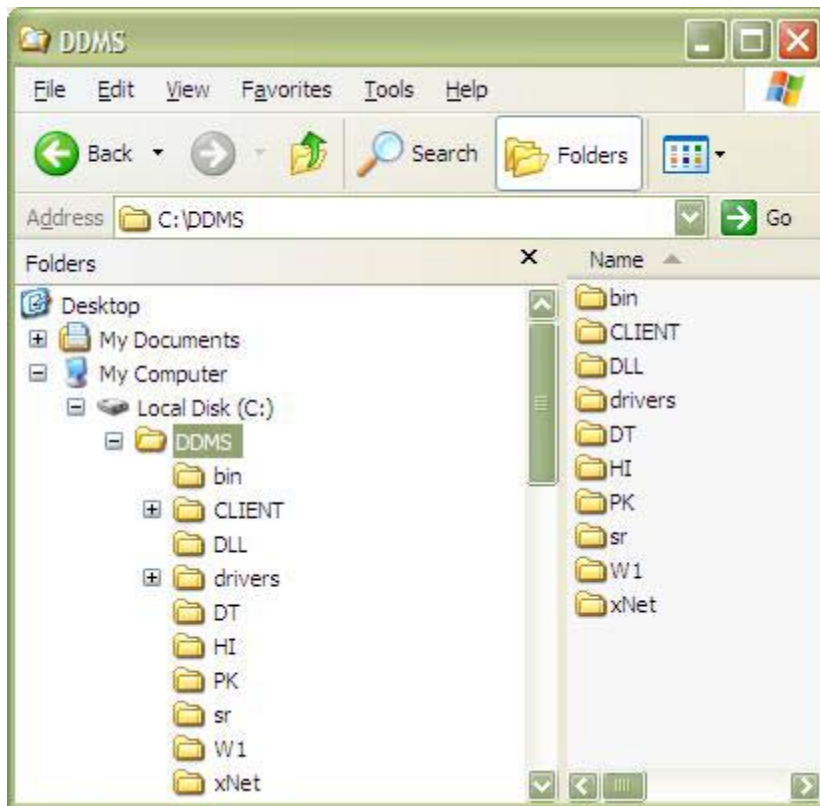
If a conflict exists between share-level and ACL permissions, the most restrictive settings are used during access of resources via the network. For example, assume a user has been granted Read-only share-level access to a resource, but has Full Control ACL access to the same resource. The user is only able to access the resource as read-only via the network; however, logging onto the machine and accessing the resource locally will grant that user full-control over the specified resource since share-level security applies only to network access of resources. *Finally, if a resource has conflicting ACL permissions setup for the same user, the user will be granted the most permissive rights to the resource.* The one exception is if one of the ACL permissions is “No Access.” In this case, the user would not have access to the resource in question. To sum this up, conflicting ACL permissions are resolved with the level of access gaining the most permissive right, unless one of the conflicting levels is “No Access.”

It is recommended that a user group be setup for all of the DDMS users. This way, permission only has to be modified for that group, and any new users that are added will only have to be added to this group. This makes administration much easier.

There are several ways to setup or restrict access to server resources in addition to ACL and share-level permissions; however, those topics are too complex to be covered in this class.

Utilizing Security with DDMS Software

There are things that should be considered when changing access rights on DDMS



servers.

First, it is important to have an understanding of the directory structure of the DDMS Software. DDMS is typically installed in the DDMS folder of a root drive. In other words, the path to the DDMS files on a server is typically: x:\ddms, where x is the root drive letter.

There are several directories that are important:

- Bin
- Client
 - Data
 - Support
 - System
- DLL
- Misc. Data Folders

DDMS

This folder should not be shared on the network; however, ACL Permissions should be set such that the users of the DDMS Software are allowed full-access to its contents (including sub-folders and their contents).

Bin

This folder contains all of the software specific files required to make the DDMS software run, and it should not be shared. The contents of this folder should never be modified without the assistance of a trained DDMS support technician. This folder should inherit ACL permissions from the “DDMS” folder.

Client

This folder contains all of the eNsite Pro specific objects, and it should not be shared. It should inherit ACL permissions from the “DDMS” Folder.

Data

This folder contains the user settings so eNsite Pro users can make changes to their eNsite Pro sessions and then save their preferences so they are the same when they log on again. This folder should not be shared. This folder should inherit ACL permissions from the “Client” folder. If the settings become corrupted, deleting the User.mdb, Global.mdb, and Machine.mdb files can help to alleviate these problems; however, this will remove **ALL** saved settings.

Support

This folder contains all of the core system files utilized by eNsite Pro software. It should be shared on the network. Its only purpose is to allow clients to automatically update across the network, and if it is not shared, then client software will not be able to automatically update itself when starting up eNsite Pro. This folder should inherit ACL permission from the “Client” folder; however, it should have **Read-Only** share-level permissions setup. This allows users across the network to update them as they connect, but it does not allow them to inadvertently damage the contents of the folder when accessing remotely. This folder is not actually utilized by the eNsite Pro software except for the purposes of running the automatic updates of clients.

System

This folder contains all of the core system files utilized by the eNsite Pro software. This folder should not be shared under any circumstances. It should inherit ACL permissions from the “Client” folder.

DLL

This folder contains core COM+ files of the eNsite Pro Server software. This folder should not be shared on the network, and it should inherit ACL permissions from the “DDMS” folder.

Misc. Data Folders

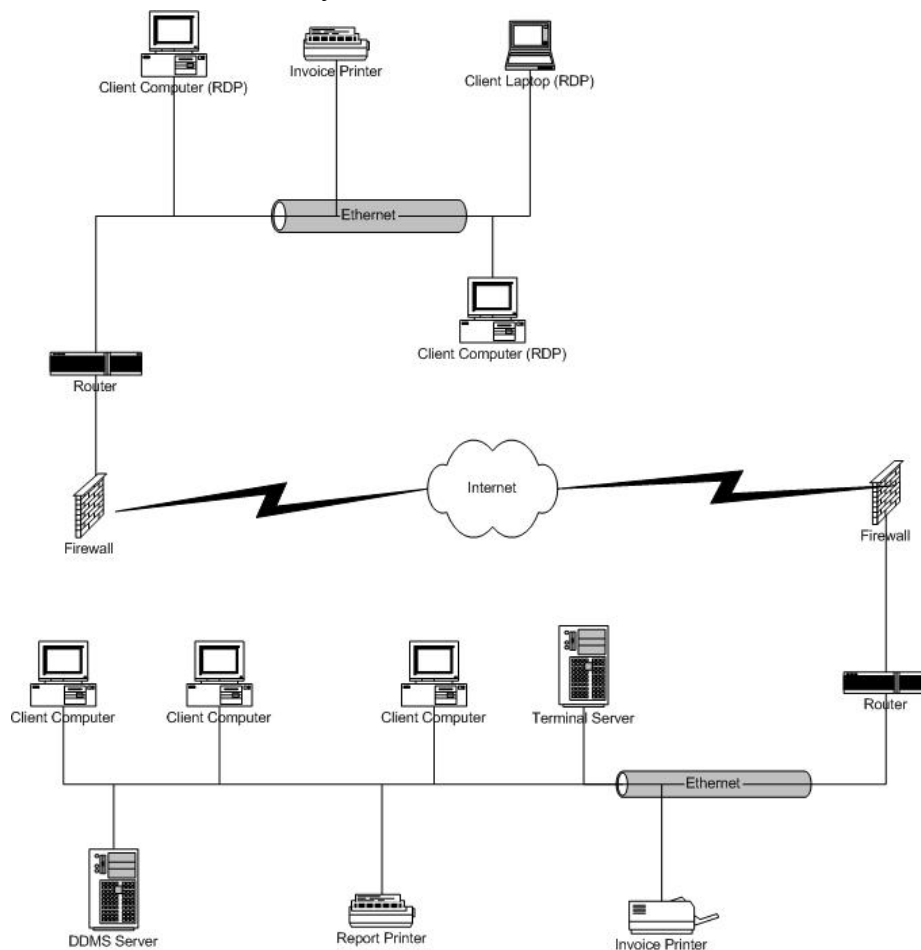
These are folders such as SR, IN, HI, etc. They contain the .dbf, .cdx, and .key files utilized to house DDMS data. These folders should **never** be shared on the network. If they are available on the network, and someone browsing them inadvertently opens one, the DDMS process that needs these files might not be able to gain exclusive access to them. This could result in system instability problems on the server, data loss, or slow performance. These folders should inherit ACL permissions from the “DDMS” folder.

Network Protocols

The important thing to remember about utilizing DDMS in a network is that DDMS is designed to operate under standard networking setups. There are a variety of methods to design a network, and most of them will work fine with DDMS. The only requirement is that the network protocol that is used be TCP/IP. Some of the other commonly used protocols include: IPX/SPX, NETBEUI, AppleTalk, etc. These protocols can be setup in addition to TCP/IP; however, it is recommended that only network protocols that are actually needed be installed. Having unused protocols setup such as NETBEUI can increase network traffic, thereby slowing down all network applications including DDMS. The topic of networking protocols is complex, and it is too advanced to be covered in this class.

Multiple Locations and eNsite Pro

Many office products dealers have multiple locations. It is important to note that eNsite Pro will work well for this type of environment; however, some special setup is required in order to effectively utilize the eNsite Pro software.



In this diagram, the top portion represents a remote location, and the bottom portion represents the home location. To utilize eNsite Pro under a setup such as this, the main location will need to have a terminal server, and the remote locations access eNsite Pro via the RDP client on the terminal server.

RDP (Remote Desktop Protocol) allows a user to access a terminal server remotely. Because eNsite Pro is a true client/server application, there is far too much data to effectively transmit via the internet. This is because internet connections have far less bandwidth than a regular local Ethernet connection. For example, a standard commercial internet connection would be a T1 or business-grade DSL connection. A T1 has a bandwidth 1.5Mbps connection, whereas a standard local Ethernet connection has a bandwidth of 100Mbps. Clearly, a local network connection is significantly faster than even a commercial grade internet connection.

Terminal server alleviates network bottlenecks by allowing remote clients to connect to a machine on the local network to run eNsite Pro. In other words, the eNsite Pro client in the previous diagram runs on the client machines in the main location; however, for remote clients, it runs on the terminal server. This allows the software to send all of the data to a local machine for processing. The terminal server is essentially doing all of the work for every remote client. If an organization has a large number of remote users, then setting up multiple terminal servers might be a necessity to ensure that the server itself is not the source of a processing bottleneck. Specific Terminal Server configuration information is too complex to be covered in this class.

DDMS Network Printing

The current DDMS software allows much more flexibility with printing than was previously available. There are many ways to configure printers for use in the DDMS system; however, the recommended method is to utilize network-ready printers, or to purchase stand-alone print servers, and connect those to the printers.

Shared Network printers

One alternative method is to attach a printer to client workstation, and share it on the network. This solution has many caveats and pitfalls. While it may seem easier and more cost-effective in the short-term, the disadvantages far outweigh any advantages that can be thus gained. For example, if a user has a problem with their machine, such as requiring a reboot, that printer is unavailable for printing from the server, resulting in delayed or lost hardcopy reports. Another problem is that if the user has any type of permission problems, it could prevent other users from printing to the printer, even if the machine is available on the network. Finally, this method requires that printers be located in close proximity to client machines. This is not always feasible in a warehouse or similar location. These types of problems require time to solve, and maintaining the permissions for future users can be a daunting task.

Network Print Servers

Some printers come designed to plug directly into a network. For those printers, the setup is very easy. Typically it involves plugging in the computer network port to your existing Ethernet, and installing software on the machines that need to print to this printer. For the purposes of DDMS, that would only be the DDMS server. This type of setup removes permissions and client computer problems as potential issues that could arise. If the

printer in question does not have native networking support, then an external print server device can be purchased that allows the connection of multiple computers. The process for setting up a device like this is very similar to connecting a printer with native network support. Typically, it involves only attaching the printer to the print server, attaching the print server to the local network, and then installing the client software on machines that need to print to this printer. DDMS highly recommends that this method be used to setup printers.