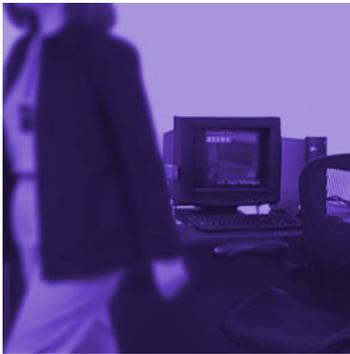




XyLoc Security Server (XSS-SQL 5.x.x)
Administrator's Guide



Contacting Ensure Technologies

Email: support@ensuretech.com
Phone: (734) 547-1600
Home Office: Ensure Technologies
135 S Prospect St
Suite 100
Ypsilanti, MI 48198
Web: www.ensuretech.com

© Ensure Technologies, 1998-2009. All rights reserved. XyLoc and Ensure Technologies are trademarks of Ensure Technologies, Inc.

Adobe® and Acrobat® are registered trademarks of Adobe Systems Incorporated.

Citrix®, MetaFrame®, and ICA® are registered trademarks of Citrix Systems, Inc. in the United States and other countries.

Microsoft®, Windows®, Windows NT®, and Active Directory® are registered trademarks of Microsoft Corporation.

Novell®, Novell Directory Services®, NDS®, NetWare®, and eDirectory® are trademarks or registered trademarks of Novell, Inc.

Technical information contained herein is subject to change without notice.

Table of Contents

CONTACTING ENSURE TECHNOLOGIES	2
TABLE OF CONTENTS	3
<u>INTRODUCTION:</u>	<u>6</u>
OVERVIEW OF XSS	6
XSS ARCHITECTURE AND RELIABILITY	6
XSS-SQL COMPONENTS	7
SQL DATABASE	7
XYLOC SECURITY SERVER SERVICE	7
WEB-BASED MANAGEMENT UI	8
XYLOC CLIENT	8
OVERVIEW OF CLIENT/XSS COMMUNICATION	9
XYLOC AND XSS TERMINOLOGY	9
<u>PREPARING FOR IMPLEMENTATION:</u>	<u>10</u>
BEFORE YOU BEGIN	10
OVERVIEW OF KIOSK AND UNIQUE ACCOUNTS	10
UNIQUE ACCOUNTS	10
KIOSK ACCOUNTS	11
KIOSK VS. UNIQUE	11
GENERAL SERVER REQUIREMENTS	12
APPLICATION INTEGRATION FILE PERMISSIONS	12
<u>INSTALLING XSS-SQL:</u>	<u>13</u>
INSTALL THE XSS DATABASE	13
INSTALLING THE XSS SERVER	15
INSTALLING THE XSS SERVICE COMPONENT	16
INSTALLING THE XSS WEB CONFIGURATION TOOL (WEBUI)	18
<u>UPGRADING FROM PREVIOUS INSTALLATION OF XSS:</u>	<u>24</u>
UPGRADING FROM XSS 2.X.X (CODEBASE) VERSION	24
UPGRADING FROM XSS 3.X.X OR 4.X.X VERSIONS	24
UPGRADING FROM EARLIER XSS 5.X.X VERSIONS	25
<u>OVERVIEW ON XSS WEB INTERFACE</u>	<u>26</u>
ACCESSING THE XSS	26
XSS ADMINISTRATIVE ACCOUNTS	26
XSS HELP MENUS	27
STATUS	27

VIEW XYLOC CLIENT AUTHENTICATION EVENTS:	27
VIEW XYLOC CLIENT HOST EVENTS:	27
VIEW XSS ADMINISTRATOR EVENTS:	27
VIEW KEY STATUS REPORT:	28
HOSTS	28
USERS	28
GROUPS	30
DOWNLOAD	30
<u>MANAGING USER ACCOUNTS AND SETTINGS</u>	<u>31</u>
PLANNING	31
CREATING A NEW USER	32
CREATE THE HOST MANUALLY (IF DESIRED)	34
CREATING A GROUP	37
ASSIGN USERS TO A GROUP	40
ASSIGN A USER TO A GROUP VIA THE USER SETTINGS	40
ASSIGN A USER TO A GROUP VIA THE GROUP SETTINGS	41
ASSIGN HOSTS TO A GROUP	43
CREATING A KIOSK	44
CREATING A LEGACY KIOSK	46
CREATE A NETWORK ACCOUNT	47
CREATE A GROUP	47
CREATE A USER TEMPLATE	49
ASSIGN USERS TO GROUP	53
CREATE THE KIOSK USERS FROM THE TEMPLATE USER	55
<u>ADMINISTERING XSS SERVICES</u>	<u>58</u>
XSS MONITOR SERVICE	58
XSS-SQL DATABASE UTILITIES	58
BACKUP THE XSS DATABASE:	61
RESTORE A BACKUP OF THE XSS DATABASE:	61
REINDEX THE XSS DATABASE:	63
LOG MAINTENANCE:	64
<u>DEPLOYMENT OF XYLOC CLIENT SOFTWARE</u>	<u>65</u>
INSTALLING THE XYLOC CLIENT LOCALLY	65
ENTERPRISE DEPLOYMENT OF THE XYLOC CLIENT:	66
<u>HELPFUL TIPS</u>	<u>67</u>
IF THE IP ADDRESS OF THE DATABASE SERVER CHANGES:	67
IF THE SQL USERNAME AND/OR PASSWORD ARE CHANGED:	67
IF THE IP ADDRESS OF THE XSS CHANGES, OR NEEDS TO BE CHANGED:	67
IF THE ADDRESS OF THE SQL SERVER CHANGES, OR NEEDS TO BE CHANGED:	67
XYLOC CLIENT UPDATE:	67
ADDITIONAL NOTES:	68

ERROR: "PAGE CANNOT BE DISPLAYED" WHEN BROWSING TO THE XSS START PAGE	69
CHANGES MADE AT THE SERVER ARE NOT PROPAGATING TO THE XYLOC CLIENTS	69
USERS AND HOSTS APPEARING IN THE XSS DATABASE	70

Introduction:

Overview of XSS

One of the objectives in implementing XyLoc Security products is to prevent unauthorized individuals from gaining access to sensitive information. The XSS allows an administrator to easily manage a large installation of XyLoc users as it provides centralized management, control and reporting with an easy to use web browser interface.

XSS makes both local and remote Web-based central management of XyLoc simple. New employees are quickly assigned Keys, and Keys used by outgoing employees can easily be disabled. Every aspect of managing a XyLoc installation can be performed quickly and easily using the XyLoc Security Server.

XSS also creates detailed audit logs of both user activity and the operation of the XSS itself. When a user logs on to the network, XSS records how they logged on (with their Key or with an override password) and the time and date of the logon. Every time the user leaves and comes back to the XyLoc-protected machine, this activity is also logged.

XSS also carries out a self-audit. Any changes to the administration of the XyLoc installation are recorded, along with the time of the change and the identity of the administrator.

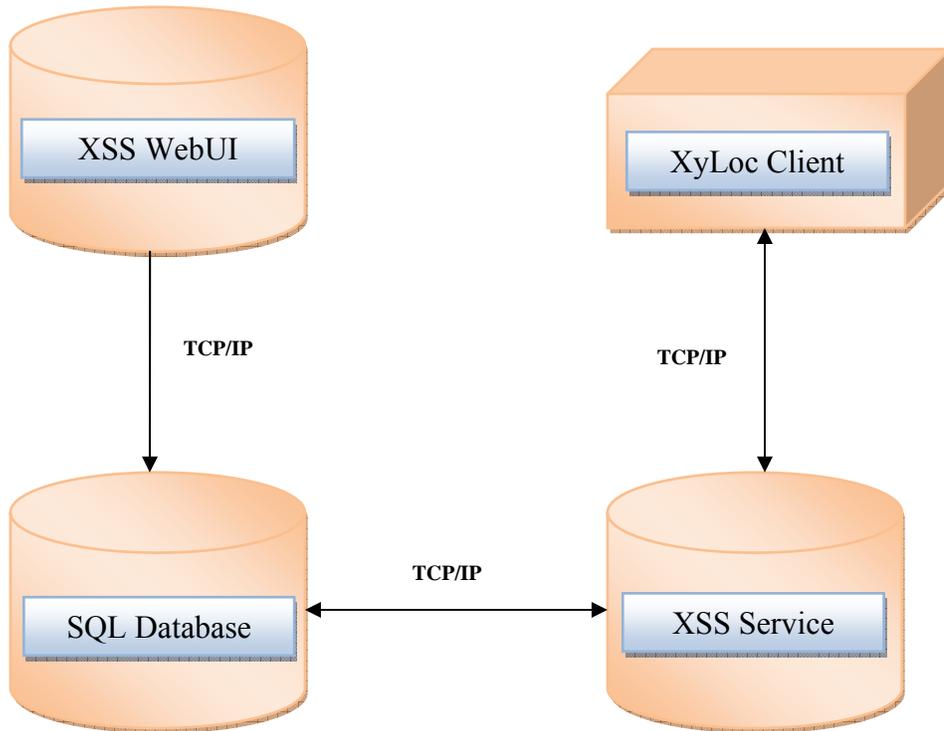
XSS Architecture and Reliability

The XSS is designed with the highest level of reliability. This is achieved by the communication mechanism employed between the XyLoc client and the XSS. In the event of a loss of communication on the network or a failure of the server running the XSS software, the XyLoc clients will remain in full operation.

The XyLoc client maintains a complete record of its configuration and log files. If the communication is interrupted between the client and the XSS, the client will continue to maintain its configuration and log files. Once communication between the XyLoc client and the XSS has been restored, the client will exchange configuration records and log files with the XSS and update each other.

During normal operation, communication between the XSS and the XyLoc client presents a minimum load on the network.

The following diagram illustrates the general system design concept:



XSS-SQL Components

XSS-SQL includes the following components:

SQL Database

The SQL database stores all of the Users, Hosts (Computers), and their respective XyLoc configuration settings.

The database also stores all of the audit log records uploaded by the XyLoc clients to record XyLoc events on the workstations (Locks, Unlocks, Logins, etc.)

XyLoc Security Server Service

XyLoc Security Server (XSS) provides the link between the XyLoc Client Software and the SQL database. It retrieves updated information stored in the database and provides this data to the XyLoc Client as on request from the XyLoc Client software through TCP/IP.

Web-based Management UI

The XSS web-based management UI is used to add/delete/modify user and host information that is stored in the SQL database and also is used to view the centralized storage of all the client Audit Logs.

The WebUI has its own user logons as well and individual XyLoc users can be given XSS Administrator rights in their respective user records on the XSS. This is separate from actual Windows or Active Directory Administrators and would be unique to just the XSS Web Interface.

XyLoc Client

XyLoc Client software is responsible for handling the XyLoc Security Device and all the security actions. Please reference the **XyLoc Client User Guide** for more information about the XyLoc Client software.

Overview of Client/XSS Communication

The XSS communicates with the XyLoc client software installed on the host by an encrypted TCP/IP protocol. When installing the XyLoc client software the client will prompt the user to enter the XSS IP address during installation. Once rebooted, the client then uploads its identity to the XSS. Once this initial upload has populated the XSS database for a given host, with the proper administrative rights, either client software or the browser interface of the XSS can enact changes, depending on the specific changes.

The XSS supports workstations with both static and dynamically assigned IP address (DHCP). For the hosts to communicate properly with the server, the following must be available:

- The XSS receives information from the XyLoc client on TCP port 5102.
- The XSS transmits information to the XyLoc client on TCP port 3510.

For the most part, the XSS will sit idle waiting for requests from the XyLoc clients. When the XyLoc client hears a XyLoc Key for the first time, if configured with an XSS IP Address, the client service will send a request via TCP/IP to the XSS for information about that KeyID. The XSS will then determine if the requested KeyID is valid for that PC and if so will generate the appropriate user record(s) and send back to the requesting PC. The client will then update the local database with information provided by the XSS and will either allow or disallow the user access with that Key, and if access is allowed, what Login Name and Password is to be used for access.

Additional Notes:

- The XSS does not push information to the client. Instead it waits for a request from the client before providing information. This limits the load on the network to only the necessary exchange of information. However, any changes made to a user, or the addition/deletion of users, will only occur on the client with the respective keys are presented to the client the next time.
- The XyLoc clients will only lookup keys that are heard when the client is in a Locked or Logged Off state. When the client is in use by a valid Key, no database updates are performed.
- As an additional load limiting feature, the XSS has multiple processing threads to support multiple requests for keys at the same time. Although this does not necessarily limit the load on the network, this allows the requests to be handled from the client in a more timely fashion for larger enterprises.

XyLoc and XSS Terminology

The following is a list of terminology used for XyLoc and XSS software within this document:

- **Host:** A “Host” is a XyLoc protected PC
- **Key:** A “Key” is the device that is worn by the individual user which transmits the RF signal. Also referred to as a “Badge”.
- **Lock:** The device that is attached to the PC which receives the RF signal that is transmitted by the “Key”. The “Lock” connects to the PC via USB and provides data to the XyLoc client software about the “Keys” whose signals have been received.
- **Client:** The XyLoc software which is installed on the PC.

Preparing for Implementation:

Before You Begin

Before starting the installation of the XSS, take a moment to consider how the XSS and XyLoc products will integrate within your environment. To assist you with this, consider the following:

- Define the user environment:
 - ❑ The number of hosts (Computers) on which XyLoc will be installed.
 - ❑ The number of users that will need XyLoc keys.
 - ❑ The type of XyLoc accounts that will be deployed.
 - **Unique user account:** one XyLoc key per system login account.
 - **Kiosk user account:** multiple XyLoc keys per system login account.
 - ❑ The desired XyLoc login and unlock authentication.
 - ❑ Each host must have an administrator account.

- Define the client server environment:
 - ❑ The static IP address, gateway and subnet mask for the XSS Server.
 - ❑ The location of the SQL database server
 - If using a separate server for SQL, this server must also have a static IP address.
 - ❑ Windows AD/Domain or Novell?
 - ❑ Is the server on a different subnet from the hosts?
 - ❑ Will all hosts be able to access this IP address?
 - Verify that the client can communicate to the server via TCP/IP
 - Verify that the server can communicate to the client via TCP/IP
 - ❑ Are there any network security devices between the hosts and the XSS?
 - ❑ Will each host have a unique IP address or is some type of address translation (NAT) being used between the clients and the XSS?
 - NOTE: In some cases both the client and server will act as a “client”, meaning that either can, and will, initiate a connection to the other. For this reason, each client must have a unique IP address as they appear to the server. For instance, if the clients are behind a router using NAT for each client, but the server is not, then the clients will appear to the server with the same IP address...that of the router. This will cause a breakdown in communication.

Overview of Kiosk and Unique Accounts

There are two main types of user accounts in the XyLoc system: Unique and Kiosk. Both have their advantages and disadvantages. Each functions very differently than the other. This section will provide an overview of how each type functions and the basic differences between the two

Unique Accounts

Unique accounts are individual user accounts with one XyLoc Key assigned to each account. Each user will log into the PC with their own individual login accounts and have their own Windows profile and desktop and settings.

Each user will login to the PC with their individual username and password, and will need to logout when they are finished for anyone else to use the computer with their account. There is

a setting in XyLoc to allow another user to force a logoff of a locked workstation in the event the previous user forgets to logoff before leaving the PC, however this is a Windows “Forced Logoff” and all unsaved data from the previous user would be lost.

Kiosk Accounts

A kiosk account is multiple users sharing one “generic” login to the PC (and in turn one Windows profile and desktop settings) but each having been assigned a unique XyLoc Key.

In a Kiosk, the system would be primarily (if not exclusively) logged in with the “generic” account all day and would be locked as the user leaves their Active Zone and could be unlocked by any other authorized Kiosk user. It would not be required to logoff the system and back on to change users.

Starting with XSS 4.2.0, the Kiosk account setup has changed to be a Host-based Kiosk account. This means that the generic account that is used by all the kiosk users is now defined in the Host settings. With this change, the XSS now supports the type of environment where each PC has its own unique login that is shared by all users (for example: each PC logs in with its hostname for the system login name).

NOTE: The legacy method of setting up a kiosk is still supported for those that already have a kiosk setup and need to upgrade for other reasons. The instructions for the Legacy Kiosk setup are also included, for those that have XSS 4.1.9 or earlier, or prefer this method.

Please see the section for [Creating a Legacy Kiosk](#)

Kiosk vs. Unique

	Advantages	Disadvantages	Common Usage
Kiosk	<ul style="list-style-type: none"> Fast, easy access for each user since there is no need to logoff of the PC before logging on. 	<ul style="list-style-type: none"> Uses a generic Windows account, so each user will share a desktop profile and application set unless other methods of application delivery are available other than local Windows installation (i.e. Citrix) 	<ul style="list-style-type: none"> Shared workstation environments where fast access to a computer is required (i.e. Hospital Nurses Station)
Unique	<ul style="list-style-type: none"> Greater network security as each user must login with their individual credentials and only has access to specific applications. Each user has their own profile and desktop settings and might maintain a more comfortable experience to the user if this is what they are used to. 	<ul style="list-style-type: none"> Slower access to the machine in multi-user environments as each user must completely logon and logoff. Although there is an option to allow a forced logoff, the time to force the logoff and then logon can be extensive. 	<ul style="list-style-type: none"> Individual workstations that are not shared by other users. Workstations that are shared, but where the speed at which the computer can be accessed is not as important as the greater security.

General Server Requirements

The following are the minimum requirements for a basic XSS installation. As with any high availability application, additional resources will improve the capacity to service more users. Unlike many client server applications, the XSS is typically idle. The XSS becomes active when client submits a request for a user record, or when an administrator updates a user's authentication rights or changes a parameter on the XSS itself (through the Web interface). These minimum requirements will typically support several hundred users and hosts:

- PIII 1GHz, 512 MB of memory, and 2GB of disk space with a **STATIC** IP Address
- Windows 2000 server, Windows Server 2003 or Windows Server 2008
 - The Server Core version of Server 2008 is not supported.
- Internet Information Services (IIS) 5.0 or greater installed and operational (for the WebUI component)
- In Server 2003 you must allow "ASP.NET" and "Active Server Pages" to be run in IIS.
- Microsoft .NET Framework 2.0 or later
- SQL Server 2000 or later for the XSS database.
- MDAC 2.7 or greater must be installed on the same server as the WebUI and the XSS Service if the SQL server is not on the same server.

Application Integration File Permissions

The application integration (.ets) file can be stored on the XSS or on a shared drive within the network. This file needs to be read accessible to everyone who will be using application integration.

Installing XSS-SQL:

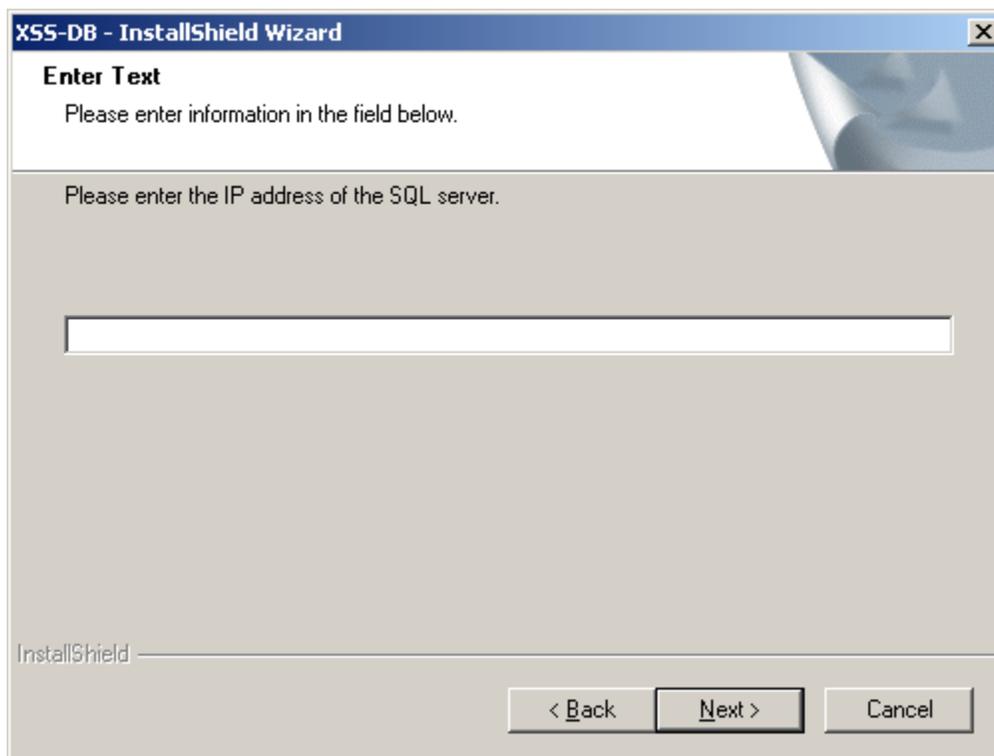
This section will provide the necessary steps to setup the XyLoc database, install the XSS Service, and to setup and install the XSS Web Interface.

IMPORTANT: These instructions are intended for a new installation. If an upgrade from a previous XSS-AD is being performed, then please contact Ensure Technologies Technical Support for proper instructions as they will vary depending on the version that is being installed and the version that is being upgraded.

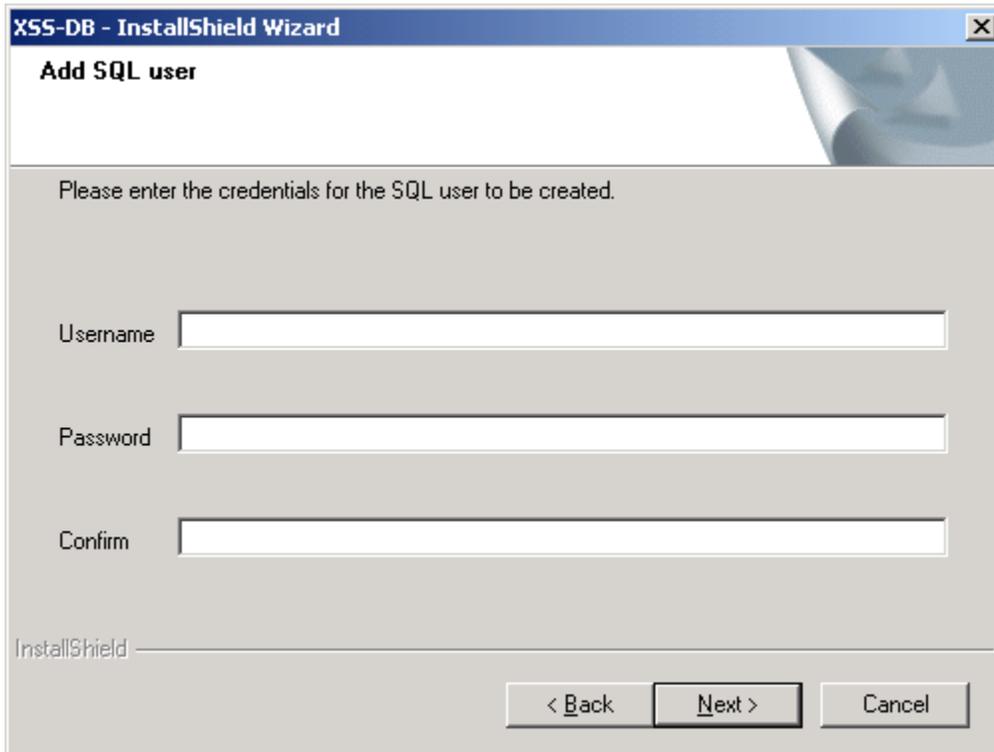
Install the XSS Database

The XSS uses a Microsoft SQL database to store the user database, the audit logs and XSS administrator users. This is created within an existing SQL server, by running the XSS_DB_5xx.exe package on the SQL server.

1. Launch XSS_DB_5xx.exe on your SQL server. NOTE: SQL must be installed and setup prior to launching this package.
2. Read and Accept the License Agreement.
3. The wizard will ask for the IP address of the SQL server. This is for when there are multiple Network Adapters in the server. Currently only one is supported, so the IP address of the desired connection must be entered here.
 - a. If using a “named instance” of SQL then the instance name needs to be specified here as well. Specify the name using the format of: **<server IP address>\instance name**
 - b. **NOTE:** If using SQL 2008 Express, even the default instance is considered a “named instance”. As a result, the named instance must be specified here. Typically the default “named” instance would be “<server address>\SQLEXPRESS”.

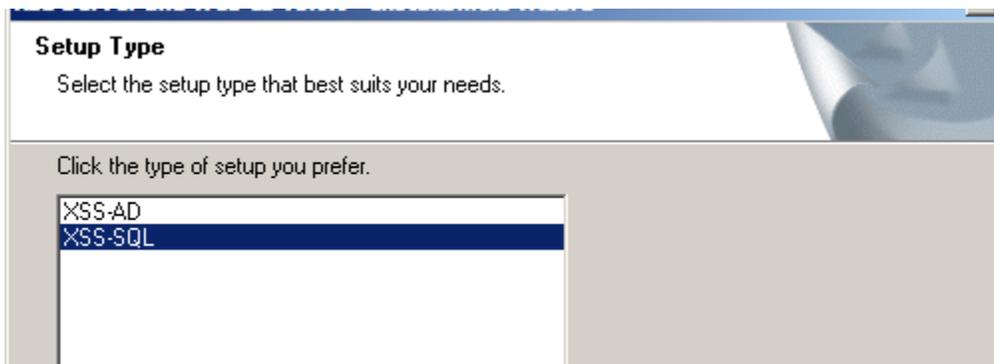


4. The installation wizard will ask to create a new user for the XSS in the SQL. The XSS server and WebUI will use this account to access the SQL database. Put in the desired username and password and click "Next"



The screenshot shows a Windows-style dialog box titled "XSS-DB - InstallShield Wizard". The main heading is "Add SQL user". Below the heading, there is a message: "Please enter the credentials for the SQL user to be created." There are three text input fields labeled "Username", "Password", and "Confirm". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted.

5. Next, select the setup type for the database. In this case, select XSS-SQL and click "Next".



The screenshot shows a dialog box titled "Setup Type". The main heading is "Setup Type". Below the heading, there is a message: "Select the setup type that best suits your needs." There is a list box with two items: "XSS-AD" and "XSS-SQL". The "XSS-SQL" item is selected and highlighted in blue. Below the list box, there is a message: "Click the type of setup you prefer."

one install package as they have been in previous versions. The instructions below will reference the separate installation packages. If using the combined package, the prompts will be basically the same as the separate versions, just combined together as well.

To run the combined installer, run the **XSS_Complete_5.x.x.exe** package.

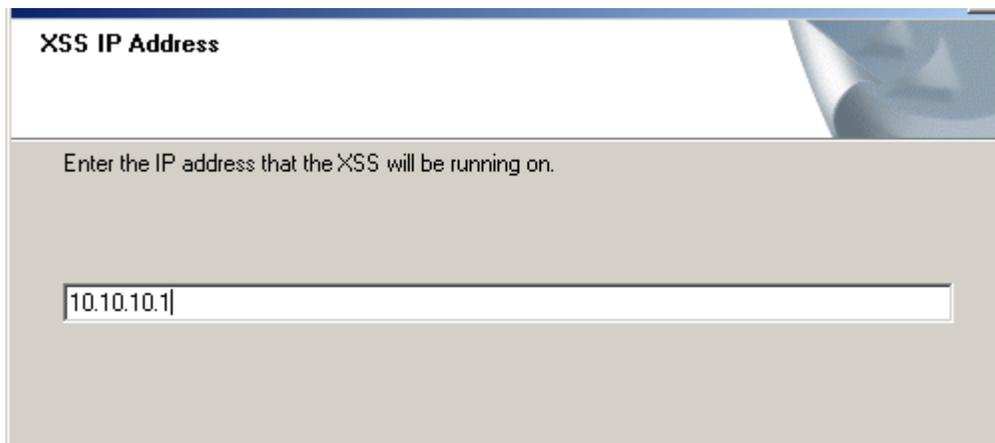
Installing the XSS Service Component

This will install the XSS service and configure the connection to the SQL database. This does not have to be installed on the same server as the database or the WebUI. Before installing the XSS, however, please verify the following:

- Be sure to login to the server as a local administrator (with Server 2003, a Domain Admin is not guaranteed all the necessary rights, so Ensure recommends a local administrative account be used).
- If using an SQL database on a different server than the XSS, make sure to have MDAC version 2.7 or later installed on the server that has the XSS Service. These files are necessary to facilitate the communication between the XSS service and the SQL database.

To install the XSS Server

1. Run the “XSS_Daemon_5xx.exe” file.
2. Read and Accept the License Agreement
3. Enter the IP address of the machine you are running on if it is not found by default:



The screenshot shows a dialog box titled "XSS IP Address". The main area contains the instruction "Enter the IP address that the XSS will be running on." Below this instruction is a text input field with the IP address "10.10.10.1" entered.

4. Enter the IP address of the SQL server. If a named instance is used in SQL, then enter the address with the instance name on it (“<server address>\<instance name>”).
 - a. Again, if using SQL 2008 Express, even the default instance is considered “named” and must be entered as such. Generally this format is “<server address>\SQLEXPRESS”

SQL Server IP Address

Enter the IP address of the PC that is running the SQL Server.

10.10.10.1

5. Enter the credentials created during the XSS-DB installation for access to SQL.

SQL Credentials

Please enter your SQL credentials.

Username: xyloc

Password: xxxxxx

Confirm Password: xxxxxx

6. The installer will attempt a connection to the SQL database with the address and credentials provided to verify. A confirmation box will appear to whether or not that connection was successful.
7. Select the setup type appropriate for the hardware that is being used. If using Japanese hardware, then use the “Japanese Lock” option. For all other locales use the “US Lock” option

Setup Type

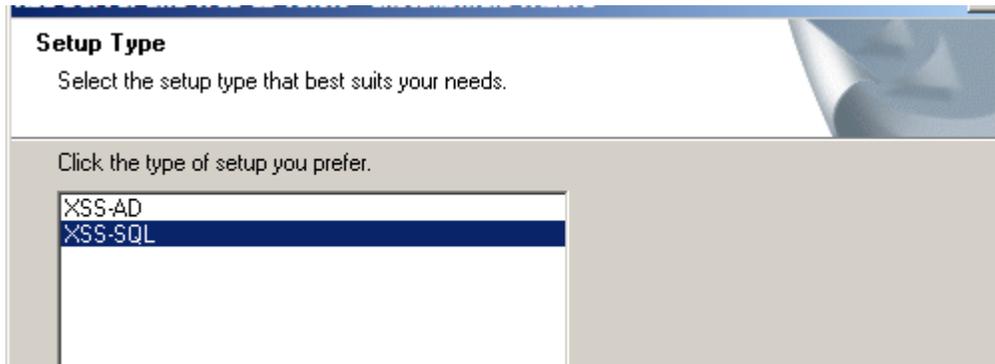
Select the setup type that best suits your needs.

Select from the types of XyLoc lock locales below:

US Lock

Japanese Lock

8. Select “SQL” for the XSS format



9. Select "Finish" when completed

Installing the XSS Web Configuration Tool (WebUI)

The XSS WebUI server can be installed on any server that has access to the SQL server via TCP connection. Before installing the WebUI, however, please verify the following:

- Be sure to login to the server as a local administrator.
- Within the IIS manager, verify that the Default Web Site service is running. The installation will abort if IIS is not installed.
- Make sure to have .NET Framework 2.0 or higher installed.
- If using an SQL database on a different server than the XSS, make sure to have MDAC version 2.7 or later installed on the server that has the XSS. These files are necessary to facilitate the communication between the XSS service and the SQL database. If this is not installed the installation will abort as well.

Installation:

1. Run the "XSS_WebIIS_5xx.exe" file.
2. Enter the IP address of the server on which the installation is being done.
3. On the XSS License Count screen, enter the correct number of licenses that were purchased. If you are going to install in Evaluation mode, enter 10 users or less. Click "Next".



4. On the next screen, you will be prompted for a Company Name and Password. For a purchased version, this password must be obtained from Ensure Technologies. You should have received a document with the software with all of the necessary information to register

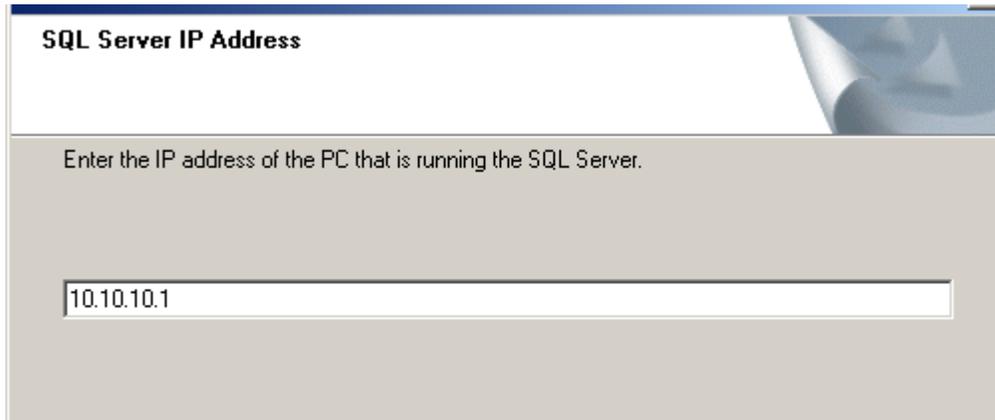
your software and obtain a password. If not, or if another registration is needed, please contact Ensure Technologies Technical Support. **NOTE:** The password that is obtained from Ensure Technologies is only valid for one installation. Once the password is used during the installation process, it cannot be used again. Because of this, make sure that you have finalized your choice for the Server you will be installing on, and make sure that this server is ready for the XSS to be installed prior to starting the XSS installation process. **NOTE:** For an evaluation version (10 users or less), you can skip the following step for retrieving a password from Ensure.

5. The password for the purchased version can be obtained from Ensure Technologies by calling 734-668-8800. To obtain a password online:
 - Copy the XSS Serial Number generated during the install process exactly as it appears.
 - Go to <http://www.xyloc.com/xssreg.aspx>

The screenshot shows a web browser window titled "http://www.ensuretech.com/xssreg/xssreg.html - Microsoft Internet Explorer". The address bar shows "http://www.ensuretech.com/xssreg/xssreg.html". The page content is titled "XyLoc Security Server License Registration". Below the title, there is a message: "Thank you for purchasing XyLoc Enterprise, XyLoc Enterprise AI or XyLoc MD. Please complete the following form to register your license for the XyLoc Security Server." This is followed by a warning: "Your XSS license can only be registered once, and the resulting XSS serial number and password are only good for the installation you are about to perform. **If you are not ready to install the XyLoc Security Server, please do not register your license at this time.**" A final note says: "Please keep a copy of your XSS serial number and password in a safe place. You will need these to obtain future upgrades or support from Ensure Technologies. If you have any questions about this process, please contact Ensure Technologies at 734-668-8800 or email us at support@ensuretech.com". The form is divided into two sections: "Purchase Information" and "Customer Information". The "Purchase Information" section has three fields: "Reseller's Company Name", "XSS License Number", and "XSS Serial Number". The "Customer Information" section has five fields: "Company Name", "Contact Name", "Address", "Phone Number", and "Email". A "Process" button is located at the bottom of the form.

- Enter the Reseller's Company name how it appears on the document provided by Ensure Technologies.
- Enter the XSS License Number how it appears on the document provided by Ensure Technologies.
- Enter the XSS Serial Number generated during the install process.
- Fill in all Customer Information fields.
- Click "Process"
- The screen should refresh and there should be a password at the bottom of the page.

6. Enter your Company Name in the Installation Wizard and then enter the password retrieved from the previous step exactly as it appears. If an Evaluation version is being used (10 users or less), enter the default password of “ensure” (w/out the quotes).
7. Click “Next” on that screen to proceed with the installation.
8. Read and Accept the License Agreement.
9. Enter the IP address of the SQL server. If a named instance is used in SQL, then enter the address with the instance name on it (“<server address>\<instance name>”).
 - b. Again, if using SQL 2008 Express, even the default instance is considered “named” and must be entered as such. Generally this format is “<server address>\SQLEXPRESS”.

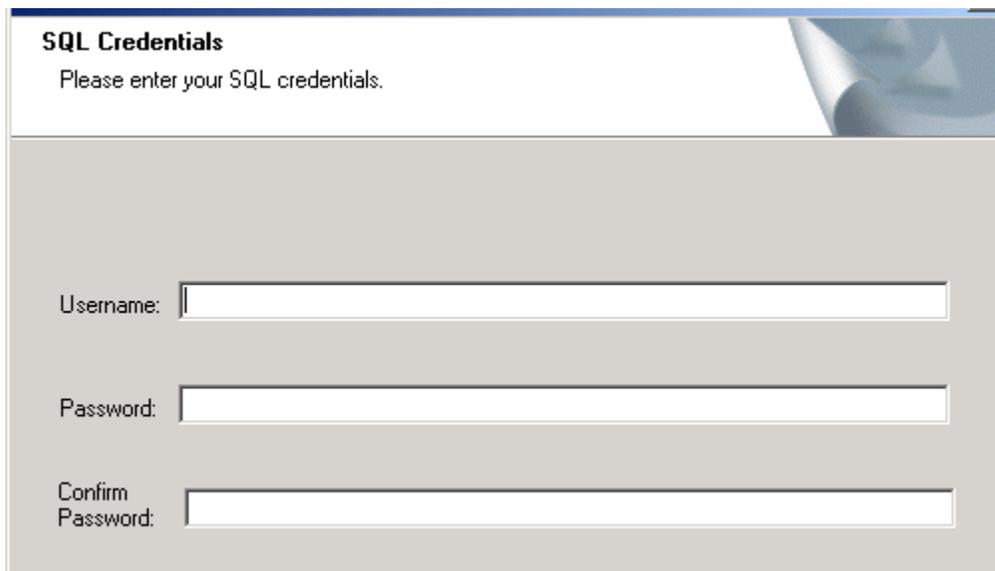


SQL Server IP Address

Enter the IP address of the PC that is running the SQL Server.

10.10.10.1

10. On the next screen, enter the username and password of the SQL account that you will be using. They are case sensitive so make sure to enter them exactly. Click "Next".



SQL Credentials

Please enter your SQL credentials.

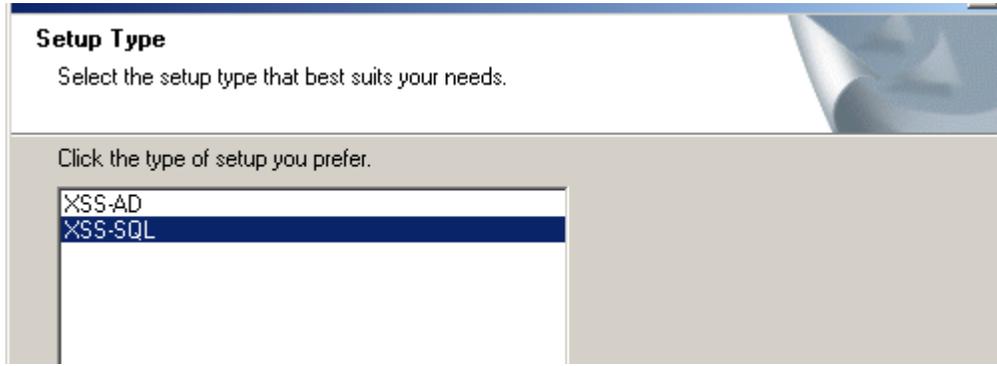
Username:

Password:

Confirm Password:

11. If the credentials and IP address are correct, you should receive a message that states that the login to the SQL server was successful. Click "OK".

12. Select the type of XSS that you are using again. Select "XSS-SQL" and click "Next".

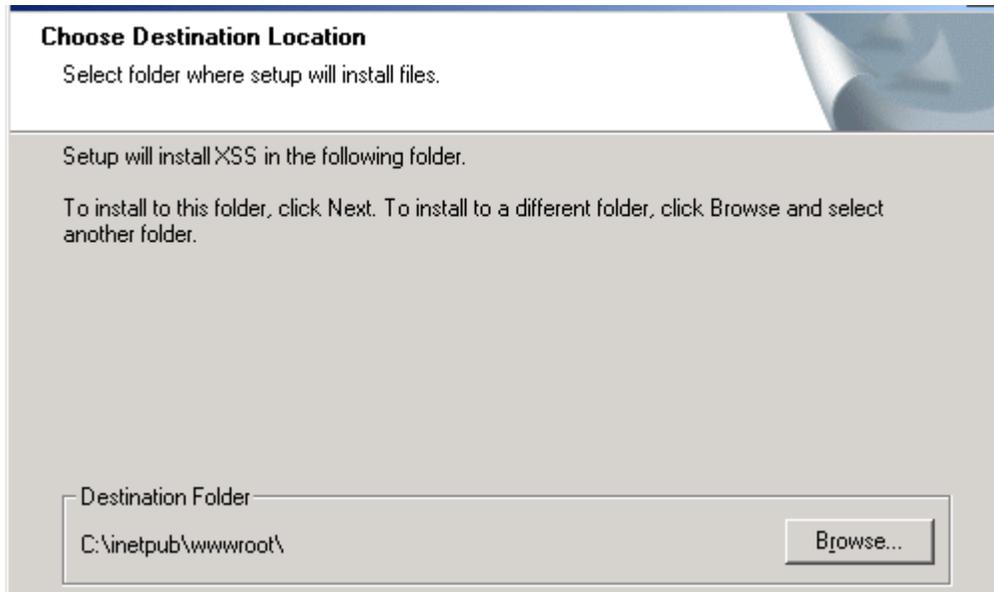


Setup Type
Select the setup type that best suits your needs.

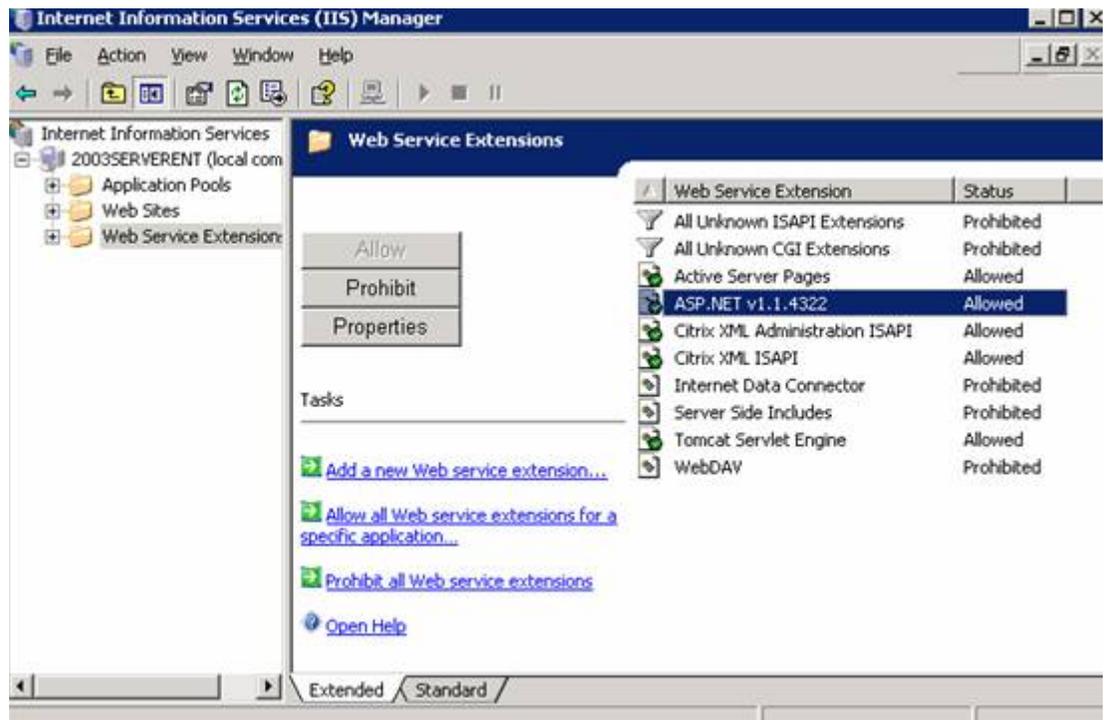
Click the type of setup you prefer.

- XSS-AD
- XSS-SQL**

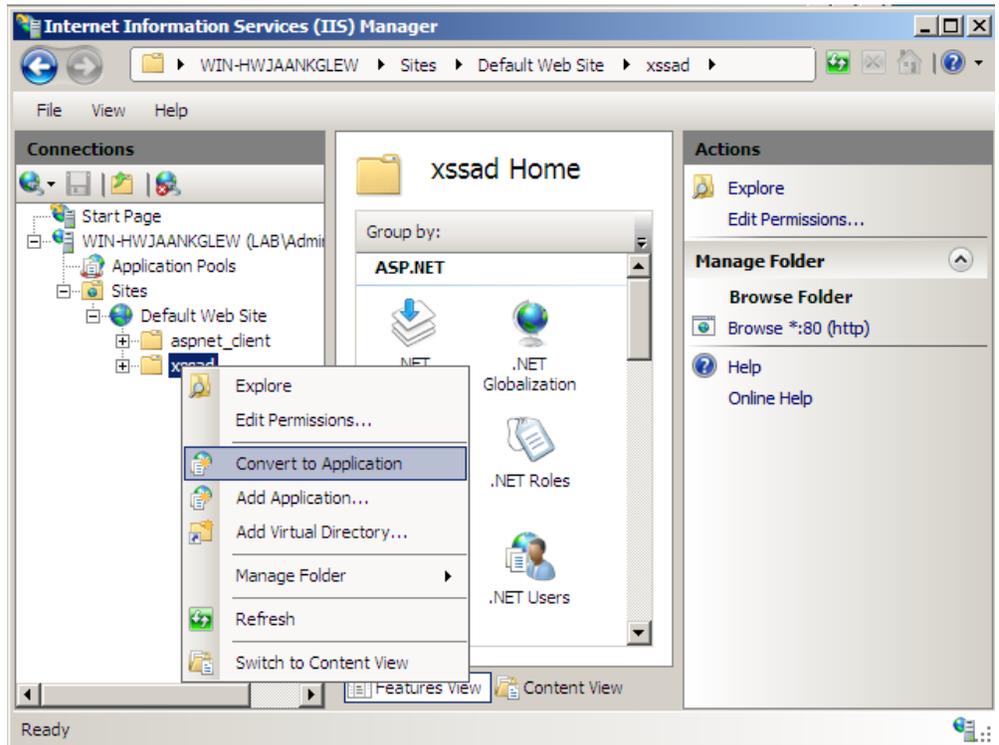
13. Choose the destination location. The default path is the default for IIS. Click "Next".



14. You may see a command line screen open up and the software will install the ASP.NET.
15. When the installation is completed, click "Finish".
16. Configure IIS
 1. If using Windows Server 2003, in IIS, under the "Web Service Extensions", the options for "ASP.NET" and "Active Server Pages" must be allowed.



2. If using Windows Server 2008, the XyLoc Web Site in IIS must be converted to an "Application". Go to the IIS Manager, under the default website and right click on "XSSAD" and then click on "Convert to Application" on the pop-up menu.



Then accept the defaults on the next window and click “OK”.

Upgrading from previous installation of XSS:

Upgrading from XSS 2.x.x (Codebase) version

Before you begin upgrading the XSS from Version 2.X.X, to 4.X.X we strongly recommend that you first backup your current XSS Database files. Also, if possible, we recommend that you bring up the 4.x.x server on a separate server from the 2.x.x version. Because of some incompatibilities between the 7.x.x version of the XyLoc client and the latest version of the XSS, you will need to upgrade your clients to a new client version as well.

1. If you have an existing XSS installation (XSS version 2.2.x or older), you will want to back up your database files (usually found in c:\ensure\xyloc\dbfiles). If you cannot install the 4.x.x version on a second server, then you will need to uninstall the previous XSS. After uninstalling you must reboot the PC. If you are able to install on a second server, then copy your backup of the DBFiles directory somewhere on the new server. You will be able to convert your existing Codebase database to the new SQL database.
2. Install XSS 4.x.x. Near the end of the installation, an SQL script will run that will create a “XyLoc” database on the SQL server (or MSDE). It will also create all of the necessary tables for configuration purposes and will also install one user for administrative purposes. The username is “XSSAdmin” and the password is “ensure” (both the username and the password are Case Sensitive). You can use this username/password for your initial logon to the XSS-Enterprise system.
3. Locate the database migration program found on the XSS installation disk. If the utility is not included, please contact Ensure Technologies for the latest Migration tool.
4. Copy these files to the directory where your previous XSS installation’s database files are located. Double-click on **XSS Database Migration.exe**.
5. Follow the prompts on the screen to convert the database from Codebase to SQL format and copy to the appropriate location.
6. A file named “xss-database_conversion_results.txt” will be created in the same folder where you executed the database conversion program. This file will tell you how many records were converted for each table.

Upgrading from XSS 3.x.x or 4.x.x versions

Follow the same steps as above for 2.x.x, except that the file **XSS Database Migration.exe** can be run from any directory for 3.x/4.x migrations. It is still a good idea to backup the existing database before uninstalling the existing XSS installation. Also, for XSS 4.x, only uninstall the previous XSS installation, not the XSS-DB installation.

1. Backup the existing SQL database.
2. Uninstall the previous XSS
3. If running on Windows 2000 Server, a reboot is required to completely remove the service. If running on Windows Server 2003, this is not necessary.
4. Extract all of the files from 'XSS Database Migration.zip' to a location on the Database server (server that is running SQL and has the XSS database)
5. Run the file 'XSS Database Migration.exe' and select the appropriate 'XSS-SQL 3.x' or 'XSS-SQL 4.x' option for the version you are upgrading from.
6. Install latest XSS 4.x.x version

Upgrading from earlier XSS 5.x.x versions

If upgrading from an earlier version of 5.x.x the specific steps for upgrade will depend on the version that is being used currently and the version that is being upgraded to. Please contact Ensure Technologies Technical Support for proper upgrade instructions.

Overview on XSS Web Interface

Accessing the XSS

To access the XSS, go to your WEB browser and type the address of the XSS along with the directory path. An example would be **http://10.10.10.10/XyLoc/xss.aspx**



Default username: *XSSAdmin* (case sensitive)

Default password: *ensure* (case sensitive)

XSS Administrative Accounts

Once administrative control of the XSS has been established, Ensure Technologies recommends configuring another user as an XSS administrator. This is not a Microsoft or Novell Administrator, just an administrative user for this application. An XSS Administrator must also be a valid user, even if that user is not assigned to any hosts/groups. Generally this is an existing individual which also has a valid XyLoc user account.

1. Select a valid XyLoc user in the XSS Database
2. Once the user is chosen, select "Edit Info"
3. Set the "XSS Access Type" as "XSS Administrator".
4. Enter a new password, confirm it, and then select "Update".
5. **NOTE:** The XSS requires at least 6 characters for the XSS Administrator password. If successful, a message will be shown at the bottom indicating "Update User Info Succeeded". If not, then a message will be shown at the bottom indicating "Update User Info Failed" and the information will not be saved.

IMPORTANT: If an XSS Administrator fails on the XSS Login three times, the account will be locked out. Another XSS administrator will have to login and unlock the account. If there is only one XSS Administrator, or if there are more than one but all but one has been locked out, the one account left will not lockout. The XSS will not lockout the last user preventing anyone from being able to access the XSS.

XSS Help Menus

For each option in the XSS you should see a picture of a question mark  to the right. This is a link to the help menu for that option.

Status

After a successful login, the next screen is the XSS Status screen. This is the main screen for the XSS, all configuration options and log files can be viewed or configured from this screen.



View XyLoc Client Authentication Events:

The XyLoc Authentication Events provide filters for the Host Name, User Name, Key ID, and Personal Name. This report is useful for the system administrator to perform a security audit.

View XyLoc Client Host Events:

The XyLoc Client Host Events provide filters for All Hosts and Host Names. This report is useful for the system administrator to perform a security audit.

View XSS Administrator Events:

The XyLoc Administrator Events provide filters for Group Name, Host Name, and User Name. This report is useful for the system administrator to keep track on what changes have been made to the XSS database.

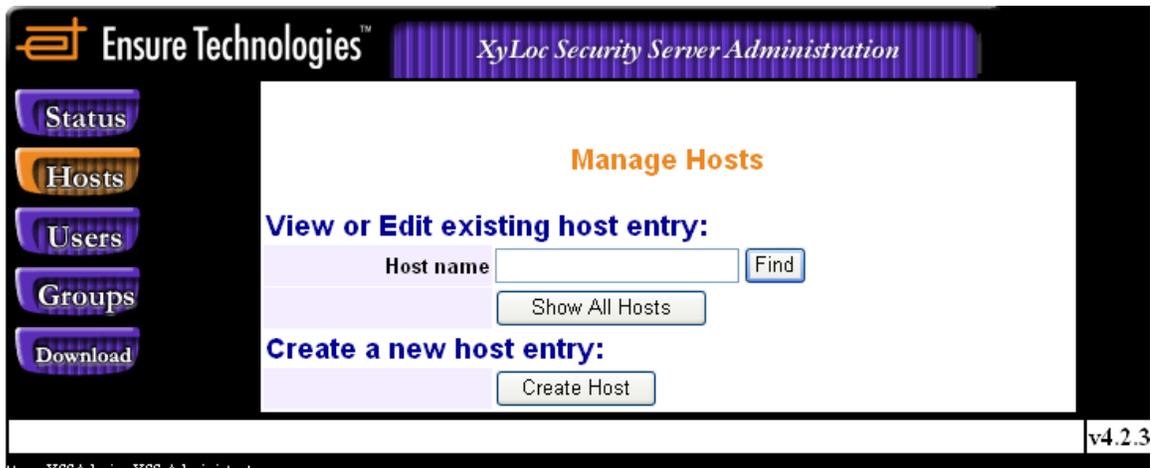
View Key Status Report:

The XyLoc Key Status Report provides a log of low battery status warnings from each key. This log is used to identify which keys will need to have their batteries replaced before they fail.

Hosts

Hosts are the machines (or PCs) that have the XyLoc client software installed and have been learned by the XSS. By clicking on hosts, one can view or edit the existing host information. A specific host name can be entered or click “Show All Hosts” to see all of the available hosts.

A Host can also be created manually and assigned to the appropriate Group(s)/User(s). Click the button for “Create Host” and then assign the Hostname and IP address for that Host.



Users

This is the screen where you manage the user database. Users are defined as being either kiosk or unique.

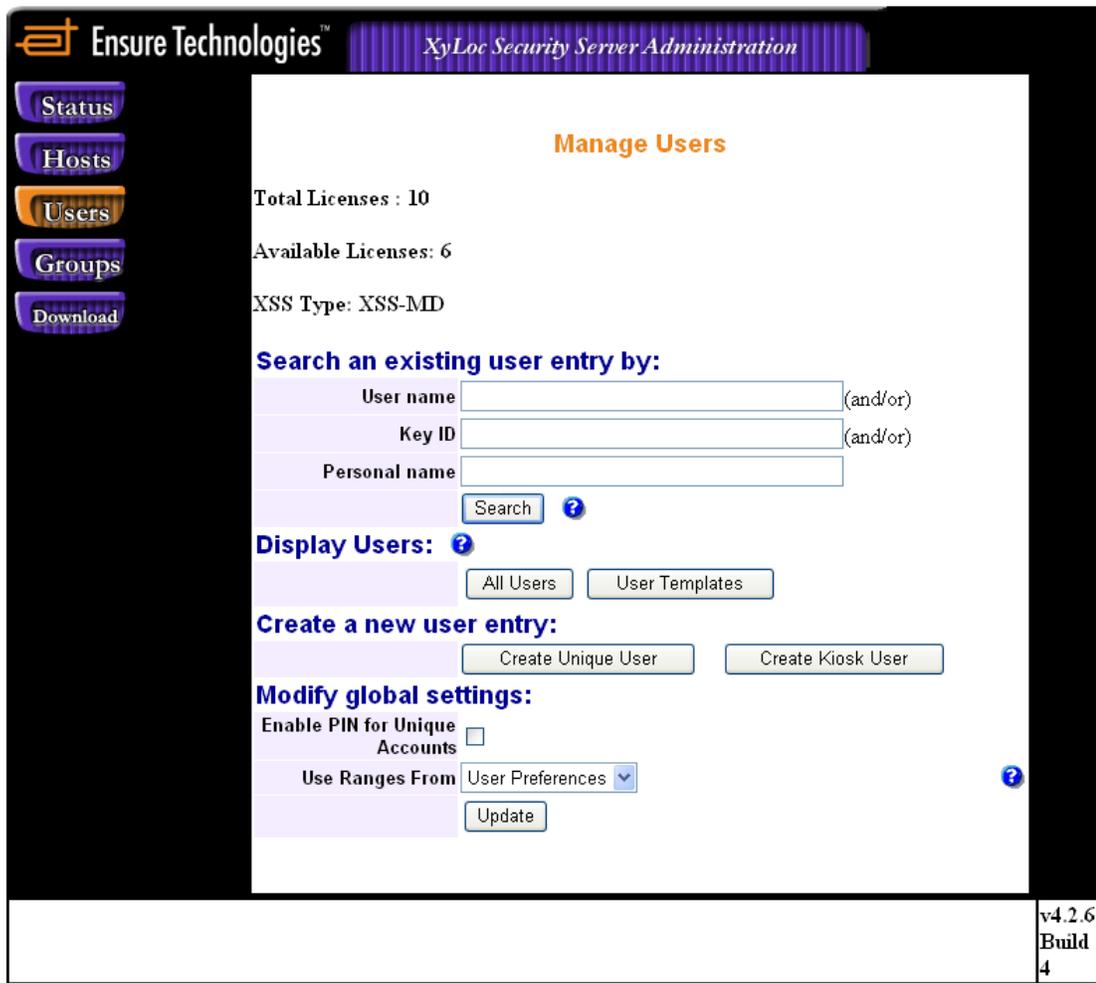
- **Unique Account:** Each user has his/her own Microsoft and/or Novell logon to the PC itself and a key is assigned to this user’s own logon account.
- **Kiosk Account:** A Kiosk account is defined by multiple users sharing one Microsoft/Novell Logon and one profile. Each user has his/her own XyLoc Key so they are still unique to the XyLoc System and is audited as such, however all share a common logon account and desktop, providing much faster access to the PC and their shared applications.

This is also the screen where some “Global” settings were available. These settings will apply across the XSS installation.

- **Enable PIN for Unique Accounts:** This is a checkbox that will enable the ability to use a XyLoc PIN for use with Unique accounts (requires XyLoc Client version 8.3.7 or later). In previous versions, a unique account had to use the user’s own Network or Windows Logon password.
- **Use Ranges From:** This is a drop down box that has two options
 - **User Preferences:** Uses the Lock/Unlock ranges defined in the user (or group) settings

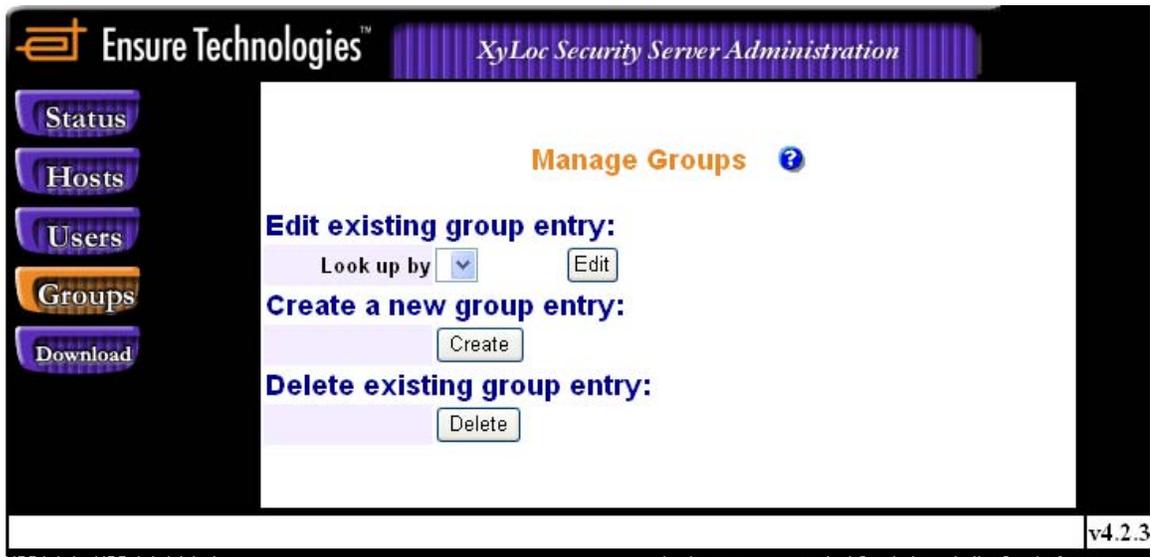
- **Host Preferences:** Uses Lock/Unlock ranges as they are defined in each individual host (NOTE: Host based ranges are not supported in groups and must be defined on each host individually)

This screen also shows the Total and Available Licenses on the XSS.



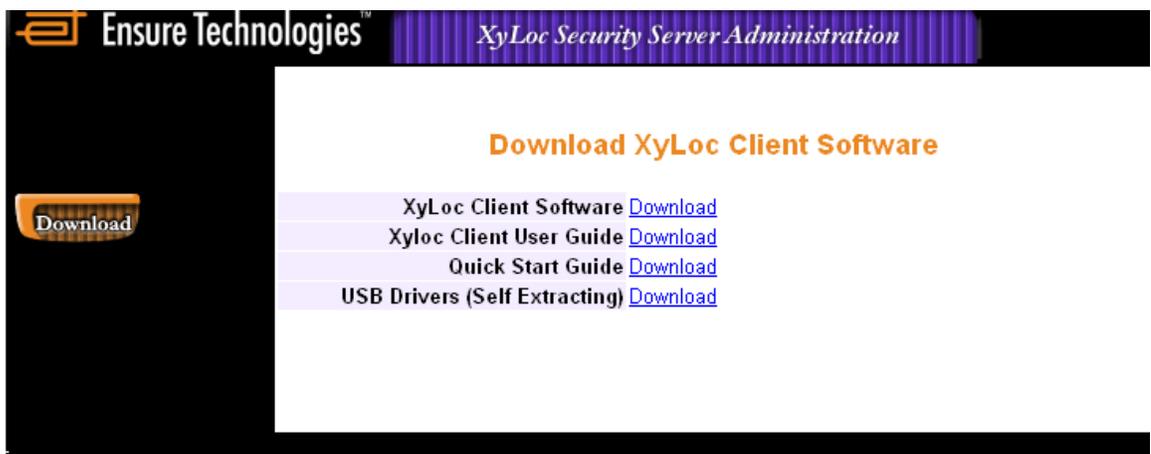
Groups

Groups are created and edited from this screen. A Group is a number of unique user or kiosk user accounts sharing the same XyLoc preferences across a group of Hosts. Groups must contain both Users and Groups.



Download

The XyLoc software, USB drivers, and user manuals are available from the screen. This is a convenient way to provide updated XyLoc software from the download directory on the XSS. When updating the XyLoc software on the host, user configurations are not changed. The Download button is available without having to login to the XSS, allowing non-XSS Administrators to install the XyLoc Client software.



Managing User Accounts and Settings

Planning

When configuring the XSS Groups and Users, it is important to define the environment and desired arrangement before starting this configuration. Changes can always be made afterward, however with some pre-planning, these changes can be minimized. The following terms and steps are provided to assist in this process.

- **Unique user account:** a unique user is one XyLoc key permitted to access a single system login account (NT or Novell). A host can have more than one unique user and a unique user can have access to multiple hosts.
- **Kiosk user account:** a kiosk user is one of many XyLoc keys permitted to access a single system login account (NT or Novell). A kiosk user can have access to multiple hosts. Each kiosk user has a unique XyLoc password.
- **Host:** a name of the machine (or PC) that has the XyLoc software installed.
- **Groups:** a number of unique user or kiosk user accounts sharing the same preferences. When configuring a group, all users within this group share its defined settings on all Hosts that are in this group unless “inherited” is disabled (default is enabled). When disabled, the user preferences will now take precedent over the group settings.

Creating a New User

Use the following steps to create a new user account.

1. Click button on the left for “Users”

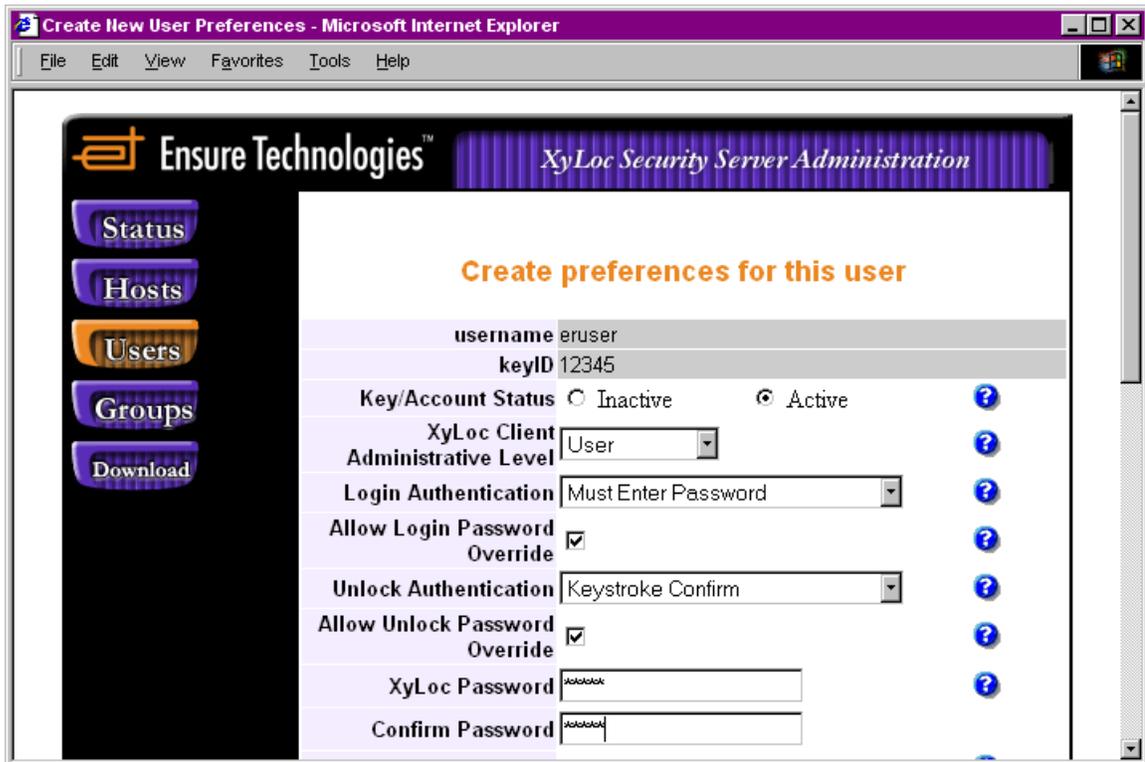
The screenshot displays the 'Manage Users' page within the XyLoc Security Server Administration interface. On the left, a vertical navigation menu contains buttons for 'Status', 'Hosts', 'Users' (highlighted in orange), 'Groups', and 'Download'. The main content area features the title 'Manage Users' in orange. Below the title, it shows 'Total Licenses : 100' and 'Available Licenses: 99'. The 'XSS Type: XSS-MD' is also displayed. A search section titled 'Search an existing user entry by:' includes input fields for 'User name', 'Key ID', and 'Personal name', each with '(and/or)' to its right. A 'Search' button and a help icon are positioned below these fields. Underneath, the 'Display Users:' section has a help icon and two buttons: 'All Users' and 'User Templates'. The 'Create a new user entry:' section contains two buttons: 'Create Unique User' and 'Create Kiosk User'. At the bottom of the interface, a status bar shows 'User: XSSAdmin- XSS Administrator' on the left and 'Look up a user, or select Create to go to the Create Us' on the right.

2. Click the button for “Create Unique User”.

The screenshot shows the 'XyLoc Security Server Administration' web interface. On the left is a navigation menu with buttons for 'Status', 'Hosts', 'Users', 'Groups', and 'Download'. The 'Users' button is highlighted. The main content area has a title 'Create a new user entry in the XSS database.' and a form with the following fields and options:

- * username: text input field with a help icon (?)
- * keyID: text input field with a help icon (?)
- Personal Name: text input field with a help icon (?)
- XSS Access Type: radio buttons for 'User(No Access)' (selected) and 'XSS Administrator' with a help icon (?)
- Administrator Password: text input field with a help icon (?)
- Use As Template: checkbox with a help icon (?)
- User Template Name: text input field
- Buttons: 'Create', 'Clear', and 'Back'

3. Type in the username (this would be the valid Microsoft NT or Novell network login name) and Key ID in the respective fields. The Key ID is the number found on the back of the key in the lower right hand corner of the Key (i.e. “KeyID: 12345”).
4. Type in a specific personal name for this user that will identify them. This is simply a real text name and does not have any requirements, however make sure that it is unique to this user.
5. Set the XSS access level for this account. Typically this would be a “User”, however this is the screen on which you can make a user an XSS Administrator. If you choose to make them and Administrator, you must give them a password of at least 6 characters.
6. Click the button for “Create”.
7. Next set preferences for this account. If used in a group, the preferences in the group setup that are inherited will take precedent over those same settings that are set here for the individual user. Only those settings which are not “inherited” from the group need to be configured at this point. If the user is not in a group, then there is also the option to assign them directly to the host. NOTE: A user MUST be assigned to a host either directly or through a group (not both) for it to work on the desired PC.

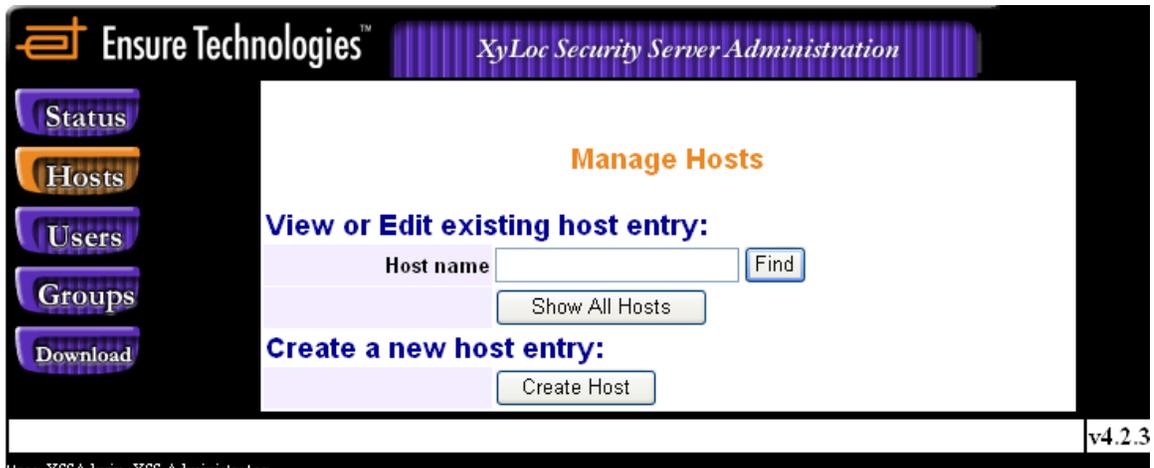


8. The XyLoc password setting is NOT included in the group settings. This password is only used if the account is a Kiosk account. For a unique account, the user's normal logon password will be cached as their XyLoc password at the first logon to a PC. NOTE: If the user is set for "Must Enter Password" for the Login Authentication, then they will be required to use a password the first time they approach the PC. However, XyLoc will not have cached their network logon password, so that password cannot be verified by XyLoc. The first logon they can use their actual KeyID number for the password, and then once they get through the Microsoft/Novell login screen, their network password will be cached and they will use that password from that point forward.
9. Click on the button for "Update" when finished.

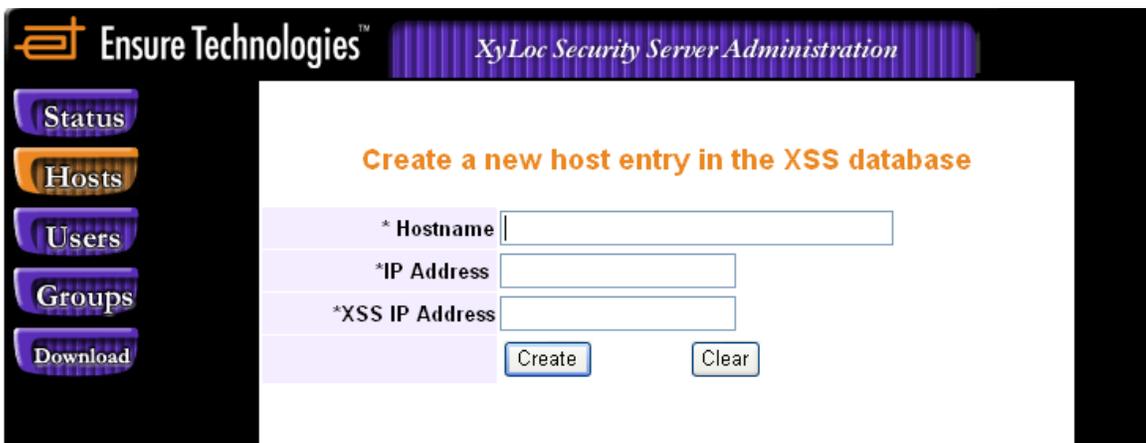
Create the Host manually (if desired)

Starting with XSS 4.1.9, the hosts can now be created manually. Previously only those PCs that had the XyLoc client installed and pointed to the IP address of the XSS would be available. This allows you to create the host ahead of time and assign the appropriate users/groups before installing to make deployment easier.

1. Click the button for “Hosts”



2. Click the button for “Create Host”
3. Enter the following information:
 - a. **Hostname** – Computer Name assigned to the PC
 - b. **IP Address** – This field is a dynamic field to support DHCP, so the address entered here does not have to be correct at this time. The correct address will be learned when the client communicates to the XSS for the first time. However, it is a required field, however, so an address must be entered.
 - c. **XSS IP Address** – Enter the IP address of the XSS so this will match what will be configured in the client. If this is not entered properly, this will overwrite the address specified in the client when it first communicates to the XSS.



4. Click “Create”

The screenshot shows the 'Host Information' configuration page in the XyLoc Security Server Administration interface. The page is titled 'Host Information' and contains several sections of configuration options:

- Fully-qualified host name:** ERPC1
- Description:** [Empty text box]
- Location:** [Empty text box]
- XyLoc Lock Attached To:** USB (dropdown menu)
- Minimum Password Length:** 1
- XSS Servers and Ports:** A table with columns 'Server' and 'Port'. The first row contains '192.168.1.32' and '5102'. The second row contains an empty server field and '5102'. The third row contains empty fields for both.
- XSS Client Port:** 3510
- Log Records To Upload:** 1 records(s) (1 - 20 records)
- Lock Range:** Medium [9] (dropdown menu)
- Unlock Range:** Medium [5] (dropdown menu)
- Kiosk Settings:**
 - Account Name:** [Empty text box]
 - System Account Password:** [Empty text box]
 - Enable Unique Account Display:**
- Last Updated:** Monday 6/19/2006 11:41:34 AM

At the bottom of the form, there are buttons for 'Update', 'Delete', 'Manage Users', and 'Manage Groups'.

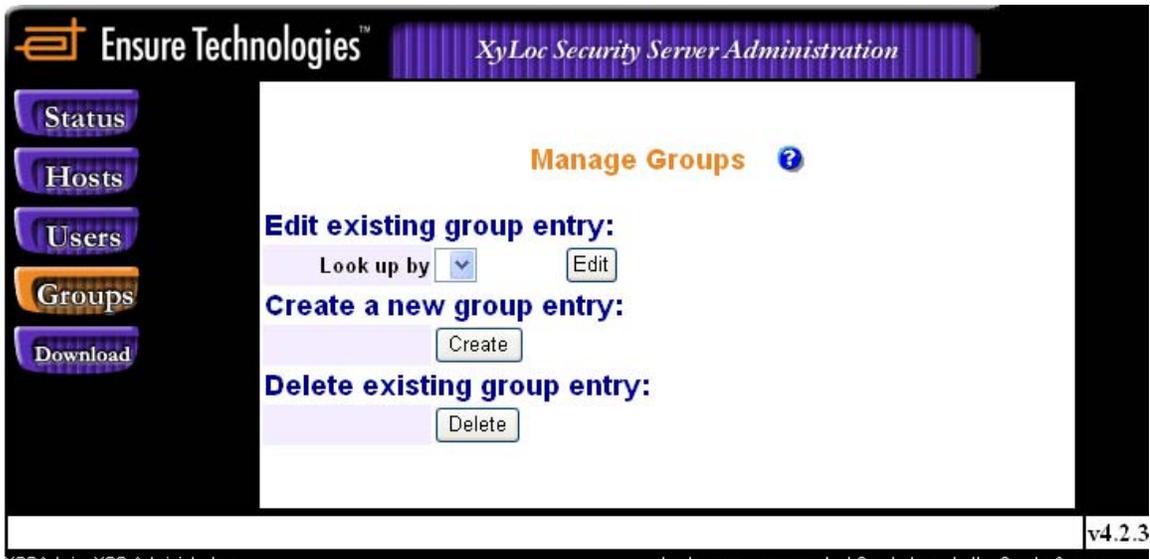
5. If using a Kiosk on this host, enter the “generic” PC/Network login ID and password that will be used for the Kiosk on this PC in the “Kiosk Settings” fields. NOTE: At this time this is not a group setting, so must be entered for each PC individually that will be using a Kiosk, even if they are using the same “generic” login account.
6. If users will be using their own unique network login accounts on these PCs, outside of the shared kiosk account, then check the box for “Enable Unique Account Display”. NOTE: This setting will apply across all users assigned to this PC.
 - a. If enabled, then at the initial login, two records are displayed for each XyLoc Key in range. One for their kiosk account (displayed as their personal name, e.g. Doctor Jones) and one for their unique login ID (displayed as their own login name, e.g. djones).
 - b. Once logged in as the kiosk account, each user will only see the kiosk account displayed, even if the “User Can Force Logoff of Locked Workstation” setting is enabled. At this point the user can simply unlock as the kiosk and then logoff gracefully to login with their unique account.

- c. At least one of these settings must be applied (either Kiosk account information, or the “Enable Unique Account Display”) or no records will be authorized for this client. This means that if this host is a single user machine, or if shared but not with a Kiosk account (users still use their unique network logon IDs) then the box for “Enable Unique Account Display” must be checked.
7. If Host-based ranges are being used (as defined in the Global Settings) then set the desired range for this Host. NOTE: If user based ranges are defined in the Global Settings, then the Range fields in the Host will be grayed out)
8. Click “Update” when finished.

Creating a Group

A group is a convenient and easy way to assign attributes and preferences to multiple users for multiple hosts. It is also an easy way to assign users to these Hosts, without having to assign users to each host individually.

1. Click the button on the left for “Groups”.

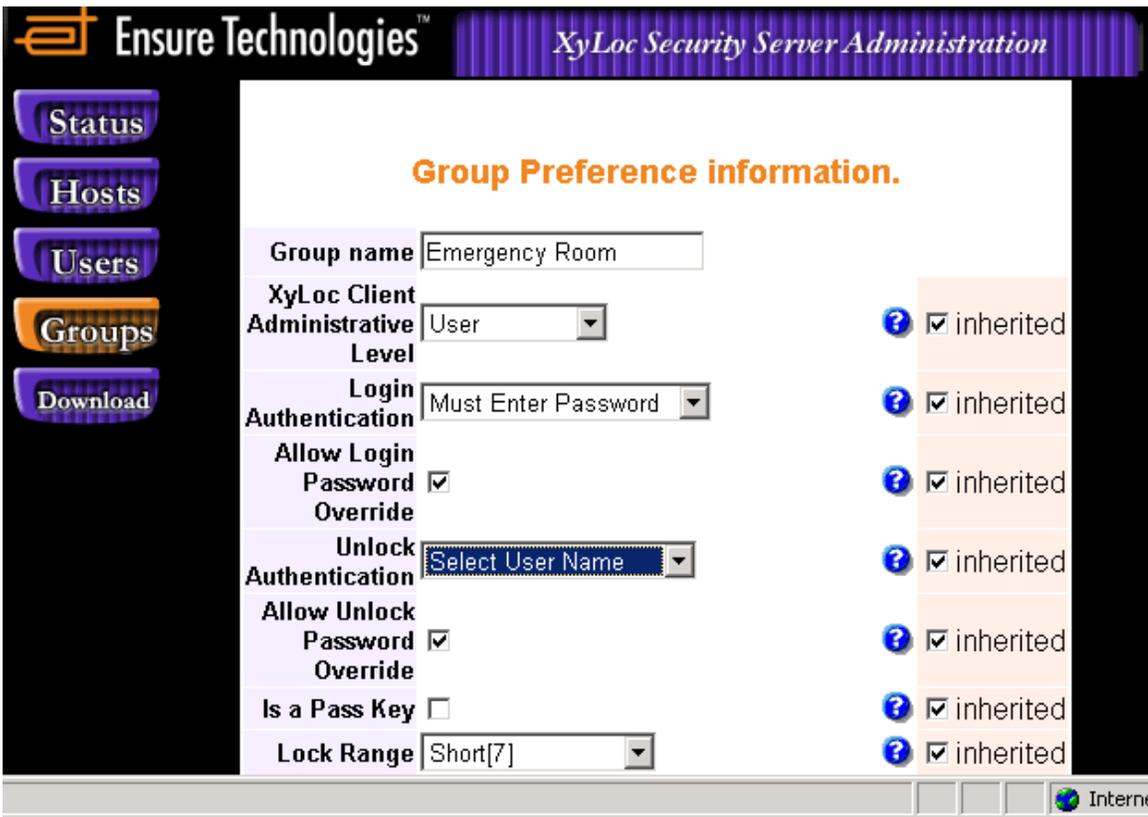


2. Click button for “Create”.

3. Type in a name for the group. There are no specific program requirements for the format of this name, but it should be something unique to this group so it can be distinguishable from others that might be setup. In this example, the Group name will be: **Emergency Room**. Once that is entered, click “Create”.



4. Next adjust preferences for the group. Any preference that has the box for “Inherited” checked will be the same for all members in the group. For any preferences that are NOT desired across the entire field of users in this group, remove the check from the “Inherited” box. For those settings that are not inherited, the preferences that are set in each individual account will be used instead. NOTE: In a Host-based Kiosk account setup, the username and password will be assigned via the host settings, so the “System Account Password” field should not be inherited



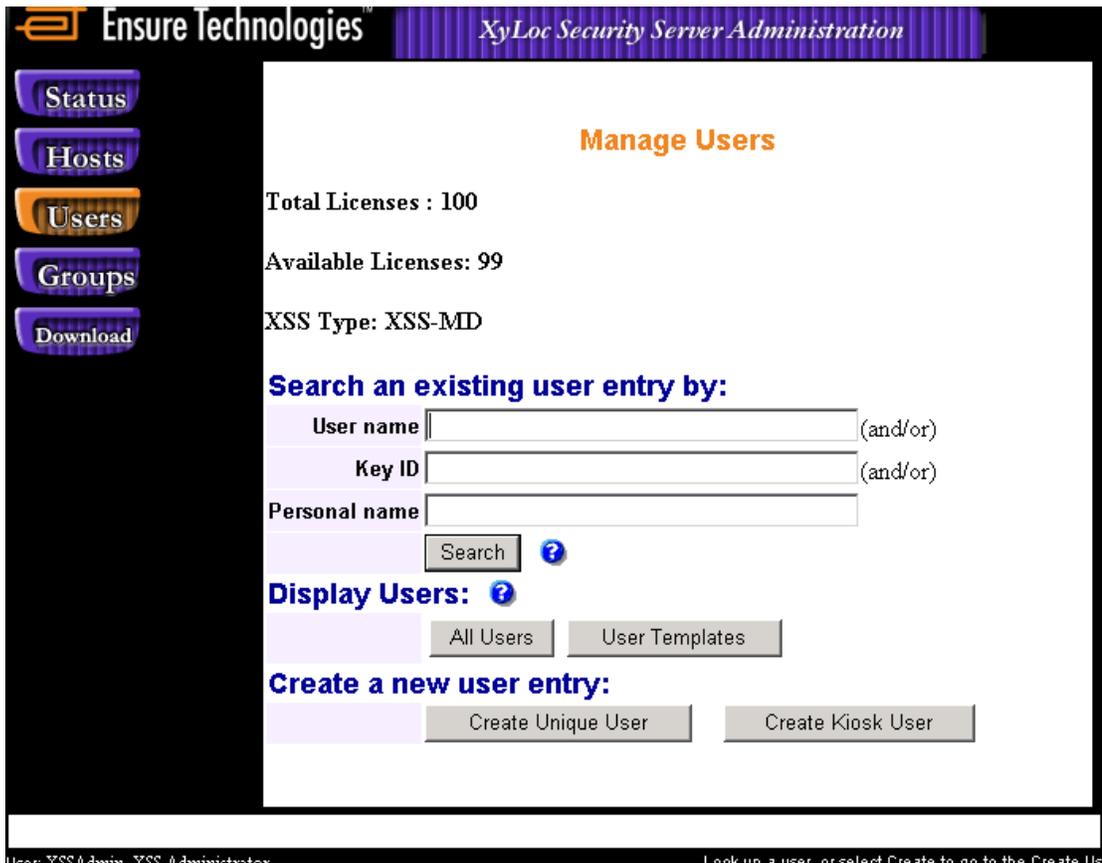
- Once finished setting group preferences, click the “Update” button at the bottom.

Assign Users to a Group

Users can be assigned to a group via the user settings or the group settings.

Assign a user to a group via the user settings

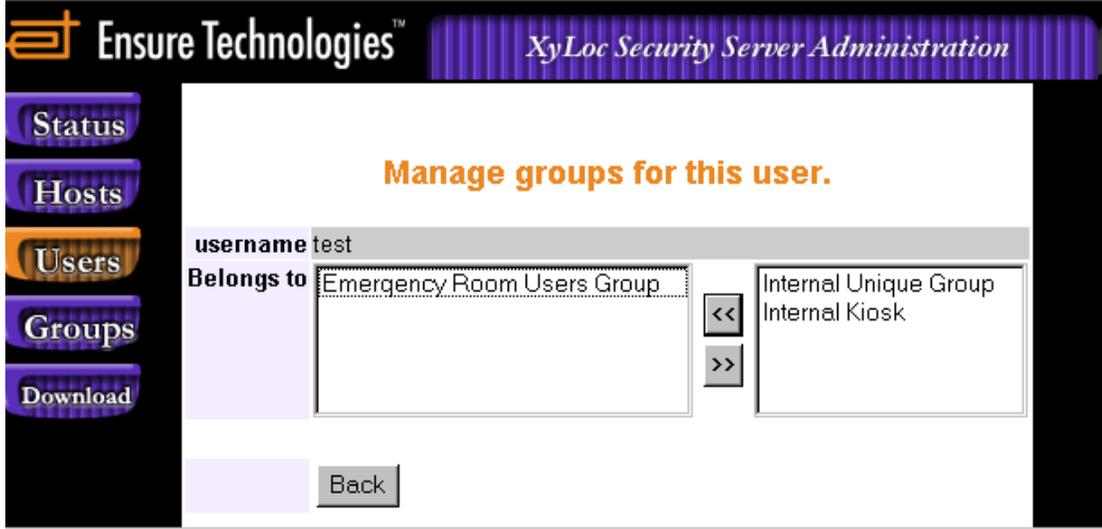
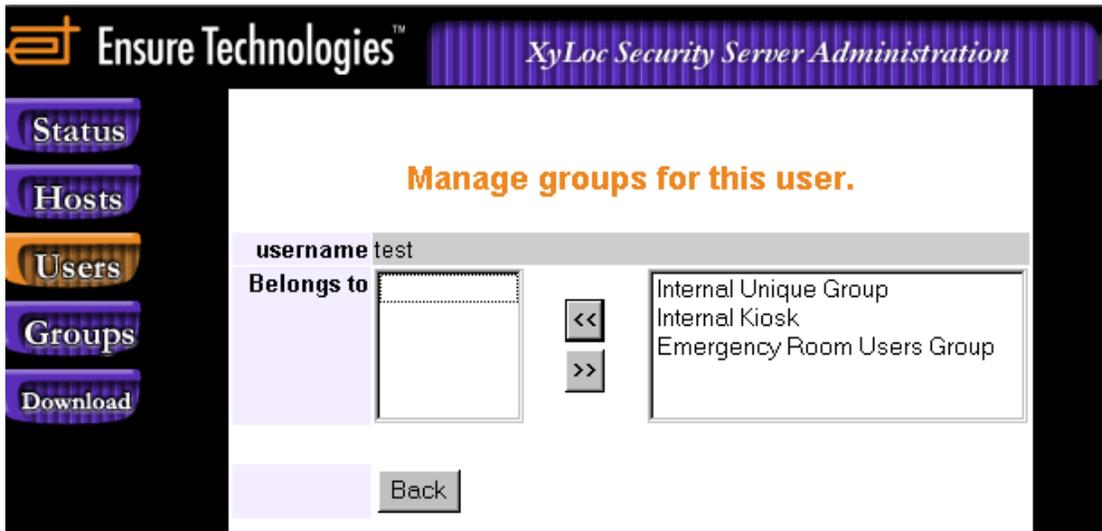
1. Click the button for “Users”.



The screenshot displays the 'XyLoc Security Server Administration' interface. On the left is a navigation menu with buttons for 'Status', 'Hosts', 'Users', 'Groups', and 'Download'. The 'Users' button is highlighted. The main content area is titled 'Manage Users' and shows the following information: 'Total Licenses : 100', 'Available Licenses: 99', and 'XSS Type: XSS-MD'. Below this is a search section titled 'Search an existing user entry by:' with input fields for 'User name', 'Key ID', and 'Personal name', each followed by '(and/or)'. A 'Search' button with a help icon is positioned below the search fields. Underneath is a 'Display Users:' section with a help icon and two buttons: 'All Users' and 'User Templates'. At the bottom of the search section is a 'Create a new user entry:' section with two buttons: 'Create Unique User' and 'Create Kiosk User'. At the very bottom of the page, there is a small footer with the text 'User: XSSAdmin, XSSAdministext' on the left and 'Look up a user, or select Create to go to the Create User' on the right.

2. If the user has not already been created, then click see the section for “Create Unique User”. If the user already exists on the XSS, then select the user either by clicking “All Users” and finding them on the list, or use the search field available here to find them if needed.
3. Click the button at the bottom for “Assign Group”.

4. Select the group to which the user is to be added, then click the left arrows. This group will move to the “Belongs to” window on the left side. Click the “Back” when completed, the user is now in this group.

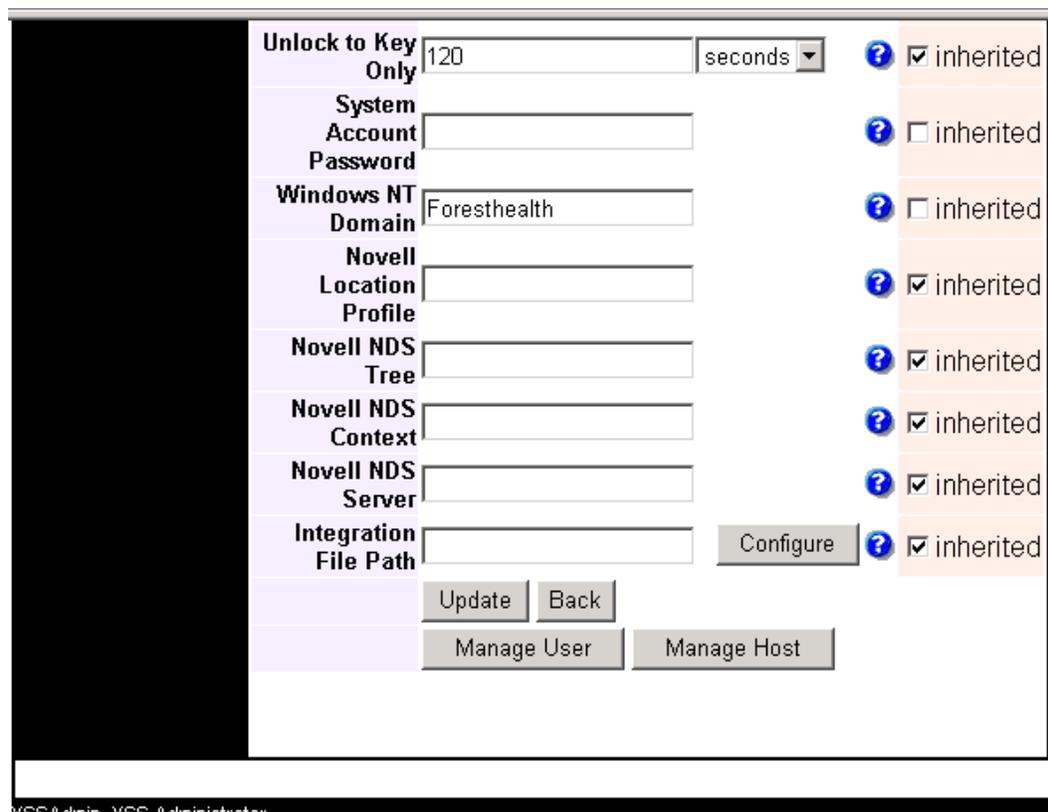


Assign a User to a Group via the Group Settings

1. Click the button on the left for “Groups”.
2. Select the group created above in the drop down menu, and click the button for “Edit”.



3. Scroll down to the bottom and click the button for “Manage Users”.



4. Select the desired users (the “Ctrl” or “Shift” keys can be used to select multiple names), and click the left facing arrows to move them over to the left hand window. The names in the “Available User” box on the right will be listed by their Personal Name that was specified for each user.



5. Click the “back” button to return to the Group Preferences screen. There is no need to click “Update” here, as the User/Group Relationship is updated immediately.

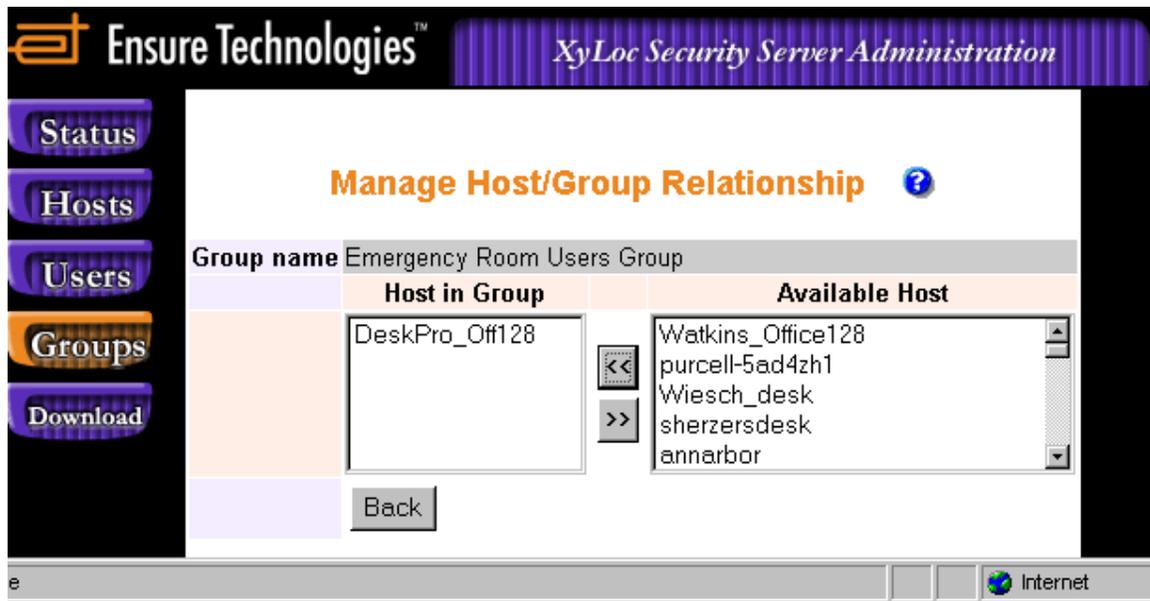
Assign Hosts to a Group

If the host was created ahead of time, then it can be added to the appropriate Group(s) prior to installing the client. If the host has not already been created manually (or if using a version prior to XSS 4.1.9, which did not support manually creation of hosts) then the host will not be available until the installation of the client has taken place and the XSS has learned the Host.

1. Click the button on the left for “Groups”.
2. Select the group created above in the drop down menu and click the button for “Edit”.



3. At the bottom, click the button for “Manage Hosts:”
4. Select the specific host in the right hand window, and click the left-facing arrow to move them to the left hand window (multiple hosts can be selected at one time by holding down the <Ctrl> key on the keyboard and click each host).



5. Click the “back” button to return to the Group Preferences screen. There is no need to click “Update” here, as the User/Group Relationship is updated immediately

Creating a Kiosk

The Kiosk account setup is a “Host-based” Kiosk account. This means that the generic account that is used by all the kiosk users is now defined in the Host settings. With this change, the XSS

now supports the type of environment where each PC has its own unique login that is shared by all users (e.g. each PC logs in with its hostname for the system login name)

NOTE: The legacy method of setting up a kiosk is still supported for those that already have a kiosk setup and need to upgrade for other reasons. The instructions for the Legacy Kiosk setup are also included, for those that have XSS 4.1.9 or earlier, or prefer this method. Please see the section below for **Legacy Kiosk Setup**

When creating a Kiosk account from the XSS, there are several steps that need to be followed. It is very important that these steps be implemented in the following order:

1. The generic network account must be created on the network or PC. This will be the account name and password that will be used to logon to the PC. This may be the same across multiple PC's or might be unique to each PC. The XyLoc software does not have the ability to create accounts in Windows or on the network, so the account must be created using the existing network/PC infrastructure.
2. Create a Group on the XSS with the appropriate preferences that will be shared by all the assigned users and hosts (machines or PCs).
3. Create all the users that will have a XyLoc badge as unique accounts.
 - a. With the Host-based Kiosk, each user in the XSS will have their own unique login account created in the XSS, whether they are going to login with that account or not.
 - b. Each user and XyLoc Key is assigned to a unique network login ID.
 - c. When used in a group, the preferences in the group setup that were inherited will take precedent over those same settings that are set for the individual user. Only those settings which were not "inherited" from the group need to be configured at this point.
 - i. However, the XyLoc Password (often referred to as a PIN) setting is NOT included in the group settings. This is the password that is used only by the XyLoc software, for login or unlock (if the authentication method to require password is selected for these users) as well as password overrides (if allowed). It is NOT necessarily the same password as the Microsoft NT or Novell login.
 - ii. A unique XyLoc Password must be defined when creating each user. The user can change their password later, if desired.
4. Assign the users to the group.
5. If desired, the Hosts can be created ahead of time and assigned to the appropriate group at this time.
6. Any hosts that were not created manually should be learned by the XSS upon the restart after the client installation. Once those are learned, assign the appropriate hosts to the Group.
7. In the settings of each Host, set the Kiosk account ID and password that is to be used on each Host. This may be different on each PC, or may be the same account for each. However, the appropriate account must be set for each host.
8. If using Host-based ranges, set the appropriate ranges on each Host.

Creating a Legacy Kiosk

In the “Host-based” Kiosk, each user is a unique account that is assigned to a host which has a specific Kiosk account defined. The “Legacy” Kiosk setup is one that has multiple records (and therefore multiple keys) created with the same actual login ID and those users are assigned to hosts that do NOT have a kiosk account defined. The kiosk account is defined by the user settings, instead of the host settings. This “legacy” setup is the only method of Kiosk that is supported by XSS version 4.1.9 or earlier. With version 4.2.0 or later, both the Legacy and the Host-based kiosks are supported.

When creating a Legacy Kiosk account from the XSS, there are several steps that need to be followed. Most of these steps are the same as the newer “Host-based” Kiosk, with a few exceptions. It is very important that these steps be implemented in the following order:

1. The generic network account must be created on the network or PC. This will be the account name and password that will be used to logon to the PC. This may be the same across multiple PC's or might be unique to each PC. The XyLoc software does not have the ability to create accounts in Windows or on the network, so the account must be created using the existing network/PC infrastructure.
2. Create a Group on the XSS with the appropriate preferences that will be shared by all the assigned users and hosts (machines or PCs).
3. Create a User Template. This is done by creating a “unique” account first with the generic username, selecting the unique user, and then specifying this as a template that will be used to create the additional users that will share the same username.
4. The template user that is created must be assigned to the Group created in the second step. By assigning the template user to the group, each user created from that template will automatically be assigned to the same group.
5. Each Kiosk user is created using the template. Repeat this step for each user that will be sharing the system account.
6. Next the XyLoc device and software is installed on each host that will be available to these users, if it has not been installed already.
7. Lastly, assign the appropriate hosts to the Group.
8. In the settings of each Host, set the Kiosk account ID and password that is to be used on each Host. This may be different on each PC, or may be the same account for each. However, the appropriate account must be set for each host.

Create a Network Account

Create a generic network account on the Microsoft NT or Novell network server. For this example we will use the name of *eruser*. All the kiosk users will log on to the network using this username and password. However the password will be set for them, and therefore hidden from view. This account can be setup with whatever rights and privileges appropriate for this group of users. There are no specific requirements from the XyLoc software regarding the setup of this account.

Create a Group

A group is a convenient and easy way to assign attributes and preferences to multiple users for multiple hosts. It is also an easy way to assign access to these Hosts, without having to assign each host individually.

1. Click the button on the left for “Groups”.



2. Click button for “Create”.
3. Type in a name for the group. This does not have to be anything in particular, but should be something unique to this group so it can be distinguishable from others that might be setup. In this example, the Group name will be: *Emergency Room*. Once that is entered, click “Create”.

4. Next adjust preferences for the group. Any preference that has the box for “Inherited” checked will be the same for all members in the group. For any preferences that are NOT desired across the entire field of users in this group, remove the check from the “Inherited” box. For those settings that are not inherited, the preferences that are set in each individual account will be used instead.

The screenshot shows the 'XyLoc Security Server Administration' interface. On the left is a navigation menu with buttons for Status, Hosts, Users, Groups (highlighted), and Download. The main content area is titled 'Group Preference information.' and displays settings for the 'Emergency Room' group. The settings are as follows:

Setting	Value	Inherited
Group name	Emergency Room	
XyLoc Client Administrative Level	User	<input checked="" type="checkbox"/>
Login Authentication	Must Enter Password	<input checked="" type="checkbox"/>
Allow Login Password Override	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unlock Authentication	Select User Name	<input checked="" type="checkbox"/>
Allow Unlock Password Override	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is a Pass Key	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lock Range	Short[7]	<input checked="" type="checkbox"/>

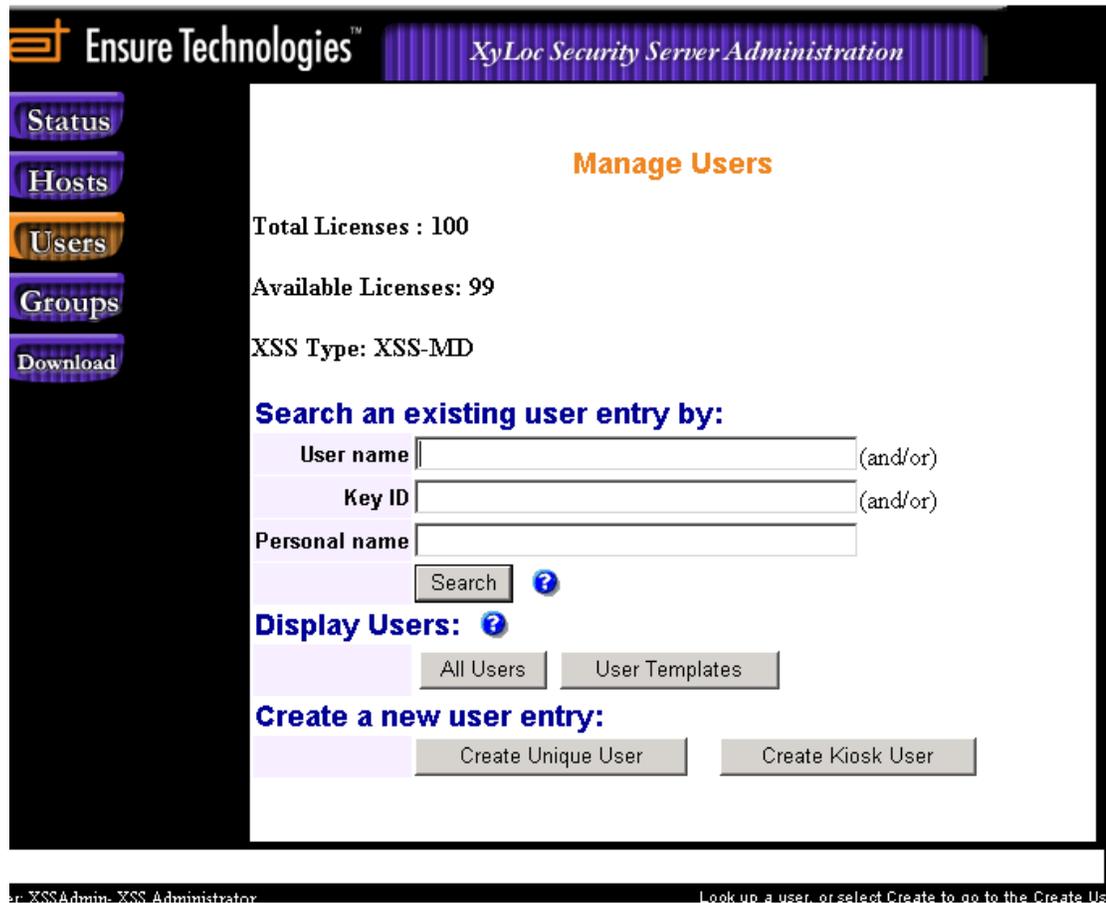
At the bottom of the window, there are several empty buttons and an 'Internet' icon.

5. In a Kiosk account setup, since all the users share the same system account on the network, the “System Account Password” field should be inherited, and the password used for the system account (*eruser*) should be entered here.
6. Each Kiosk user will also share the details of the network setup. Therefore, the specifics of the actual network (Windows NT Domain and/or Novell NDS information) should also be entered appropriately, and inherited.
 - By entering the password and network setup information here, and inheriting the settings, that information is automatically set for each user that is in the group, without having to manually type it in each time a user is created, but at the same time is hidden from each user. NOTE: For security reasons, whatever is entered in the password field disappears, not even asterisks are visible, once “Update” is clicked.
 - Once finished setting group preferences, click the “Update” button at the bottom.

Create a User Template

A template is used to create a list of settings for an account, and then multiple users will be setup to use that same account, with its preferences. This can be an actual user record, or can be a generic record that is only used for the template and not by an actual user. The advantage of creating a generic record, is that you don't have to worry about accidentally deleting the template account if the user that you made the template ever leaves your organization. However, using another record exclusively as a template user will consume a license as you have to give the user a KeyID; even it is not a real number. Either method will function normally, so you can decide which works better for you.

1. Click button for "Create Unique User".



The screenshot displays the 'XyLoc Security Server Administration' web interface. On the left is a navigation menu with buttons for 'Status', 'Hosts', 'Users', 'Groups', and 'Download'. The main content area is titled 'Manage Users' and shows the following information:

- Total Licenses : 100
- Available Licenses: 99
- XSS Type: XSS-MD

Below this is a search section titled 'Search an existing user entry by:' with three input fields: 'User name', 'Key ID', and 'Personal name'. Each field has a '(and/or)' label to its right. A 'Search' button and a help icon (?) are positioned below the fields.

Underneath the search section is the 'Display Users:' label with a help icon (?). Two buttons, 'All Users' and 'User Templates', are provided for selection.

At the bottom of the main content area is the section 'Create a new user entry:' with two buttons: 'Create Unique User' and 'Create Kiosk User'.

At the very bottom of the browser window, a status bar shows the text: 'r: XSSAdmin: XSS Administrator' on the left and 'Look up a user, or select Create to go to the Create Us' on the right.

Ensure Technologies™ XyLoc Security Server Administration

Status
Hosts
Users
Groups
Download

Create a new user entry in the XSS database.

* username ?

* keyID ?

Personal Name ?

XSS Access Type User(No Access) XSS Administrator ?

Administrator Password ?

Use As Template ?

User Template Name

Create Clear Back

2. Type in the username (this would be the Microsoft NT or Novell network login name that was created first. In this example, it would be the *eruser* account) and Key ID in the respective fields. The Key ID is the number found on the back of the key on the label. If you are using a record just for the template, then give it a key that will not be used, like 12345.
3. Type in a specific personal name for this user that will identify them. This is simply a real text name and does not have any requirements, however make sure that it is unique to this user. For this example, “Nurse Ann” will be used. Again, if using a record for the template that will not be used by a user, then you will want to use a personal name that identifies the account as the template (i.e. “Kiosk Template – DO NOT DELETE”)
4. Set the XSS access level for this account (Typically the default of “User”)
5. Put a check in the box for “Use as Template”.

- Type in a name to identify the template. Again, this does not have to be anything in particular, but should be something easily identifiable as what it is for. For this example, the Template name of: *Emergency Room Users Template* will be used.

The screenshot shows the 'XyLoc Security Server Administration' web interface. On the left is a navigation menu with buttons for 'Status', 'Hosts', 'Users', 'Groups', and 'Download'. The main content area is titled 'Create a new user entry in the XSS database.' and contains the following form fields:

- * username: eruser
- * keyID: 12345
- Personal Name: Nurse Ann
- XSS Access Type: User(No Access) Host Administrator XSS Administrator
- Administrator Password: (empty)
- Use As Template:
- User Template Name: ER Users Template

At the bottom of the form are three buttons: 'Create', 'Clear', and 'Back'. The browser's address bar at the bottom shows 'Internet'.

- Click the button for "Create".

- Next set preferences for this account. When used in a group, the preferences in the group setup that were inherited will take precedent over those same settings that are set here for the individual user. Only those settings which were not “inherited” from the group need to be configured at this point. However, the XyLoc password setting is NOT included in the group settings. This is the password that is used only by the XyLoc software, for login or unlock (if the authentication method to require password is selected for these users) as well as password overrides (if allowed). It is NOT the same password as the Microsoft NT or Novell login. You can type in a password for this one user (the other users will have their own unique passwords as well) for XyLoc. If this field is left blank, the user’s KeyID will be assigned as their default XyLoc Password.

The screenshot shows the 'XyLoc Security Server Administration' interface. On the left is a navigation menu with buttons for 'Status', 'Hosts', 'Users', 'Groups', and 'Download'. The main content area is titled 'Create preferences for this user' and contains a form with the following fields:

username	eruser	
keyID	12345	
Key/Account Status	<input type="radio"/> Inactive <input checked="" type="radio"/> Active	?
XyLoc Client Administrative Level	User	?
Login Authentication	Must Enter Password	?
Allow Login Password Override	<input checked="" type="checkbox"/>	?
Unlock Authentication	Keystroke Confirm	?
Allow Unlock Password Override	<input checked="" type="checkbox"/>	?
XyLoc Password	xxxxxx	?
Confirm Password	xxxxxx	?

- Click on the button for “Update” when finished.

Assign Users to Group

1. Click the button on the left for “Groups”.



2. Select the group created above in the drop down menu, and click the button for “Edit”.
3. Scroll down to the bottom and click the button for “Manage Users”.
4. Select the user created above, and click the left facing arrows to move that account over to the left hand window. The names in the “Available User” box on the right will be listed by their Personal Name that was specified for each user.





5. Click the “back” button to return to the Group Preferences screen. There is no need to click “Update” here, as the User/Group Relationship is updated immediately.

Create the Kiosk Users from the Template user

A kiosk is used when multiple users share a single system login account. Each user has a unique Key ID and will use the same system login account (NT or Novell) plus the preferences defined in the template user account (Nurse Ann).

1. Click the button for “Create Kiosk User”.

The screenshot displays the 'XyLoc Security Server Administration' web interface. On the left is a navigation menu with buttons for 'Status', 'Hosts', 'Users', 'Groups', and 'Download'. The main content area is titled 'Manage Users' and shows the following information:

- Total Licenses : 100
- Available Licenses: 99
- XSS Type: XSS-MD

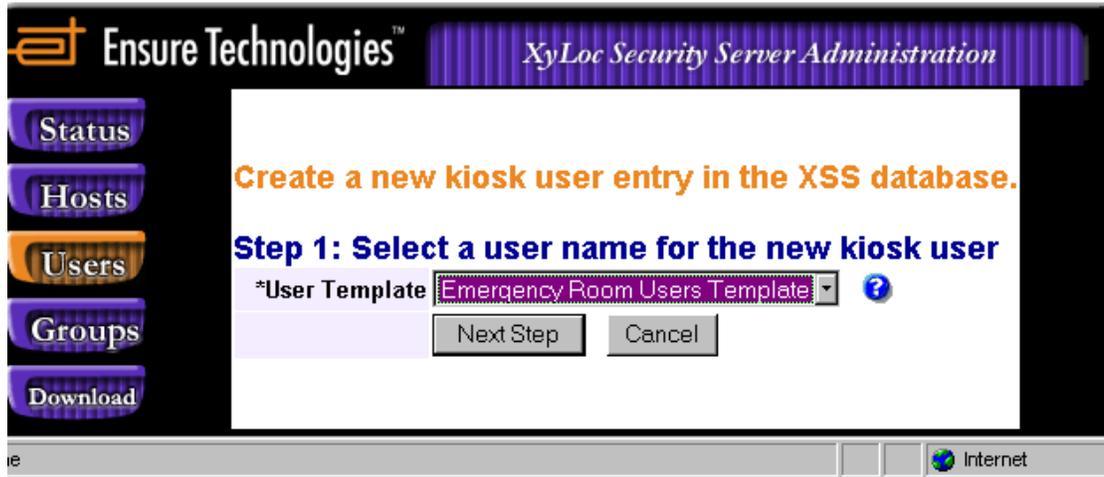
Below this information is a search section titled 'Search an existing user entry by:'. It contains three input fields: 'User name', 'Key ID', and 'Personal name'. Each field has a '(and/or)' label to its right. A 'Search' button and a help icon are positioned below the 'Personal name' field.

Under the search section is a 'Display Users:' section with a help icon and two buttons: 'All Users' and 'User Templates'.

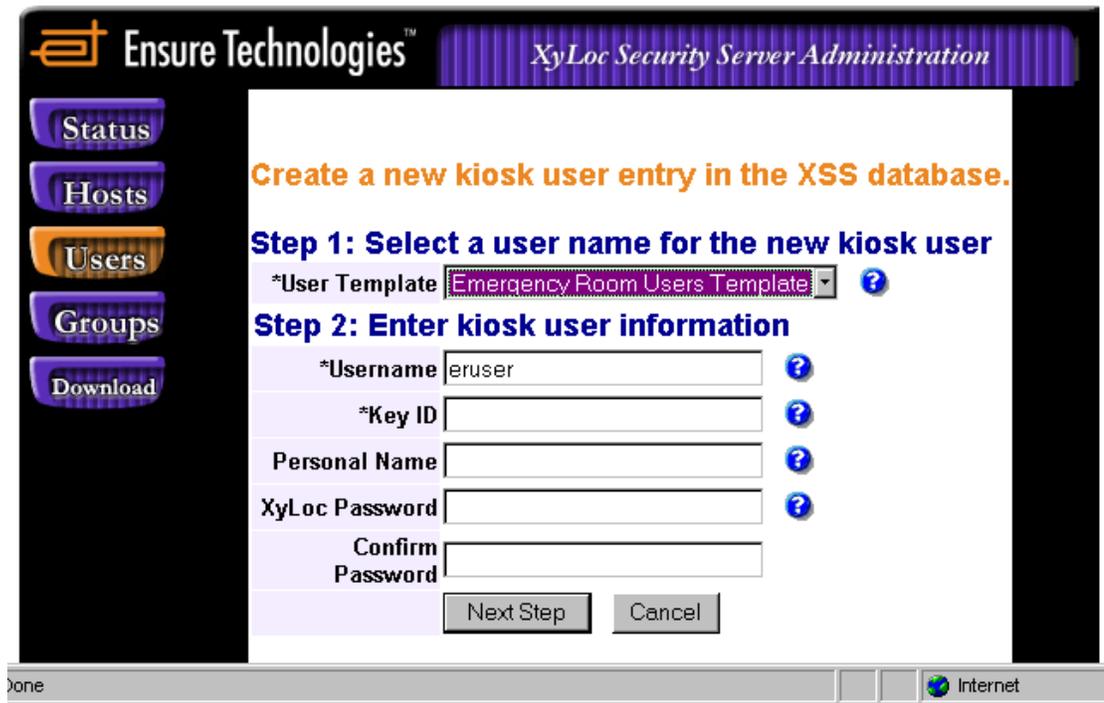
At the bottom of the main content area is a 'Create a new user entry:' section with two buttons: 'Create Unique User' and 'Create Kiosk User'.

The footer of the interface shows the user 'User: XSSAdmin- XSS Administrator' and a status bar with the text 'Look up a user, or select Create to go to the Create User'.

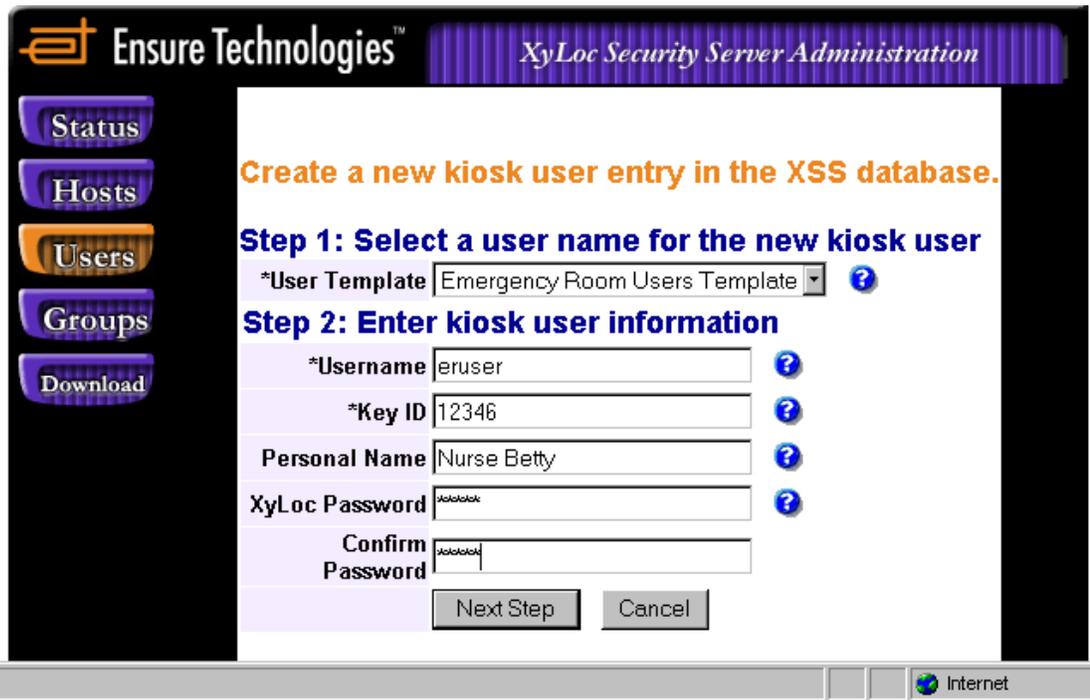
2. Select the Template created above from the drop down menu, and then click the button for “Next Step”.



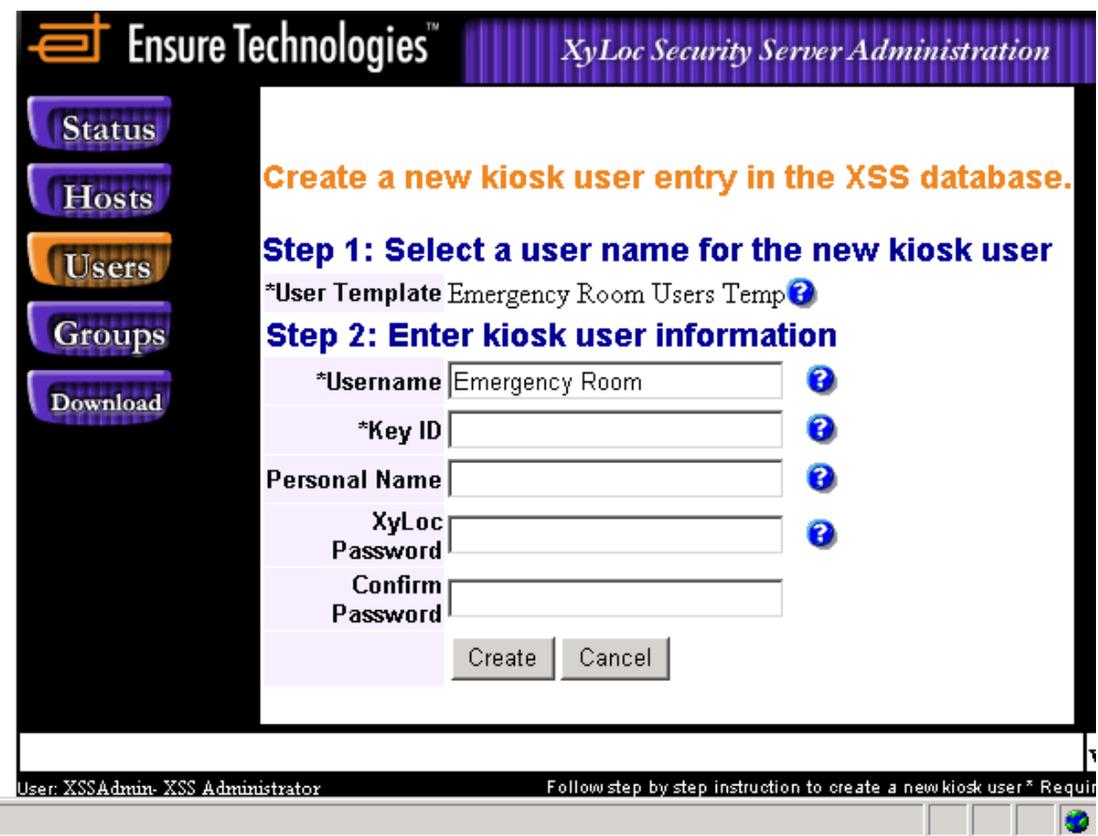
3. The Username should be set for you already. In this example, the system username is *eruser*; it will be the same for every kiosk user using this template. The XyLoc software sets this for you automatically. Leave that name set to its default.



4. Type in the specific Key ID for this user (12346).
5. Type in a personal name. As with the personal name used for the template user, this does not have requirements for what the name is. However, it would be best to use something that would identify this particular user, separate from the other users to eliminate any possible confusion. For this user, the name of “Nurse Betty” will be used.
6. Type in a password for the user. Again, this password is NOT the network password. This password is exclusive for XyLoc (for Password Override Unlock and Login). If the field is left blank, the user’s KeyID will be used as the default password.



7. Click the button for “Next Step”.



8. Click the button for “Create”.
9. Repeat steps for each desired kiosk user.

Administering XSS Services

XSS Monitor Service

The XSS includes a monitoring service that acts like a “Watchdog” on the XSS service. This service will automatically restart the XyLoc Security Service if it detects it is stopped for any reason.

Optionally, this service can be configured to automatically restart the service at a given time each day. This is done through a registry setting on the XSS Server. To enable this functionality, create the following registry value:

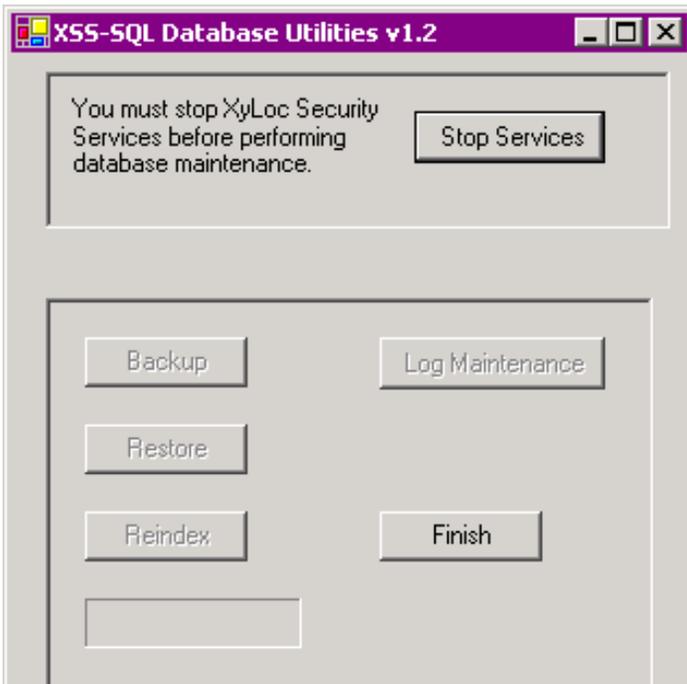
- Location: HKLM\Software\Ensure Technologies\XSS\
 - Name: MonitorTime
 - Type: String
 - Value: Set the value to the hour that the XSS service is desired to be restarted in military time format (0-23).

NOTE: The service does not stop immediately when given a stop command. It can take up to 3 minutes for the services to completely stop in some cases. Because of this, there is a built in 3 minute delay in the monitor tool before the XSS service is restarted.

XSS-SQL Database Utilities

If the XSS was installed using the MSDE database (instead of a full SQL server) there is a database maintenance tool that is available to perform basic maintenance of the MSDE database. If a full SQL database is used, then Ensure Technologies recommends that the standard SQL maintenance tools provided by Microsoft be used.

The XSS Database Utility is located in the directory specified in the XSS-DB installation. The default for this location is C:\Ensure\XyLoc\DBFiles. Select the file called “XSS-SQL-DBUtility.exe”.

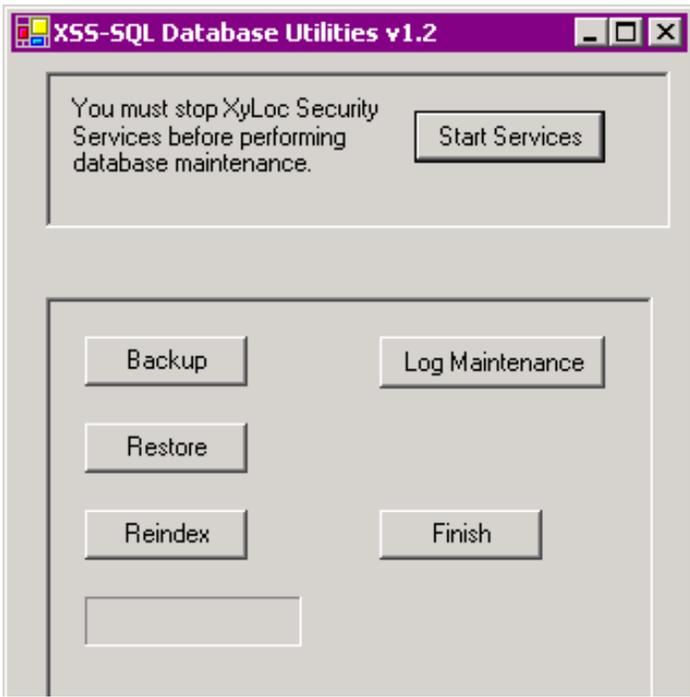


From this utility there are a several options:

1. Stop and Start the XSS Service
2. Backup the XSS Database
3. Restore a previous backup of the XSS Database
4. Re-index the database
5. Purge old log files

Before any maintenance can be performed, you must stop the XSS Services. Click the “Stop Services” button at the top to enable the buttons for the maintenance.

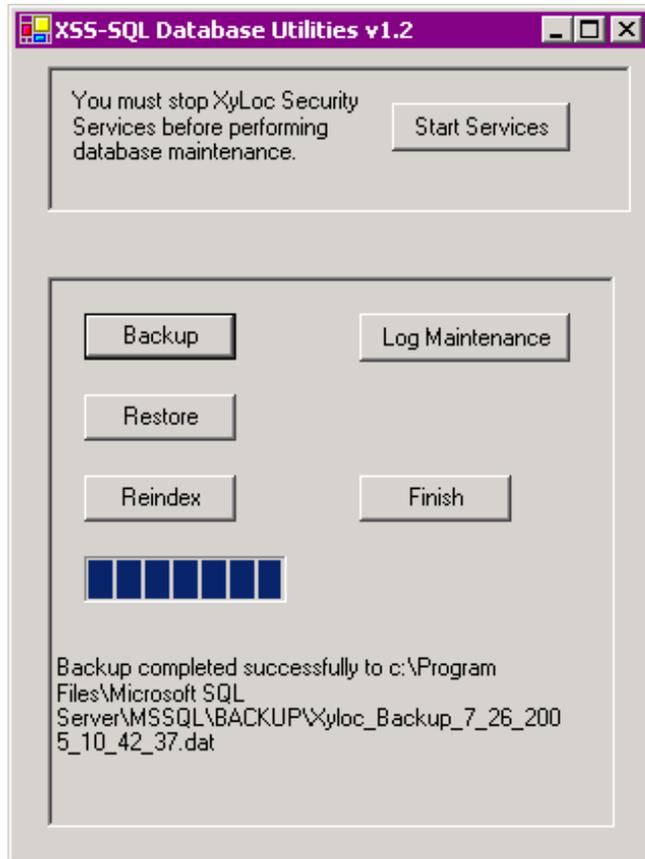
When finished with the XSS-SQL Database Utility, click “Start Services” to restart the XSS service, and then click “Finish”.



Backup the XSS Database:

Use the following instructions to perform a backup of the XyLoc database.

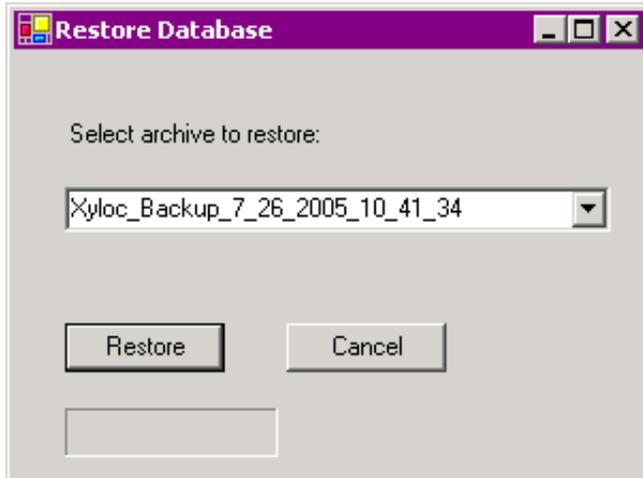
1. Click the button for “Backup”.
2. This will create a backup directory in the installation directory for the MSDE. By default, this directory will be C:\Program Files\Microsoft SQL Server\.
3. The XSS Backup file will have the date and time in the file name (see below)



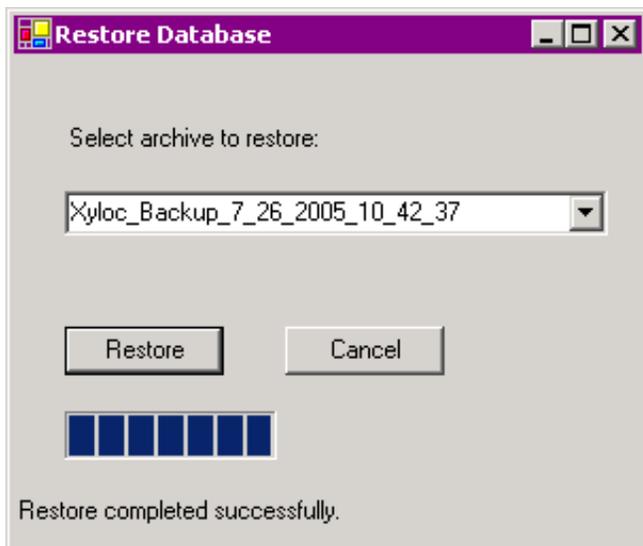
Restore a backup of the XSS database:

Use the following instructions for restoring a previous backup of the XyLoc database

1. Click the button for “Restore”
2. A “Restore Database” window will appear with a drop down box. On this drop down box, select the backup file that is desired. NOTE: The application automatically looks to the “BACKUP” folder in the Microsoft SQL Server installation directory. The desired backup file must be in this directory first.

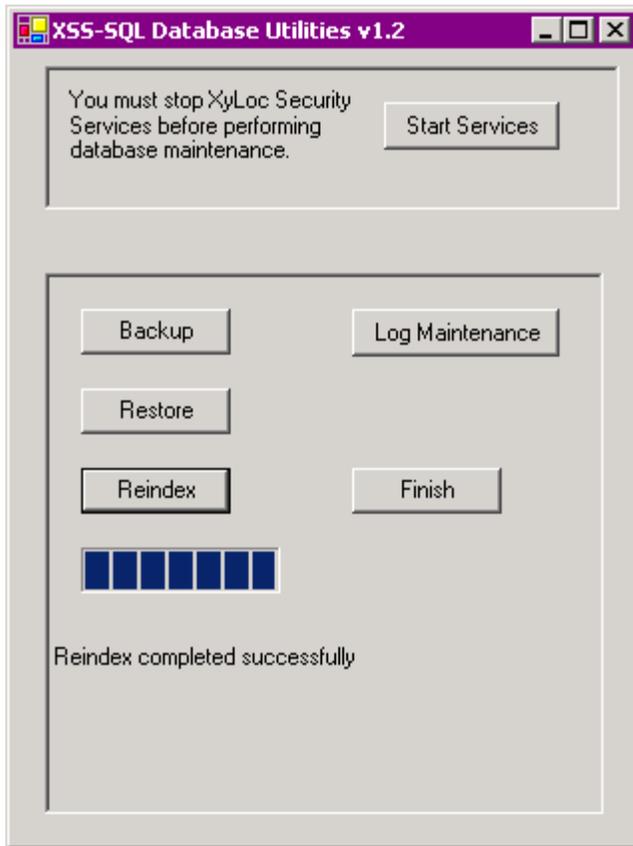


3. Once the desired backup is selected, click “Restore”.



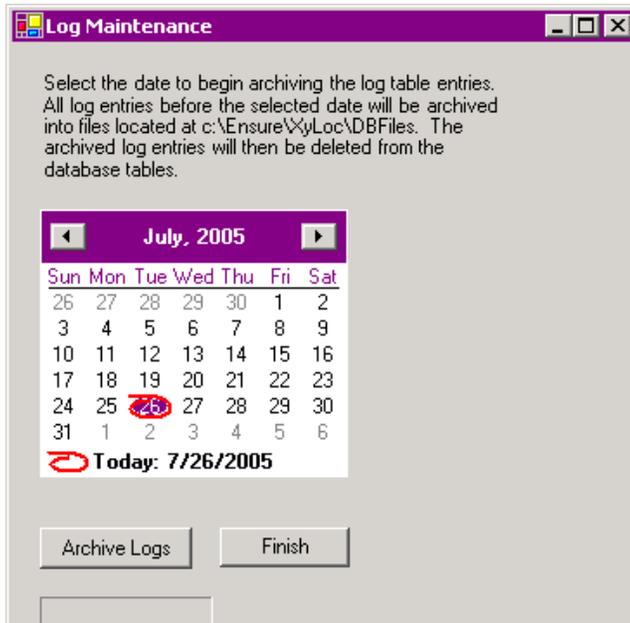
Reindex the XSS Database:

1. Click the button for “Reindex”

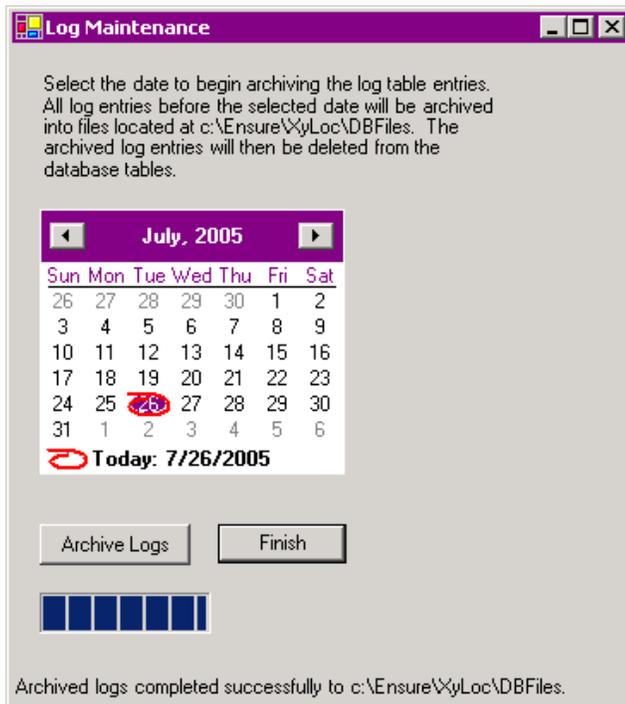


Log Maintenance:

1. Click the button for “Log Maintenance”



2. On this screen, select the date from which you want to keep. All logs prior to this date will be removed from the SQL database and copied to the C:\Ensure\XyLoc\DBFiles\ directory as txt files.



3. Click “Finish” when completed.

Deployment of XyLoc Client Software

Once the user database is completed, the XyLoc client software will need to be installed on the workstations, if it has not been already. This can be installed locally (with at CD provided from Ensure Technologies, via a Download from the XSS or Ensuretech.com website) or via an MSI that is “pushed” with some type of third party Enterprise Deployment software.

NOTE: If the Host is not created manually then it will not show up in the XSS database until the XyLoc Client software is installed and the client begins communicating to the XSS.

Installing the XyLoc Client Locally

Please see the XyLoc Client User Guide for step by step instructions on a local installation of the XyLoc client.

In an Enterprise installation, generally the Host will be put into a Group on the XSS. When the host is going to be used in a Group, there are a few things that need to be considered before installing the XyLoc client.

1. To install the XyLoc client on a host, one must be logged in with a valid administrative level account. NOTE: The account must have **local** Administrative rights in order to install the XyLoc software. Sometimes a Domain Administrator does not have the necessary rights (especially in Windows XP). Ensure Technologies recommends logging in as the actual Administrator of the host to install the software.
2. During the installation, a dialog box will appear to setup an account. These fields must be filled in. However, the software will create the record in the database on the local host. This record is then uploaded automatically to the XSS and stored there as a unique user for that host.

IMPORTANT: These unique user settings will override group settings on that specified host. Be sure to use a different account name to log onto the desktop for installation, than what will be used by the Kiosk account for login.

- a. Ensure Technologies recommends setting up an administrative account to be used to log into the workstation before installing the software. This account will need to be created either on the host, or on the server that is used for user authentication (NT Domain controller or Novell Server) if there is one. This account will need to have **local** administrative rights.
 - b. By logging into the host with this account, the XyLoc software will inherently create this account as well. This account would be a “super user” of sorts, allowing access to the desktop by anyone that has access to the Key ID or the password configured for that account.
 - c. This key will need to be protected as it will have administrative rights.
3. There are also some things that must be considered when deciding what Key ID to use. There are two possibilities when entering the Key ID. (a) Entering a valid Key or (b) entering an invalid Key ID:
 - a. A valid Key ID can be used, and then access to the desktop is available by either the password (through the Password Override feature) or via the valid Key, or possibly, if dual authentication is required, the password can be required in addition to the

- Key. However, if only the key is required, and that key is stolen or lost, whoever recovers the key will have administrative access and will not need a password.
- b. An invalid key can be used instead. Something must be entered for the Key ID (it won't continue with the field left blank), so just enter a series of numbers (i.e. 123) in the Key ID field, making sure there is no actual key with that ID number. Since there is no key with that actual ID number the account will not be accessible by a XyLoc key. Keep in mind the option for Password Override must be enabled, as this will be the only option to log in with the "Admin" account.
 - c. Regardless of which method is used for the Key ID entry, be sure the same Key ID is used for all the installations. Any Key ID used equates to one license on the XSS. If multiple Key IDs are used, it will use multiple licenses. If only one Key ID is used, regardless of how many hosts it is used for, it will still only use one license on the XSS.

When the software is installed a prompt will appear during the installation of the client for the XSS IP address. Be sure to enter it properly before moving on to the next step. If for some reason the IP address does not get set properly, and you need to correct it:

- a. Open the XyLoc Configuration Manager (by double-clicking the icon in the system tray).
- b. Click the tab at the top for "PC Setup".
- c. The IP address of the XSS should be listed in the field for "XyLoc Security Server (XSS) Search Order". If not, then click on "Add" and enter it manually.
- d. Click the button to save the changes and then restart the PC.

Enterprise Deployment of the XyLoc client:

Beginning with client version 8.2.4, the XyLoc client is available in an MSI format, which will allow it to be deployed remotely. This has been tested and used successfully with Active Directory Group Policy deployment. There is a separate document available from Ensure Technologies that describes this process.

When considering a remote installation of the XyLoc client it is important to remember that for an initial installation of the client it is also necessary to install and the XyLoc Lock as well as ensure proper placement of the hardware. Generally some user orientation is also necessary. Proper placement and user education are crucial to a successful deployment of the XyLoc solution.

IMPORTANT: Because of these extra "needs", even though it is technically supported, Ensure Technologies does not recommend a remote installation for the initial installation of the XyLoc client. A remote install is certainly very useful for later upgrades of the client software.

Since the file is an MSI format, it should be able to be deployed using other third-party deployment utilities. However, Ensure Technologies has no specific information on the specific steps necessary for deployment using those utilities. Please consult the vendor of the utility that is being used and/or a local system administrator with the necessary experience in that utility.

If a remote deployment is desired, please contact Ensure Technologies to obtain the appropriate language version of the MSI installation file (English, French, and German language are currently supported).

If the IP address of the database server changes:

If the XSS database is moved to another server or IP address, then you will have to go to the registry on the XSS server and update the address that it points to for the database. Go to the registry editor and go to HKey Local Machine > Software > Ensure Technologies > XSS and change the IP address in the "SQL_DB_Address" setting. You will need to restart the XSS service for the change to take effect. NOTE: This is assuming that the credentials that were put into the XSS for administering the XyLoc database are unchanged.

If the SQL Username and/or Password are changed:

If the SQL account used by the XSS to read/write to the database is changed, the XSS will need to be reinstalled. There is not currently a utility to change the stored SQL password as it is encrypted once it is saved. Contact Ensure Technologies Technical support for assistance, if needed.

If the IP address of the XSS changes, or needs to be changed:

If the IP address of the XSS changes, the following steps must be performed:

- Update the xss.config file found in c:\Ensure\XyLoc\bin. You need to update the entry for 'ServerIP' in this text file
- Update the XSS IP address in the XyLoc client in the PC Setup tab on the XyLoc Configuration Manager.
- If the SQL database is on the same server as the XSS Service, then the steps outlined below for changing the SQL Server Address will be necessary as well.

If the address of the SQL Server changes, or needs to be changed:

The following registry key will need to be updated on the server that is running the XSS Service as well as the server that is running the WebUI (if they are not on the same server).

- HKey Local Machine > Software > Ensure Technologies > XSS and change the IP address in the "SQL_DB_Address" setting.

The XSS Service will need to be restarted following these changes. The WebUI does not need to be restarted.

The XSS Service will need to be restarted following these changes.

XyLoc Client Update:

Go to c:\ensure\xyloc\download, and place the latest Client "install.exe" software version in the download directory. This will make available the latest client software via the download button on the XSS.

Additional Notes:

- Windows Server 2008 has a built in firewall that will block the communication from the XyLoc clients as well as the communication from the server to the client. An exception for TCP Ports 5102 (incoming) and 3510 (outgoing) will need to be setup in the firewall settings.
- The 7.x.x version of the XyLoc client is not fully compatible with the 4.x.x (SQL) version of the XSS. Once the database is converted to SQL, the existing 7.x.x clients will need to be upgraded to an 8.x.x version in order for all the settings to function correctly.
- If the XSS-SQL is installed on a different server than the XSS 2.x (Codebase) with a different IP address, the records for each “Host” will need to be edited to reflect this change. When the host begins to communicate with the XSS-SQL, if the record still has the original IP address, the XSS will change the IP address setting in the client to the original address, and the client will no longer be communicating with the XSS-SQL. Also, when the XyLoc Client is upgraded to 8.x.x the setting in “PC Setup” on the client for the XSS IP address will need to be changed to reflect the new XSS server

Error: “page cannot be displayed” when browsing to the XSS start page

1. Check the address to make sure that it is correct. This address will be `http://<IPaddress>/xyloc/xss.aspx`
2. Check to make sure that the IIS service is running and the Default Website is started within IIS.
3. If running Windows Server 2003, make sure to allow ASP.NET and Active Server Pages in IIS.
4. If running Windows Server 2008, be sure to convert the XyLoc website in IIS to an Application. Right-click on the XyLoc site in there and “Convert to Application” is an available option on the pop-up menu.

Changes made at the server are not propagating to the XyLoc clients

If changes that you make at the server are not getting downloaded by the XyLoc client, check the following:

- If the user is in a Group
 - Make sure that the setting you are changing is inherited.
 - If the setting is not inherited, and you don't want to inherit the setting, then make sure to change it in the “User Preference” section under the individual record.
 - Make sure that the user does not also have an individual record for the specific host. If the user has a record for the host directly and also a record in a group for the same host, the individual record takes precedent.
- If the client PC is using Windows XP SP2, make sure that the firewall is either turned off, or a proper exception is created for the XSS port (TCP port 3510)
- If the server is running Server 2008, make sure to create the proper exception for TCP ports 3510 and 5102 for communication to/from the XyLoc client.
- Check to make sure the XSS service is running
- Make sure the IP address of the server is in the PC Setup tab on the XyLoc Configuration Manager on the XyLoc Client.
- Check the license count on the server to make sure that there are still available licenses. To check this, login to the XSS and click on the “Users” button. This screen will display the Total Licenses and the Available Licenses.
- On the XyLoc client, check the exception.txt log (in `C:\Program Files\Ensure Technologies\XyLoc`) for any errors regarding communication to the XSS. If there are, then send this log to Ensure Technologies Technical Support.
- Check the `xsslog.log` file (available on the XSS server in `C:\Documents and Settings\All Users\Application Data\Ensure`) for any errors regarding communication to the client.
 - By default the `xsslog.log` will only generate events when the XSS service is stopped/started and when specific exceptions occur.
 - To turn on more detail, go to the registry in `HKeyLocalMachine\Software\Ensure Technologies\XSS` and change the value of “TraceOn” to “1” and restart the XSS Service.
 - Send this log to Ensure Technologies Technical Support for more assistance.
 - NOTE: This log will grow quickly once the trace is turned on and should only be used for troubleshooting. Once the problem is resolved, make sure to turn that logging back off so as to not use excessive disk space.

Users and Hosts Appearing in the XSS Database

As soon as the server IP address is saved in the XyLoc host, audit log entries should begin to appear in the XSS. If the host has learned the server IP address (in the “PC Setup” tab of the XyLoc Configuration Manager) and the local XyLoc users have still not been uploaded to the XSS, the most probable reasons are:

- ❑ A permissions issue on the server (servers using NTFS).
- ❑ The host cannot reach the server due to a problem with the TCP/IP communications (try ping and tracert from the client to the server).
- ❑ The “XyLoc Security Server Daemon” is not running.
- ❑ There are no more licenses left on the XSS. Check ‘Users’ page on Web Browser to see how many licenses are available.
- ❑ **NOTE:** If running Windows XP with SP2, check the firewall settings. By default, the firewall is on and will block communication. You will either need to create an exception for port 3510, or turn off the firewall altogether.

Revision History:

Revision	Date	Description	Author
2.00	09-04-2009	Modified documentation for XSS 5.x.x.	RS