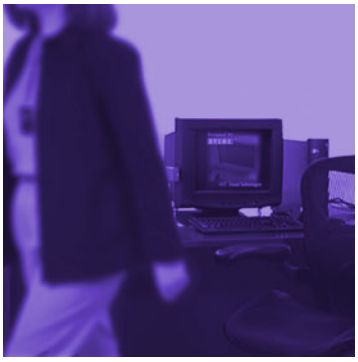
Ensure Technologies™

XyLoc Security Server w/ AD Integration
(XSS-AD 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**

Technical information contained herein is subject to change without notice.

Table of Contents

Overview of XSS

XSS-AD is designed to take full advantage of the enterprise-class directory services and management capabilities of Microsoft® Windows 2000/2003 Active Directory.

By using the existing Active Directory infrastructure, XSS-AD integrates with the Active Directory seamlessly to store XyLoc information in the Active Directory repository and use the same Active Directory management tool to manage the XyLoc information for either users or computers.

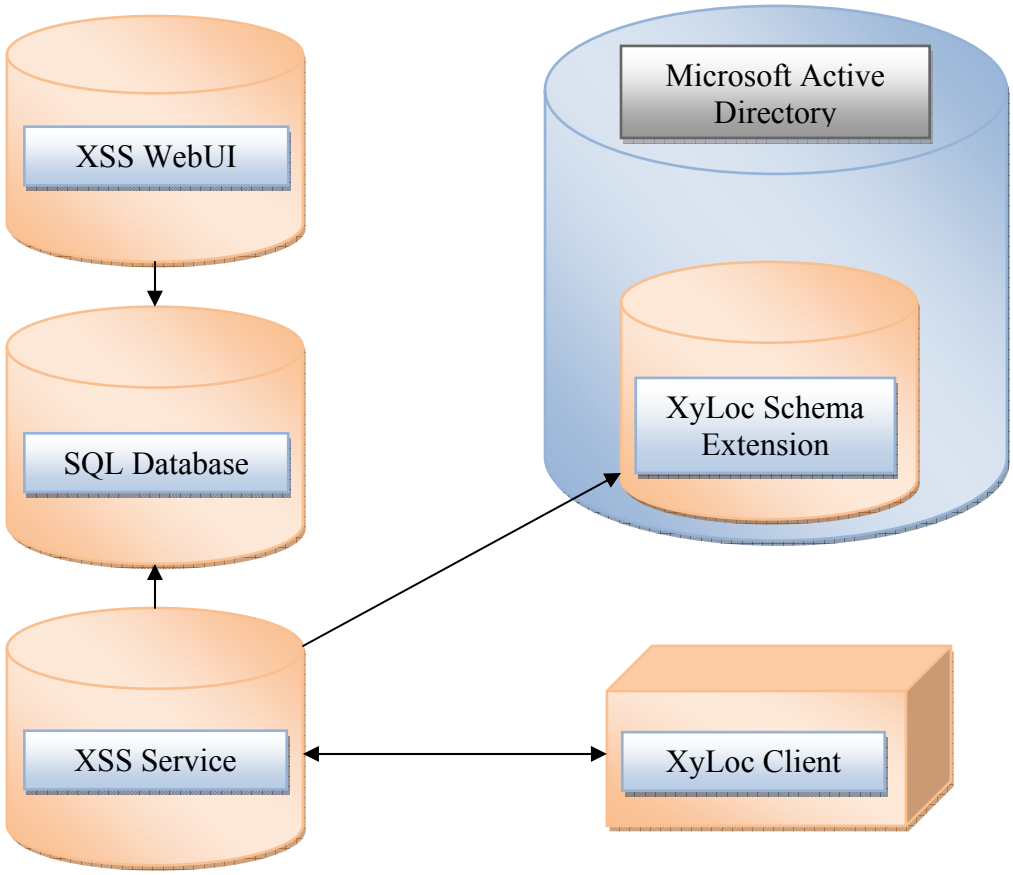
Because XSS-AD leverages Microsoft® Windows 2000/2003/2008 Active Directory management tools, additional administrative training is minimal. Administrators can use the same tools to quickly deploy the XyLoc Security System and meet the organization's security needs.

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 current configuration and log files. If the communication is interrupted between the client and the XSS, the client will continue to maintain its current 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.

The following diagram illustrates the general system design concept:



XSS-AD Components

XSS-AD includes the following components:

XyLoc AD Schema Extension

XyLoc extends the Active Directory schema to include classes and attributes that are used for XyLoc.

The details of these new classes and attributes are described in the **Technical Reference: Schema Extension for XSS-AD** document available from Ensure Technologies (Drawing#: 510-0100-009)

XyLoc AD Management UI

This is the UI extension for the new classes and attributes which adds the appropriate "tabs" in the Active Directory Users and Computers MMC.

XyLoc Database

XyLoc Database stores the daily event logs generated from the XyLoc Client.

XyLoc Security Server Service

XyLoc Security Server (XSS) provides the link between the XyLoc Client Software and the Active Directory. It retrieves updated information stored in the Active Directory using ADSI (Active Directory Service Interface) and provides this data to the XyLoc Client as well as handling requests from the XyLoc Client software through TCP/IP.

Web-based Management UI

The XSS web-based management UI is used for the following:

1. Manage XSS Administrators (the XSS Administrator is separate with the actual user, and it is only used by XSS).
2. View Event logs

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 Service is used as a centralized communication point between the XyLoc Client and Active Directory. The clients themselves do not communicate directly to AD, but rather communicate to the XSS, and the XSS in turn communicates to AD and then back to the client.

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.

For the hosts to communicate properly with the server, the following must be true:

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

All user and computer configuration is performed within the AD Schema and the installed XyLoc UI using standard AD format.

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 send a query to AD for that KeyID. Based on the information returned from that query, 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.

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
  - 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.

NOTE: 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 **not** supported in version 4.2.0 or higher. If an earlier version of the XSS is currently used with a kiosk setup, the kiosk setup will need to be rebuilt if an upgrade to 4.2.0 or later is performed.

Kiosk vs. Unique

	Advantages	Disadvantages	Common Usage
Kiosk	• Fast, easy access for each user since there is no need to logoff of the PC before logging on.	• 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)	• Shared workstation environments where fast access to a computer is required (i.e. Hospital Nurses Station)
Unique	• 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.	• 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.	• 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.

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 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 XSS if the SQL server is not on the same server as the XSS.

IMPORTANT: In addition, since the XSS will typically not reside on the actual AD Schema Master, the installation will require a Domain account to use for the XSS Services. This allows the XSS to read and write data to the AD Schema in our attributes. This account will need to have the permissions necessary in order to read and write to the schema (typically, at least a member of the "Account Operators" group on the Domain unless given specific permissions).

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.

This section will provide the necessary steps to setup the XyLoc attributes in the Active Directory, install the XSS database, 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 Active Directory Schema Manager:

1. From Start menu, select "Run…"
2. Type in "regsvr32 schmmgmt.dll" (without the quotes) to register the DLL.

NOTE: The following steps are not necessary in Windows Server 2003/2008. They are only required if using Windows 2000 Server

3. Go back to the Start menu and select "Run…" again.
4. Type in "MMC" (without the quotes) to launch the Management Console.
5. From the "Console" menu, select "Add/Remove Snap-in…"
6. Click on the Add…
7. From the list, select "Active Directory Schema" and click on "Add".
8. Now the Active Directory Schema should shows up in the Management Console.
9. From Console menu, select "Save As…"
10. On the Save in, select a location.
11. Name the file name "Active Directory Schema" and save the file.
12. The selected location should now have the Active Directory Schema icon.

Enable Active Directory Schema Update:

NOTE: As above, if installing on a Windows Server 2003/2008, there is no need to enable the Schema update either. If you are a Schema Administrator, the necessary permissions are already assigned.

1. Make sure you login with an account that belongs to the Schema Admin and Enterprise Domain Admin group.
2. Launch the Active Directory Schema Management console.
3. Right click on the Active Directory Schema and select "Operation Master…"
4. Check "The Schema may be modified on this Domain Controller" box.

Install XSS-AD Schema:

1. Run XyLocADSchemaSetup.exe on the Active Directory server to install and configure the XyLoc Active Directory Schema
2. Check c:\etschema-install.log. Every line in the log file should end up with (0).

Install XSS-AD User Interface:

1. Run the XyLocADUISetup.exe to add the XyLoc UI extension to the Active Directory Users and Computers console. This will need to be done on any machine that will be used to

configure XyLoc users. This can be done on the domain controller and/or on any workstation that has the Active Directory Admin tool installed.

2. If the environment has sub-domains that also will require the XyLoc UI extension, then run the XyLocADUISetup.exe on each sub-domain as well, if you will be configuring users from that interface.

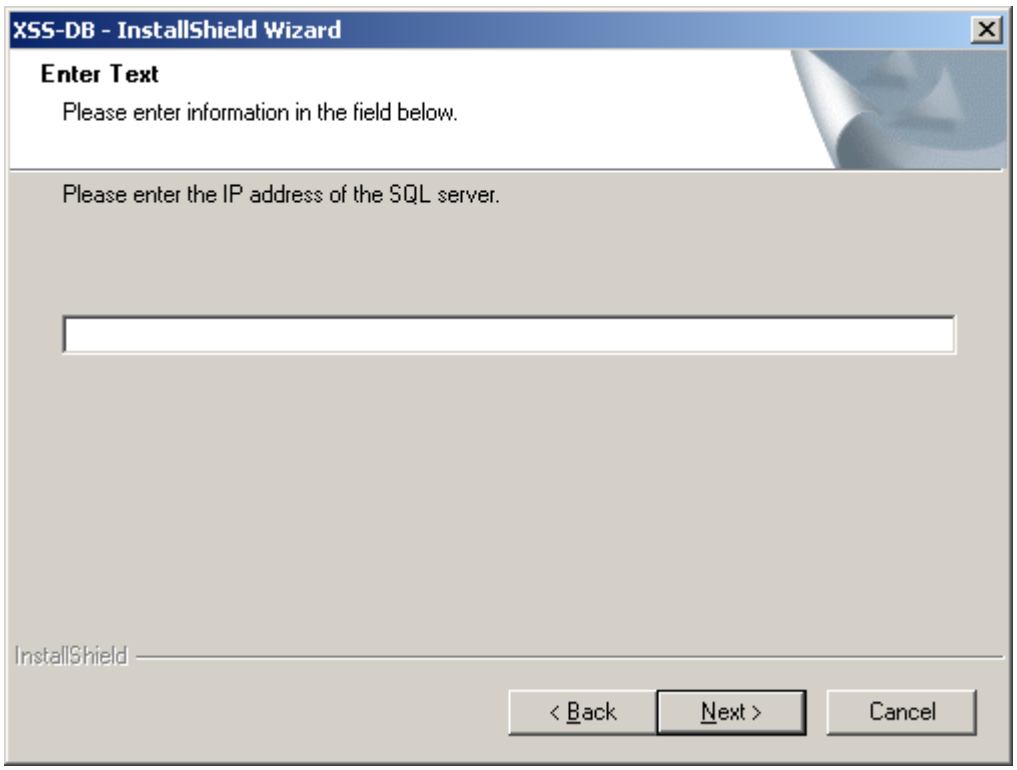
Verify the XSS-AD Schema Extension:

1. Launch the Active Directory Users and Computers applet.
2. Select a user and check the property. There should be two new tabs for XyLoc. Make sure the attributes are visible (NOT grayed out).
3. Select a computer and check the property. There should have one new tab for XyLoc.

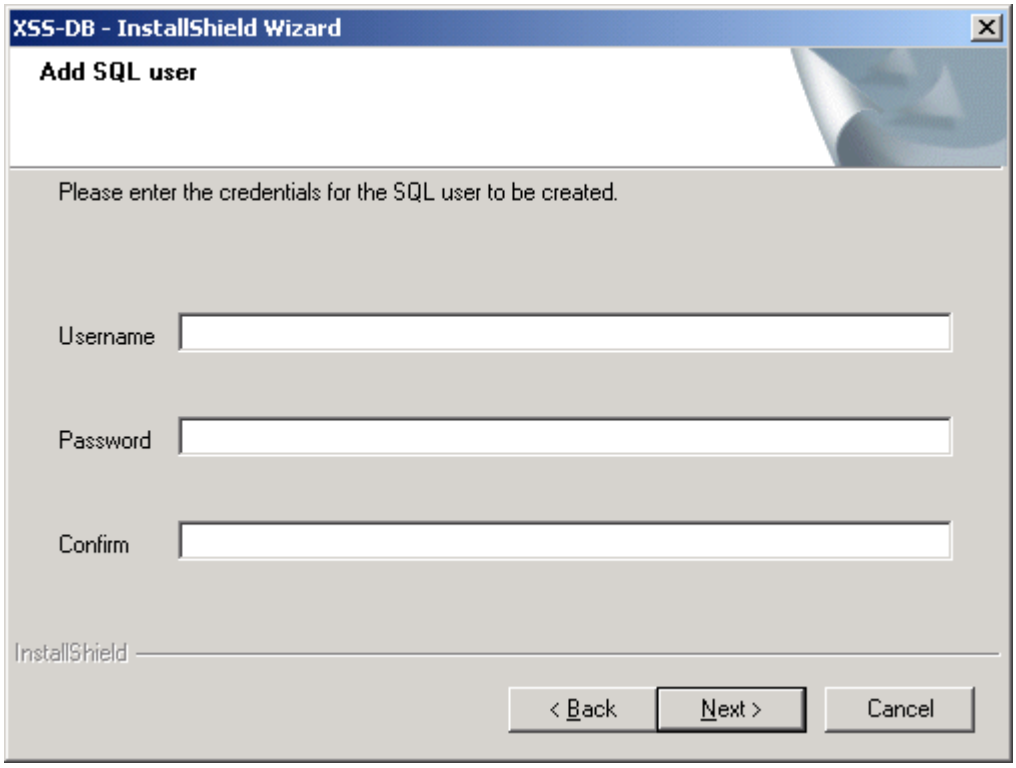
Install the XSS Database:

The XSS uses the Microsoft SQL database to store the audit logs and XSS administrator users. This utility will create the necessary tables within an existing SQL server.

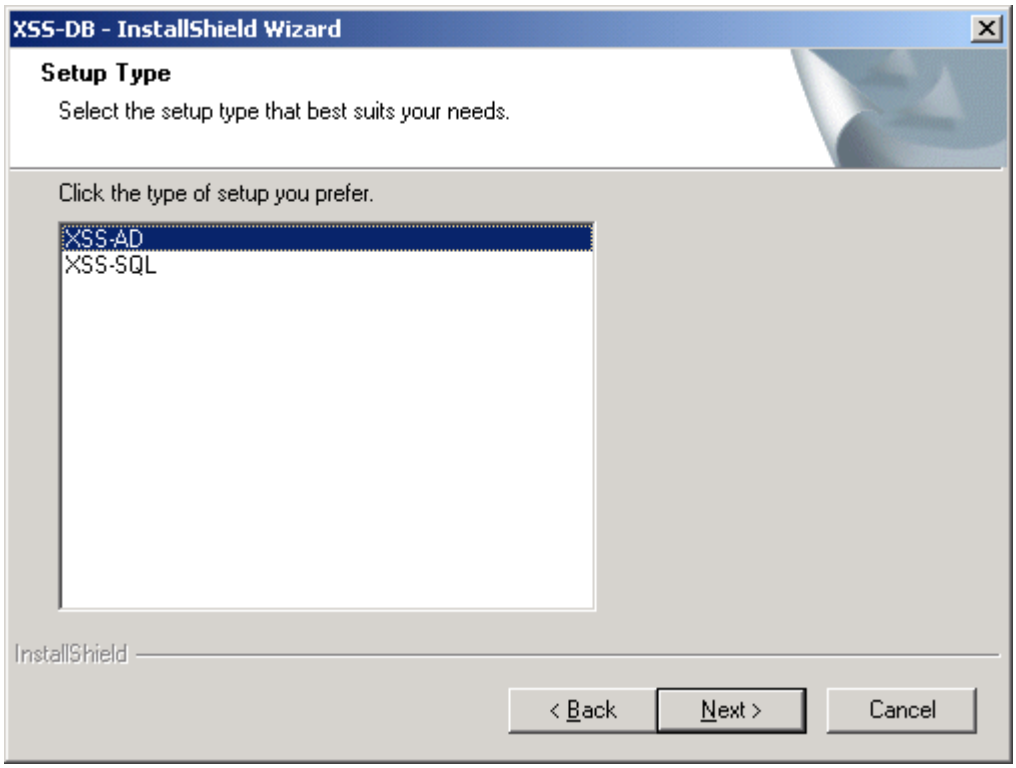
1. Run XSS-DB.exe on your SQL server.
2. Read and Accept the License Agreement.
3. The wizard will ask for the IP address of the SQL server. This is for when there are multiple Network Adapters in the server. Currently only one adapter is supported, so the IP address of the desired connection must be entered here.
    a. If using a "named instance" of SQL then the instance name needs to be specified here as well.
        i. Specify the name like: "<server 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".

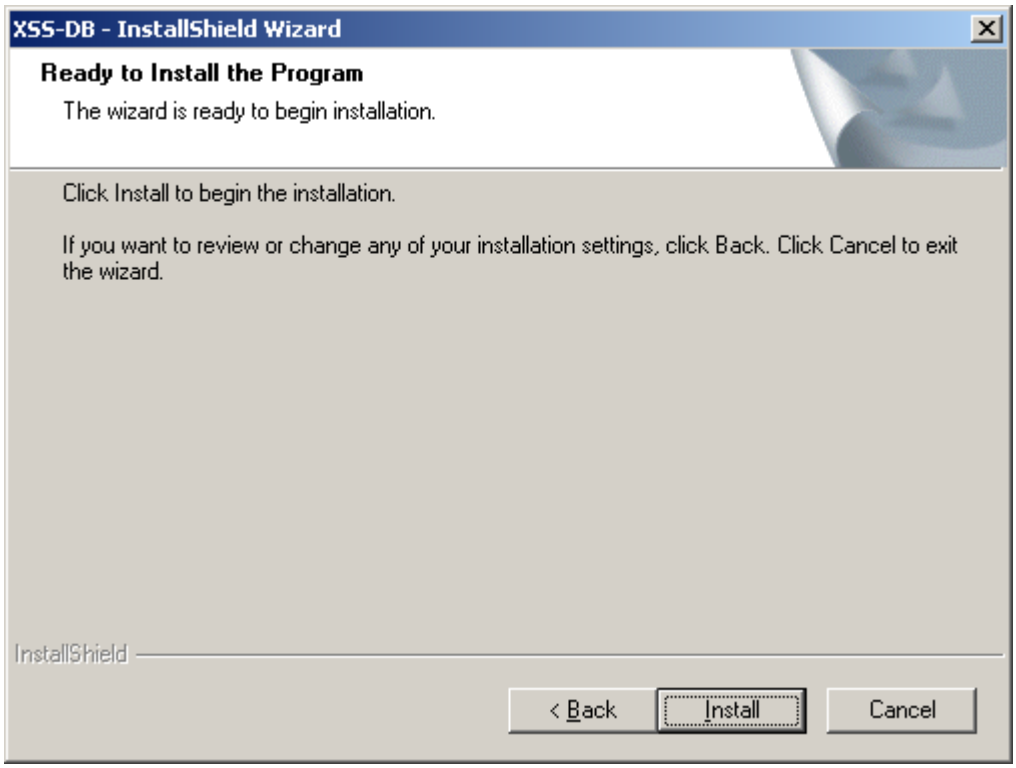


4. Then you will get screen requesting the login information for the SQL account to be created. Put in the desired username and password and click "Next"

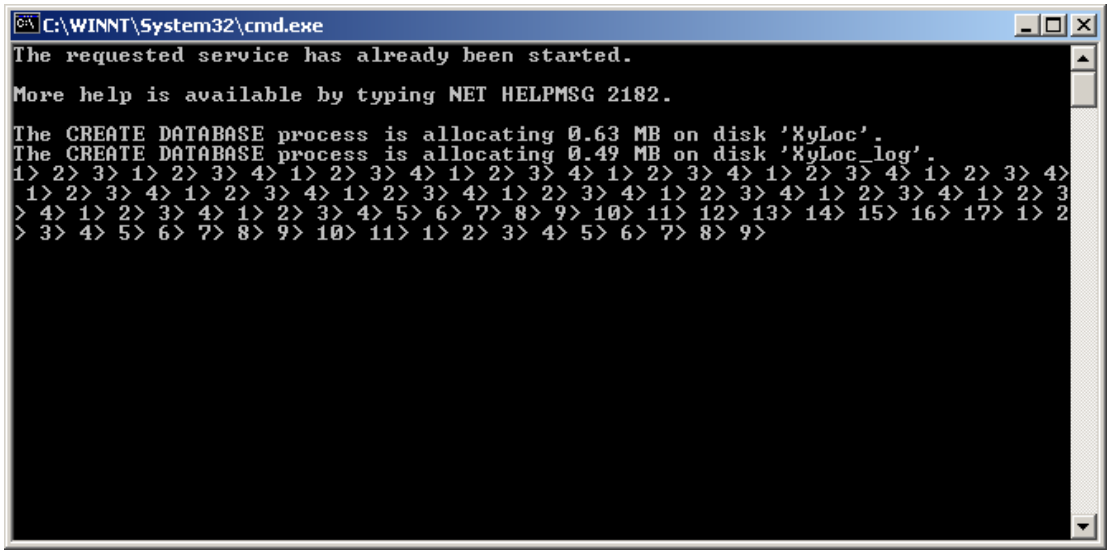


5. Next, select the setup type for the database. In this case, select XSS-AD and click "Next".

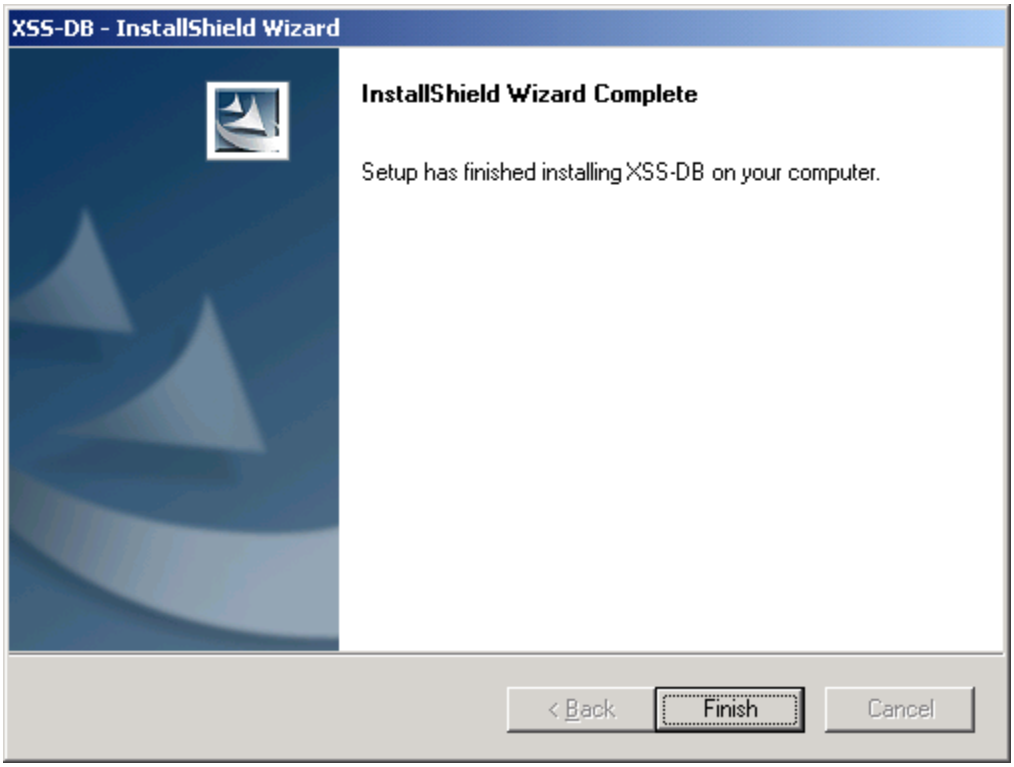




6. The XSS database tables will now be created.



7. Once the installation is completed, if prompted, click on "Finish".



Installing the XSS Server

There are two options available for installing the XSS Server. With 5.0.0 the installation of the XSS Service and the WebUI can be done in separate installation packages or as 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.

Install the XSS Service Component:

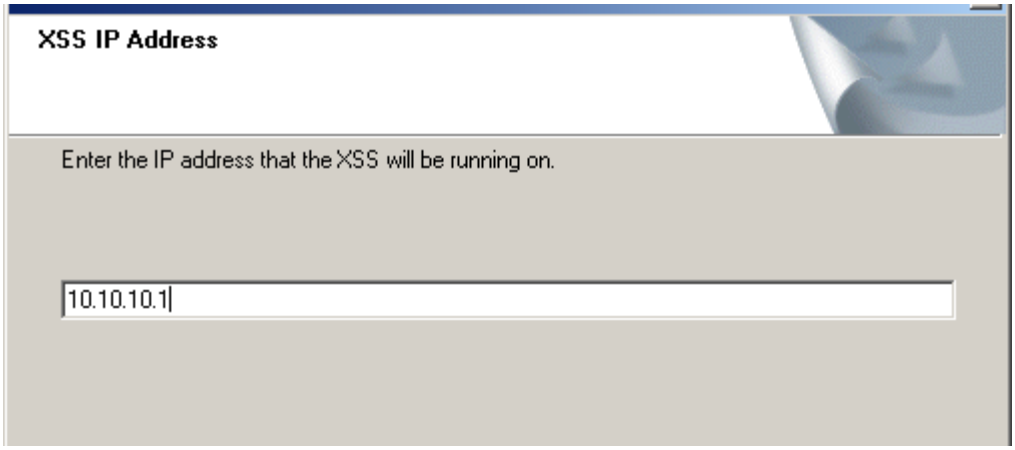
This service can be installed on any server. However, it must be a member of the desired domain. It does not have to be installed on the same server as the SQL database.

Before installing the XSS, however, please verify the following:

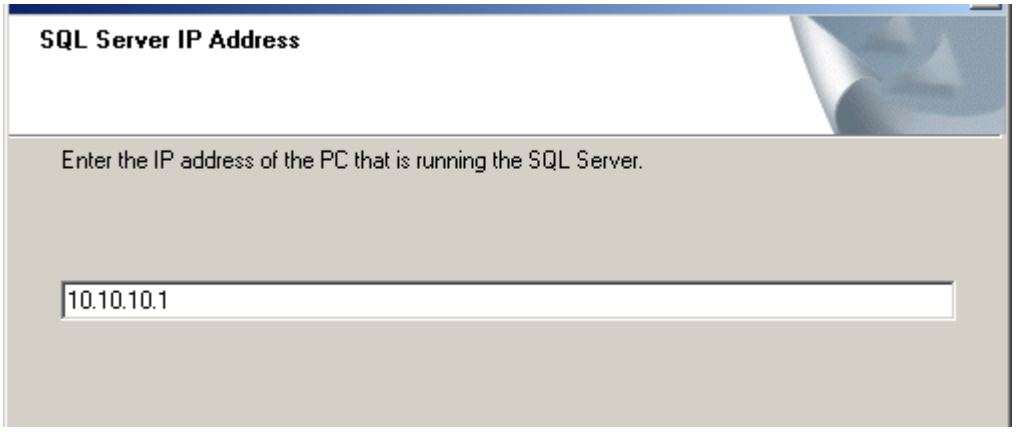
- Be sure to login to the server as a local administrator (with Server 2003, a Domain Admin is not guaranteed all the necessary rights, so Ensure recommends a local administrative account be used).
- If using an SQL database on a different server than the XSS, make sure to have MDAC version 2.7 or later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

To install the XSS Server:

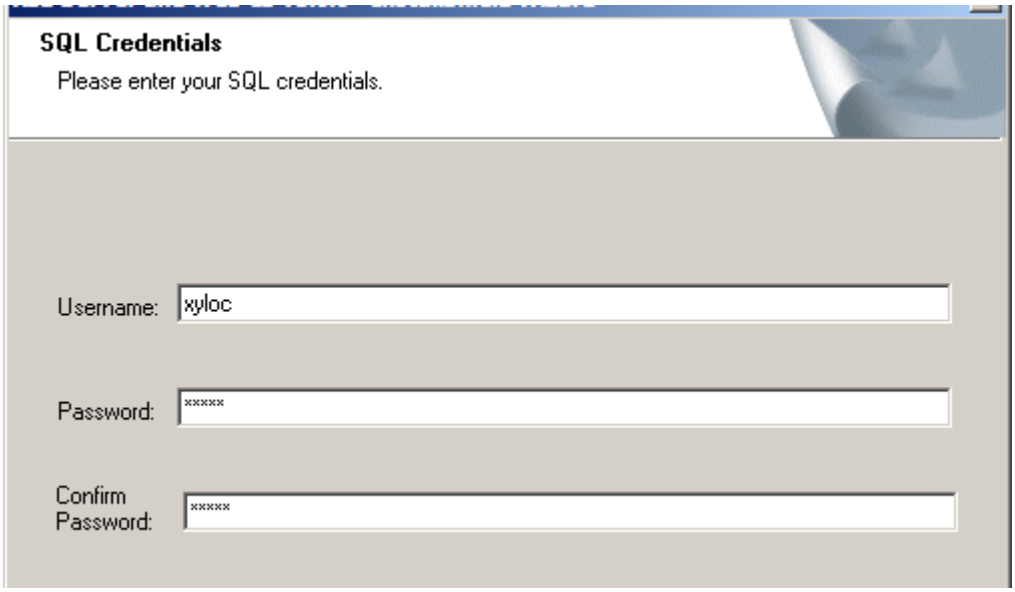
1. Run the "XSS_Daemon_5xx.exe" file.
2. Read and Accept the License Agreement.
3. Enter the IP address of the machine you are running on if it is not found by default:



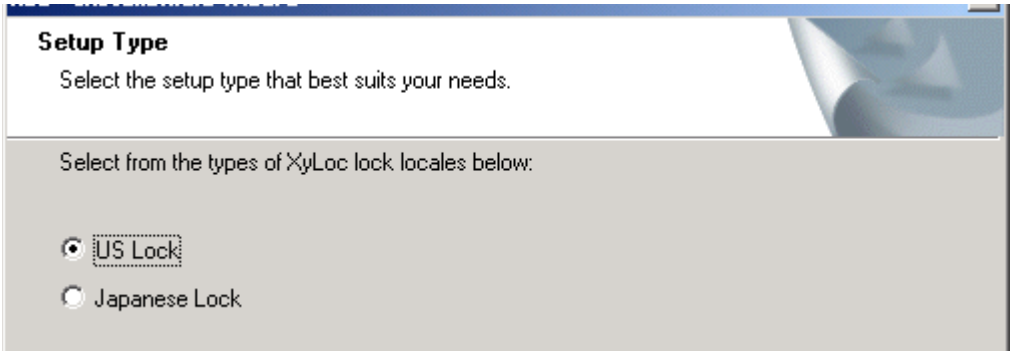
4. Enter the IP address of the SQL server. If a named instance is used in SQL, then enter the address with the instance name on it ("<server address>\<instance name>").
    a. Again, if using SQL 2008 Express, even the default instance is considered "named" and must be entered as such. Generally this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



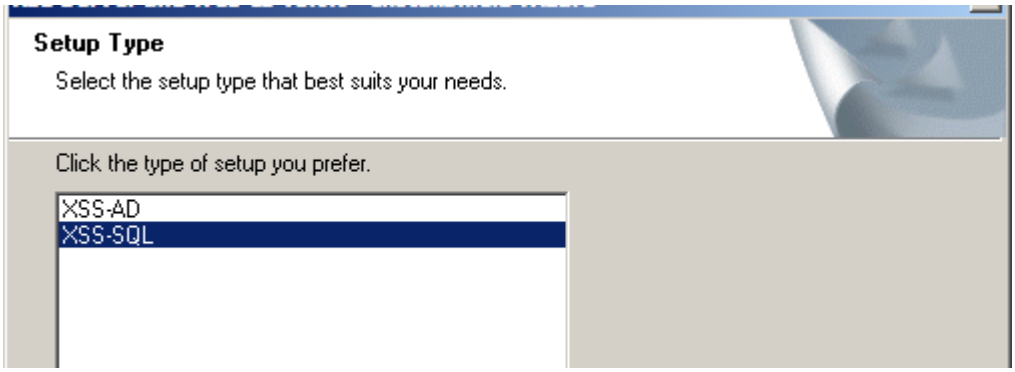
5. Enter the credentials created during the XSS-DB installation for access to SQL.



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



8. Select “AD” for the XSS format



9. The installation wizard will request credentials to assign to the XSS service. Enter credentials for an account that has permissions to write to the AD Schema to write password changes for the users. (**NOTE:** Generally this has to be a member of the “Account Operator” group in AD that has been given specific permissions to write to the AD Schema. See your Active Directory Administrator for more details.) The username is in the format of “domain\username” (without the quotes) where “domain” is the domain name and “username” is the account’s Login ID. Enter the appropriate credentials and click “Next”.
10. The installation wizard will attempt to start the service with the supplied credentials. A prompt will appear to inform if that was successful.
11. When completed click on “Finish”.

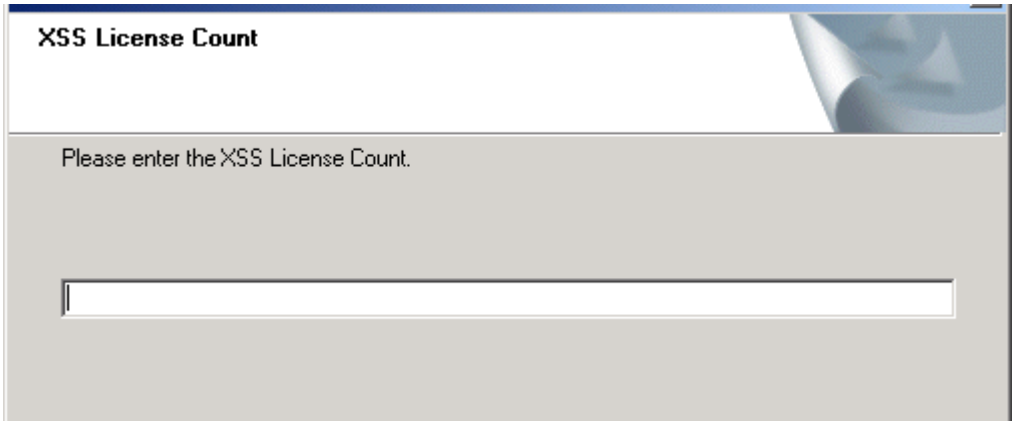
Install the XSS WebUI Server:

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:

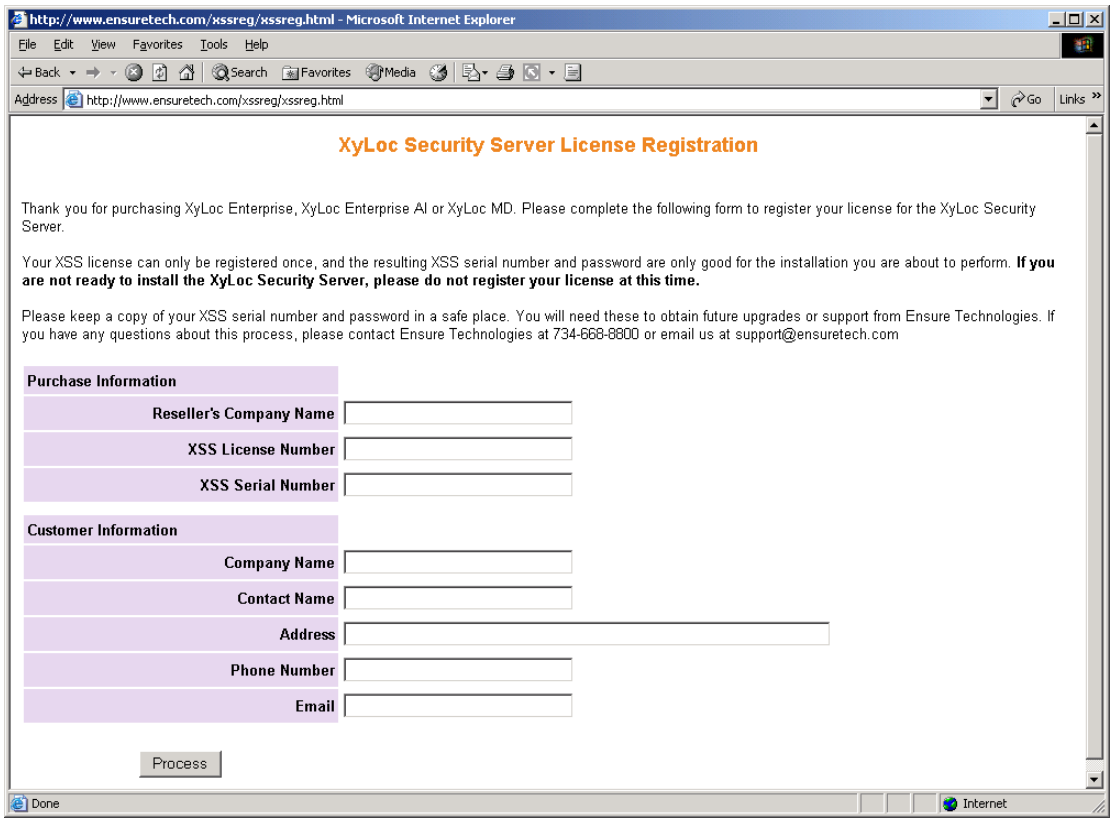
1. Run the "XSS_WebIIS_5.x.x.exe" file.
2. Enter the IP Address of the Server on which the WebUI is being installed (the local IP address in this case).
3. On the XSS License Count screen, enter the correct number of licenses that were purchased. If you are going to install in Evaluation mode, enter 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.

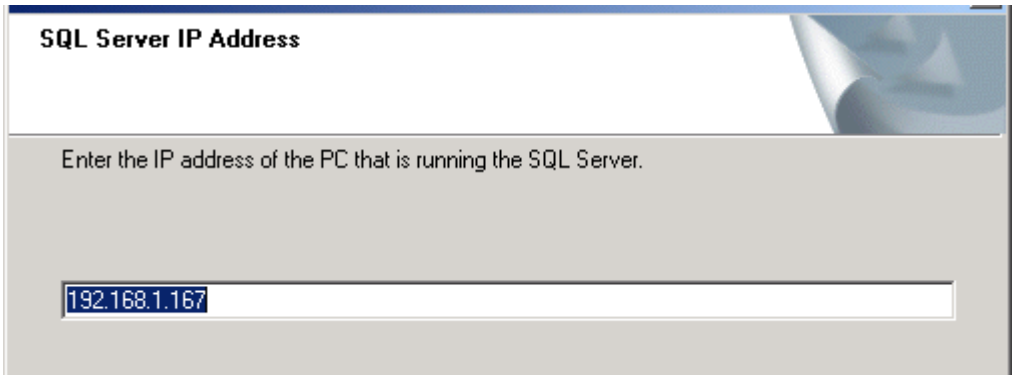
5. The password for the purchased version can be obtained from Ensure Technologies by calling 734-668-8800. To obtain a password online:

   - Copy the XSS Serial Number generated during the install process exactly as it appears.
   - Go to **http://www.xyloc.com/xssreg.aspx**

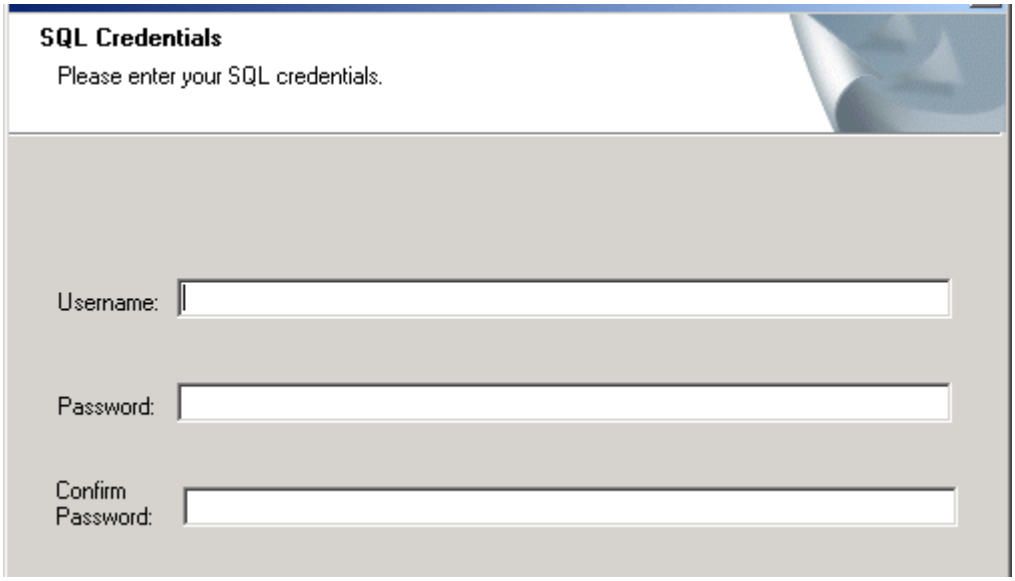


   - Enter the Reseller's Company name how it appears on the document provided by Ensure Technologies.
   - Enter the XSS License Number how it appears on the document provided by Ensure Technologies.
   - Enter the XSS Serial Number generated during the install process.
   - Fill in all Customer Information 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>").
    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.

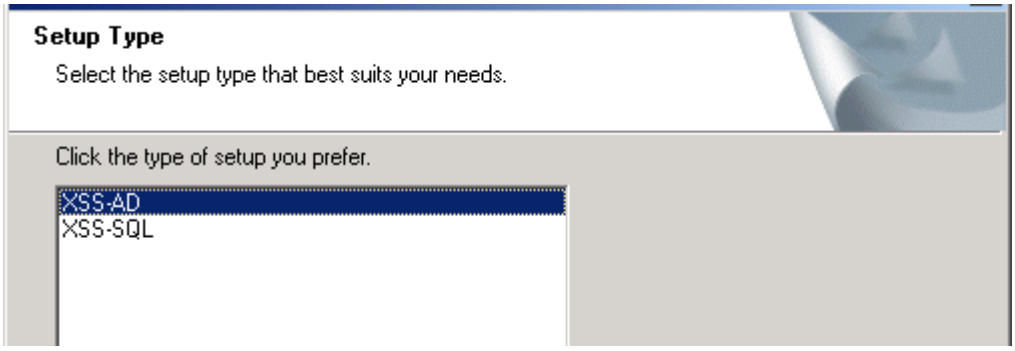


10. On the next screen, enter the username and password of the SQL account that you will be using. They are case sensitive so make sure to enter them exactly. Click "Next".

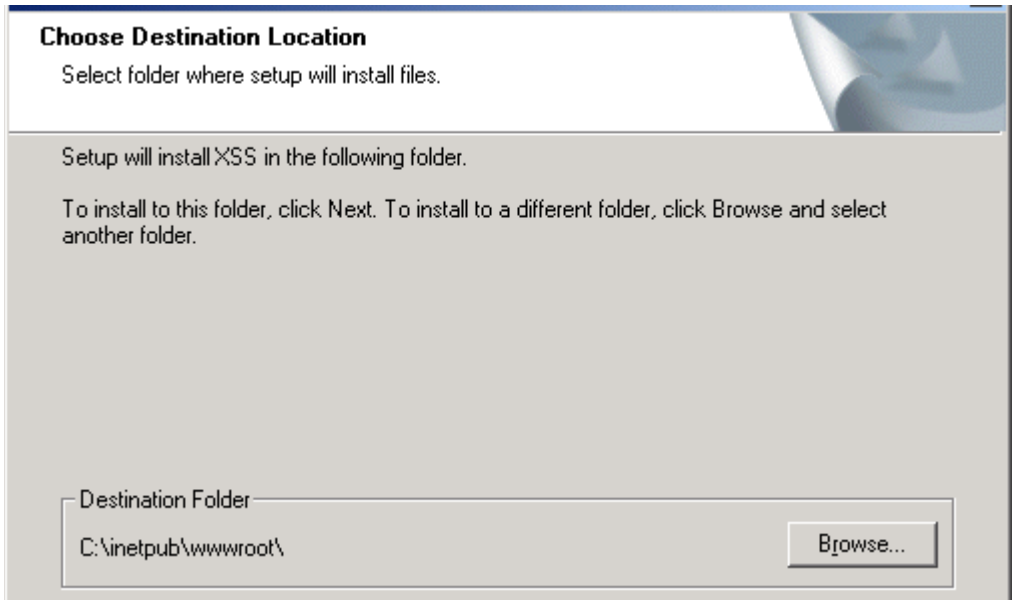


11. If the credentials and IP address are correct, you should receive a message that states that the login to the SQL server was successful. Click "OK".

12. Select the type of XSS that you are using again. In this case you will select "XSS-AD" and click "Next".

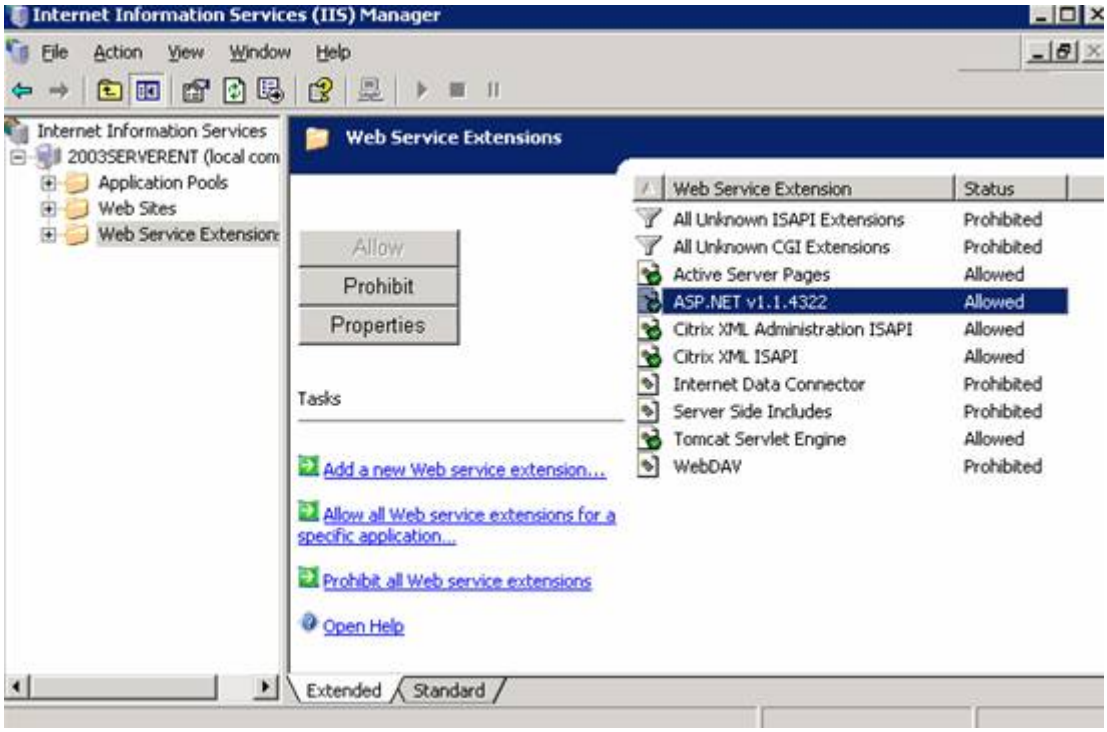


13. Choose the destination location. The default path is the default for IIS. Click "Next".

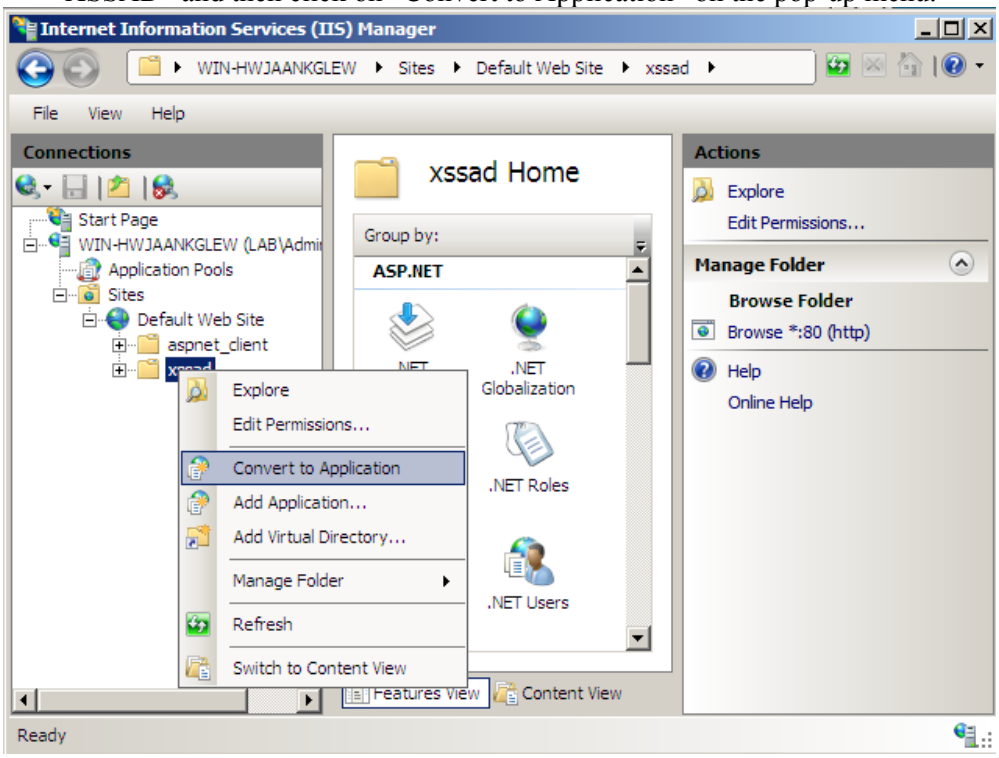


14. You may see a command line screen open up and the software will install the ASP.NET.
15. When the installation is completed, click "Finish".

16. Configure IIS
    a. If using Windows Server 2003, in IIS, under the "Web Service Extensions", the options for "ASP.NET" and "Active Server Pages" must be allowed.



b. 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 XSS 2.x.x (Codebase) version

Currently there is no process for upgrading from XSS versions 2.x.x to any of the 4.x.x versions. If XSS 2.x.x is currently being used, it is recommended to upgrade to XSS-SQL 4.x.x instead of XSS-AD. If it is desired to use the XSS-AD software, the configuration will need to be completely rebuilt. Please contact Ensure Technologies for assistance.

Upgrading from XSS 3.x.x or earlier 4.xx version

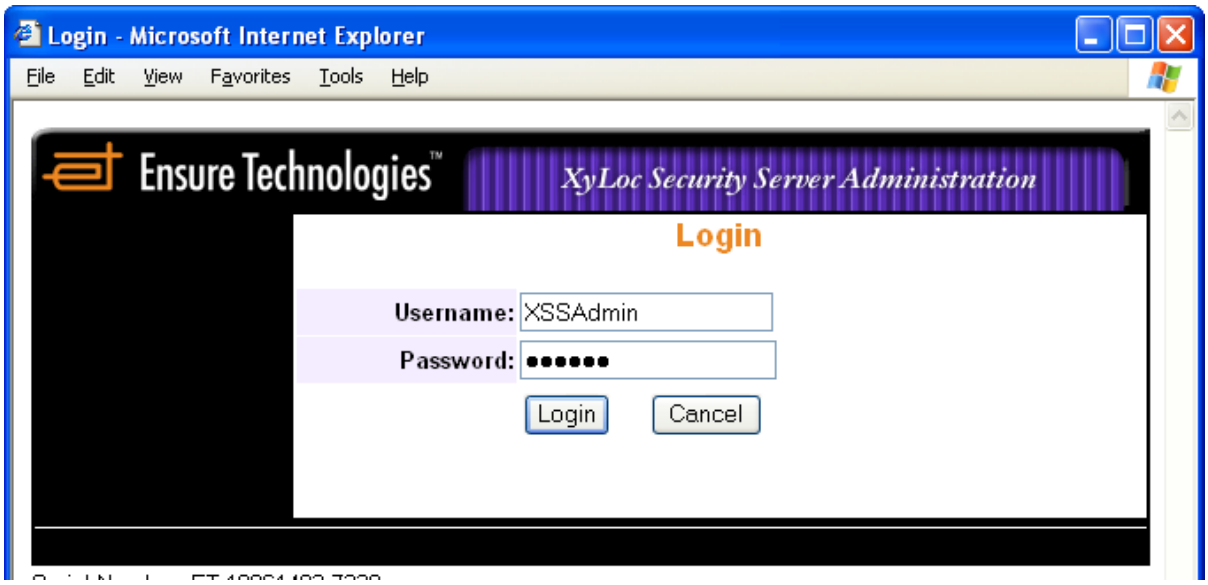
If using XSS-AD version 3.x or an earlier 4.x version of XSS-AD and it is desired to upgrade to a later version of 4.x the specific steps for upgrade will depend on the version that is being used currently and the version that is being upgraded to. Please contact Ensure Technologies Technical Support for proper upgrade instructions.

With the XSS-AD, the XSS is used to create a link between the XyLoc client software and Active Directory. This is done through the XyLoc Security Server Daemon running on the XSS server.

There is still an XSS Web Browser interface, but this interface is only used to view the stored XyLoc Audit Logs and available licenses. Also, additional XSS Administrator accounts can be created in this web interface to give them access to the interface itself.

Accessing the XSS

To access the XSS, go to your WEB browser and type the static IP address of XSS along with the directory path of the server installation. An example would be: http://10.10.10.10/xssad/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.

NOTE: The software does require at lease 6 characters for the XSS Administrator password. If successful, a message will be shown at the bottom indicating "Update User Info Succeeded". If there is something wrong (the password and confirmed password do not match), a message will be shown at the bottom indicating "Update User Info Failed".

IMPORTANT: If a user mistypes the password for 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 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 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.

Users

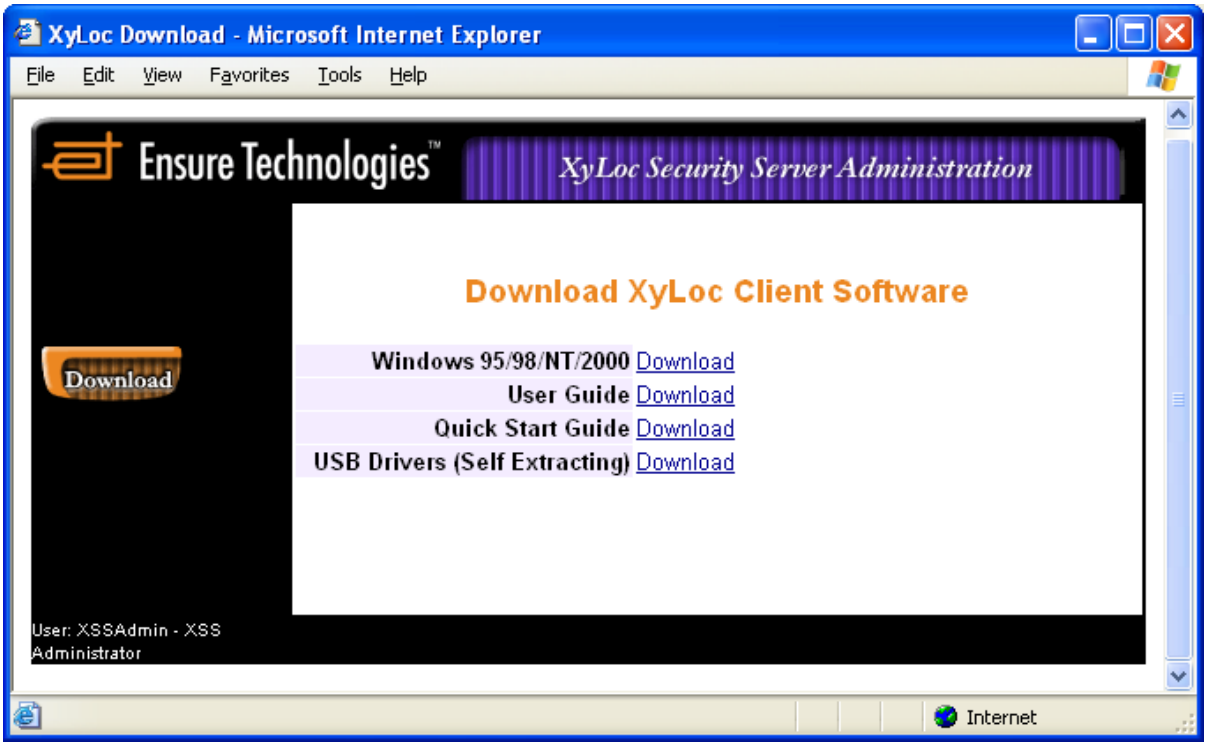
These are only users of the XSS Web Interface. Additional XSS Administrators can be created and managed from this page. This is a separate database from Active Directory, and used only for this web interface.

This screen also shows the user license information. The licenses are based on the number of configured XyLoc Keys in Active Directory.

As of version 4.2.1 this interface can now also be used to view all of the configured XyLoc users in Active Directory.

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.



Host-based Kiosk

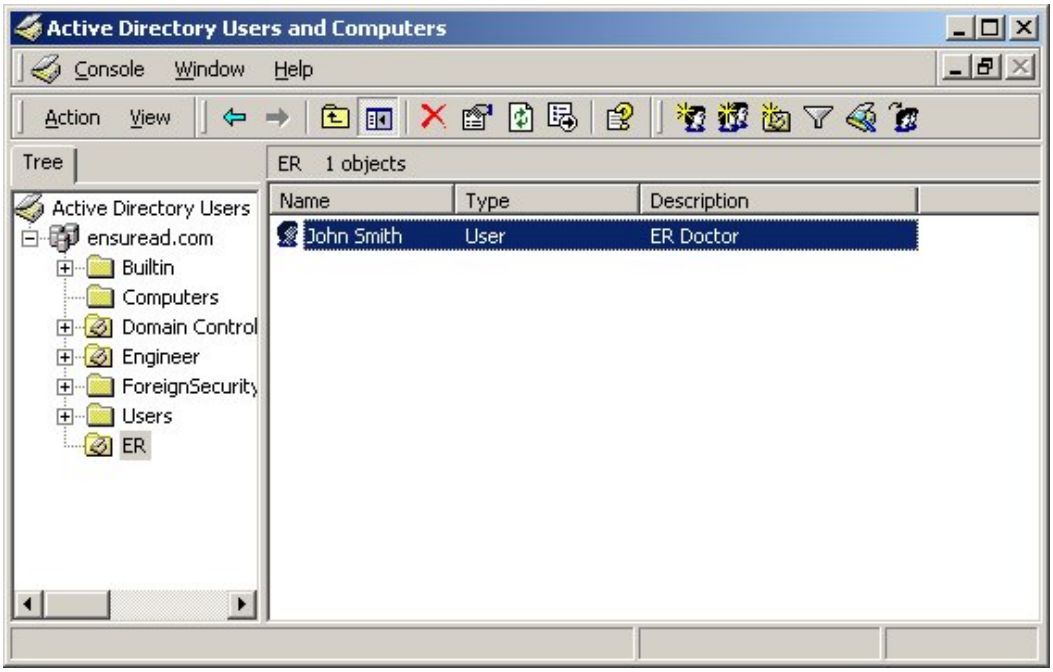
In XSS version 4.2.0, the process of managing Users and Computers in the XSS changed to support a new Host-based Kiosk setup. This allows the setup where an organization would like to have a different kiosk account for each machine (for instance, using the machine name as AD Username). This required a change in the way users and computers were configured. Unfortunately, the "legacy" management process is no longer supported in version 4.2.0 or later. In this document both methods are described. If version 4.1.9a or earlier is being used, then please skip down to the section for "**Legacy XSS-AD Management**" for the correct details on managing users and computer.

Managing XyLoc Users

There are two basic types of accounts within XyLoc:

- **Unique user account:** a unique user is a **single** XyLoc key permitted to access a single Active Directory account.
- **Kiosk user account (available in the XSS-MD):** a kiosk user is one of **many** XyLoc keys permitted to access a single Active Directory account. Each kiosk user, however, has a unique XyLoc password. This password is synched to their individual Active Directory account password. Because of this, each user in the kiosk must also have an individual Active Directory account.

To manage XyLoc user and computer, start the "Active Directory Users and Computers" management tool from the Administrative Tools.



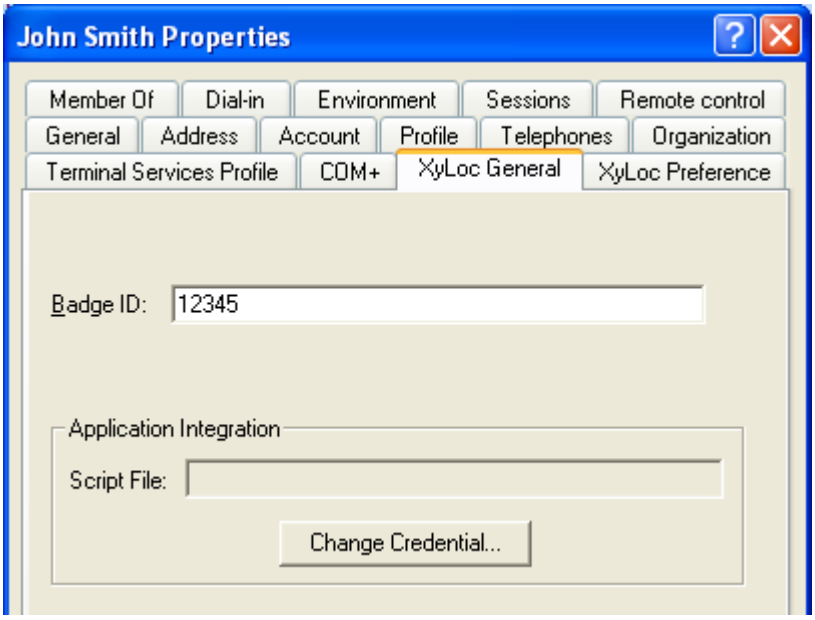
From the user properties sheet, there are two new property pages that are used to manage XyLoc users.

- **XyLoc General**
- **XyLoc Preference**

XyLoc General Property Page

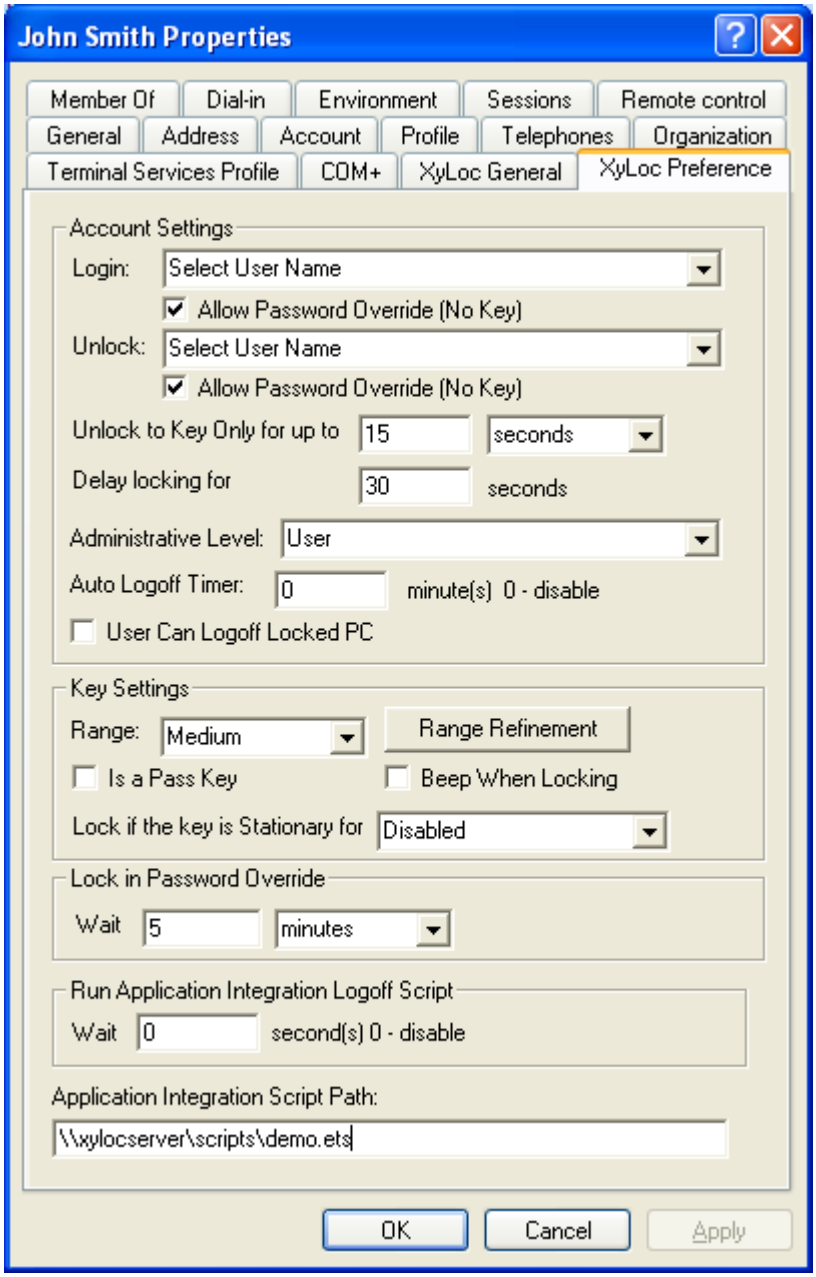
Click on the "XyLoc General" tab to manage the XyLoc user general information. In "XyLoc General" there are settings related to the user themselves.

- **Badge ID:** This is where the XyLoc KeyID is configured for this user (if this account is to be used as a Kiosk, then don't configure a Badge ID for this user)
- **Script File:** Displays the file path to the AI script that is assigned to the user (if any).
- **Change Credential:** Allows the administrator to set the credentials for the user's applications that are setup with Application Integration scripts. For this option to work, the AI Script file must be in a network share that is located on the same server as the Active Directory. If not, then the user must manage the passwords for their applications at the XyLoc client. Please refer to the XyLoc Client User Guide for more information.



XyLoc Preference Property Page

Click on the "XyLoc Preference" to manage the XyLoc preferences for this user.



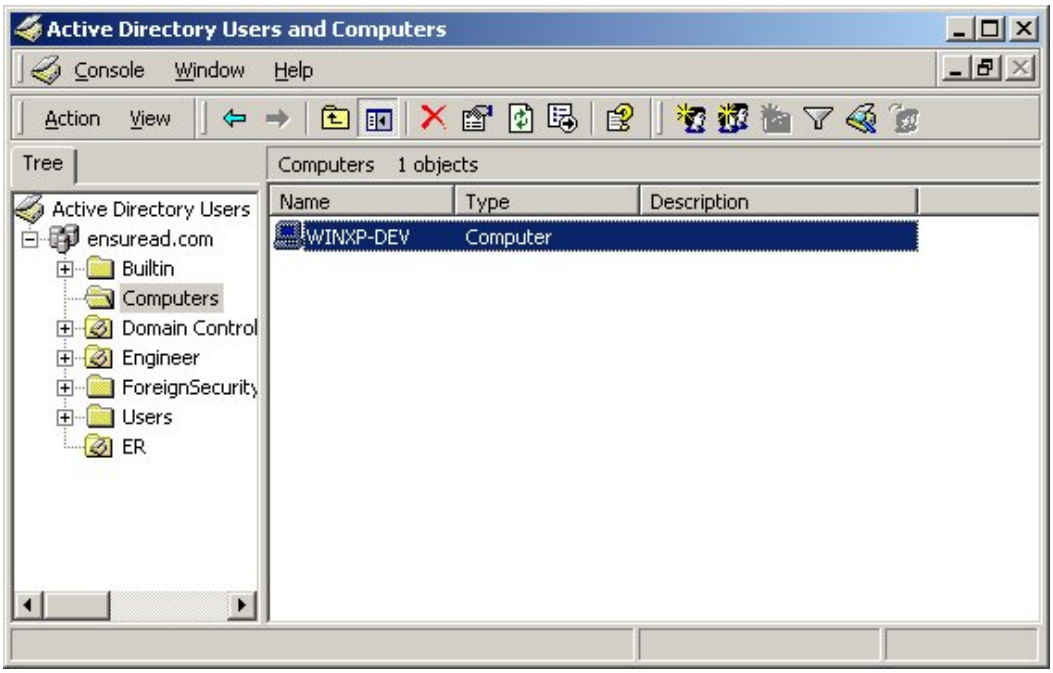
In this property page, Administrator can determine this user's XyLoc preference, such as Authentication options, XyLoc Proximity badge ranges for lock and unlock, etc.

The setting for "Application Integration Script Path" is used to direct the user's record to a specific location for a XyLoc Application Integration script, if one is being used.

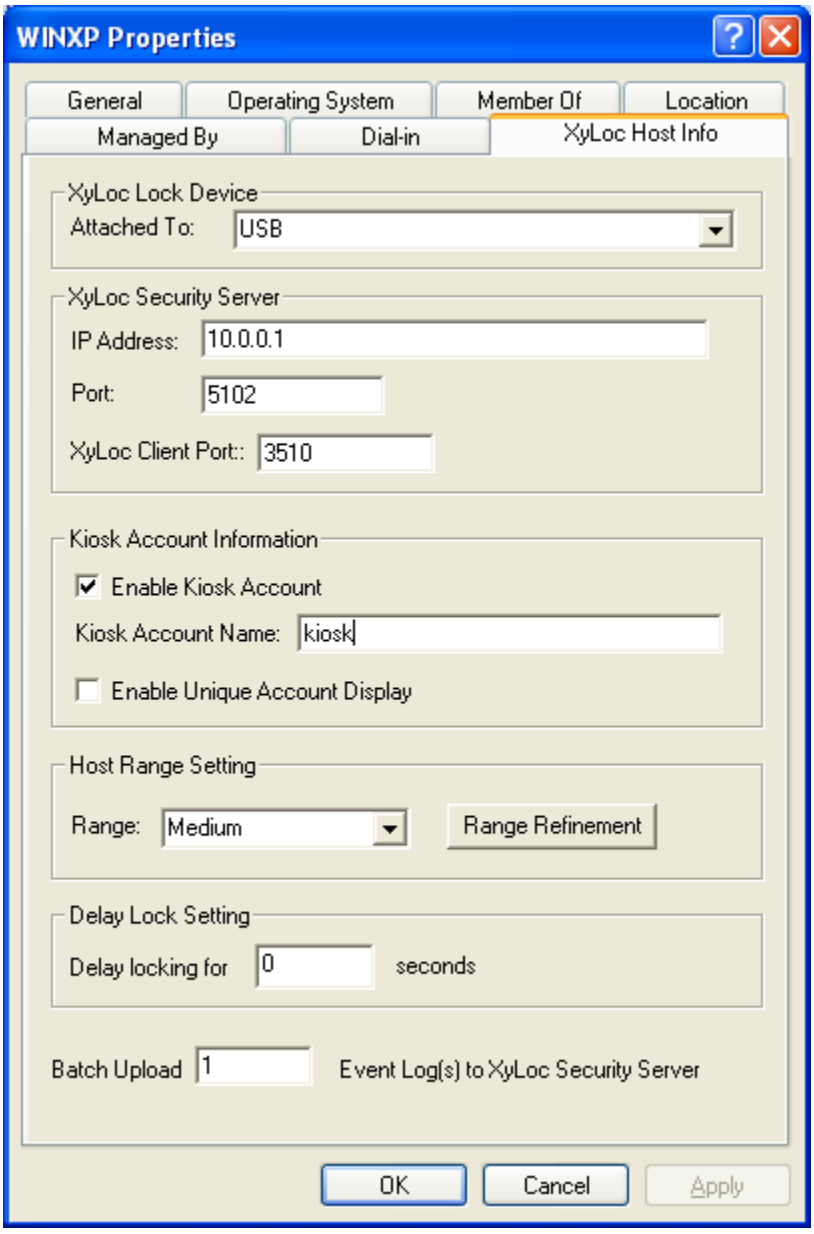
Managing XyLoc Computers

XSS-AD also provides one property page to manage any computers that are equipped with the XyLoc proximity device.

- To manage the computer, from the "Active Directory Users and Computers" management console, select and right click on the computer and select "properties".



- From the Computer property sheet, there is one new property page “XyLoc Host Info” that is used to manage computer with XyLoc device.
- Click on the “XyLoc Host Info” to manage the XyLoc information for this computer.



- In this property page, Administrator can manage information that is associated with this computer. The field that **MUST** be configured is the XSS IP address. The XSS IP address is blank by default and the correct XSS IP address must be entered here. If the IP address is not configured in this setting, then the first time the client communicates to the server, the AD will send back a blank setting and will remove the IP address from the client, causing it to no longer communicate to the server. It is very important to populate this field prior to installing the XyLoc client software on the PC.
- Under the “Kiosk Account Information” section, at least one of the boxes must be checked. If neither box is checked, then **no** keys will be authorized on this PC.

- If this PC is going to be Kiosk only, then only check the "Enable Kiosk Account" box.
- If this is to be Unique only, then only check the box for "Enable Unique Account Display".
- If both are desired then check both.

- NOTE: The option under "XyLoc Host Info" for "Host Range Setting" will always be visible even if Host Based Ranges is not enabled (see section for **User vs. Host Based Ranges**). If this setting is enabled, then the desired Lock/Unlock range must be set on each Computer and will apply to all users that access this particular computer regardless of what their range settings are defined as.

User Grouping

Active Directory uses Groups to manage shared resources and security policies. The XSS-AD utilizes the capabilities of Active Directory groups to arrange users into manageable units. All XyLoc Security/Preference settings can be applied to all users within the appropriate security group.

To manage the XyLoc users from the Active Directory group, the Administrator needs to:

A) Create a new security group or select an existing security group in the active directory.
B) Check the box at the top for "Enable XyLoc Preferences" in the XyLoc tab.
C) Determine the XyLoc users that will be in this security group
D) Assign the XyLoc user to be a member of this group if they are not already

XyLoc Setting Precedence

XyLoc will use the following order to determine the precedence of the XyLoc settings for a user:

A) Use the group XyLoc Preference if the user is the member of this group and the group XyLoc preference is enabled.
B) Use the user's XyLoc preference if the user does not belong to a group or the group XyLoc Preference is disabled.

NOTE: If Host-based ranges are being used, then the ranges must be set on each individual Host. Any ranges set in the group will not be used. If User-based ranges are configured, then the range setting is subject the same precedence as described above.

Functional Limitation

Active Directory allows a user to be a member of more than one group and a group can also be a member of another group. To simplify the management tasks and avoid ambiguous conflicts, XyLoc Active Directory will not support multiple groups or hierarchy groups.

Administrators can still setup a user to be a member of multiple groups or a hierarchy group structure for other policies or settings, but XyLoc will only tie to one XyLoc Group preference setting.

To help the Administrator manage the XyLoc Preference for the group, a new setting "Enable XyLoc Preference Setting" is added to the XyLoc Preference. The default value of this setting is unchecked which means that the XyLoc Preference is **not** used for this group. If the Administrator wants the XyLoc Preference setting to be used for this group, he/she must check this setting to turn on the XyLoc Preference.

Computer Grouping

As with the user settings, the computer settings can be grouped as well, except Host Ranges (at this time Host Range settings do not support Grouping. Each computer's range must be defined individually). However, keep in mind that when using a group, ALL of the settings for the XyLoc Host Info will be defined. There is not a way to specify which of the XyLoc settings will apply and which will not. This includes the "Enable Kiosk Account" setting and the "Kiosk Account Name" that are defined.

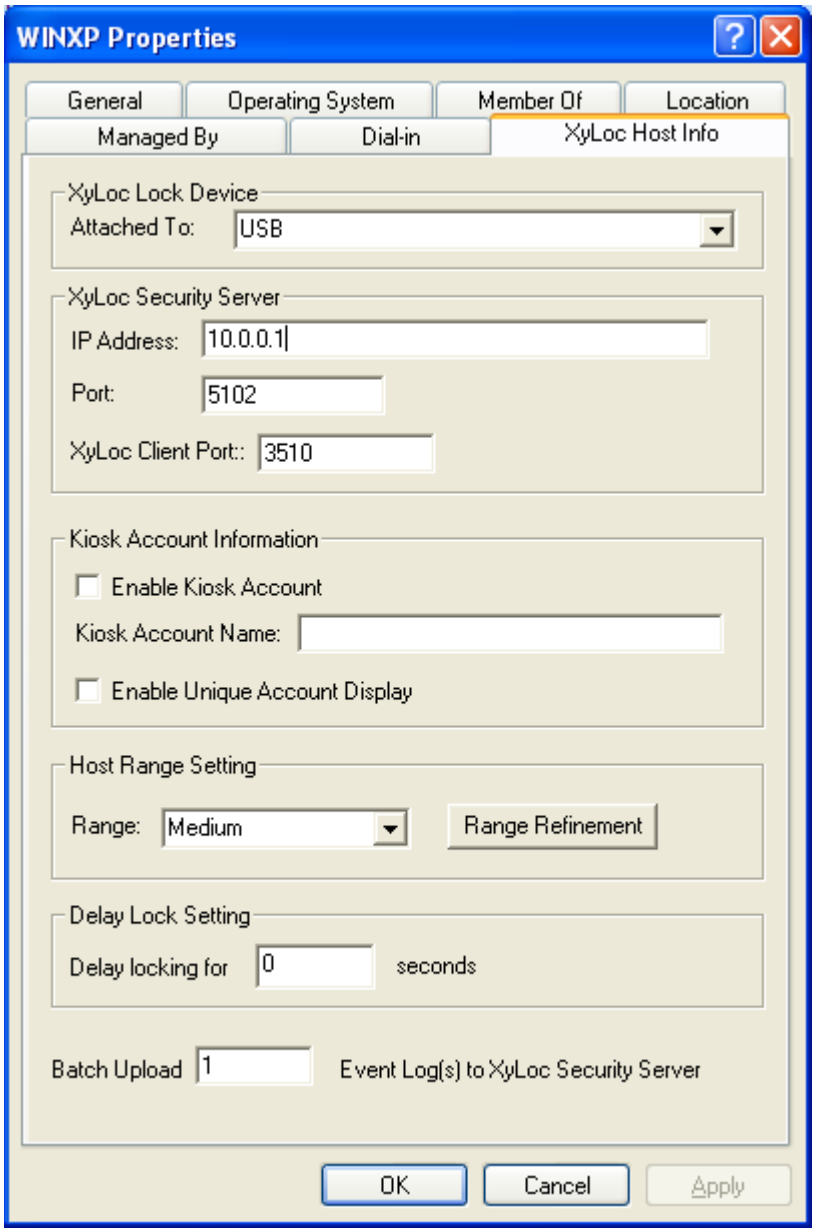
Kiosk Accounts

Ensure has developed the Kiosk account to help improve the efficiency of the shared PC environment. Ensure will utilize the Active Directory Schema extension and the UI extension associated with the computer to allow the Administrator to create the Kiosk. All XyLoc users will use the defined shared kiosk account for login on that PC. **NOTE**: There is an option to also allow a unique account logon to the PC.

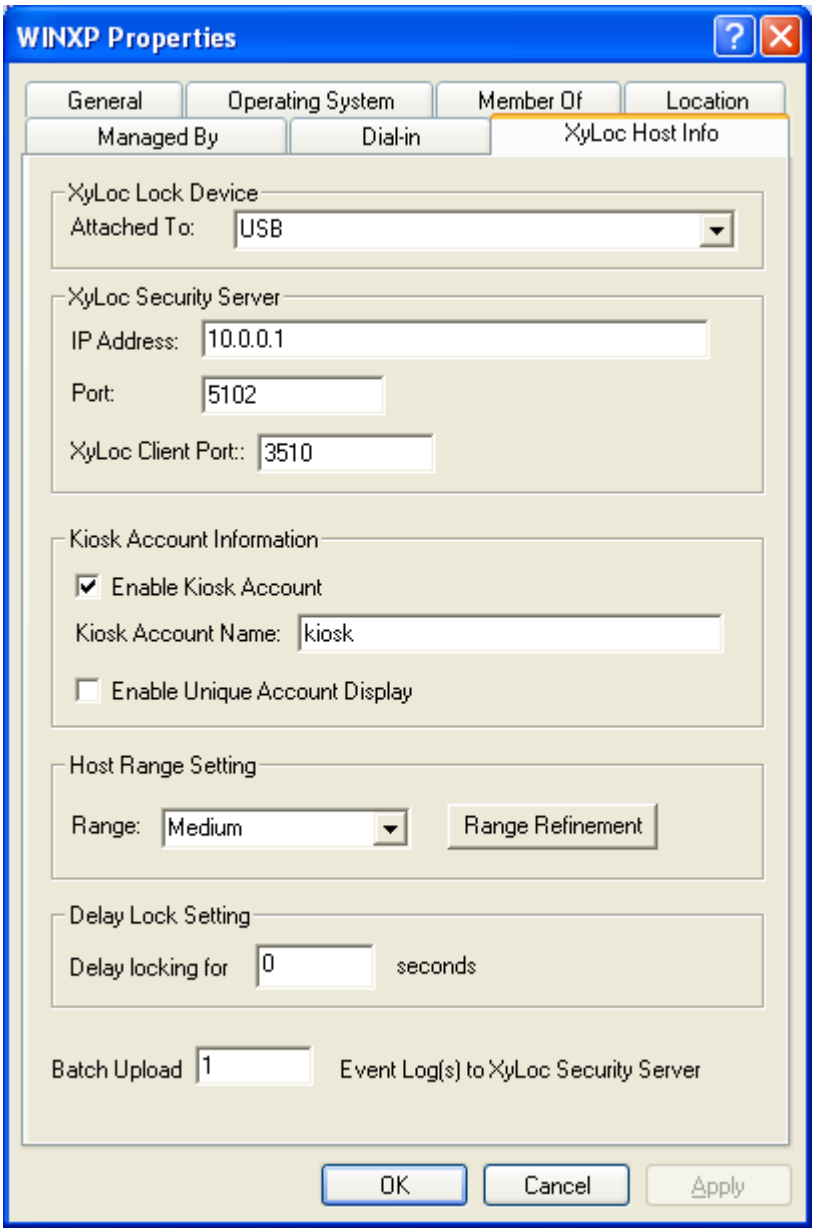
When creating a Kiosk account from the XSS over a network, there are several steps that need to be followed. It is very important that these steps be implemented in the following order.

1. Create the desired Kiosk account in Active Directory, or select an existing "Shared" account that has already been created. For this example, the account is called "kiosk".
2. Select the Computer that is to be used for the Kiosk account and go to Properties. **NOTE**: These instruction refer to one specific host, however a group can be used as well. All of the following settings are listed in the AD Group settings, so an existing group of PCs can be used, or a new group of PCs can be created.
    a. To use a group, however, all of the PCs in the group will have to be using the same shared kiosk account, since this is a setting in the group as well and there is no way at this time to specify which settings are defined and which are not.
    b. If each host will have its own unique shared login account, then each PC must be configured individually.

3. Make sure the XSS IP Address is defined



4. Check the box for "Enable Kiosk Account" and define the specific AD Username to be used on this PC for the shared kiosk account.



NOTE: Here are some details about the functionality of the Kiosk accounts in XSS-AD:

1. If desired, the user's unique account can also be displayed, allowing the user to login with either the Kiosk account or their unique account.

    a. Keep in mind that this will be true for ALL users of this PC. There is no way to define which users will be able to see their unique accounts and which will not. Any users that approach this PC with a valid XyLoc Key will be given the option to login with either account.
    b. Also, the unique account will only be displayed at the initial login screen. If the kiosk account is already logged on, and the screen is simply locked, the user will only see his/her kiosk account displayed as there is no need to display their unique account. If they want to login with the unique account, they can simply

unlock with the Kiosk account and then logoff the PC gracefully. Then, once logged off, they will see their unique account displayed for them to login with.

c. If a user logs in with their unique account, then only that user's Key will be displayed at a locked screen until it is logged off, unless the other users have the option enabled for "User can logoff locked PC".
d. **IMPORTANT**: If this is to be Kiosk only, then only check the "Enable Kiosk Account" box. If this is to be Unique only, then only check the box for "Enable Unique Account Display". If both are desired then check both. However, at least one must always be checked. If neither box is checked, then **no** keys will be authorized on this PC.

2. In a Kiosk account, each user is sharing the same Active Directory account, as well as the same Active Directory password, with regards to the Microsoft Login. However, XyLoc will require a unique password from the individual users for additional security (if the Login or Unlock Authentication is set for "Must Enter Password"). In the Kiosk account, the user's unique XyLoc password will be their individual Active Directory account password.
3. If both the unique account and kiosk account are enabled then both accounts are displayed at the **Login**. We use the following formatting to distinguish which name is which account in the selection box at login since both will be displayed. NOTE: In this example the kiosk account name is "kiosk", the user's AD account name is "tom" and the user's display name is "Tom Xydis". In this example, the user would see the both of the following names on the list (at login only):

   Tom Xydis
   (tom)

   a. "**Tom Xydis**" is the unique account. When this name is selected, the user's AD account, which is "tom", will be logged on.
   b. "**(tom)**" is the kiosk account. When this name is selected, the user will be logged into the shared kiosk account, which in this example is "kiosk".
   c. This is also impactful in password override mode, if using the method of Password Override. To use password override in unique account, the user will simply enter their normal AD username and password. In the kiosk password override mode, the user must enter "(tom)" (including the parenthesis) as the username and then their AD password. This will set the XyLoc system to login to the kiosk account.

XyLoc Setting Precedence

In the Kiosk account mode, the user's unique account preferences will be used for the kiosk as well as the unique account (if allowed). For example, Dr Smith has his Active Directory account "jsmith" and he is also a member of kiosk account "kiosk". When XyLoc queries the Active Directory, XyLoc will find two separate accounts, but will use only the preference defined in "jsmith" for both accounts. If a group is used, then the settings from the group will take precedence over the user settings.

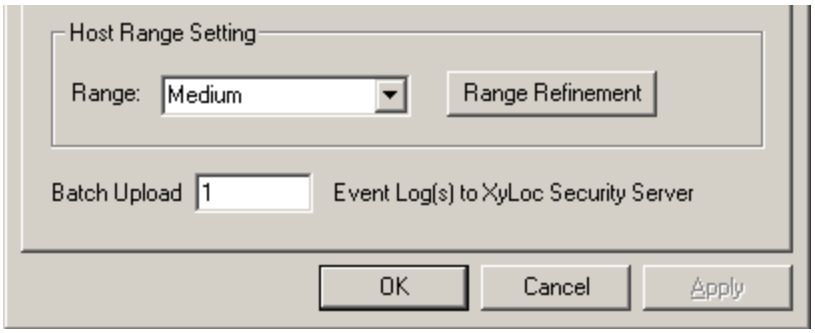
User vs. Host Based Range Settings

By default, the ranges are set per user (or user group). If it is desired to set the range per user or user group, then nothing different needs to be done since this is the default. If it is preferred to set

the range specific to the computer (Host) then please use the following steps to enable this functionality:

1. Create a new user in Active Directory with the username of **xylocglobalconfig**
    a. This account does not need any specific permissions as it is just a placeholder for the global settings used by the XSS.
2. Go to the properties of this user and click on the tab for "XyLoc Config"
3. Change the drop down box to "Host Based Ranges"

4. Click "OK" to save the change.
5. Go to the properties of the computer in Active Directory and click on "XyLoc Host Info" and set the desired range for this PC.
    a. The default range setting is Lock: 9 and Unlock: 5



6. Click "OK" when finished.

NOTE: Groups are **not** supported for Host-based ranges. The PC can still be in a group for Kiosk Settings, XSS IP Address, etc. However, if Host-based ranges are going to be used then they must be set on each host individually.

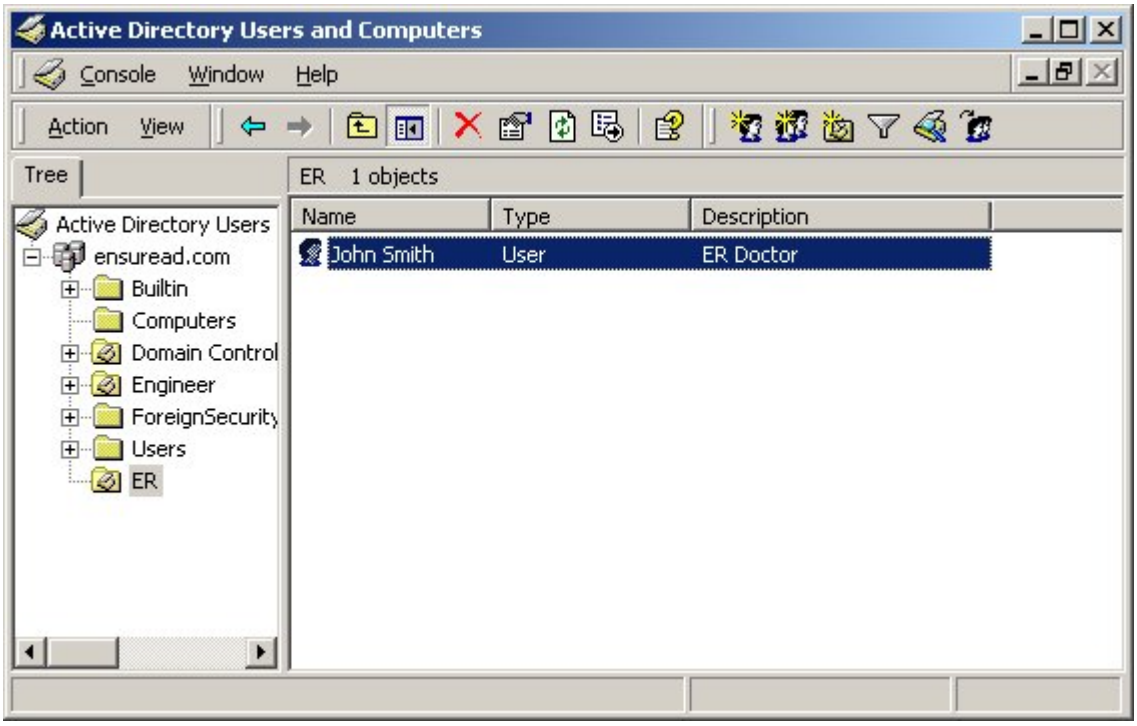
This section contains the details for managing users and compute in XSS-AD version 4.1.9a or earlier. If using version 4.2.0 or later, then please refer to the previous section for "Using XSS-AD".

Managing XyLoc Users:

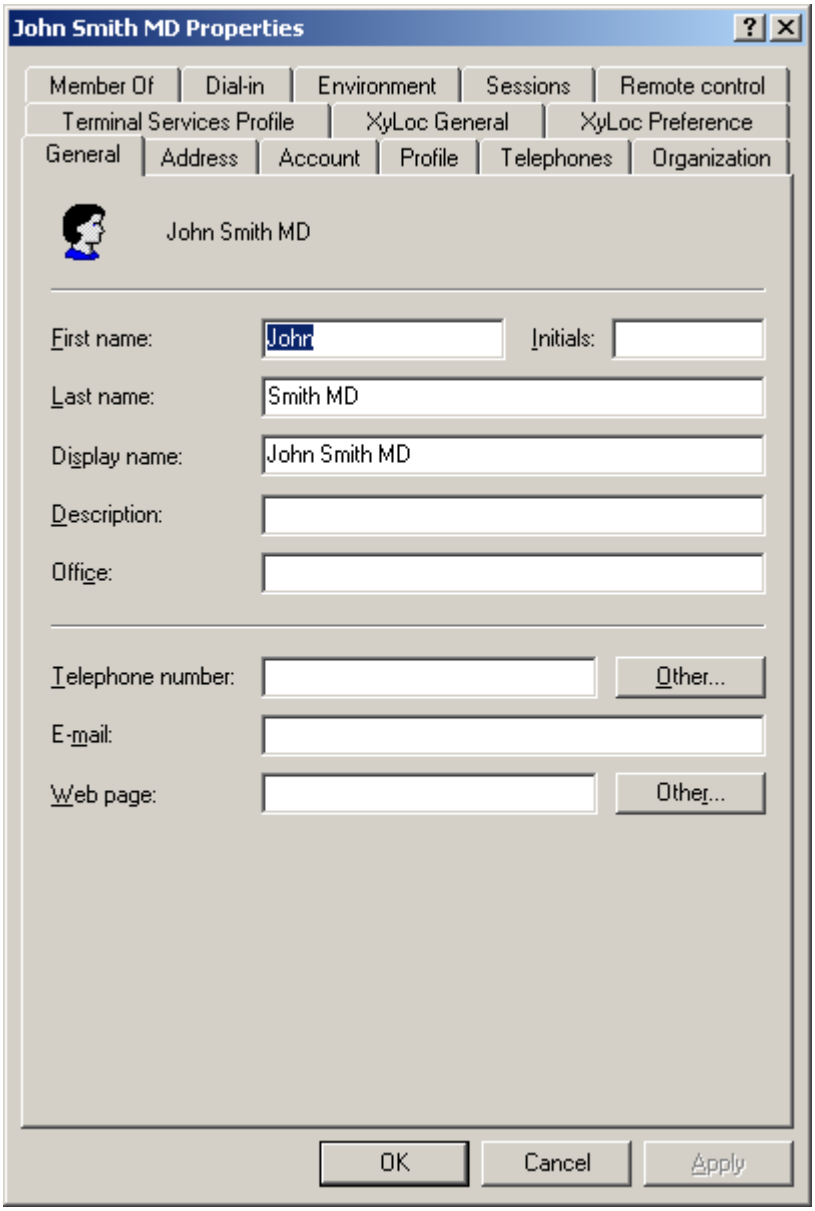
There are two basic types of accounts within XyLoc:

- **Unique user account:** a unique user is a **single** XyLoc key permitted to access a single Active Directory account.
- **Kiosk user account (available in the XSS-MD):** a kiosk user is one of **many** XyLoc keys permitted to access a single Active Directory account. Each kiosk user, however, has a unique XyLoc password. This password is synched to their individual Active Directory account password. Because of this, each user in the kiosk must also have an individual Active Directory account.

To manage XyLoc user and computer, start the "Active Directory Users and Computers" management tool from the Administrative Tools.



- In this example, right click on the user "John Smith" and select "properties".
- From the user properties sheet, there are two new property pages "XyLoc General" and "XyLoc Preference" that are used to manage XyLoc users.



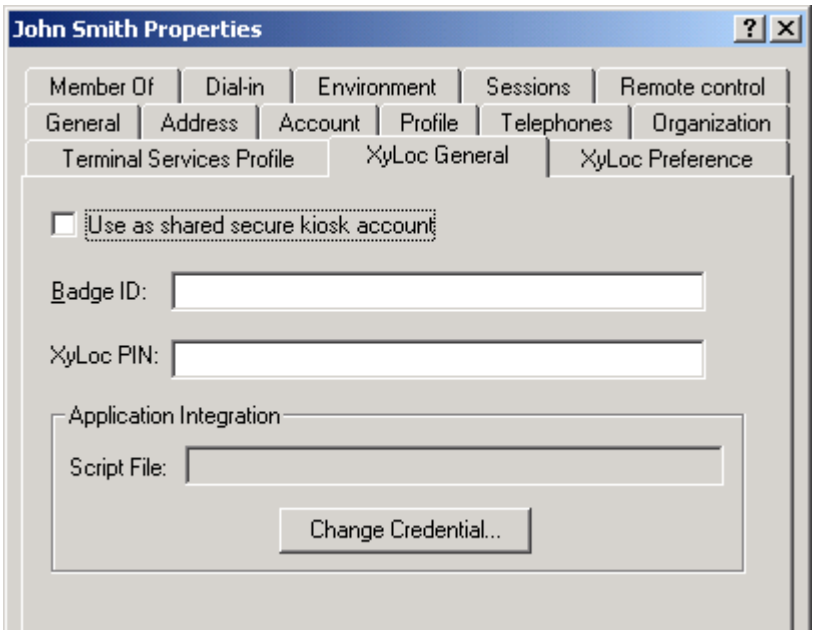
XyLoc General Property Page

- Click on the "XyLoc General" tab to manage the XyLoc user general information.
- In "XyLoc General" there are settings related to the user themselves.

  - **Use as shared secure kiosk account:** This is allows an administrator to designate this account as a shared kiosk account for multiple users to share.
  - **Badge ID:** This is where the XyLoc KeyID is configured for this user (if this account is to be used as a Kiosk, then don't configure a Badge ID for this user)
  - **XyLoc PIN:** Used to enable a XyLoc password for the user in place of the AD password. This setting is ONLY used for when the user is assigned to a kiosk and

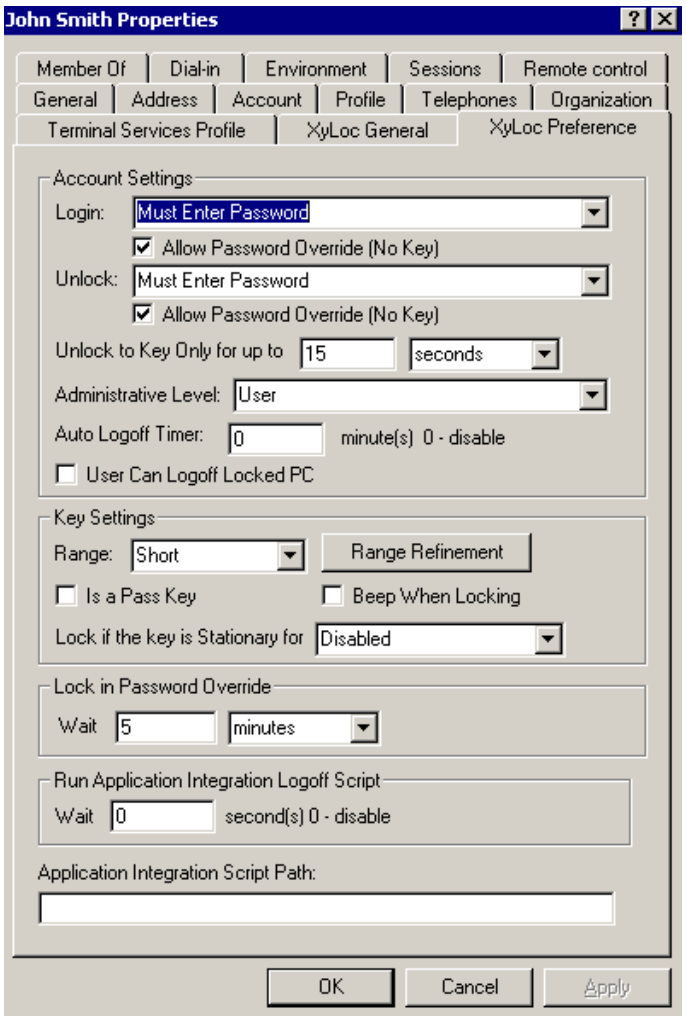
will only be valid in the kiosk login. The user's unique account will synchronize with the user's AD password automatically.

- **Change Credential:** Allows the administrator to set the credentials for the user's applications that are setup with Application Integration scripts. For this option to work, the AI Script file must be in a network share that is located on the same server as the Active Directory. If not, then the user must manage the passwords for their applications at the XyLoc client. Please refer to the XyLoc Client User Guide for more information.



XyLoc Preference Property Page:

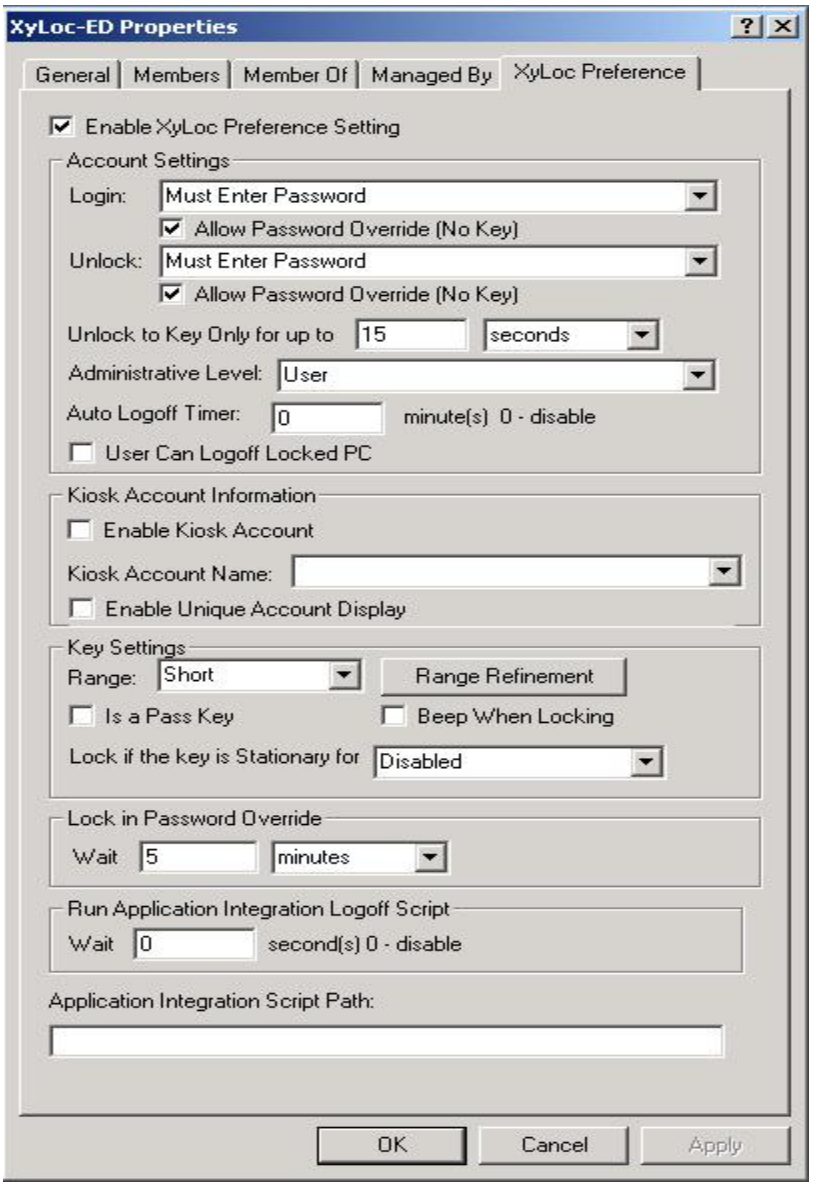
- Click on the "XyLoc Preference" to manage the XyLoc preferences for this user.



- In this property page, Administrator can determine this user's XyLoc preference, such as Authentication options, XyLoc Proximity badge ranges for lock and unlock, etc.
- The setting for "Application Integration Script Path" is used to direct the user's record to a specific location for a XyLoc Application Integration script, if one is being used.

Grouping

Active Directory uses Groups to manage shared resources and security policies. The XSS-AD utilizes the capabilities of Active Directory groups to arrange users into manageable units. All XyLoc Security/Preference settings can be applied to all users within the appropriate security group. The following screenshot is a sample of the XyLoc Preference integrated into the group "XyLoc-ED"



To manage the XyLoc users from the Active Directory group, the Administrator needs to:

A) Create a new security group or select an existing security group in the active directory.
B) Determine the XyLoc users that will be in this security group
C) Assign the XyLoc user to be a member of this group

XyLoc Setting Precedence

XyLoc will use the following order to determine the precedence of the XyLoc settings for a user:

A) Use the group XyLoc Preference if the user is the member of this group and the group XyLoc preference is enabled.
B) Use the user's XyLoc preference if the user does not belong to a group or the group XyLoc Preference is disabled.

Functional Limitation

Active Directory allows a user to be a member of more than one group and a group can also be a member of another group. To simplify the management tasks and avoid ambiguous conflicts, XyLoc Active Directory will not support multiple groups or hierarchy groups.

Administrators can still setup a user to be a member of multiple groups or a hierarchy of groups for other policies or settings, but XyLoc will only tie to one XyLoc Group preference setting.

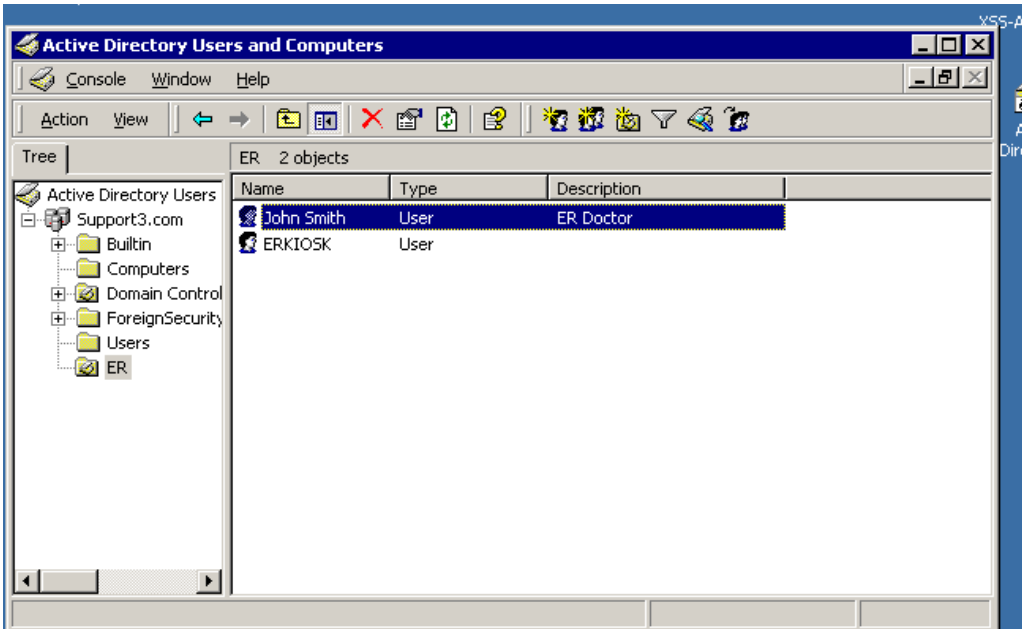
To help the Administrator manage the XyLoc Preference for the group, a new setting "Enable XyLoc Preference Setting" is added to the XyLoc Preference. The default value of this setting is unchecked which means that the XyLoc Preference is not used for this group. If the Administrator wants the XyLoc Preference setting to be used for this group, he/she can simply check this setting to turn on the XyLoc Preference.

Kiosk Accounts (available in XSS-MD)

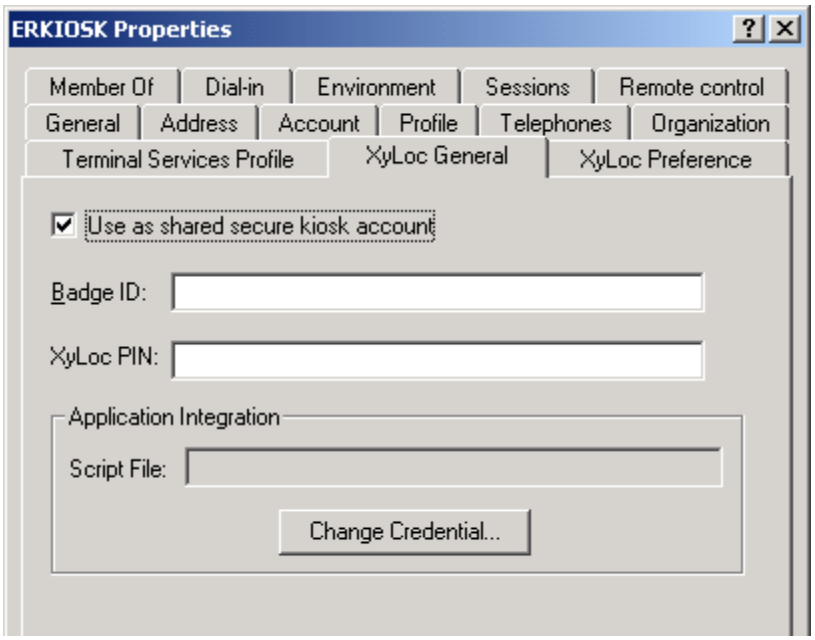
Ensure has developed the Kiosk account to help improve the efficiency of the shared PC environment. Ensure will utilize the Active Directory Schema extension and the UI extension associated with the Active Directory group to allow the Administrator to create the Kiosk group. All users in the group will use the (single) shared kiosk account for Active Directory login.

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

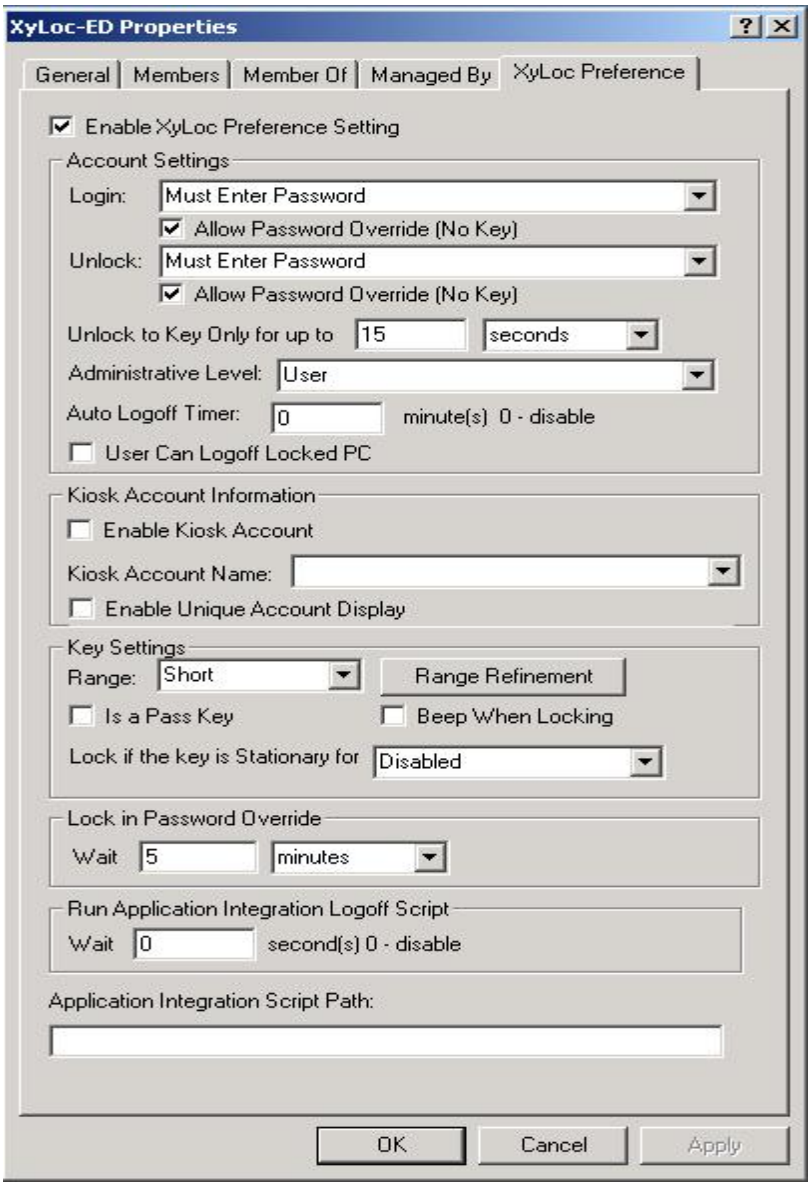
1. Create the desired Kiosk account in Active Directory, or select an existing "Generic" account that has already been created. For this example, the account is called "ERKIOSK".



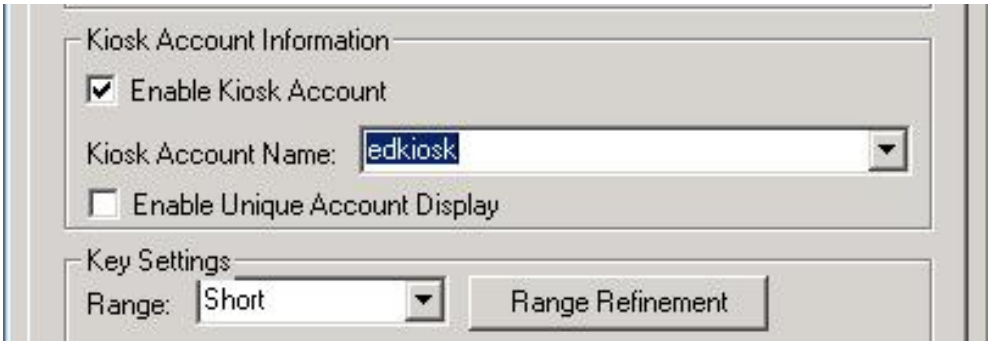
2. Setup the user as the kiosk account.



3. Create a new Security Group (or use existing group if desired) and under the XyLoc Preferences tab check the box for "Enable XyLoc Preference".



4. Under XyLoc Preferences check the box for "Enable Kiosk Account" and select the Kiosk account that this group will use.



5. Make the users that are to be part of the kiosk a member of the new Kiosk group.

NOTE: Here are some details about the functionality of the Kiosk accounts in XSS-AD:

- The Administrator can decide if the user's unique account should also be displayed during login by checking the "Enable Unique Account Display". This box is NOT checked by default.

- If the box to Enable Unique Account Display is checked, then at login, both the user's unique account and kiosk account will be displayed as authorized users to login. If the box is unchecked, then only the Kiosk account will be displayed.
- At unlock, only the account that is authorized to unlock the PC will be displayed. For instance, if the PC is logged into the Kiosk account, then only the user's Kiosk name will be displayed.
- In a Kiosk account, each user is sharing the same Active Directory account, as well as the same Active Directory password, with regards to the Microsoft Login. However, XyLoc has the ability to require a unique password from the individual users for additional security (Login or Unlock Authentication must be set for "Must Enter Password"). In the Kiosk account, the user's unique XyLoc password will be synched with their individual Active Directory account password so the users do not have to remember multiple passwords.

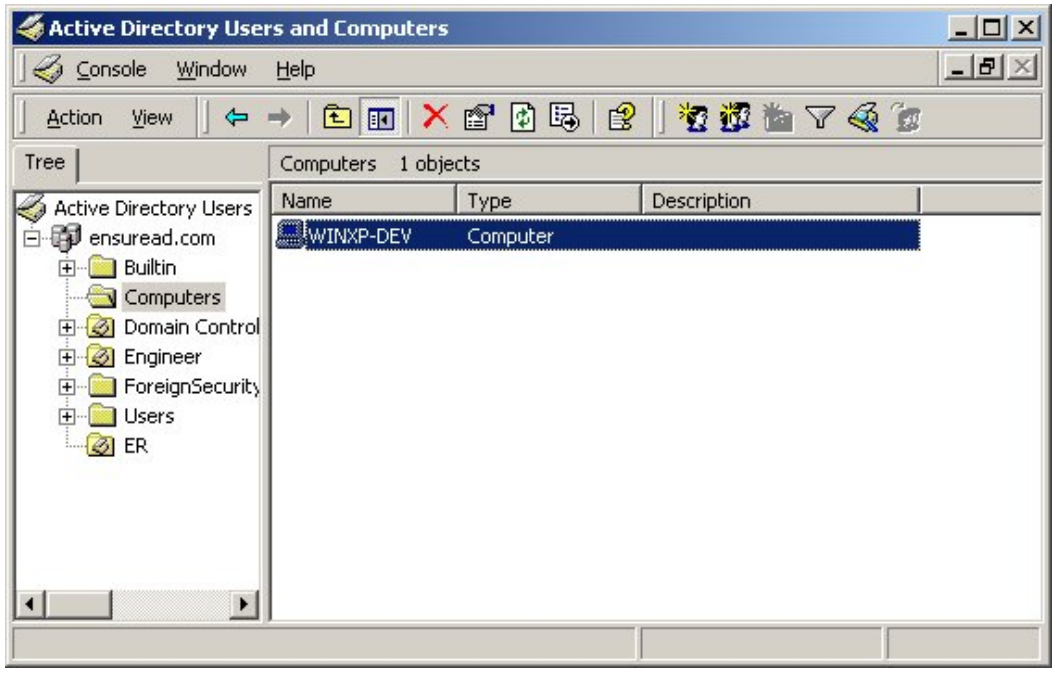
XyLoc Setting Precedence

In the Kiosk account mode, the group XyLoc Preference will be used for the kiosk as well as the unique account, if used. For example, Dr Smith has his Active Directory account "drsmith" and he is also a member of the Kiosk Group which uses the kiosk account "edkiosk". When XyLoc queries the Active Directory, XyLoc will find two separate accounts, but will use only the Kiosk Group Preference settings for both accounts.

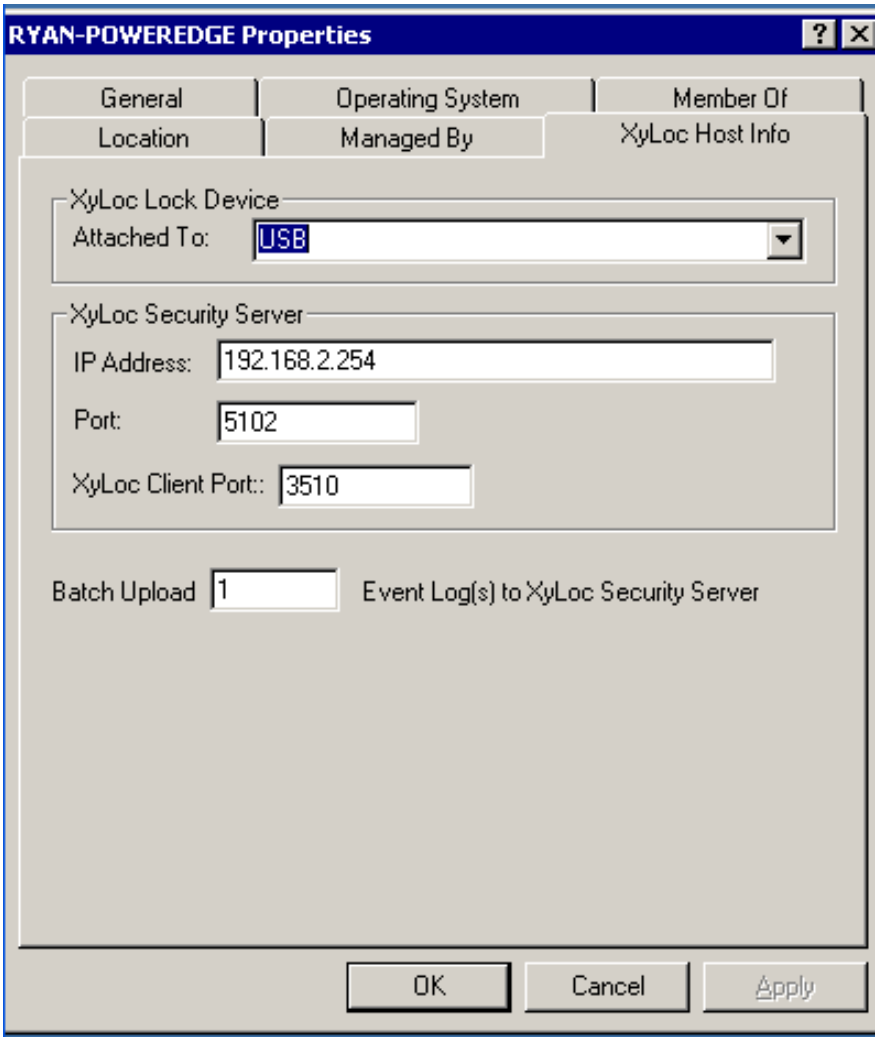
XyLoc Computer Property Page

XSS-AD also provides one property page to manage any computers that are equipped with the XyLoc proximity device.

- To manage the computer, from the "Active Directory Users and Computers" management console, select and right click on the computer and select "properties".


Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Computers 1 objects
Active Directory Users
ensuread.com
Builtin
Computers
Domain Control
Engineer
ForeignSecurity
Users
ER
Name
Type
Description
WINXP-DEV
Computer

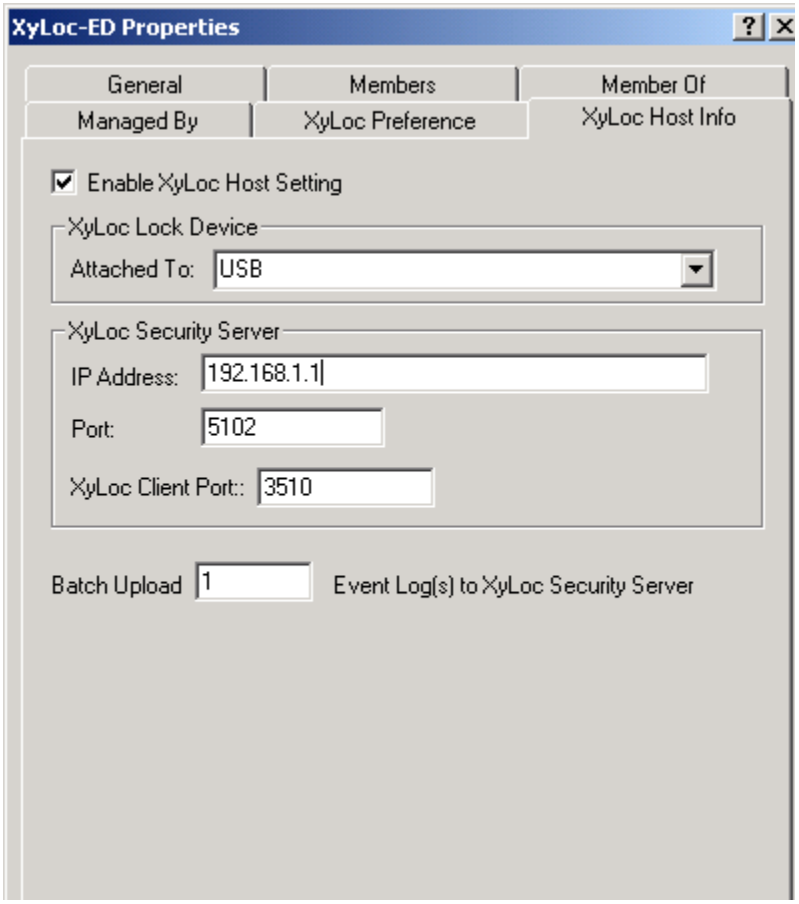
- From the Computer property sheet, there is one new property page “XyLoc Host Info” that is used to manage computer with XyLoc device.
- Click on the “XyLoc Host Info” to manage the XyLoc information for this computer.



- In this property page, Administrator can manage information that is associated with this computer. The field that **MUST** be configured is the XSS IP address. The XSS IP address is blank by default and the correct XSS IP address must be entered here. If the IP address is not configured in this setting, then the first time the client communicates to the server, the AD will send back a blank setting and will remove the IP address from the client, causing it to no longer communicate to the server. It is very important to populate this field prior to installing the XyLoc client software on the PC.

Grouping

As with the user settings, the computer settings can be grouped as well.



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.

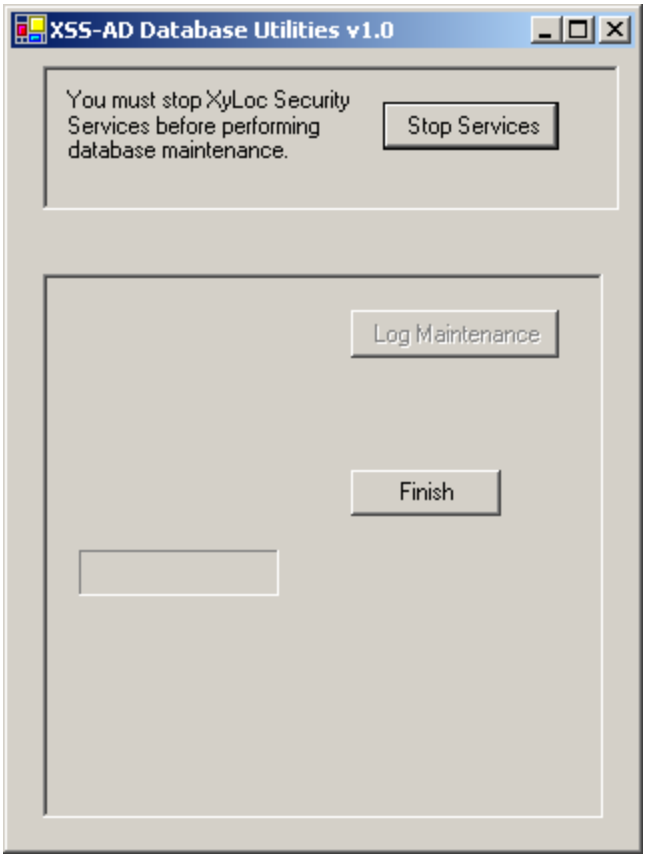
Optionally, this service can be configured to automatically restart the service at a given time each day. This is done through a registry setting on the XSS Server. To enable this functionality, create a string registry value named 'MonitorTime' under HKEY_LOCAL_MACHINE\SOFTWARE\Ensure Technologies\XSS. Set the value of 'MonitorTime' to the hour that the XSS service is desired 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

There is a SQL Database maintenance utility available with the XSS that can be used to perform basic maintenance of the SQL database. If a full SQL database is used, then Ensure Technologies recommends that the standard SQL maintenance tools provided by Microsoft be used as they will provide much more functionality and flexibility.

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-AD-DBUtility.exe".



In the XSS-AD, the user configuration is contained in Active Directory. Only the XyLoc logs are stored in the XSS database. From this utility the following options are available:

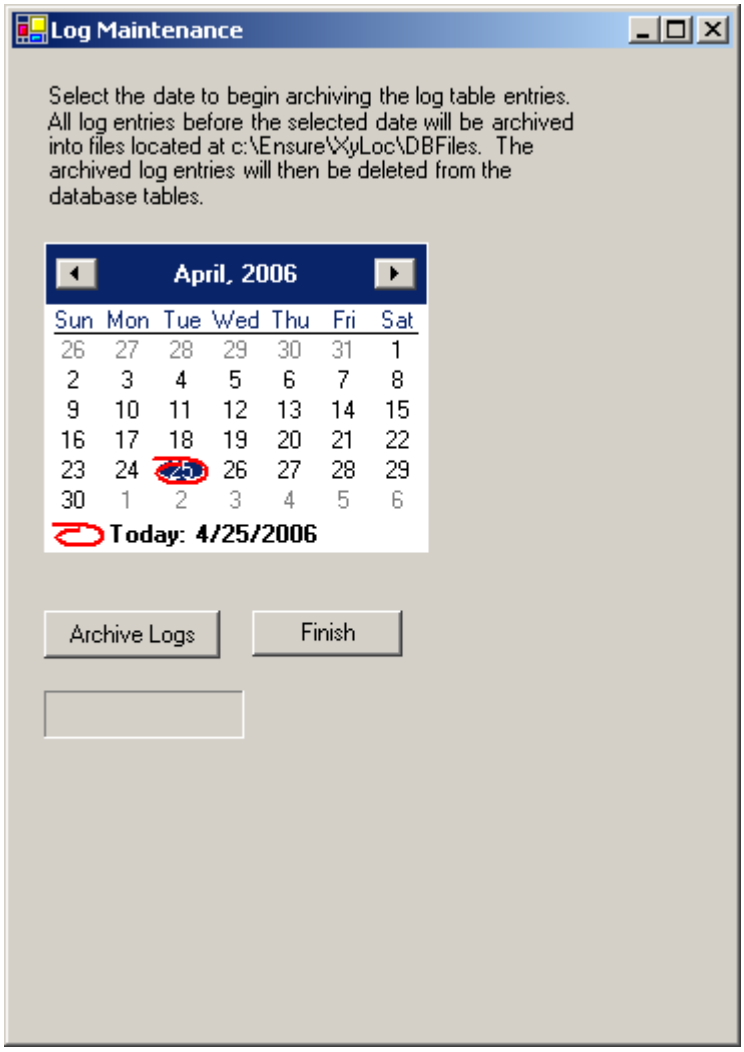
1. Stop and Start the XSS Service
2. Purge old log files

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".

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.

When finished with the XSS-AD Database Utility, click "Start Services" to restart the XSS service, and then click "Finish".

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 IP address of the XSS Server 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.

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.

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, make sure the XSSAD installation was converted to an application in IIS.

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).
- Server 2008 has a similar firewall to XP. This firewall will block communication to and from the server. If the XSS is installed on Server 2008 and the firewall is enabled, then an exception would have to be defined for both the incoming and outgoing ports for the XSS and Client communication:
    - Transmit to Client: TCP Port 3510
    - Receive from Client: TCP Port 5102
- 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.
- 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.

User's Application Integration credentials are not propagating to other clients

Check the permissions on the XSS Service. Go to the services applet and right click on the "XyLoc Security Server" service and click on Properties. In the tab for "Log On" the setting is likely at the default of "local system account". Change this to a specific account and specify an account that is at least a member of the "Account Operator" group in AD.

Revision History:

Revision	Date	Description	Author
2.0.0	09-04-2009	Created	RS