XyLoc Windows XP Client Release Notes

Support Information:

Ensure Technologies Technical Support is available to provide any needed assistance. Please contact us at (734) 547-1600 or at support@ensuretech.com.

Requirements:

- ❑ Microsoft .NET Framework 3.5 (for new Low Battery Warning message)
- ❑ Basic RAM and CPU Requirements for Windows XP Operating System
- ❑ 100 MB disk space
- ❑ Available USB port
- ❑ Local Administrator privileges for installation.
- ❑ If using in conjunction with the XSS then the appropriate TCP ports for XSS communication must be allowed through the firewall (if firewall is enabled):
    1. Client → Server: 5102
    2. Server → Client: 3510

Compatibility:

- ❑ This XyLoc client is compatible with 32-bit versions of Windows XP and XPe.
- ❑ ***NEW* XyLoc Client 9.3.0.8 requires XSS version 5.1.3 or later of the XSS.**
- ❑ XyLoc supports fingerprint authentication (instead of a password) in conjunction with the XyLoc badge (when using "Must Enter Password" mode of authentication).
    1. Authentec AES3500 and AES4000 (supported in previous versions of XyLoc)
    2. Authentec AES3400 (added in 8.5.0)
    3. Digital Persona "UareU" 4000 series sensors (added in 8.5.0)
    4. All UPEK sensors (according to UPEK documentation)
        1. **NOTE**: Not all of the UPEK sensors have been tested by Ensure. Support is based on UPEK SDK documentation.
        2. Ensure has specifically tested UPEK TSC2 TouchChip® sensor with Cherry Keyboard Model SPOS
- ❑ XyLoc supports Microsoft Windows Auto Logon functionality
    1. To set up this, add a DWORD value "UseAutoLogon" in HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon and set it to 1.
    2. This will also require that Microsoft AutoAdminLogon information to be set up in HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon as per Microsoft specifications.
        1. "AutoAdminLogon" String value set to 1
        2. "DefaultUserName" String value set to the login account name
        3. "DefaultPassword" String value set to the login account's password
        4. "DefaultDomainName" String value set to the login domain name
    3. XyLoc will then automatically lock the workstation immediately upon login to prevent the machine from sitting in a generic password override state.
        1. **NOTE:** The automatic lock will only occur if a login is detected under the name defined in the Winlogon settings.

2. If the Auto Logon is interrupted and a user logs in with a different username, XyLoc will NOT automatically lock and will stay in Password Override mode as before.

3. **NOTE**: If the same account defined in the Winlogon registry is logged in manually (instead of letting the Auto Logon do it for you), XyLoc will recognize that as the same account and WILL automatically lock the workstation as well as long as the "UseAutoLogon" value is defined.

4. For more information on Auto Logon, please review the following Microsoft KB Article: http://support.microsoft.com/kb/310584/en-us

General Client Notes:

- ***NEW* Kiosk vs. Unique Logins:** XyLoc has always supported both a generic shared login (Kiosk) as well as Unique logins. However, there are a number of rules related to authentication that are different for each. In order make sure that those are applied properly we have added a new setting at the workstation level to clearly define whether a workstation is setup for Kiosk or setup for Unique users.
    - This is defined in the registry under "HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)\"
        - Name: "computerAccountType"
        - Value:
            - 0 = Undefined
            - 1 = Kiosk Account
            - 2 = Unique Accounts
- **Lock Delay**: The default user lock delay has been set to 5 seconds in version 9.2 or later.
    - This will cause the lock distance to fluctuate a bit more than before as the locking action also has a time component added to it vs. just distance.
    - This was determined to be the most ideal setting based on testing and customer feedback.
- **"Tap-In" Solutions:** XyLoc now supports two different "tap-in" style solutions.
    - One is using standard XyLoc badges which provides support for a "tap-in" style authentication but maintains walk away security support using active RF (see AppNote 530-0200-023 "Description of 'Tap-in' option with standard XyLoc client" for more details on how to setup and use this feature).
    - The second is using actual Passive Proximity (i.e. HID) cards with an RF Ideas PCProx reader. **NOTE**: This is true passive support for those that may want to use already deployed passive prox badge, but since no Active Proximity is used, it does not offer automatic walk-away security.
- **Custom Logo**: XyLoc can display a customized logo/image at Login or Unlock screens
    - The logo bitmap is in a separate resource (LogoRes.dll), so the logo is independent from the main code.
    - A custom resource dll with a customized logo bitmap can be used in place of the default, or Ensure can create one for a customer as a service.
- **Remote Desktop**: The following must be considered when using Remote Desktop to gain access to a XyLoc protected workstation.
    - When logging in remotely, the XyLoc client will be in a Password Override mode. However, when the "Lock in Password Override" timer expires, the lock request is ignored and XyLocIcon is informed to continue displaying the password Override dialog. The host workstation does <u>not</u> lock.
    - During RDP session, remote Ctrl+Alt+End sequence is ignored and PC is <u>not</u> locked.
    - Remote Disconnect is **<u>required</u>** after session is complete. Access to the host machine is denied as long as an active Remote session is in place.
- **Windows Firewall**: If using an XSS, the communication to the XyLoc client will be blocked by the firewall, if enabled. An exception must be created for TCP Port 3510, or the firewall must be disabled for communication to be restored.
- **Windows XP Fast-User Switching**: Microsoft disables Fast-User Switching when XyLoc is installed (reference Microsoft TechNet article Q294739).
- **Screen Saver:** The "Password Protect" check box in the Screen Saver will no longer have any effect once XyLoc is installed. A screen saver can still be used, but the password protection feature will no longer work.
- **Customizable options for command line or "push" installations of the client:** The client has command line installation options that are available to define some specific registry settings:
    - **fpOverrideFilter**: "msiexec /i XyLoc.msi FP_DLG_FILTER=1

- Used to set the flag as to whether or not to prompt a user for fingerprint when performing an override (see specific enhancements below)
  - **FPRType**: "msiexec /i XyLoc.msi FPR_TYPE=x
    - Used to define the type of Fingerprint reader being used ("x" is the number that corresponds to the fingerprint reader type)
      - 0 = None
      - 1 = Authentec 3500/4000
      - 2 = DP UareU 4000
      - 3 = Authentec 3400
      - 4 = UPEK (all models)
    - ***NEW*** If UPEK is specified, this will automatically use the new "Fast Fingerprint Authentication" added as of 9.3.0.8.

Enhancements:

XyLoc version 9.3.0.8 includes the following enhancements from the previous release:

1) **Added Account Type definition to clearly define Kiosk vs. Unique Logins for a given workstation.**
   a. This is defined in the registry under "HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)\"
      i. Name: "computerAccountType"
      ii. Value:
         1. 0 = Undefined
         2. 1 = Kiosk Account
         3. 2 = Unique Accounts

2) **Added a Fail Safe Override option to be able to allow any AD user to unlock a locked kiosk account via an override in the event of an issue.**
   a. Requires that the Kiosk login credentials be defined in the registry (as the cached credentials will not be relied on just in case they are the reason for the problem.
      i. "HKLM\Software\Ensure Technologies\Gina"
         1. "autoLogonDomain"   = Domain
         2. "autoLogonPassword"   = Generic Kiosk Account Password
         3. "autoLogonUserName"   = Generic Kiosk Account Name
   b. When enabled, when "override" is selected, their credentials are validated against Active Directory and if successful, the system will unlock into the kiosk specified above.
      i. Option is also Registry enabled: "HKLM\Software\Ensure Technologies\Gina"
         1. Name: "EnableFailsafeKioskOverride
         2. Value: 0 = off (default) / 1 = on
      ii. **NOTE:** A reboot is required.

3) **Removed the parenthesis on the personal names of Kiosk users when used with the AD version of the XSS**.

4) **Enhanced the Gina list box sorting algorithm to prevent names from "bouncing" around on the screen.**

5) **Added option for "Rapid Fingerprint" authentication (64-bit version ONLY)**
   a. This is only supported with the UPEK fingerprint readers
   b. This feature only requires the user to put the fingerprint down on the reader and that fingerprint is compared against the images that are assigned to any badges within their unlock range (that would appear on the unlock list box)
   c. This allows a rapid two-factor authentication while only requiring on action by the user.
   d. **NOTE: User must already have enrolled a fingerprint and must be using a XyLoc badge**.

6) **Modifications to Stationary Key Algorithm:**
   a. Found that the Stationary Key feature was not working properly with the newer XL-U2 USB locks due to the fact they only have one antenna vs. two in the previous XL-U USB locks and so a change to the algorithm was required

7) **Implemented a new stand-alone low battery warning message**.
   a. Previously message appeared on the XyLoc status pop-up from the XyLoc icon, however it was reported that users were not seeing it there.

b. Changed to a stand-alone pop-up message that the user must click "OK" on to confirm they saw the message.

c. **NOTE:** This new message requires Microsoft .NET Framework 3.5 or later

8) **Fixed an issue with the unlock process where the system would cycle through the unlock-lock-unlock screens**.

9) **Added option to Logoff (instead of lock) on the One Session feature added in 9.2.8**.
   a. Previously, when a user would authenticate on a new machine, the machine they were using previously would lock.
   b. With this change, the system can be configured to completely logoff instead of just lock (used for those that are using Unique AD logins to the PC, but still want to share the workstations between users).
   c. **NOTE:** This setting works in conjunction with the One Session feature that has to already be enabled at the XSS. This modification only changes the behavior of the client if the One Session feature is enabled.
   d. Registry configurable: "HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)\"
      i. Name: "OneSessionLogoff"
      ii. Type: DWORD
      iii. Value: 0 = off / 1 = on

10) **Added new "Smooth Hands Free Switching" feature.**
    a. With this enabled, if set to Hands-Free Unlock, when there are multiple badges in the area the XyLoc client will just smoothly switch to the next available badge in range when a user leaves range.
    b. If no badges are in range, then the system will lock as always.
    c. This is for customers that aren't really concerned about which particular user is in use of the workstation, but still want to make sure that only authorized users are able to use it.
    d. Registry configurable: "HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)\"
       i. Name: "UseSmoothHandsFreeSwitching"
       ii. Type: DWORD
       iii. Value: 0 = off / 1 = on

11) **Added the option to run the AI Auto Launch script at every unlock event, instead of just at a change of user.**
    a. Registry configurable: "HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)\"
       i. Name: "AlwaysRunUnlockScript"
       ii. Type: DWORD
       iii. Value: 0 = off / 1 = on

12) **Added option to allow a user with an expired password in Active Directory to continue to authenticate and unlock in a Kiosk**
    a. Had customers where the user needed to be able to get into the desktop in order to reset their password but couldn't because their AD password had expired.
    b. Registry configurable: "HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)\"
       i. Name: "IgnoreExpiredPasswords"
       ii. Type: DWORD
       iii. Value: 0 = off / 1 = on (meaning if enabled, a user with an expired password can still unlock. If disabled, then the authentication will fail and user cannot unlock)

13) **Alternate domain authentication method added.**
    a. This addition allows for authentication against A.D. from a workstation that is not a domain member (i.e. XPe Thin Clients)
    b. This is configured via registry values located in: HKLM\Software\Ensure Technologies\XyLoc - Serial Version (Multi_key)\.
        i. Name: "UseAltADAuth"
        ii. Type: DWORD
        iii. Value: 0 = off / 1 = on

14) **Added ability to launch a URL from the Gina for third-party SSPR support**
    a. Configured via registry value in HKLM\Software\Ensure Technologies\XyLoc - Serial Version (Multi_key)\
        i. Name: "URLAddrString"
        ii. Type: String
        iii. Value: "C:\\Program Files\\Internet Explorer\\IEXPLORE.EXE" http://www.google.com/
        iv. Replace the URL with the appropriate URL for your SSPR software.

15) **Fixed issue in XyLoc Configuration manager for viewing local User Audit Logs**

16) **Enhanced support for Passive Prox (HID).**

17) **Misc. Lock and Badge tracking algorithm fixes to improve lock/unlock behavior**

For reference, this client version also includes the following features, changes and bug fixes from earlier releases:

1) **Added "One Session" feature**
   a. NOTE: This feature requires an XSS version 5.0.3 or later.
   b. No configuration changes are made at the client to enable. This feature is enabled or disabled from the XSS.
   c. If enabled, when a user unlocks a computer it will send a notification to the XSS and the XSS will then lock any other computers that user has still unlocked and the grace period will be cancelled. This is to prevent the other computer from simply unlocking again if the user is still in proximity.

2) **Added a "System-wide" Two Factor grace period timer**.
   a. NOTE: This feature also requires the XSS, version 5.0.3 or later and is also enabled/disabled from the XSS. No configuration has to be done at the client.
   b. When enabled, there will be a defined time period on the XSS for the timer. When a user authenticates with their password or fingerprint (2-factor) then the authentication method for that user will change to Select Username for that period of time and so as their record is downloaded to each ensuing workstation the user will not have to enter their 2nd factor again. After that time expires it will revert back to "Must Enter Password" and for the next authentication attempt.
      i. Requires Must Enter Password to be used otherwise there is no 2nd factor to begin with and thus no need for a grace period.
      ii. Will change for both Login and Unlock.
   c. Feature uses the standard user lookups that are done all the time, but those are not always immediate as there is a built in "black-out" period for lookups for the same badge from the same machine. The default on this is 5 minutes so there could be a small delay of that time in getting the update. If a user were to try to authenticate a second time within that time period, it is possible that they might have to use their 2nd factor a couple of times before the clients get the notification.

3) **Enhanced support for Passive Prox (i.e. HID) cards and readers.**
   a. To enable this feature:
      i. In the Host settings on the XSS and the client side configuration manager set the XyLoc lock port to "HID-USB".
      ii. In HKLM\SOFTWARE\Ensure Technologies\XyLoc - Serial Version (Multi key)
         1. Value: HIDReaderPresent
         2. Type: DWORD
         3. Data: 1   (default = 0)
   b. To ensure easy switching between accounts with the passive system, which allows one tap on the passive reader to switch between kiosk users:
      i. In HKLM\SOFTWARE\Ensure Technologies\XyLoc - Serial Version (Multi key)
         1. Value: HIDForceLogoff
         2. Type: DWORD
         3. Data: 1   (default = 1)

4) **A splash screen can now be enabled to hide the user's desktop during the application logoff script at a change of user.**
   a. This would be used to protect potentially sensitive data visible on the screen during the brief period where the system is changing users and closing the previous user's applications
   b. To enable this feature create/modify the following registry value:
      i. Value: ShowSplashDuration
      ii. Type: DWORD
      iii. Data: 1   (default = 0)

5) **Added some additional algorithms to account for when a key's signal is lost entirely while still "in range" vs. when a key's signal just drops below the lock threshold normally.**
   a. Previously these were handled as the same event.
   b. Found that there were cases where, due to possible RF packet collisions with multiple badges, as well as possible interference from a potentially unknown source, at times individual packets or series of packets from a badge were lost even though the user was still in proximity of the workstation. This caused a lock event to trigger and the system to lock. Then within a second or two following the packets were picked up again and the system would unlock.
   c. Change the algorithm to better account for dropped packets specifically so as to not also cause an increase in the normal walk-away range when the key packets are still received and out of range.

6) **Enhanced the Gina screen to be able to better support keyboard only use (without a mouse) for navigation.**

7) **Modified the Range Refinement utility in the Configuration Manager to allow more flexibility on range settings.**
   a. Previously the slider had a minimum setting of "6" for the Lock range and "2" for the unlock range.
   b. It also enforced a minimum hysteresis value of 2 (value between lock and unlock).
   c. Restrictions have been removed except that the Lock still cannot be set lower than the unlock range.

8) **Fixed an issue with lock algorithm that caused the Stationary Key feature to not work properly when using the XL-U2 USB.**

9) **Fixed a bug that could intermittently cause a lock event that ignored the lock delay values**

10) **Fixed a bug where the client would attempt multiple spurious authentication attempts on a failed password override by a kiosk user which in turn could, in some cases, cause the AD account to get locked out.**

11) **Fixed a bug with a missing DLL used for UPEK Fingerprint sensor support**

12) **Added the "XyLoc Tap-in" feature.**
   a. Works similar to using a passive prox (i.e HID) card where a user has to bring their XyLoc badge right up to a reader to unlock.
   b. Normal XyLoc unlock range is used for the "walk-away" lock threshold.
   c. Please see Ensure AppNote AN023 for detailed description of this feature and how to enable.

13) **Added a "Password Reset" feature in the XyLoc Gina.**

d. On the Gina screen at both a locked workstation and a logged off workstation, there is a button for "New Password". Selecting this button will present a new dialog box that the user can use to reset their AD password for authentication.
e. Supports both Unique and Kiosk accounts.
f. The user must provide their username, old password, and new password where requested.
g. New Password is subject to whatever complexity requirements are already in place within the Domain.
h. Text formatting for the dialog box was also updated from previous "Beta" versions.

14) **Fixed an issue with performing a "Manual Lock" when using "Hands-Free Unlock" authentication method.**
   i. Previously this would put the service and Gina in a constant loop that required the user to override to recover from.
   j. This issue has been resolved in the Unique Account environment <u>only</u>.
      i. **NOTE**: The issue still exists in the Kiosk environment. However, for a variety of other security and workflow reasons, it is strongly recommended that Hands-Free modes are **NOT** used for Kiosk users.
      ii. As an alternative to using Hands-Free in the Kiosk mode, when convenience is preferred over security, Ensure recommends using "Select Username" and then set the "Unlock to Key Only" timer to a large enough value to retain the desired level of convenience.

15) **Addressed an issue with the kiosk user being able to authenticate with an expired/disabled/locked-out account and/or password when their AD password matches the Kiosk account password.**
   k. Scenario: Kiosk user has the same password value as the generic account. When the user's password is expired, the XyLoc client was checking against both generic Windows password value as well as the User's AD password value, and since the Generic account password matched, it was authorized.
   l. Modified the Gina so that when a return code of Expired, Disabled, or Locked-Out is received, the secondary check is not performed.
   m. The secondary check is still performed if the response is "Invalid Password".
   n. **NOTE**: The return code received when the user is set for "Must change password at next Login" is the same as "Invalid" and therefore is indistinguishable. As a result, the secondary check against the Windows password is still performed and the user would still be let in. This scenario is still under investigation for a solution.

16) **Incorporated XyView Diagnostic Utility into the installation package**.
   o. Will continue to be available as separate utility as it is compatible with previous versions of XyLoc that did not have it included.
   p. The XyView program is available in the installation directory of the XyLoc client (default is C:\Program Files\Ensure Technologies\XyLoc).

17) **Enhanced the Lock/Unlock algorithm used in the XyLoc client.**
   q. Specifically, this is the algorithm that determines when to lock the desktop based on signal strength and in turn, when to unlock based on signal strength.
   r. This was done to address inconsistencies in the previous algorithm related to lock and unlock range.

18) **Added a "Lock Delay" feature**
   s. This will allow a configurable time delay before XyLoc locks the workstation after a Key's signal has gone out of range.
      i. This can be configured through the XyLoc configuration manager in a Solo installation, or through the XSS in an enterprise installation.

ii. The time can be configured in both the user setting and the machine settings and the client will use the larger of the two values.

t. LED on the USB lock will turn "orange" during a delay time period.

u. If the user's key returned within the unlock signal strength threshold before the delay expires, the lock action is canceled and the LED returns to Green.

v. Once the delay is allowed to expire, the system will lock regardless of activity.

w. NOTE: The lock delay only applies when a key's signal strength goes out of range. It does not apply for other lock triggers (i.e. Turning off the Key, Manual Lock, Password Override lock timer, etc.)

19) **Added support for the AD account lockout/disable or Password Expired functionality (requires XSS-AD)**

x. Modified Gina to account for AD return error code for Expired, Disabled, and Locked Out accounts so as to not allow the user access to the PC.

y. Previously if a user's AD account was locked out or disabled, the user could still authenticate in XyLoc.

20) **Added Support for UPEK fingerprint readers**.

21) **Feature: Modified the ETWSS-SDK so that the same UserID is provided at the "Personal Name" in unique accounts instead of the AD Display Name**.

a. This was done to make integration of the WSS-SDK by a third party function the same in a Unique account as it currently does in the Kiosk accounts.

22) **Refined determination of Kiosk account vs. Unique account. New algorithm is as follows**:

a. if (Registry."computerAccountType" is 2), account is unique

b. if (Registry."computerAccountType" is 1), account is kiosk

c. (Registry."computerAccountType" is 0 or undefined), account is mixed, do more checks

d. Try reading the LBE. If we can't read the LBE, the account is unique

e. if (Registry.XssType is "AD") then
   i. if (user has an Entrust Profile), the account is unique
   ii. else the account is kiosk'

f. else
   i. if the user name is repeated in the LBE, the account is unique
   ii. else the account is kiosk

23) **Prevent duplicate "stale" records in the local database from interfering with XyLoc login**.

a. Issue: previously in a unique account environment, if a legacy record was still in the local database (i.e. due to KeyID change for said user) for the user, the XyLoc system would treat the user as a Kiosk user, and thus changing the rules for password authentication and in turn preventing the user from gaining access.

b. Solution: To change the rules so they are the same for both kiosk and unique, and making the duplicate record irrelevant.

24) **Fixed a bug that caused the XyLocIcon to not display intermittently or sometimes to display duplicate icons.**

25) **Increased the vertical length of the user listbox to accommodate up to 10 names**

26) **Fixed issue with XyLoc client installation and Internet Explorer 7 on XPe Thin Clients**

a. Removed file PSAPI.DLL from installation package

b. This file was installed as part of the Windows package and was being overwritten by the XyLoc installer.
c. The existing file was used by IE7 and when overwritten caused IE7 to no longer run.
d. This file was used by a legacy feature that is no longer used by XyLoc, and therefore was simply removed from the install package.

27) **During installation copy the current Gina from registry key "winlogon" and save in Ensure registry key "Gina" and restore during the uninstall process**
   a. This allows etGina01 to be the topmost Gina while preserving the Gina chain

28) **Fixed an issue with the Password Override where the dialog displays indefinitely after a character is entered**
   a. This has been modified so that the dialog will time-out following 15 seconds of inactivity.

29) **Allow setting authentication timer interval via Registry**
   a. Provides a mechanism by which the user may control the XyLoc list box update frequency during authentication.
   b. Use Case: When the user either logs on or unlocks via XyLoc and there is a list of nearby XyLoc users that appear in the authentication list box causing the list to refresh quickly making it difficult to select the desired name.
   c. Location: HKLM\Software\Ensure Technologies\Gina\LockDlgUpdateIntervalMSec
   d. Type: DWORD
   e. Value:
        i.   0 = off (meaning default)
        ii.   Permissible range (decimal) = 1-30000 (desired time in Milliseconds)
   f. **NOTE**: This has a default value of 250ms if it is not defined in the registry however the installation package sets the registry value to 500ms.

30) **Prevent premature closing of password override dialog box should the count of badges detected change**
   a. Gina now closes the box after the prescribed time (from existing registry setting "DialogTimeout") elapses

31) **Increased the maximum size of exception.txt file to 1 MB**

32) **Fixed an issue with an Interactive Logon message box**
   a. In some cases, when enable the message box would continue to flicker until <Enter> Key was used (selecting the "OK" button on the message box).

33) **Allow detection of badge numbers less than 4000; this is most relevant in the case of "Passive Prox" badges**

34) **Modified the installation script and service to leave the AutoAdminLogon registry value (for winlogon) intact**.

35) **Fixed an issue where a message appeared erroneously, stating the key could not be found and to check the battery**.

36) **Enhanced local database handling of large user databases**.
   a. Add "maximum key list" counter in the registry with range from 1-1000 (default.eq.1000)
        i.   HKLM\SOFTWARE\Ensure Technologies\XyLoc - Serial Version (Multi key)
        ii.   Value: maxKeyList

iii.   Type: DWORD
                        iv.   Data: 000003e8 (Decimal = 1000)
         b.   Add debug registry key to log current key counts
                        i.   HKLM\SOFTWARE\Ensure Technologies\XyLoc - Serial Version (Multi
                               key)
                        ii.   Value: xylocLogMode
                        iii.   Type: DWORD
                        iv.   Data: 00000001

37) **Modified the handling of Fingerprints in Password Override to allow a customer to turn
    off the Fingerprint ability in override**.
         a.   New registry value must be configured;
                        i.   HKLM\SOFTWARE\Ensure Technologies\XylocFPR]
                        ii.   Value: fpOverrideFilter
                        iii.   Type: DWORD
                        iv.   Data:
                                    1.   1 = FP is disabled for override
                                    2.   0 = FP is enabled for override

         b.   This is set to "1" by default and is also added as an argument to the MSIEXEC
               command line install
                        i.   "msiexec /i xyloc.msi FP_DLG_FILTER=1"

38) **Fixed an error message stating "XyLoc Service not Started. Please wait" that was
    displayed at boot up on Windows XP**.

39) **Add a series of enhancements to XyLocAIT to correct or address reported script errors**

40) **Added Low Battery warning (Requires 8.5.0 or later)**
         a.   If status packet is detected below the battery voltage threshold the existing Status
               pop-up message from the system tray will show a "Low Battery" message in red.
         b.   Once the appropriate status packet with a voltage reading back above the threshold
               is received, the notification will disappear.

41) **Modified the client to include additional information in the Key Lookup messaging to
    the XSS to differentiate between "new" key lookups and lookups for "existing" keys.**
         a.   "New" key lookups are for keys that do not currently have a record in the local XyLoc
               database.
         b.   This additional detail will be used by an upcoming release of the XSS (version 4.2.8
               or greater) to prioritize the "new" key lookups to ensure the fastest possible response
               vs. updates to existing records.

42) **Modified the functionality of the "XSSLookupRetry" time setting in the system registry
    to reduce the number of redundant lookups to the XSS.**
         a.   Previously this timer was conditional on the key being in continuous communication
               to the lock.
         b.   Regardless of what the timer was set for, if the key went "out of range" (meaning the
               power dropping below a static threshold as defined in code or was turned off or
               dropped out entirely) and then came back in range, the timer was reset and an
               immediate lookup was performed again.
         c.   With this modification, the timer is static. Once a lookup is performed, another lookup
               is not done until at least the specified time has elapsed, regardless of key activity and
               signal strength

d. This time uses the same DWORD value in the Registry as before under HKLM\Software\Ensure Technologies\XyLoc - Serial Version (Multi key)\XSSLookupRetry and is defined in seconds (in decimal).

43) **Includes additional messaging on the override screen to remind the user to put their name in parenthesis if they are unlocking in the kiosk**.
   a. This process is only valid when using XSS-AD, so the feature checks the "XSSType" registry key to verify that the AD version is being used.
   b. If this is set to SQL or not defined at all, the extra messaging will not appear.

.

44) **Added the ability to change the timeout on the password field at login and unlock.**
   a. When a user selects their name at the login/unlock screen, they have 5 seconds to start typing or the field times out and the screen refreshes back to the list of keys. This time is now adjustable with a registry value.
      i.   Value Name: DialogTimeout
      ii. Type: DWORD
   b. The time is in seconds, and the default is "5" (in Decimal)
   c. **NOTE:** The longer the time, the longer the user will have to wait if the wrong name is selected before the list returns to where they can select the correct name. However, there is still the "Refresh" button on the screen that can be used and not wait for the timeout.

45) **Added additional debug logging to trace WSS-SDK issues**.
   a. There are two registry values that can be created in the XyLoc registry for the ETWSS debug logging.
      i.   ETWSSDebugLogging
         1. Type: DWORD
         2. Value: 1 – turn on debug logging, 0 – turn off debug logging
      ii. ETWSSLogPath
         1. Type: String
         2. Value: Specify the full path for the debug log, for example, "C:\Log"
   b. The path specified in the ETWSSLogPath must have appropriate permission for the log to be created/written.
   c. If the ETWSSLogPath registry value is missing, the log file's default path is the common application data folder: C:\Documents and Settings\All Users\Application Data

46) **Added a registry value to specify the path for the Exception.txt file**.
   a. This is so that it can be created in a folder which the necessary XyLoc processes have permission to write debug logging to the exception.txt file.
   b. Name: ExceptionLogPath
   c. Type: String
   d. Value: Specify the full path for the debug log, for example, "C:\Log"
   e. If this registry value is missing, the default path is XyLoc installed folder (i.e. C:\Program Files\Ensure Technologies\XyLoc)

47) **Created option to enable/disable scripts to run while in Password Override Mode**
   a. Added the registry setting 'RunScriptsInPwdOverride' that controls whether or not scripts will run while in password override mode.
      i.   The default setting of 'RunScriptsInPwdOverride' is '1', indicating that AI scripts will run while in password override mode.
      ii. To turn them off, change the setting to '0' and restart the PC.
   b. **NOTE:** For security reasons, the logoff scripts always run regardless of the registry setting.

48) **Added registry setting to hide the XyLoc status popup.**
   a. A registry entry can be created to disable the XyLoc Status Popup on the screen:
       i. The registry value is "HideXyLocStatus".
       ii. Type: DWORD
       iii. To **not** show the status, set this value to 1. If it is set to 0, the status will continue to display.
   b. **NOTE:** This registry entry is not created by default and will need to be created manually.

49) **User Configurable display position for the XyLoc status and Lock button**
   a. The offset is relative to the lower right corner, so when a value of 100 is specified, it means 100 pixels from the lower right corner.
   b. For the XyLoc Status, modify the registry value "StatusOffset". The default is 0.
   c. For the Lock button, modify the registry value "LockButtonOffset". The default is 50.
   d. **NOTE:** These values are Decimal values (not Hexadecimal) in the registry.
   e. The changes will not take effect until the logoff and logon again.

Revision History:

Revision	Date	Description	Author
9.0.0	07-31-09	Created	RS
9.1.0	05-18-10	Added v9.1.0 notes	RS
9.1.0.3	12-13-10	Added v9.1.0.3 notes ("Tap-in" feature)	RS
9.2.0	09-28-11	Added v9.2.0 notes. Also added general client note regarding new tap-in options.	RS
9.3.0.8	10-30-12	Added v9.3.0.8 notes. Added requirements section.	RS