Ensure Technologies™

XyLoc Windows7 Client Release Notes

Support Information:

Ensure Technologies Technical Support is available to provide any needed assistance. Please contact us at (734) 547-1631 or at support@ensuretech.com.

Compatibility:

- The XyLoc Windows 7 client has been tested to be compatible with both 32-bit and 64-bit versions of Windows 7.
  - Has not been tested with Windows 7 “Starter” edition.
- XyLoc Windows 7 Client 9.2 can be used as a Solo, or in an enterprise environment in conjunction with the XyLoc Security Server. Any 5.x version of the XSS is supported, however, to **support the newer features for the One Session and System-wide Two Factor grace period (see Enhancements below) version 5.0.3 of the XSS is required**.
- **Auto Logon**: Auto Logon is supported in Windows 7. As of Build 29, the XyLoc Credential Provider will read the values from the “Winlogon” key. This is located in HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon. Those values are as follows:
  - “DefaultUserName” = desired username
  - “DefaultPassword” = desired user password
  - “DefaultDomainName” = domain name (or local machine name if no domain is used)
  - “enableAutoLogon” = (dword) **1** for “enable” and **0** for “disable”.
  - **NOTE:** Password Override must be allowed in the user’s XyLoc settings, at least for logon, in order for the Auto Logon to work.
- The 32-bit XyLoc client supports fingerprint authentication with the following readers:
  - Digital Persona “UareU” 4000 series readers.
  - Authentec AES3400, 3500, and 4000 series readers.
  - All UPEK sensors (according to UPEK documentation)
    - **NOTE**: Not all of the UPEK sensors have been tested by Ensure. Support is based on UPEK SDK documentation.
    - Ensure has specifically tested UPEK TSC2 TouchChip® sensor with Cherry Keyboard Model SPOS
  - **NOTE:** In 64-bit, only UPEK models are supported
- **The On Demand scripting for Application Integration tool will only support 32-bit applications, even on the x64 client.**

General Windows 7 Client Notes:

- **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 not lock.
  - During RDP session, remote Ctrl+Alt+End sequence is ignored and PC is not locked.
  - Remote Disconnect is **required** after session is complete. Access to the host machine is denied as long as an active Remote session is in place.
- ❑ **Fast User Switching**: The XyLoc client does not support the Win7 Fast User Switching and as a result will disable this feature upon installation.
- ❑ **Windows Firewall**: If using the XyLoc Security Server software (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.
- ❑ **Credential Providers:** XyLoc is required to be the only credential provider and will enforce this setting.
  - An administrative override for login only is still supported by clicking on “Action” at the top of the Credential Provider screen and then clicking on “Administrator Override”.
- ❑ **Additional requirements for Kiosk**: It is highly recommended that Auto Logon be used on machines that are being used in a Kiosk setup. However, if Auto Logon is not desired, the credential values in the registry are still required in order for all the functionality of the Kiosk accounts to work properly (specifically Password Overrides and unlocks within Grace Period).
  - The Auto Logon credentials must be set in the registry, however the “enableAutoLogon” value does not have to be enabled.
- ❑ **Non-XyLoc user overrides**: The XyLoc client supports an override via a user that is not a XyLoc user (i.e. an Administrator account). Click on the “Action” menu option at the top of the Credential Provider and then clicking “Administrator Override” (please note that the user does **not** actually have to be an Administrator account in order to successfully override).
  - When this type of override is performed, the XyLoc client is completely overridden. There is no tracking of badges being performed and if the user manually locks the desktop the XyLoc Credential Provider will not be displayed. Only the standard Microsoft login is available to unlock.
  - To return to normal XyLoc behavior, the non-XyLoc user must logout.
- ❑ **Web Application Scripting with Application Integration:** The add-on used in Internet Explorer for the Web Scripting to trigger an On Demand script does not work unless the IE8 setting in the Security Options for “Protected Mode” is turned off.
- ❑ **Screen Saver**: In the normal Windows Screen Saver options, there is a setting for “On resume, display logon screen”. If this option is enabled, when the screen saver timer expires, the system will lock and the XyLoc Credential Provider will be displayed for the user to unlock.
  - This is recorded as a Manual Lock in the logs.
  - Even if no actual screen saver is selected (i.e. “(none)” is selected) the timer and the logon option is still available and as such would still lock the desktop after said timer expires.

Installation Notes:

The installation package has changed from the XyLoc client release for Windows XP. The following are some specific items to note with this package:

- Make sure to accept the driver from “Ensure Technologies” if prompted.
- On a new installation, the user will be prompted for user data to populate at least one user in the local database. This was true of the XP version as well, but was prompted in individual dialog boxes for each instead of all at once.
  - All fields except the XSS Address are required.
- After the reboot at first login, the client will request the password and the “Domain” name, even if it is a local account and even if just set to Select Username for the login authentication. This is to obtain the necessary Windows/Domain credentials to pass on for future logins. This will only occur once at the first login attempt.
  - If a domain name is not entered, the client will use whatever was the previous login’s domain name (or local machine name if a local account).
  - If using with an XSS-SQL, make sure to include the domain name in the XSS record for that user as well.
- When the software is uninstalled, the hardware drivers and local database files are not removed in order to ease a future re-install if desired.

Known Issues:

The XyLoc client for Windows 7 has the following known issues:

- **RDP:** After a user connects remotely to a XyLoc workstation they must reboot the workstation when they are finished.
    - When a RDP connection is established to a locked XyLoc workstation another instance of the Credential Provider is instantiated and is in communication with the XyLoc service. The service does not handle multiple Credential Providers communicating simultaneously and becomes unstable. As a result, a local user on the XyLoc workstation could have difficulty unlocking and/or logging in through the XyLoc Credential Provider.

- **Hibernate/Sleep:** The XyLoc client has some issues periodically with Hibernate and Sleep power saving options.
    - LED on the lock always comes on Green instead of Red when the system first wakes up and is still locked. Normally the lock LED should be red when the system is locked and only turn green when unlocked.
    - The icon program at times reports the wrong system state, however functionality seems to be as it should be with regards to locking and unlocking and tracking badges.
    - Very intermittently the Credential Provider will not display any keys to unlock.
        - Putting the computer into "Sleep" mode again and then waking it back up corrected that issue when it occurred**.**
- **Start Menu:** XyLoc program menu does not appear in "All Programs" in the Start Menu, however both the Configuration Manager and the XyLoc AIT utilities can be opened through their respective icons in the Windows "systray".
    - If the icons are not available for some reason, both programs are located in the XyLoc directory (C:\Program Files\Ensure Technologies\XyLoc\) as well and could be opened manually from there:
        - Configuration manager: "xylocconfig.exe"
        - XyLoc AIT Utility: "XyLoc AI Tool.exe"

In addition the x64 version of the XyLoc client for Windows 7 has the following additional issues:

- **Driver Installation:** The Windows Driver signing testing has not yet been completed. This causes a confirmation box to appear during the driver installation that the person installing must click through to complete the install. This prevents a truly "silent" installation of the client.
- **Application Integration:** For "On Demand" scripts, only 32-bit applications are supported.

Enhancements:

XyLoc version 9.2.6 x32 / XyLoc version 9.2.6 x64:

1) **Added a “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) **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)
    c. For easier use when tapping, also set the following value. This will set the Credential Provider so that when a tap occurs, the user doesn’t also have to select his/her name on the screen.
        i. In HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)
            1. Value: IsUsingTapLockorHID
            2. Type: DWORD
            3. Value: 1 (enabled)

4) **Added the "Active 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, but uses the standard XyLoc active proximity badges.
    b. Normal XyLoc unlock range is used for the "walk-away" lock threshold.
    c. For easier use when tapping, also set the following value. This will set the Credential Provider so that when a tap occurs, the user doesn't also have to select his/her name on the screen.
        i. In HKLM\Software\Ensure Technologies\XyLoc – Serial Version (Multi key)
            1. Value: IsUsingTapLockorHID
            2. Type: DWORD
            3. Value: 1 (enabled)
    d. Please see Ensure AppNote AN023 for detailed description of this feature and how to enable.

5) **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)

6) **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.

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) **Added ability to display a customized logo/image at Login or Unlock screens (as has been available in XP version)**

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

10) **Fixed an issue where the UPEK Fingerprint sensors were not working properly with XyLoc.**

11) **Fixed an issue with the Application Integration logoff timer not working on Win7 x64**.

12) **Fixed an issue with Application Integration Credential reset utility not having proper elevated rights to write the credentials to the local database**.

13) **Fixed an issue with the computer locking or logging off while the service was stopped**.

    a. User would not be able to re-authenticate because the XyLoc service was stopped.
    b. Added code to the Credential Provider to properly start the service in this scenario.

XyLoc version 9.1.0 x32 Build35 / XyLoc version 9.1.0 x64 Build17:

1) **Added support for x64 versions of Windows 7**

2) **Fixed an issue with Forced Logoffs being halted when an open application required some sort of confirmation from the user to close.**

3) **Fixed an issue with logging via a Password Override with an account that was assigned a non-existent badge ID**

4) **Fixed an intermittent issue with a Unique AD account not being able to logon**

5) **Modified the ETAITReset.exe utility (utility to reset the AI credentials accessed from the AI icon in the systray) to not require Administrator credentials when UAC is enabled.**

6) **Added ability for a "Forced Logoff" on the locked workstation Credential Provider via the menu option at the top.**
    a. This is to allow an Administrator to forcibly logoff the current user in an emergency situation.

7) **Fixed various timing conditions that caused the XyLoc Service and Credential Provider to become unstable when a user quickly locked and unlocked the workstation.**

8) **Fixed an issue with Hiberation where the workstation would be unlocked, but the service would still believe it to be locked.**
    a. XyLocIcon detects the condition and will issue a manual lock so a user can unlock through the XyLoc CP and get the CP and Service back into sync.

9) **Fixed issues with Auto Logon**
    a. Found that on some machines, intermittently, the Auto Logon would fail.
    b. Also found that in some of these instances, the XyLoc CP was unresponsive after this failure.
    c. These were a result of a timing condition at the first login following a system boot, where the CP was attempting to logon before the service was ready to accept the login credentials.
    d. A timer was added so that the first login following a system boot is delayed for a set period of time to allow the service to initiate fully.
        i. The default is 30 seconds but can be overridden via a registry setting:

1. Location: [HKLM\Software\Ensure Technologies\Gina]
2. Value: "waitTime4FirstLogonSec"
3. Type: DWORD
4. Data: Number of Seconds (in Decimal)

XyLoc version 9.1.0 Build29:

1) Modified how Auto Logon credentials are defined (see "Auto Logon" notes under "General Windows 7 Notes" section above).
   a. Previously these values were stored in the Ensure Technologies\Gina\ key.
   b. Reading them from Winlogon is consistent with standard Windows functionality and also allows the values to persist after removal (and reinstall later if done) of the XyLoc client.

2) Fixed various issues that caused the system to not unlock properly "Hands Free" during the "Unlock to Key Only" grace period time.
   a. User had to re-authenticate by either selecting their name and, if set to "Must Enter Password, re-entering their password at each unlock regardless of time.

3) Fixed an issue in the install package that caused an installation failure if the user hit the <Enter> key (instead of clicking "OK") after populating the user information (if prompted by an installation dialog).

4) Fixed an issue where the XyLoc client would not perform key lookups after a manual lock.

5) Fixed additional interoperability issues with XyLoc AIT (Application Integration) and Windows UAC.

6) Addressed issues when using the XyLoc v910 client in conjunction with a 4.x version of the XSS-AD that could prevent the user from being able to logon.

   NOTE: Fixes to issues requires that some or all of the Auto Logon values are populated in the Winlogon registry.
   a. Values located in HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\
   b. For Unique accounts:
      i. "DefaultDomainName" value must be populated with the proper Domain Name.
   c. For Kiosk Accounts:
      i. "DefaultDomainName" value must be populated with the proper Domain Name.
      ii. "DefaultUserName" value must be populated with the Kiosk network account name.
      iii. "DefaultPassword" value must be populated with the Kiosk network account password.
         1. This value may not be already created if Auto Logon is not being currently used. This must be created as a "String Value" for full kiosk functionality.
   d. NOTE: If using XSS-SQL or as a Solo, then only the "DefaultDomainName" value is necessary, and then only if logging into a domain.

7) Addressed issues that could prevent a Unique account user from logging back in after a password change.

XyLoc version 9.1.0 Build17:

1) Addressed additional issues with Forced Logoffs

2) Fixed issues related to using UPEK fingerprint readers

3) Fixed issues in installation of the client when installing over top of a previous install.

XyLoc version 9.1.0 Build 2:

1) Modified the client to support User Account Control (UAC).

2) Fixed issues found related to performing a Forced Logoff

XyLoc version 9.1.0 for Windows 7 includes the following additional enhancements from the previous production Windows XP release (9.0.0):

1) **Windows Password Reset utility:**
    a. From the Credential Provider, via the menu at the top left hand side, a user can reset their Windows or Domain account password.
    b. Password reset capability is available even in a kiosk account. The user simply has to provide the utility with their unique Domain username.

Revision History:

Revision	Date	Description	Author
9.0.0.0	10-13-09	Created	RS
9.1.0.2	05-13-10	Updated release notes for Build 2	RS
9.1.0.17	06-24-10	Updated release notes for Build 17	RS
9.1.0.29	08-26-10	Updated release notes for Build 29	RS
9.1.0.35	10-28-10	Updated release notes for x32 Build 35 / x64 Build 17	RS
9.2.6	11-14-11	Updated release notes for 9.2.6 release	RS