Ensure Technologies™

Software Release Notes for XSS AD/SQL version 5.1.0

Support Information:

Ensure Technologies Technical Support is available to provide any needed assistance. Please contact us at (734) 668-8800 or at support@ensuretech.com.

Compatibility:

- The XSS version 5.1.0 is compatible with 32-bit versions of Microsoft Windows 2000 Server, Windows Server 2003, Windows Server 2008 (x86 and x64) and Server 2008 R2.
- **.NET Framework**: XSS version 5.1.0 now required Microsoft .NET Framework version 4.0 or higher.

Upgrading from earlier versions:

XSS 5.1.0 is also available as a patch upgrade from an earlier 5.x installation or as a stand-alone installation.

Please see Ensure AppNote AN025 for instructions on how to perform the upgrade or contact Technical Support.

General Notes:

1) **IMPORTANT:** Due to the changes in the lookup process both at the client and the server, changes in user information can take up to 5 minutes. This is a result of timers that are put in to reduce redundant lookups.
   a) These timers are adjustable via the registry, so it can be shortened, although not recommended. This is done at the potential expense of performance and possibly causing even slower response from the XSS. Contact Ensure Technical Support for more details, if needed.

Enhancements:

XyLoc Security Server (XSS) version 5.1.0 includes the following enhancements from the previous releases:

1) **Added "One Session" feature.** This feature will automatically lock any other workstations a user may have open, allowing a user to have only one workstation unlocked at a time.
   a) To enable One Session the following registry value must be modified.

   [HKEY_LOCAL_MACHINE\SOFTWARE\Ensure Technologies\XSS]: "UnlockNotify"
      i) Description: Enables/Disable the One Session feature
         (1) Type: STRING (REG_SZ)
         (2) Value:
            (a) 1 = One Session enabled.
            (b) 0 = One Session disabled

2) **Added "Two Factor Grace Period" feature** – Requires the user to only enter their password once across the installation base for a set period of time, switching from "Must Enter Password" to "Select Username" for this time period, before revering back to "Must Enter Password
   a) To enable Two Factor Authentication the following registry value must be modified.
   [HKEY_LOCAL_MACHINE\SOFTWARE\Ensure Technologies\XSS]: " SystemGracePeriod"
      i) Description: The amount of time (in minutes) before the user must authenticate with their password again.
         (1) Type: STRING (REG_SZ)
         (2) Value:
            (a) An integer between 1 and 255 representing minutes.
            (b) 0 = SystemGracePeriod disabled

3) **Modified ADUI plugin for XSS-AD with new range slider that removes previous restrictions on the available range values.**

4) **Modified XSS-AD version to remove SQL queries from the Key Lookups**
   a) All user data for the record is stored in AD schema
   b) Done to increase performance by eliminating one server connection.
   c) Also removes previous issue of halting all lookups if the SQL server was unavailable for some reason.

5) **Fixed an issue with encryption logging that was generating a potentially extraneously large log file that was no longer needed.**

6) **Fixed issue in XSS-DB installation package that would not properly find an installation of SQL Server 2008 and this would cause the installation to quit.**

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

1) **Added new "Delay Lock" feature (requires version 9.0.0 or later of XyLoc client):**
   a) A timer can bet set to delay the locking on the XyLoc client when a key is taken out of range for a defined period (defined in seconds).
   b) Delay value can be set at both the workstation level and the user level (for each individual user, the highest of the two values are used at the client)
   c) This will only apply for an "out of range" lock. It does not apply for other lock events such as turning off a key or a key timing out at the end of the day or a "manual" lock (i.e. Ctrl+Alt+Del keystroke)**.**

2) **Added Support for multiple fingerprint types in the same installation (requires version 9.0.0 of XyLoc Client)**
   a) For instance, an Authentec Fingerprint could be used at one machine and a Digital Persona reader could be used at another within the same XSS.
   b) NOTE: Only one particular read can be used on any given workstation at a time.
   c) Due to the differences in the images that each reader uses, a user will be required to re-enroll on each fingerprint type used, but only for the initial caching of fingerprint image types.
3) **Fixed an issue in XSS-AD where apostrophe's in the username and/or the Personal Name were not supported**
   a) In previous version the lookup process to AD would fail if the username or the user's First or Last Name field had an apostrophe in it.
   b) Also when passwords were changed on the clients the new passwords were not getting cached in the user's AD record.

4) **Added Support for Windows Server 2008**

5) **Fixed an issue in XSS-AD where apostrophe's in the username and/or the Personal Name were not supported**
   a) In previous version the lookup process to AD would fail if the username or the user's First or Last Name field had an apostrophe in it.
   b) This has been corrected.

6) **Corrected an issue in XSS-AD environment where unique user's passwords were not being accepted**
   a) Original issue only applied to XSS-AD with "unique" users (no issue with Kiosk users).
   b) When the user's record was provided to the client software, the data for "Domain Name" was garbage characters, which caused the user's authentication with their AD password.
   c) Corrected the issue in the XSS service with how the data is gathered out of the SQL database.

7) **Fixed an issue with Fingerprints in XSS-AD and how they are stored in the database and applied to the user on the workstation.**
   a) Changed to search for KeyID instead of username or Personal Name
   b) This is to accommodate the move of the fingerprints to the SQL database (done in an earlier version of the XSS, but the XSS didn't search properly.

8) **Added "Priority Queue" in the XSS**
   a) This is in addition to the "standard" queue that is already in place, meaning there are now 2 message processing queues at the XSS
   b) Requires XyLoc client version 8.4.9 or later to take full advantage of the benefit.
   c) The Key Lookup requests sent to the XSS by the XyLoc client now include additional information to define whether it is a "new" key or an "existing" key.

d) "New" key lookups will be put into the priority queue. Existing key lookups will go to the "standard" queue.
e) "Password Override" lookups will also be handled by the priority queue
   i) **NOTE**: Because these messages are already different in their structure, the XSS can see these from older clients (pre-8.4.9) as well and assign them to the priority queue.
f) Log messages and FPData requests will go to the standard queue as well.
g) **NOTE**: The Highwater/Lowwater feature that was implemented in an earlier version only applies to the "standard" queue, not the priority queue.
h) The purpose of this additional queue is to prioritize lookups for new users to a workstation, as well as the lookups for users that don't have a badge on them, but are authorized to access the workstation.

9) Modified code and database to significantly improve key lookup performance:
a) Changes primarily effect performance on XSS-AD, although some changes will improve XSS-SQL performance as well.
b) Changes include improved AD group lookups as well as reducing redundant lookups.

10) Fixed issue with the calendar in the Audit Logs when installed on non-US servers.

11) Corrected issue with Host Based Ranges in XSS-SQL.
a) Found cases when using Host-Based Ranges on XSS-SQL, where the range settings would inadvertently get set back to the factory default.
b) This was not an issue with XSS-AD

12) Added the ability to define the Lock/Unlock range based on the host, instead of the user ("Host-Based Ranges").
a) Both host and user based are supported and the setting to define whether the ranges are determined by the user preferences or host preferences is a Global setting in the XSS.
b) In the XSS-SQL, the Global settings are available in the general "Users" page.
c) In the XSS-AD the Global settings require a special "global config" user to be created and the Global settings are listed there.
   i) Create a user in AD with the username of "xylocglobalconfig"
   ii) In the properties of that user, there will be a tab for "XyLoc Config". All Global settings are defined in this user account.

13) Fixed a memory leak that was discovered in the XSS service

14) Store fingerprint data in SQL database (XSS-SQL & AD)
a) Previously the Fingerprint data was stored as ".dat" files in a separate folder on the XSS with a matching .dat file on the client side.
b) It is still stored on the client side as a .dat file, and this file is generated as needed by the XSS from the data stored in the SQL database.
c) This provides better redundancy for the fingerprint data as well as more efficient management at the server.

15) Added 'Delete Fingerprint Data' button in XSS-SQL browser
a) Allows an administrator to delete the fingerprint data for a specified user.
b) This user must then use a password the next time they authenticate on the XyLoc client and then re-enroll their fingerprint (if desired).

16) Eliminated PIN support for XSS-AD
a) Found that the extra XyLoc Password (PIN) was problematic in the Active Directory version due to limitations in AD.
b) The ability to use a PIN (instead of the user's AD password) has been eliminated and is no longer supported by the AD version of the XSS. The user must now use their own

unique account password for all XyLoc authentication (if a password is required)

c) The XyLoc PIN **is** still supported by the XSS-SQL version.

17) Fixed XSS-DB installation for SQL installations that do not have a default SQL instance (i.e. the SQL installation uses only named instances).

a) During the XSS-DB installation, when asked for the IP address of the SQL server, enter the named instance as: <server IP address>\<instance name> (for example 192.168.1.143\ensuresql)

b) If an instance name is not specified, then SQL will just use the default instance name

18) Modified the XSS Service so that a deleted fingerprint will propagate to the client.

a) The XSS service now responds to fingerprint data requests for a user that has no fingerprint data on the XSS with the 'not enrolled' response.

b) This allows the client the ability to determine that the particular user has no fingerprint data configured and to then delete its local copy of the fingerprint data.

19) Communicate XSS version number and XSS database type to the client.

20) Client version number is logged in the XSS log when the debug logging is enabled.

.

21) Send information to the client indicating whether or not the PIN should be synchronized.

a) For kiosk accounts the PIN will not synchronize

b) For unique accounts the PIN will still synchronize, unless the new global setting 'Enable PIN for Unique Accounts' is enabled.

c) NOTE: The new method of determining whether a PIN should be synchronized requires XyLoc 8.3.5 or later. If using a version of the client prior to 8.3.5, the old method of determining whether a PIN should synchronize is still used.

22) Change the xssd.log location from C:\ to the 'Common Application Data' folder.

a) This change is necessary so that we can still can write to the log when using a non-Administrator account for the XSS Service.

b) The common application data folder is in C:\Documents and Settings\All Users\Application Data and is generally a Hidden folder. Hidden folders will have to be viewable to see this folder, although all data will still write to this directory even if not viewable.

c) The XSS log file (xsslog.log) rolls over to a new log file when the xsslog.log file grows more than 50 MB in size. The previous log file is saved off to a new file in the root of C:\ and the filename is generated with the date and time the file was rolled over.

23) Changed the XSS-SQL service so that it ignores any client updates to the Entrust profile name and Entrust password fields.

i) This is to resolve an issue that can occur when the Entrust profile data in the database can be changed to "garbage" characters by an older client and then the XSS send those garbage characters back to clients as part of the Application Integration credentials.

24) Added global XSS setting 'Enable PIN for unique accounts'.

a) This is found in the 'Manager Users' page.

b) The default for this setting is disabled, meaning that PINs are disabled for unique accounts and all unique account PINs will synchronize with the user's system account password as before.

25) Generate a random PIN when creating unique/kiosk accounts.

a) This is only the case if no PIN (in the XSS it is called the XyLoc Password) is specified for

that user.

b) Previously, if the XyLoc Password field was left blank, then the XSS used the user's KeyID as the default password. This creates a potential security risk.
c) The XyLoc Password (PIN) can still be set or changed manually on the XSS (if using XSS-SQL) by the administrator or using the Credential Reset utility on the client by the user themselves.

26) Modified the XSS-AD installation so that it prompts the user to enter the credentials for a user account that has at least 'Account Operator' privileges.

a) The Account Operator is the minimum necessary to write the required data into the AD schema.
b) However, a Domain Account Operator account does not have the necessary permissions to write data to the local C: drive on the XSS to write the log file. This is what prompted the change listed above to move the XSS log from C: to the "Common Application Data" folder.

27) Added kiosk 'system account password' and 'enable unique account display' settings for the host.

28) Fixed issue in XSS-SQL browser with editing a group.

a) If you select a user and go to the 'User Information' page, then select a group that the user is associated with, then select the 'Manager Users' button, sometimes an error would get generated.

29) Fixed password update issue in XSS-SQL browser.

a) When the user updates the XyLoc PIN in the "User Preferences" field, we added feedback for the user so they will know whether or not the PIN update has been successful.

30) Fixed an issue with the XSS-SQL browser where the password override timer was not able to display or set values greater than a signed integer (32,767).

31) Added support for storing the secret store information within the database (SQL/AD).

a) Used only by the XyLoc Client WSSSDK
b) Modified on the XSS-DB installation as well.

32) Implemented host-based kiosk design for XSS-SQL and XSS-AD.

a) Starting with XSS version 4.2.1, we have implemented the new Host-Based kiosk setup.
b) With this, the kiosk account used is defined in the settings for each individual PC, allowing you to have a different "generic" account for different PCs.
c) Upgrades from earlier versions to XSS-AD v4.2.1 or later will not support the legacy kiosk method and the kiosk account setup will need to be recreated. Contact Technical Support for the proper upgrade procedure for your setup.

33) Added a "Create Host" button on the XSS browser (XSS-SQL only).

a) This allows the administrator to create the host prior to installing the XyLoc client.
b) In previous versions, the client must be installed and then learned by the XSS after the installation.

Revision History:

Revision	Date	Description	Author
5.0.0	09-04-09	Created	RS
5.1.0	11-11-11	Added notes for version 5.1.0	RS