Security White Paper for
Streamline NX Authentication and Accounting Manager
Version 1.2.0.0

Solution Value proposition Section
Global Technology Support Department
Service and Support Center
Global Marketing Group

Document version
SLNXAAMV1.2.0-1.0

Notice:
This document may not be reproduced or distributed in whole or in part, for any purpose or in any fashion without the prior written consent of Ricoh Company Limited. Ricoh Company Limited retains the sole discretion to grant or deny consent to any person or party.

Copyright © 2011 by Ricoh Company Ltd.

All product names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

Document version history:

Version	Date of Issue	Revision
1.0	August, 2011	・ Initial Release

1. Introduction

This paper provides security information about Streamline NX Authentication and Accounting Manager (AAM), which is comprised of two primary components: AAM Server (AAM-S) and AAM Embedded (AAM-E).

AAA (Authentication/Authorization/Accounting) Security

Authentication

The authentication methods and the operation are explained in the following table.

Operation	Authentication	
Panel	Authentication runs with entered username and password.	- Kerberos Authentication - LDAP Authentication
Card	[Enter password] The username is obtained from the Card ID. After using the card, the user must enter a Password from the operation panel. [Do not enter password (Proxy User)] The username is obtained from the Card ID. Authentication is performed by a proxy user that searches the LDAP directory for username. If the username exists, authentication succeeds. [Do not enter password (Saved password)] The username is obtained from the Card ID. The LDAP server is accessed to verify the username as well as the stored password for that user.	
Printer	If Secure Print Manager or Direct Print is used, it is possible to print.	

<u>About the Saved Password function</u>

If this function is enabled, when authentication succeeds for a user for the first time when using the operation panel, the password will be encrypted (AES128) and saved in the SQL DB.

The saved password cannot be accessed or changed from the operation panel, even with administrator privileges.

If the user’s password is changed, the user needs to login again (using the new password) from the operation panel in order to update the password saved in the DB of AAM-S.

Authorization

Authorization (privileges) is assigned to individual users or to groups.
When a user is newly registered to the user information table kept by AAM-S, the user will be assigned default privileges.

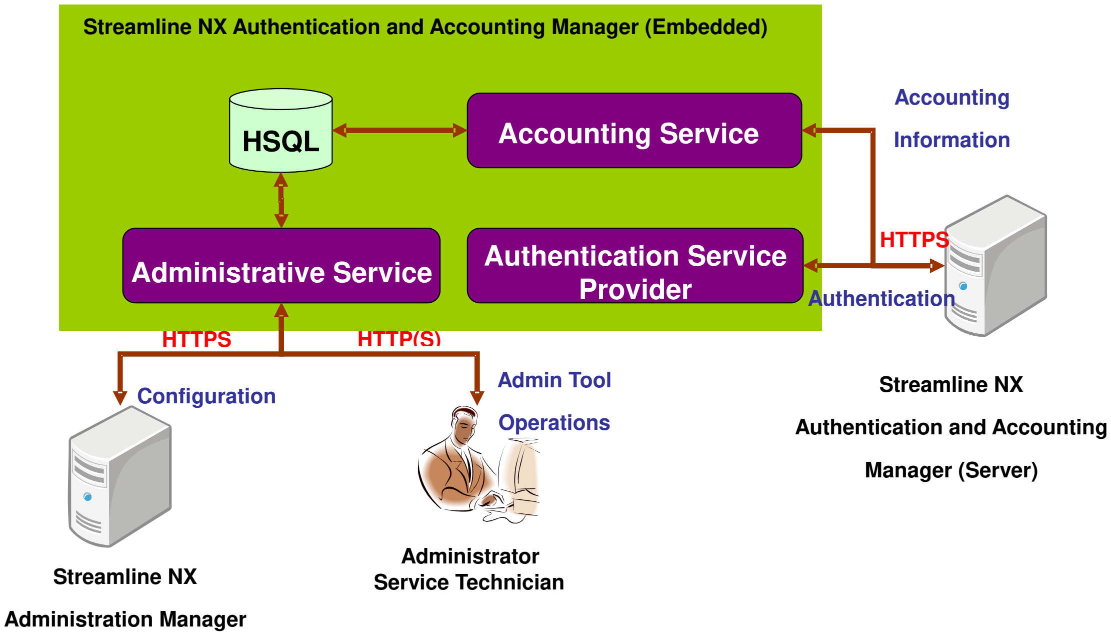
Accounting

The Accounting logs (username, page count, job type, etc.) are temporarily stored in AAM-E's HSQL DB.
AAM-E sends the information to AAM-S for use by Streamline NX's Report Generator.
There is a special procedure for collecting the accounting logs from LPs when using SPM. Please see the SPM white paper for details.

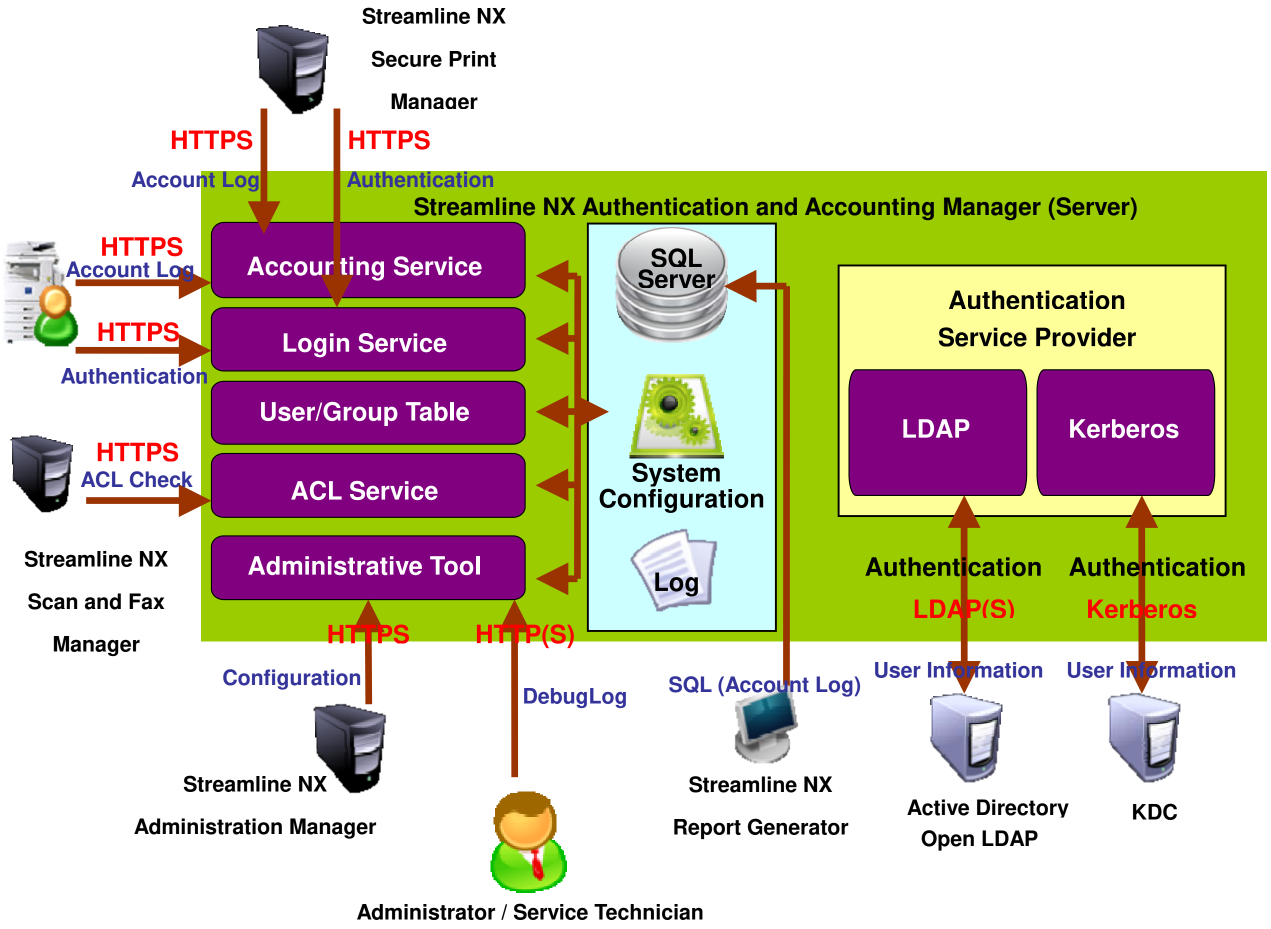
2. System

This section describes the security of data stored on the HDD and as it travels over the network.

[Streamline NX Authentication and Accounting Manager (Embedded)]



[Streamline NX Authentication and Accounting Manager (Server)]



3. Network Protocols

3.1 Ports and Protocols

[AAM (Embedded)]

Features	Protocol	Service	Port No	Destination	Description
Administrative Service	TCP	http	8080	From client PC/ADM to AAM (Embedded)	
	TCP	https	51443		Used only when SSL is enabled
Authentication Service Provider, **Accounting Service**	TCP	https	8443 (*1)	AAM (Server)	

(*1) Default port. This can be changed.

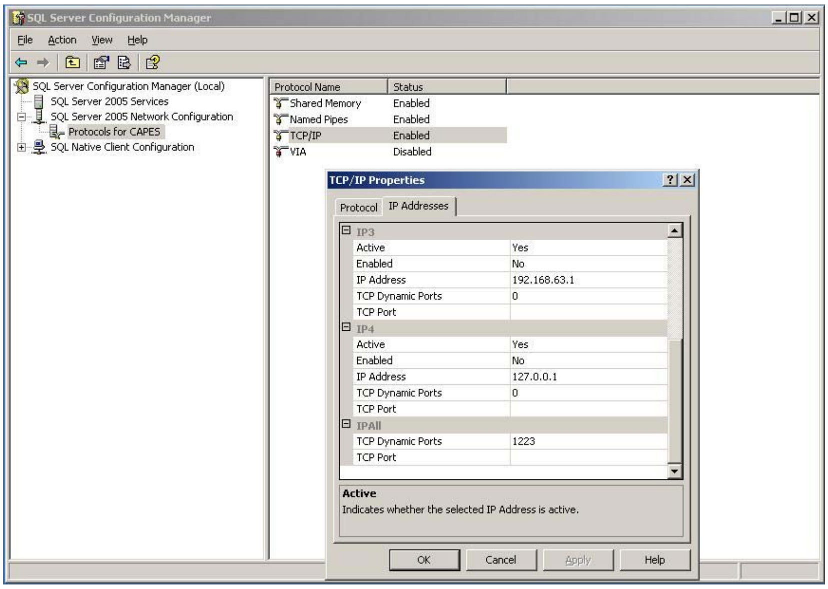
[AAM (Server)]

Features	Protocol	Service	Port No	Destination	Description
Administrative Tool	TCP	http	8080 (*1)	AAM (Server)	
	TCP	https	8443 (*1)		
Login Service	TCP	https	8443 (*1)	AAM (Server)	
Authentication Kerberos	TCP	Kerberos	88	KDC	
	UDP	Kerberos	88		
Authentication LDAP Authentication (Other LDAP Servers)	TCP	LDAP	389 (*1)	LDAP server	
	TCP	LDAPS	636 (*1)		
SQL Server	TCP	http	(*2)	DB server	

(*1) Default port. This can be changed.

(*2) A random open port on the SQL server (1024 – 65536) is used.

The current SQL server port can be found using:
“SQL Server Configuration Manager”→ “SQL Server Network Configuration” → “Protocols for <Instance Name>” → “TCP/IP” → “IP Addresses” → “IP ALL” → “TCP Dynamic Ports”.


SQL Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
Protocols for CAPES
SQL Native Client Configuration
TCP/IP Properties
Protocol
IP Addresses
OK
Cancel
Apply
Help

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

IP3	
Active	Yes
Enabled	No
IP Address	192.168.63.1
TCP Dynamic Ports	0
TCP Port	
IP4	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	0
TCP Port	
IPAll	
TCP Dynamic Ports	1223
TCP Port	

Active
Indicates whether the selected IP Address is active.

3.2 Recommended Precautions

[Using the AAM-E Administrative Service]
AAM-E can be accessed from a browser using either http or https.
When using http, the password sent over the network is not encrypted.
We recommend using https for security purposes.

Streamline NX Administration Manager only uses https to send configuration information to AAM-E.

AAM-E uses TLS v1.0 when https is enabled.

[Using the AAM (Server) Administrative Tool]
AAM-S can be accessed from a browser using either http or https. For enhanced security, using https is recommended.

AAM-S only uses https to handle requests from AAM-E, Streamline NX Administration Manager, and Streamline NX Scan and Fax Manager. AAM-S uses TLS v1.0 for https connections.

[Authentication Security]
For enhanced security, using https is recommended.

AAM-S uses TLS v1.0 for communication with LDAP authentication servers when LDAPS is used.
If Kerberos is used to access an AD authentication server, the encryption used by AAM-S depends on the security level of the authenticating AD server (RC4-HMAC/AES128, etc.).

4. Data Flow and Storage

4.1. Data Storage and Data Access Permissions - AAM (Embedded)

4.1.1 Stored Data

Data Type	Transmitted Data	Specification
System Configuration	Server settings, accounting settings, Admin information (Username, Password), Service information (Username, Password), Server certificate, etc.	Admin privileges are required in order to import/export the system configuration file. All passwords in the system configuration are encrypted using DES.
Accounting Log (HSQL Database)	Accounting information (Usercode, job type, etc.) Device information (IP address, Device code, Model code)	Service privileges are required in order to export the log file. Access from other SDK applications or via a remote connection is not available. The database and file are not encrypted.
Accounting Error Log	Accounting error information (Usercode, job type, etc.)	Service privileges are required in order to export the log file. The file is not encrypted.
Event Log	Operation information (Date, Event code, PC information, Username, etc…)	Service privileges are required in order to export the log file. The file is not encrypted.

4.1.2 Data Access Permissions

Data	Account Type	Permission	Description
System Configuration	Administrator	Read Edit	Managed using the web UI or Streamline NX Administration Manager.
Accounting Log (HSQL Database)	Service (*1)	Read	The service account can only export the accounting log in a CSV format.
	System	Write Edit Delete	The system generates the file if it does not exist. The system edits the logs when accounting data is generated. The system deletes the logs after the logs have been sent to the server. (*2)
Accounting Error Log	Service (*1)	Read	The service account exports the accounting error log as a ZIP archive.
	System	Write Edit Delete	The system generates the file if it does not exist. The system edits the file when an accounting error occurs. The log supports up to 10240 entries. When this limit is reached, the oldest information is overwritten.

Event Log	Service (*1)	Read	The service account exports the event log as a ZIP archive.
	System	Write Edit Delete	The system generates the file if it does not exist. The system edits the file when an operation occurs. Up to 5 1MB files are used to store the log data.

(*1) SSL is recommended.

(*2) Accounting logs are sent to the server according to the following rules:

Timing	Target accounting logs
At startup	All current accounting logs.
At user logout	All current accounting logs for the user.
Periodic processing	At the specified interval (Count Interval).
FAX transmission	The accounting logs for the transmitted fax.

4.1.3 Caution

[Backup]

Regular backups are recommended for the System Configuration file.

Backups are recommended for the Accounting Log file and the Accounting Error Log file in case of database failure.

4.2. Data Storage and Data Access Permissions - AAM (Server)

4.2.1 Stored Data

Data	Specification
SQL Server Database	An unique account is used to access the SQL server. When installing AAM-S, the HostName/DB Name/Instance Name/Account/Password are set. The User/ADM Administrator/Web UI's Service password is encrypted using AES128.
Import User Information Log	Admin privileges are required in order to export the User Information log. The log is not encrypted.
Import Group Authorization Information Log	Admin privileges are required in order to export the Group Authorization Information log. The log is not encrypted.
Delete Disabled User Log	Admin privileges are required in order to export the Disabled User log. The log is not encrypted.
Delete Count Data Log	Admin privileges are required in order to export the Count Data log. The log is not encrypted.
Info Log File	Service privileges are required in order to export the Info Log file. The log is not encrypted.
Debug Log File	Service privileges are required in order to export the Debug Log file. The log is not encrypted.

4.2.2 Data Access Permissions

Data	Account type	Permission	Description
SQL Server Database	Administrator	Write Edit Delete	Managed using the Administrative Tool.
	User	Write	For Card Registration (AAM-E)
Export/Import User Information Log	Administrator (*)	Read	The admin account can export the User Information log as a ZIP archive.
	System	Write Delete	When users are imported, the System account logs the results.
Export/Import Group Authorization Information Log	Administrator (*)	Read	The admin account can export the Group Authorization Information log as a ZIP archive.
	System	Write Delete	When Group Authorization information is imported, the System account logs the results.
Export/Delete Disabled User Log	Administrator (*)	Read	The admin account can export the Disabled User log as a ZIP archive.
	System	Write Delete	The system account can write new logs and delete the old log.

Export/Delete Accounting Data Log	Administrator (*)	Read	The admin account can export the Delete Accounting Data log as a ZIP archive.
	System	Write	The system account can write new logs and delete the old log.
Info Log File	Service (*)	Read	The service account can export the Info Log, which contains 2 days worth of entries, as a ZIP archive.
	System	Write Delete	Generates up to 10 days of logs and updates everyday.
Debug Log File	Service (*)	Read	The service account can export the Debug Log, which contains 2 days worth of entries, as a ZIP archive.
	System	Write Delete	Generates up to 10 days of logs and updates everyday.

(*) SSL is recommended.

4.2.3 Caution

[Resource Protection]

The security of AAM-S depends on the security of the server on which it is hosted. In order to protect the system, it should be kept in a secure location, physical access should be limited. Also, some sort of virus/malware protection is recommended.

[Backup]

Regular backups are recommended. At a minimum, backups should include the following:

Streamline NX Authentication and Accounting Manager (Server): User/Group Attributes