Security White Paper

Card Authentication Package and

Card Authentication Package Enterprise Server V2

Document Version 1.1.0

Solution Support Department
Service and Support Center
Global Marketing Group

Document version history:

Version	Date of Issue	Revision
1.0.0	August, 2011	Initial release This document applies to the following products: ・ Card Authentication Package v2.0 ・ Card Authentication Package Enterprise Server v2.0
1.1.0	March, 2011	This document applies to the following products: ・ Card Authentication Package v2.1 ・ Card Authentication Package Enterprise Server v2.1

1 Summary

This paper provides security information about Card Authentication Package V2 (CAP V2) and Card Authentication Package Enterprise Server V2 (CAP-ES V2).
The use of Card Authentication Package V1 (CAP V1) with Card Authentication Package Enterprise Server V2 (CAP-ES V2) authentication is also covered by this paper.

2 AAA (Authentication/ Authorization/ Accounting) Security

2.1 Authentication

CAP V2 allows for the use of card authentication. Using CAP V2, users can login to the MFP by swiping a card instead of entering a username and password on the Operation Panel. CAP V2 supports the use of Local DB/Active Directory/LDAP/CAP-ES V2 authentication methods. These authentication methods are explained in the following table.

Authentication	Location	Credentials used to authenticate:	Supported Auth. Methods
CAP V2 with Cache	Panel	Username and password entered manually	
	WIM		
	Printer Driver	Username and password entered manually in the printer driver * The password requirement can be changed using the Configuration Tool	
	Card	There are two authentication types: 1. The username is obtained from the Card ID, and the local DB is searched for username that is associated with the Card ID. If the username exists, authentication succeeds. 2. The username is obtained from the Card ID. After using the card, the user must enter a password which is checked against the password in the local DB. * Configurable from the Configuration Tool	
CAP V2 with Active Directory CAP V2 with LDAP Server	Panel	Username and password entered manually	- LDAP Authentication. - LDAP Authentication with Kerberos token
	WIM		
	Print Driver	Username and password entered manually in the printer driver * The password requirement can be changed using the Configuration Tool	

<table>
<tr><th>Authentication</th><th>Location</th><th>Credentials used to authenticate:</th><th>Supported Auth. Methods</th></tr>
<tr><td></td><td>Card</td><td>1. Authentication is performed by a proxy user that searches the LDAP directory for username that is attached to the Card ID. If the username exists, authentication succeeds.
2. The username is obtained from the Card ID. After using the card, the user must enter a password.
3. The username is obtained from the Card ID, and the local DB is search for password that is associated with this username. The password stored in CAP V2 and the obtained username are used for authentication.
* (1.) is only supported in LDAP authentication.</td><td></td></tr>
<tr><td rowspan="4">CAP V2 with CAP-ES V2</td><td>Panel</td><td rowspan="2">Username and password entered manually</td><td rowspan="4">- Kerberos Authentication
- NTLM Authentication
- ADSI Authentication
- LDAP Authentication
- Internal Authentication</td></tr>
<tr><td>WIM</td></tr>
<tr><td>Printer Driver</td><td>1. The Username and Password are obtained from the received print job
2. The Username is obtained from the received print job
*Configurable from the Configuration Tool</td></tr>
<tr><td>Card</td><td>1. Authentication is performed by a proxy user that searches the LDAP directory for username that is attached to the Card ID. If the username exists, authentication succeeds.
2. The username is obtained from the Card ID. After using the card, the user must enter a password.
3. The username is obtained from the Card ID, and the local DB is search for password that is associated with this username. The password stored in local DB and the obtained username are used for authentication.
* (1.) is only supported by ADSI and LDAP authentication.</td></tr>
<tr><td rowspan="3">CAP V1 with CAP-ES V2</td><td>Panel</td><td rowspan="2">Username and password entered manually</td><td rowspan="3">- Kerberos Authentication
- NTLM Authentication
- LDAP Authentication</td></tr>
<tr><td>WIM</td></tr>
<tr><td>Printer Driver</td><td>1. The Username and Password are obtained from the received print job.</td></tr>
</table>

Authentication	Location	Credentials used to authenticate:	Supported Auth. Methods
		2. The Username is obtained from the received print job. Then authentication is performed by a proxy user that searches the LDAP directory for the obtained username. If the username exists, authentication succeeds. 3. The username is obtained from the received print job. Then a password stored in local DB and the obtained username are used for authentication *Configurable from the Configuration Tool * (2.) is only supported by LDAP authentication.	
	Card	1. The username is obtained from the Card ID. After using the card, the user must enter a password. 2. Authentication is performed by a proxy user that searches the LDAP directory for username that is attached to the Card ID. If the username exists, authentication succeeds. 3. The username is obtained from the Card ID, and the local DB is search for password that is associated with this username. The password stored in local DB and the obtained username are used for authentication. * Configurable from the Configuration Tool * (2.) is only supported by LDAP authentication.	

About the Saved Password function in CAP-ES V2:

When authentication succeeds for a user for the first time when using the operation panel, the password will be encrypted and saved in the CAP-ES V2 DB while this function is active.

The saved password cannot be accessed or changed from the Operation Panel or from Web Image Monitor, even with administrator privileges.

If the user's password has changed, a password input dialog box will be displayed when the user next attempts to login, and the stored password will then be updated.

2.2 Authorization

Authorization (privileges) is assigned to individual users or to groups.

System Structure	Authorization (privileges)
CAP V2 with Cache CAP V2 with Active Directory CAP V2 with LDAP Server	As assigned by the local DB user information. If a user does not exist in the local DB, the user will be assigned default permissions. Default permissions are configurable from the Configuration Tool.
CAP V2 with CAP-ES V2	Users can also be assigned unique permissions. Users with no assigned permissions are assigned permissions based on the user's group memberships (direct membership and parent groups). The users with no assigned permissions and that do not belong to any group will be assigned default permissions. New CAP-ES V2 users are automatically assigned the default permissions. Permissions are divided by function (copy, print, etc.). Default permissions, group-based and user-based permissions are configured from the Configuration Tool.
CAP V1 with CAP-ES V2	Users can also be assigned unique permissions. Users with no assigned permissions are assigned permissions based on the user's group memberships (direct membership only). The users with no assigned permissions and that do not belong to any group will be assigned default permissions. New CAP-ES V2 users are automatically assigned the default permissions. Permissions are divided by function (copy, print, etc.). Default permissions, group-based and user-based permissions are configured from the Configuration Tool.

2.3 Accounting

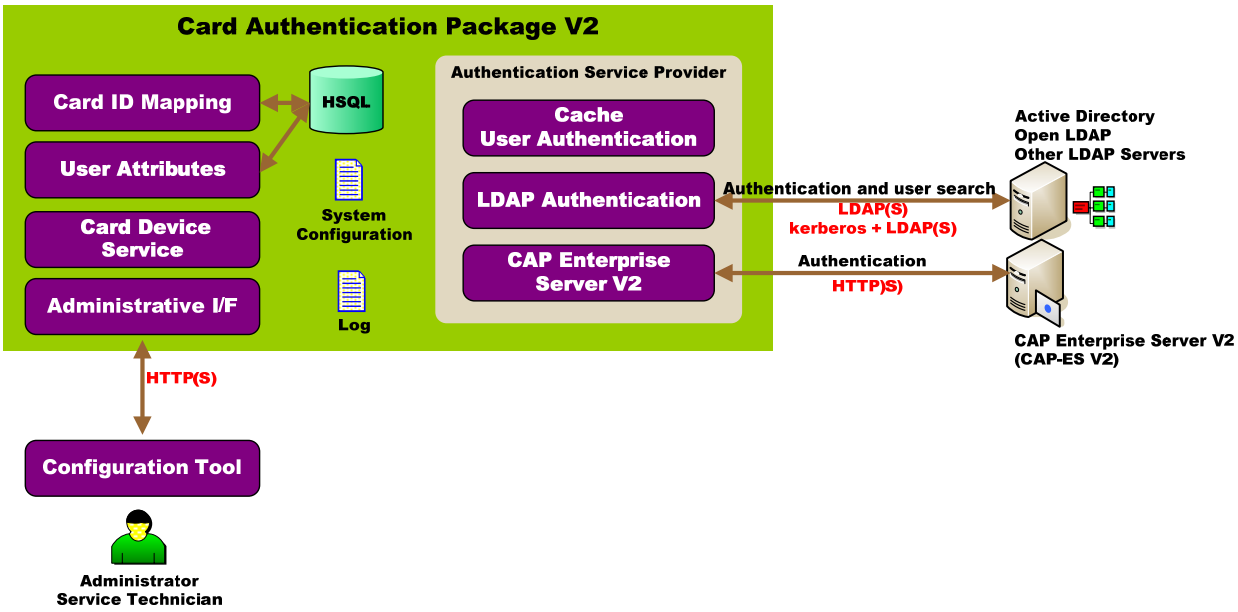
Page counters are maintained for each individual user. These can be retrieved using a tool such as Remote Communication Gate S Pro.

3 Data Security

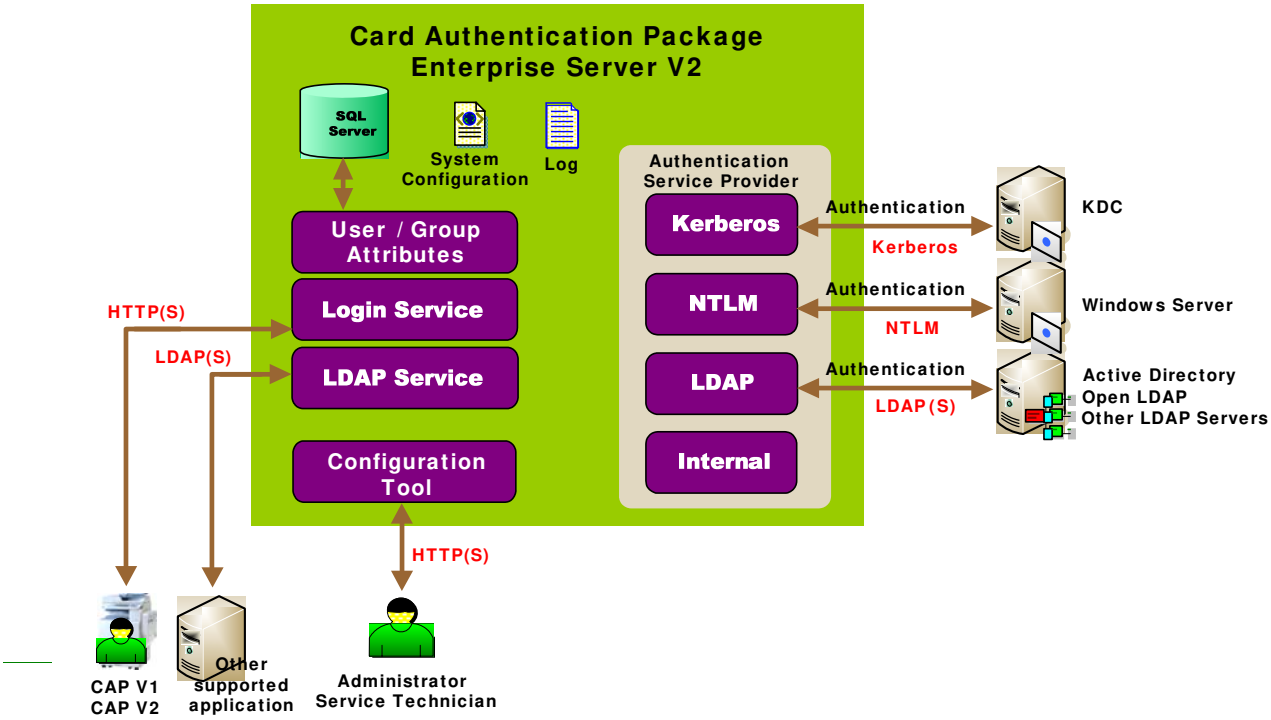
This section describes the security of data stored on the HDD and as it travels over the network.

3.1 Overview

CAP V2:



CAP-ES V2:



3.2 Network

Ports and Protocols

CAP V2:

Features	Protocol	Service	Port No	Destination	Description
Configuration Tool	TCP	http	8080 (*1)	CAP	
	TCP	https	51443 (*1)		Only when SSL is enabled.
	UDP		50006 (*1)		Device Discovery
Cache Authentication	-	-	-	-	-
LDAP Authentication (Active Directory)	TCP	LDAP	389 (*2)(*3)	Active Directory Server	
	TCP	LDAPS	636 (*2)(*3)		Only when SSL is enabled.
	TCP	Kerberos	88 (*2)		Used when the Authentication method is set to Kerberos
LDAP Authentication (Other LDAP servers)	TCP	LDAP	389 (*2)(*3)	LDAP Server	
	TCP	LDAPS	636 (*2)(*3)		Only when SSL is enabled.
CAP Enterprise Server V2 Authentication	TCP	http	18080 (*2)(*3)	CAP-ES V2	
	TCP	https	18443 (*2)(*3)		Only when SSL is enabled.

(*1) Ports opened by the SDK/J Platform

(*2) Ports opened on the server side when CAP-ES V2 connects to the server as a client.

(*3) Default ports that can be changed. If these are changed, the server-side port numbers also must be changed.

CAP-ES V2:

Features	Protocol	Service	Port No	Destination	Description
Administrative Tool	TCP	http	18080 (*1)(*3)	CAP-ES	
	TCP	https	18443 (*1)(*3)		Only used when SSL connection is used with the browser.
Login Service	TCP	http	18080 (*1)(*3)	From CAP V2 to Login Server	User permissions, etc.
	TCP	https	18443 (*1)(*3)		Only used for SSL connections.
	TCP	http	8080 (*1)		Only used for CAP V1 connections.
	TCP	https	8443 (*1)		Only used for CAP V1 connections when SSL is enabled.
LDAP Service	TCP	Ldap	10389 (*1)(*3)	Other supported application	
	TCP	Ldaps	10636 (*1)(*3)		Only when SSL is enabled.
Authentication Active Directory	TCP	Kerberos	88 (*2)	AD server	
	TCP	Ldap	389 (*2)(*3)		
	TCP	Ldaps	636 (*2)(*3)		Only when SSL is enabled.
	TCP	Msft-gc	3268 (*2)		Only used for Global Catalog connections.
	TCP	MSft-gc-ssl	3269 (*2)		Only used for Global Catalog connections when SSL is enabled.
Authentication NTLM	TCP/UDP	netbios-ns	137 (*2)	Domain Controller	
	TCP/UDP	netbios-dgm	138 (*2)		
	TCP/UDP	netbios-ssn	139 (*2)		
	TCP/UDP	microsoft-ds	445 (*2)		
Authentication LDAP Authentication (Other LDAP Servers)	TCP	Ldap	389 (*2) (*3)	LDAP server	
	TCP	Ldaps	636 (*2) (*3)		Only when SSL is enabled.
SQL Server	TCP	http	(*4)	SQL server	

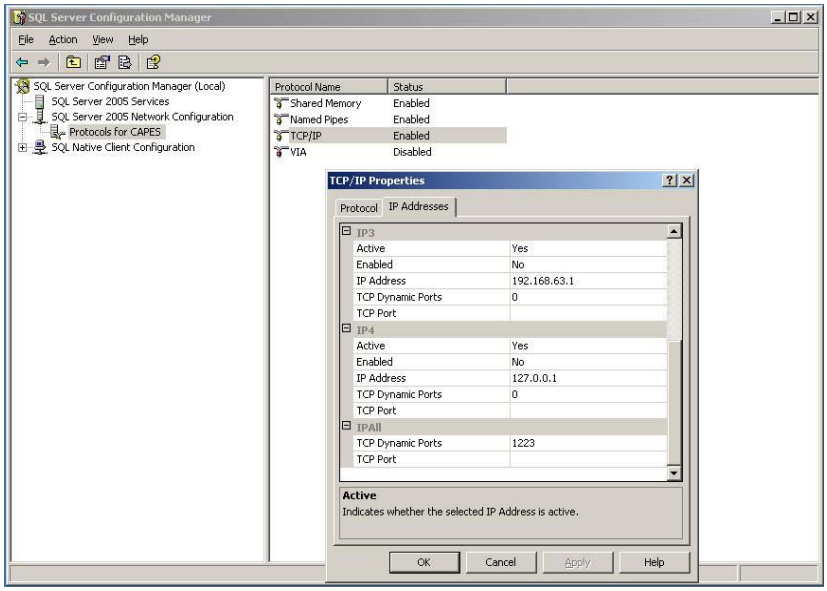
(*1) Ports opened by CAP-ES V2

(*2) Ports opened on the server side when CAP-ES V2 connects to the server as a client.

(*3) Default ports that can be changed. If these are changed, the server-side port numbers must also be changed.

(*4) A random, free port is automatically retrieved and used by the SQL Server. The SQL server port can be found using:

"SQL Server Configuration Manager" → "SQL Server 2005 Network Configuration" → "Protocols for CAPES" → "TCP/IP" → "IP Addresses" → "IP ALL" → "TCP Dynamic Ports".



Remarks

Using the Configuration Tool and Administrative Tool:
CAP V2 or CAP-ES V2 can be accessed using either http or https.
The CAP admin password can be changed using the Configuration Tool, and CAP-ES V2 admin password can be changed using the Administrative Tool. If this is done over http, the password will be sent as clear text. We recommend using https for such activity.

Login Service
CAP-ES communicates with CAP V1 and CAP V2 using either http or https. For enhanced security, using https is recommended.

LDAP security:
We recommend using LDAPS instead of LDAP whenever possible.

3.3 Data Storage

Data Storage

CAP V2

Data	Specification
HSQL Database	A fixed username and password are used to connect to the HSQL DB. The user name and password are encrypted in CAP V2 (AES128). Access from other SDK/J applications or via a remote connection is not available.
System Configuration	Admin privileges are required in order to import/export the system configuration file. All passwords in the system configuration are encrypted using AES128.
Log-Login History Log-System Log	Admin privileges are required in order to export the logs from the Configuration Tool. The logs are not encrypted. Information can be masked with the Log Masking Tool.

CAP-ES V2

Data	Specification
SQL Server Database	The sa account is used to access the SQL server. The sa password is configured when SQL is installed. Information in the DB is encrypted by SQL server.
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.
Import Card ID Information Log	Admin privileges are required in order to export the Card ID information log. The log is not encrypted.
Import Integrated Information Log	Admin privileges are required in order to export the Integrated Information log. The log is not encrypted.
Task Synchronization Log	Admin privileges are required in order to export the Task Synchronization log. The log is not encrypted.
Archival Record Log	Admin privileges are required in order to export the Archival Record log. The log is not encrypted.
Info Log File	Admin or Service privileges are required in order to export the Info log. The log is not encrypted.
Debug Log	Admin or Service privileges are required in order to export the Debug log. The log is not encrypted.

Data Access Permissions

CAP V2

Data	Primary Account	Permission	
HSQL Database	Administrator	Write Edit Delete	Managed using the Configuration Tool.
	User	Write Edit	Users can edit their personal information using the Card Registration tool. Users can register their IC card, and change their password from the operation panel using the application launcher.
System Configuration	Administrator (*)	Read Edit	Managed using the Configuration Tool.
	System	Write Edit	If no system configuration file exists one will be generated automatically at startup.
Log-Login History	Administrator (*)	Read	Exported from the Configuration Tool as a plain text file.
	System	Write Delete	Contains only 60 days of logs.
Log- System Log	Serviceman (*)	Read	Exported from the Configuration Tool as a plain text file.
	System	Write Delete	Contains only 14 days of logs.

Note: The combined maximum size for the Login History and System Logs is 60MB.

CAP-ES V2

Data	Primary Account	Permission	
SQL Server Database	Administrator	Write Edit Delete	Managed using the web UI.
Import User Information Log	Administrator (*)	Read	Exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	When users are imported, the System account logs the results.
Import Group Authorization Information Log	Administrator (*)	Read	Exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	When groups are imported, the System account logs the as a ZIP archive.
Import Card ID Information Log	Administrator (*)	Read	Exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	When the card ID information is imported, the System account logs the results.

Import Integrated Information Log	Administrator (*)	Read	Exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	When the Integrated information is imported, the System account logs the results.
Task Synchronization Log	Administrator (*)	Read	Exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	When the Task synchronization information is imported, the System account logs the results.
Archival Record Log	Administrator (*)	Read	Exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	The system account deletes logs older than 397 days (approx. 13 months). The logs can be exported prior to deletion. When the Archival Record is imported, the System account logs the results.
Info Log File	Service	Read	The entire log exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	Only 1 Log containing 1 day entries, with the file size limit of 100MB. Up to 20 logs can be stored.
Debug Log File	Administrator (*)	Read	The entire log exported from the Administrative Tool as a ZIP archive.
	System	Write Delete	Only 1 Log containing 1 day entries, with the file size limit of 100MB. Up to 20 logs can be stored.

(*) SSL is recommended.

Caution

Resource Protection:
The security of CAP-ES V2 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, access should be limited, and some sort of virus protection is recommended.

Backup
Regular backups are recommended for below files. At minimum, backups should include the following:
CAP V2: System Configuration, Card ID Mapping User Attributes
CAP-ES V2: System Configuration (Files/DB Data), User/Group/Card Attributes (DB Data)