

TA / UTAX aQrate:

Security White Paper

Version 8.2

Document Version: 0122022

12/2022

1. INTRODUCTION	2
1.1. Purpose	2
1.2. Target Audience	2
1.3. Document Structure	2
1.4. Edition Notice	2
2. TA/UTAX AQRATE OVERVIEW	3
3. TA/UTAX AQRATE SECURITY	4
3.1. Registration into TA/UTAX aQrate	5
3.2. Identification and Authentication	5
3.3. Auto-Logout Policy	6
3.4. Account Lockout Policy	6
3.5. Password Policy	7
3.6. Authorization	7
3.7. Audit Logs	8
3.8. Data Security	9
3.8.1. Job Privacy Mode (Option)	9
3.8.2. Private Queue (Option)	9
3.8.3. Encrypt Firebird Database (Option)	10
3.9. Document Security	10
3.9.1. Secure Print	10
3.9.2. Watermark (Option)	11
3.9.3. Scan policy	11
3.10. Network Security	11
3.10.1. TA/UTAX aQrate Port Settings for Secure Communication	11
3.10.2. FTP Server for Secure Scan Job Receiving	14
3.10.3. Protection of Communication Data	14
3.11. Register for exception list	17
4. Network Ports	19
5. THE TA/UTAX COMMITMENT TO TA/UTAX AQRATE SECURITY	24

1. Introduction

1.1. Purpose

The purpose of this document is to inform you about security measures taken by TA/UTAX for the protection of TA/UTAX aQrate users.

TA/UTAX's first priority is to provide rigorous protection of information assets.

1.2. Target Audience

The target audience for this document is staff members at TA Triumph-Adler and local partners.

1.3. Document Structure

The document is organized into the following sections:

- TA/UTAX aQrate Overview
- TA/UTAX aQrate Security
- The TA/UTAX Commitment to Security

1.4. Edition Notice

The information contained in this document is accurate and current as of January 22, 2021. Changes and improvements in TA/UTAX aQrate may be incorporated in later editions without prior notice.

2. TA/UTAX aQrate Overview

TA/UTAX provides:

- Rigorous protection of customers' important information assets
- Management and control of overall output (copies, prints, and scans)
- Generation of detailed reports containing operational information about MFPs and printers

Through:

- Secure copying, printing, and scanning
- User authentication
- Printer device administration
- Print job management
- Access control
- Accounting and reports

For example, through a simplified document workflow process for job handling:

- Print jobs can be hosted at the TA/UTAX aQrate server after completion of user registration in TA/UTAX aQrate
- Settings are configured in printer drivers and mobile applications necessary for printing from any client PC or mobile device.
- Once a user is successfully authenticated, they choose the print job on the operational panel of a MFP/Printer device, and the document data is released from the TA/UTAX aQrate server.

Users have access to TA/UTAX aQrate via a web browser and can check their personal printing costs and print jobs. Statistical reports containing information about print volume and printing device usage by individual users and groups of users can be generated, providing a visual way to see print costs and device operational status.

3. TA/UTAX aQrate Security

TA/UTAX ensures secure protection of the following data:

- The data used by TA/UTAX aQrate
- The document data such as copying, printing and scanning
- The data traveling through communication paths within TA/UTAX aQrate

This section explains in detail how this data is rigorously protected by TA/UTAX aQrate's secure configuration and its various security features. TA/UTAX aQrate allows system administrators to set the rules on TA/UTAX aQrate usage in accordance with the security policy defined by our customers, and ensures their secure environment.

TA/UTAX informs our customers that the personal data listed in Table 1 is monitored, stored and handled by TA/UTAX aQrate. Customers define their security policy depending on their environment so that the customer's data can be securely protected.

Table 1 Personal Data

Personal data used in TA/UTAX aQrate	<ul style="list-style-type: none"> • User name (required) • Login name (required) • ID card • ID number • PIN code • Password • Email address • Phone number • Personal number • Print job data • Print job names • Shared folder path • Credit • PDF previews of print jobs (with the optional job preview feature) • Authentication server (when using authentication server) • Synchronization source
Personal data contained in TA/UTAX aQrate reports	<ul style="list-style-type: none"> • Coverage counters (users) • Environmental impact (users)

	<ul style="list-style-type: none"> • Group counters (current membership) • Group counters (current membership details) • Projects (project per user) • Projects (user total summary) • User counters (daily summary, session summary, total summary for details, amount on a weekly basis) • User credit statement • User list (credit balances, recharge credit)
--	--

Note:

Environmental impact (expired or deleted jobs) contains user name and name of the job.

Project job (daily summary) contains name of the job.

3.1. Registration into TA/UTAX aQrate

Users must register for TA/UTAX aQrate via its web user interface before they can use TA/UTAX aQrate. One way to do this is to register with a name and an email address. Then, a PIN code is generated and registration is complete.

Since users must identify themselves to use TA/UTAX aQrate, unauthorized access to TA/UTAX aQrate is prevented.

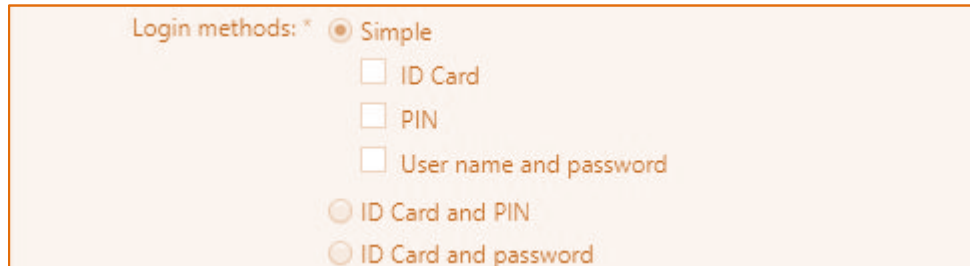
The logs record who, when and to where the access occurred. This information can be used to help trace unauthorized access.

3.2. Identification and Authentication

When a user enters a login information via the web user interface that agrees with the one that has been registered, the authorized user is authenticated and then granted access to TA/UTAX aQrate.

Once the user logs into TA/UTAX aQrate, they can execute the job stored on TA/UTAX aQrate server at a MFP/Printer device. Access logs are recorded at this time.

To strengthen security, it is possible for a user to select two-level authentication. For example, they can select either a combination of an ID card and PIN or a combination of an ID card and password.



Login methods: * ☒ Simple
☐ ID Card
☐ PIN
☐ User name and password
☐ ID Card and PIN
☐ ID Card and password

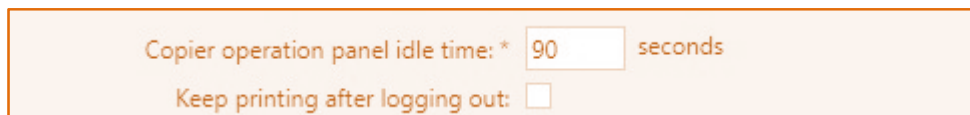
Login Methods

Only after entering valid login information can the user gain access to TA/UTAX aQrate, thereby protecting TA/UTAX aQrate against unauthorized use.

The access logs are used to investigate and help trace issues that occur.

3.3. Auto-Logout Policy

The user will be automatically logged out if their account has been idle for a certain amount of time. The auto-logout time is set by an administrator.



Copier operation panel idle time: * 90 seconds
 Keep printing after logging out: ☐

Auto-Logout Policy

The feature prevents a malicious or an unintentional act by a third person if the user has forgotten to logout from TA/UTAX aQrate and has left their MFP/Printer device. For example, the residual data remaining in the memory inside a MFP/Printer device could be released by anyone in the office without permission.

3.4. Account Lockout Policy

When the wrong passwords are repeatedly used to attempt to log into the TA/UTAX aQrate server more than a pre-determined number of times, the account will be locked out.

As shown in the screenshot below, when reaching the account lockout threshold for failed login attempts of five times, the account will be locked out. The security setting will unlock the account after 15 minutes.

Account lockout

Attempts before lockout: *

5

Lockout time: *

15

minute(s)

Account Lockout Policy

The Account Lockout Policy setting guards against password cracking attacks in TA/UTAX aQrate.

3.5. Password Policy

An administrator can set a strong password that is difficult to be analyzed depending on the user environment. The password length and complexity are defined as shown below.

Password complexity

Minimum length: *

8

Enforce password complexity: *

2

of 4 rules

At least one upper-case letter

At least one lower-case letter

At least one number

At least one special (non-alphanumeric) character

Password Policy

Table 2 Password Policy

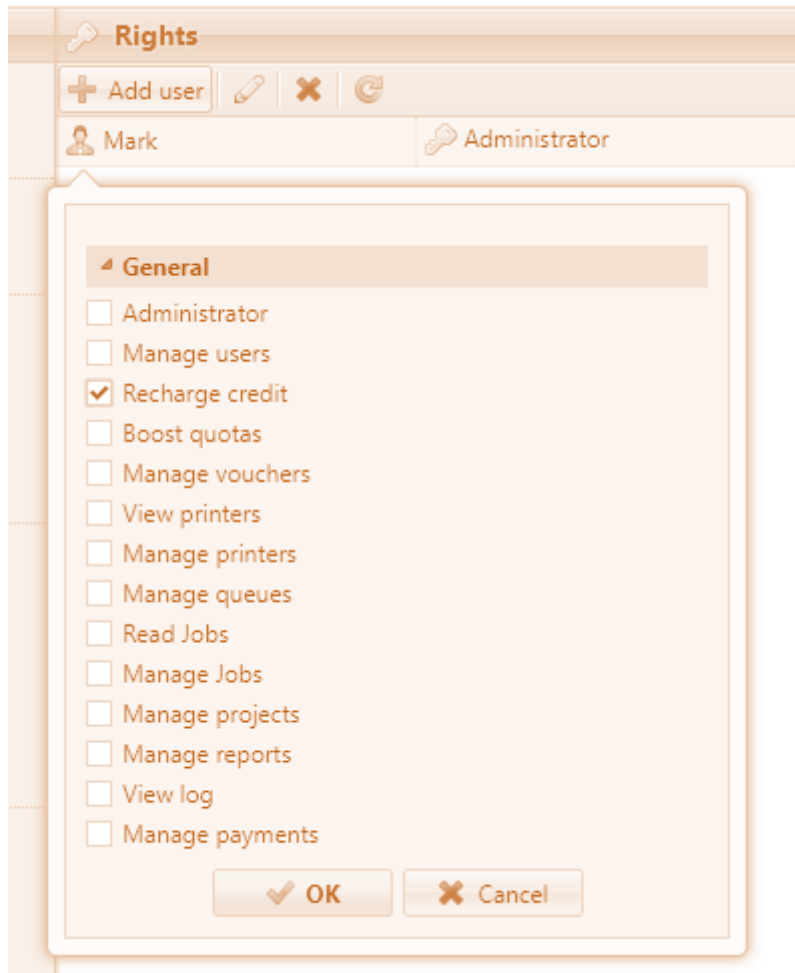
Password Length	At least 8 characters (8 characters by default)
Password Complexity	Must include at least one number between 0 and 9, one uppercase letter, one lowercase letter and one special symbol (2 of 4 rules by default)

A password that does not meet the password policy is prohibited. This prevents simple passwords from being set by users and guards against unauthorized access.

3.6. Authorization

Access to TA/UTAX aQrate can be restricted by user roles – administrator or user. In addition, access to features set in TA/UTAX aQrate can be restricted according to the rights defined in TA/UTAX aQrate on an authorized user basis. For example, user management, device management, and credit

recharge can be limited. Users are permitted access to features based on the users' authorization levels. This restriction prevents data leaks from TA/UTAX aQrate. Therefore, users who have no authorization cannot use the particular features, which are not granted to unauthorized users.



Authorization

3.7. Audit Logs

By checking the audit logs, TA/UTAX aQrate can be analyzed to see if it is secure and has not been exposed to risks. Access authorization to the audit logs can be set by an administrator who can restrict who can access the audit logs in the user environment.

TA/UTAX aQrate records audit logs of the following operations:

- Log in and log out to and from the TA/UTAX aQrate server
- TA/UTAX aQrate server version up
- Database backup
- Database restore

- Add, edit, and delete to and from the TA/UTAX aQrate server
- Add, edit, and delete to and from user attributes
- Add, edit, and delete groups and queues

Audit logs include the following information:

- Operation result
- Date and time of the result (success or failure)
- Login ID of the logged in user

In the event of alteration or data leaks, the audit logs can be used to investigate and help trace the unauthorized access.

3.8. Data Security

For highly security-conscious customers, maximum protection of personal data can be achieved.

The range of personal data to be secured can be set depending on the customer's environment. The use of the following features prevents personal data from unauthorized access and viewing by third parties without access permission.

3.8.1. Job Privacy Mode (Option)

Job Privacy Mode is available when a Job Privacy License is inserted and activated on the TA/UTAX aQrate server. The Job Privacy Mode hides user names and all the names of print jobs. Logged in users can view only the names of their own print jobs. The names of all the other jobs are masked by ***. This rule can be applied to any user role, and even the system administrator cannot view the names of the jobs of other users.

In Job Privacy Mode, it is impossible to track the names of print jobs and the Job Preview feature is disabled. Once the Job Privacy License is activated, the license cannot be removed.

In addition, user-based reports can be limited. Group-based and MFP/Printer-based information can be available in the reports by completely deleting user-based reports. The report can also be displayed by authorized users only. The user-based information can be hidden from a third party by TA/UTAX aQrate user authorization management.

3.8.2. Private Queue (Option)

When handling highly confidential personal data, unauthorized access to the released print jobs

stored on the TA/UTAX aQrate server needs to be restricted. An administrator can allow the users or the groups to use the Private Queue feature, where print jobs are deleted immediately after they are released. This feature prevents unauthorized access to the confidential personal data while maintaining user-friendliness.

3.8.3. Encrypt Firebird Database (Option)

No matter how tightly you control access to your database or take an audit trail (Log), you can't prevent fraud that copies data to another system or medium if your data is not encrypted.

In the event of an eventual unauthorized access, it is important that the data itself be encrypted to protect the data. TA/UTAX aQrate allows you to select encryption/decryption from Easy Config's Database tab when using Firebird DB.



Encrypt/Decrypt Firebird DB

3.9. Document Security

The range of personal data to be secured can be set depending on the customer's environment. The use of the following features achieves maximum protection of the confidential personal data that has been printed, copied and scanned.

3.9.1. Secure Print

Secure Print prevents the possibility of leaving printed documents on an MFP/printer and having the document viewed by unauthorized personnel. Secure Print holds a print job and releases it only after a user walks up to the MFP/printer device and authorizes their access with an ID card, a PIN, or a username plus password. This way, highly confidential documents are released under full control of

the authorized person. This feature helps maintain relatively high security when printing highly confidential documents containing personal data.

3.9.2. Watermark (Option)

After a job is printed, the printed document must not fall into the wrong hands. The document can be securely managed with the TA/UTAX aQrate watermark feature, which prevents unauthorized copying. The watermark feature has several options: you can mark the document as confidential, add print data, and the name of the user who printed the document. Macros can be applied to every page of the printed document or only to selected pages. The watermark clearly indicates that an unauthorized copy was made and helps detect data leaks and identify the user who is responsible for it.

3.9.3. Scan policy

TA/UTAX aQrate administrator can restrict scanning to pre-defined folders and use an integrated Optical Character Recognition/Reader (OCR) or Document Management System (DMS) to provide notifications and restrictions based on the contents of the scanned documents. The documents can be restricted based on the kinds of the document contents by employing the best available tools to analyze the document contents.

In addition, it is possible to set a fixed destination for users so that they can send documents only to the approved destinations. This helps prevent sending documents to the wrong address and achieves secure protection of the documents.

Users can set access rights to codes and codebooks. The code inherits its parent's codebook access rights. Parent access rights can be applied to the selected codebooks and these child codes. This convenient feature maintains security.

Further, it is possible to forcibly send a secure link regardless of its file size. A secure link is generated for each scanned attachment. The files are encrypted with AES-128, which prevents data leaks and alteration. The download link is valid only for the amount of time pre-set by an administrator. When the pre-defined time is reached, the files are immediately deleted from the file system. Otherwise, keeping files longer than necessary could create risks. Timely deletion helps maintain security.

3.10. Network Security

3.10.1. TA/UTAX aQrate Port Settings for Secure Communication

When using TA/UTAX aQrate, the following port numbers need to be enabled for secure communications on a network and the TA/UTAX aQrate server in the customer environment. This helps deny unauthorized access to the TA/UTAX aQrate system.

Table 3 Port Number Descriptions

Port Number	Source	Destination	Description
TCP 21	MFP/Printer	TA/UTAX aQrate Server	Used by the FTP server to receive files.
TCP 49152-65535	MFP/Printer	TA/UTAX aQrate Server	FTP for actual file copy
TCP 25	MFP/Printer	TA/UTAX aQrate Server	Used to send scanned data from MFP/Printer device to the TA/UTAX aQrate server.
TCP 25/465/587	TA/UTAX aQrate Server	SMTP Server	Used by SMTP protocol for sending outgoing emails from TA/UTAX. Port depends on SMTP server
TCP 80	TA/UTAX aQrate Server	License Activation Server	Used by TA/UTAX aQrate to activate the license.
TCP 110	TA/UTAX aQrate Server	POP3 Server	POP3
TCP 143	TA/UTAX aQrate Server	IMAP Server	IMAP
UDP 161	TA/UTAX aQrate Server	MFP/Printer	SNMP
TCP 389	TA/UTAX aQrate Server	LDAP Server	LDAP
TCP 443	TA/UTAX aQrate Server	MFP/Printer	Use for IPPS protocol for print job transmission from TA/UTAX aQrate to MFP/Printer
TCP 515	SJM/User PC	TA/UTAX aQrate Server	Use for LPR protocol to send a print job from clients.
TCP 631	TA/UTAX Mobile Print	TA/UTAX aQrate Server	This port is used by IPP (Internet Printing Protocol) to send jobs from Mobile Print to the server.
TCP 631	TA/UTAX aQrate Server	MFP/Printer	Used by IPP protocol for print job transmission from TA/UTAX aQrate to MFP/Printer
TCP 636	TA/UTAX aQrate Server	LDAP Server	LDAPS
TCP 717	TA/UTAX Mobile Print	TA/UTAX aQrate Server	Mobile print via IPPS
TCP 993	TA/UTAX aQrate Server	IMAPS Server	IMPAS
TCP 3050	TA/UTAX aQrate Master Server	TA/UTAX aQrate Site Server	This port is used by communication with the Firebird. In a standalone environment where the database is installed with TA/UTAX aQrate on the same server, the port is not required to be opened. If the database is located in separate hardware or if a Master/Site server configuration is used, open this port in both the Master and Site servers for data replication purposes.
TCP 8081	Embedded Terminal	TA/UTAX aQrate Server	Used to communicate with embedded terminals using the REST API. And also, when using TA/UTAX aQrate and TACM (Triumph-Adler Capture Manager) together, the integrated connector uses this port. This port is secured with TLS v1.0/v1.2

TCP 8090	Various	TA/UTAX aQrate Server	Used by protocol for accessing TA/UTAX aQrate web interface, Communication with Embedded Terminals, job roaming, REST API, and Central-Site communication
TCP 8631	User PC	TA/UTAX aQrate Server	This port is used by IPPS to receive jobs securely.
TCP 8631	Mobile applications	TA/UTAX aQrate Server	Job spooling via the AirPrint/Mopria protocol.
TCP 9090	TA/UTAX aQrate Server	Embedded Terminal	This port is used by Remote Printer Setup of the device. It is called Enhanced WSD on the device. Please use 9091 for TLS v1.0/v1.2 communication.
TCP 9091	TA/UTAX aQrate Server	Embedded Terminal	This is the TLS v1.0/v1.2 communication layer of port number 9090.
TCP 9093	Terminal Lite	TA/UTAX Provider	Used between Embedded Lite terminals and a TA/UTAX Provider for authentication. This port is secured with TLS v1.0/v1.2. A TA/UTAX Provider can only be installed along with the TA/UTAX aQrate server.
TCP 9094	KX Mobile Print Driver	TA/UTAX Provider	Used between the KX Driver, TA/UTAX Mobile Printer and TA/UTAX Provider for authentication features. This port is secured with TLS v1.0/v1.2.
TCP 9095	TA/UTAX Provider	Terminal Lite	Used between Embedded Lite terminals and TA/UTAX Provider to provide Print&Follow features. This port is secured with TLS v1.0/v1.2.
TCP 9097	TA/UTAX Provider	Terminal Lite	This port is used between Embedded Lite terminals and TA/UTAX Provider to receive job log notifications.
TCP 9098	TA/UTAX Provider	Terminal Lite	This port is used between Embedded Lite terminals and TA/UTAX Provider to receive job log status notifications.
TCP 9099	TA/UTAX Provider	TA/UTAX aQrate Server	Used between TA/UTAX aQrate server and TA/UTAX Provider for Thrift access. TA/UTAX Provider can only be installed along with the server, so this port does not have to be opened.
TCP 9100	TA/UTAX aQrate Server	MFP/Printer	This is the RAW port used to send jobs from the server to the device. If you want to secure the jobs, use the IPPS port.
TCP 9101	TA/UTAX aQrate Server	TA/UTAX Provider	This port is used by communication (TLS v1.0/v1.2) between TA/UTAX Service and TA/UTAX Provider.
TCP 10010	User PC	Embedded Terminal	This port is used by Direct Printing for local print spooling. It is only available when Local Print Spooling is enabled by the server.
TCP 10011	User PC	Embedded Terminal	This port is used by Hold Printing for local print spooling. It is only available when Local Print Spooling is enabled by the server.
TCP 10012	User PC	Embedded Terminal	This port is used by Print&Follow for local print spooling. It is only available when Local Print Spooling is enabled by the server.
TCP 10013	User PC	Embedded Terminal	This port is used by Delegated Printing for local print spooling. It is only available when Local Print Spooling is enabled by the server.
TCP 10025	TA/UTAX aQrate Server	SMTP Server	This port is the Offline SMTP port. It re-directs the SMTP communication from a device to the customer's SMTP server. It will be enabled on under the following condi-

			<p>tions:</p> <ul style="list-style-type: none"> SMTP server information is set to the TA/UTAX aQrate server Offline authentication is enabled on the TA/UTAX aQrate server <p>The TA/UTAX server is offline and EMB is in offline mode</p>
TCP 10040	TA/UTAX aQrate Server	Embedded Terminal	<p>Use for following 2 connections.</p> <ul style="list-style-type: none"> MPP: TA/UTAX Printing Protocol MPPS: TA/UTAX Printing Protocol Secured
UDP 11108	Embedded Terminal	TA/UTAX aQrate Server	<ul style="list-style-type: none"> Used by Embedded Terminal to provide discovery functions and connection checking functionalities.
TCP 11108	Terminal Manager	Embedded Terminal	This port is used between Terminal Manager and Embedded Terminal.
UDP/ TCP 11112	TA/UTAX aQrate Server	SJM/SPS	This port is used between Smart Job Manager and Smart Print Service.
UDP/ TCP 11112	TA/UTAX aQrate Server	Smart job manager	TA/UTAX aQrate sending data to Smart job manager.

3.10.2. FTP Server for Secure Scan Job Receiving

One of the ways that TA/UTAX aQrate obtains the scan jobs (SMTP, FTP), is by using the FTP protocol from the MFP. A plugin FTP server with this functionality is provided inside the TA/UTAX aQrate server. The TA/UTAX aQrate server listens in on the standard FTP port (21) and accepts all anonymous FTP connections. When a file is uploaded to the FTP server, the TA/UTAX aQrate server checks the IP address that sent the file and verifies that the address belongs to the MFP. The file is only accepted if the address belongs to the MFP. If it does, the file is processed in a conventional way – the MFP scans through JAMP (Java API for Multifunctional Products) with the HyPAS application, stores the image, and sends it to the FTP server. A set range of IP address can limit access from the MFP.

The FTP server supports the TLS (FTPS, not SFTP) encryption protocol, thereby preventing alteration of data and tapping data on network.

The TA/UTAX aQrate server sets up the FTP server to use the same TLS certificate and private key, which can be set over the web UI. This ensures authenticity of the server for extra security, in addition to the security of the communication paths.

3.10.3. Protection of Communication Data

In accordance with the security policy defined by the customer, TA/UTAX aQrate communication data is encrypted, and TA/UTAX aQrate components are mutually authenticated. Secure communications occur during the following:

- Data communication between TA/UTAX aQrate components
 - Data communication between TA/UTAX aQrate components can be secured by TLS encryption. Supported TLS versions is TLS 1.2, and TLS 1.3 is also supported from TA/UTAX aQrate 8.0.
 - TA/UTAX aQrate supports and uses the most recent protocols to support user security. Vulnerable protocols and ciphers are disabled by default.
- The following communication protocols can be encrypted with TA/UTAX aQrate:
- ✧ Communication among TA/UTAX aQrate Servers — HTTPS
 - ✧ Communication between the TA/UTAX aQrate Server and an Embedded terminal — HTTPS
 - ✧ Communication between the TA/UTAX aQrate client application and the TA/UTAX aQrate Server —HTTPS
 - ✧ Communication between the TA/UTAX aQrate Server and AD/eDirectory/OpenLDAP —LDAPS
 - ✧ Communication between the TA/UTAX aQrate Server and a mail server — SMTPS
 - ✧ Print from a workstation to the TA/UTAX aQrate Server — LPR over SSL
 - ✧ Print from the TA/UTAX aQrate Server to a printing device — IPPS or MPPS
 - ✧ Print from user's computer to server can also be done using IPPS instead of the standard LPR.

Further, all the network communications including the connections to other services and applications can be encrypted using either TA/UTAX aQrate self-signed certificate (by default) or the customer's CA signed certificate, according to the customer's policy. This prevents the man-in-the-middle attack.

Communication Security

- TA/UTAX aQrate Document Workflow
 - Print jobs can be sent as encrypted data from the client PC to the TA/UTAX aQrate server.
 - Encrypted print jobs can be sent from the TA/UTAX aQrate server to a MFP/Printer device connected to the network.

To protect TA/UTAX aQrate communication between the respective components from masquerading, tapping, or modifying the data, the print job can be encrypted.

3.11 Register for exception list

If the antivirus software that installed on Windows server detects KNM and is unable to start up KNM, add the following executable file to exception list of the antivirus software:

- **aQrate Central Server 8.2**

- This append if you install it on default setup/directories and you use Firebird as database engine.
(Directories recursive)

New installation:

C:\Program Files\AQrate Central Server\
C:\ProgramData\AQrate Central Server\
C:\ProgramData\Firebird\
(Service)

Upgrade:

C:\Program Files (x86)\AQrate Central Server\
C:\ProgramData\AQrate Central Server\
C:\ProgramData\Firebird\
(Service)

Display name	Service name	Path (new installation)*
MyQ Central Server	myqm_platform	C:\Program Files\AQrate Central Server\Server\MyQCentral.exe
MyQ Central HTTP Server	myqm_apache	C:\Program Files\AQrate Central Server\Apache\bin\httpd.exe
Firebird Server – MasterInstance	FirebirdServer MasterInstance	C:\Program Files\AQrate Central Server\Firebird\Firebird.exe

* for upgrade is the root-path C:\Program Files (x86)\AQrate Central Server\

- **aQrate Standalone/aQrate site 8.2**

This append if you install it on default setup/directories.

(Directories recursive)

C:\Program Files (x86)\AQrate\
C:\Program Files\Firebird\
C:\Program Files\AQrate\
C:\ProgramData\AQrate\
C:\ProgramData\Firebird\
(Service)

Display name	Service name	Path
Firebird Server – DefaultInstance	FirebirdServerDefaultInstance	C:\Program Files\AQrate\Firebird\Firebird.exe
MyQ HTTP Router	Traefik	C:\Program Files\AQrate\Server\Nssm.exe
MyQ HTTP Server	Apache	C:\Program Files\AQrate\Apache\bin\httpd.exe
MyQ Print Server	MyQ	C:\Program Files\AQrate\Server\myq.exe
KYOCERA Net Manager Server	KNM_PM	C:\Program Files\AQrate\PMServer\bin\Knum.Server.exe

- **TA/UTAX Embedded 8.2**

This append if you install it on default setup/directories.

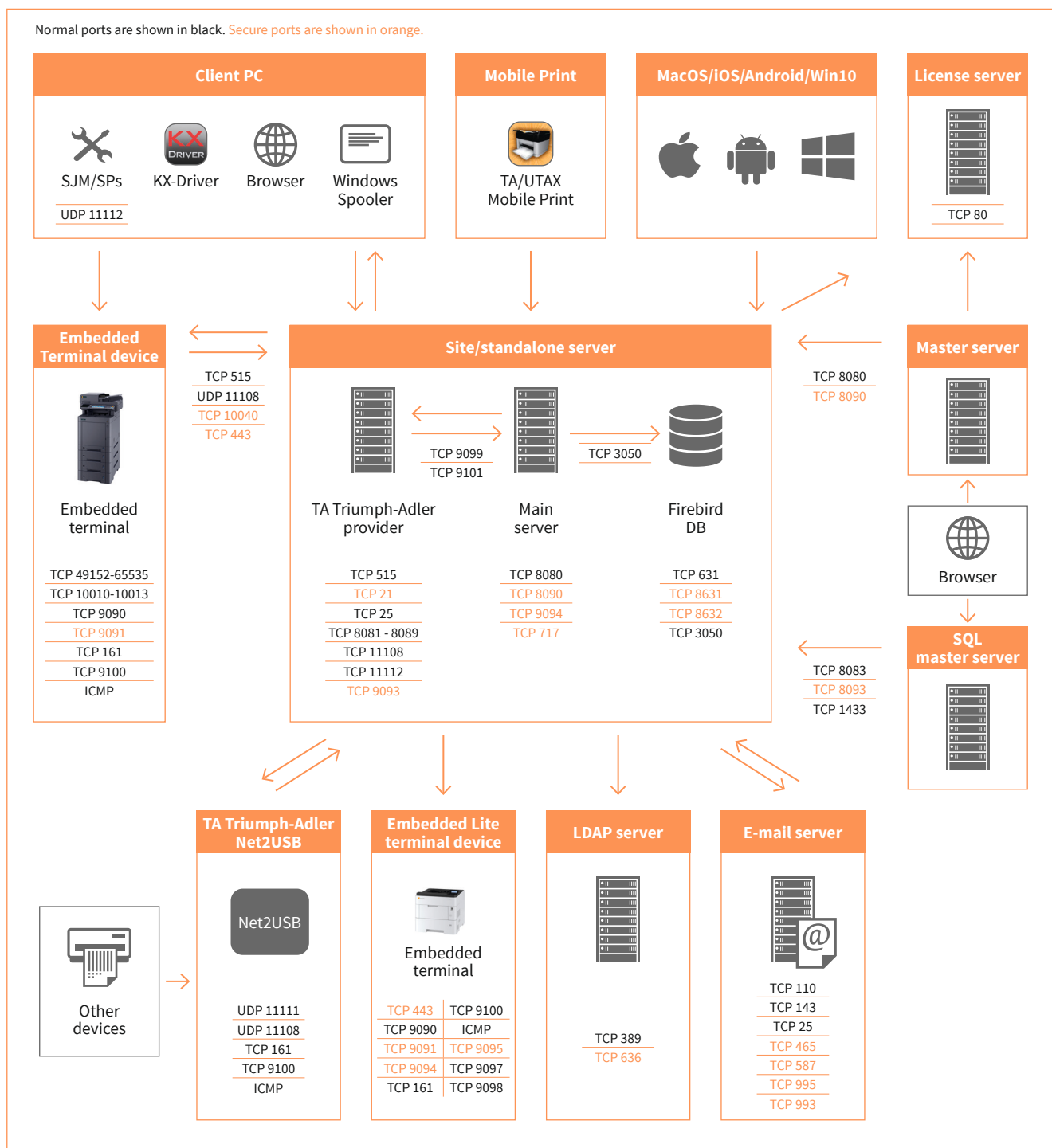
(Service)

Display name	Service name	Path
aQrate TA Triumph-Adler/UTAX Terminals	aQrate_TA	C:\Program Files\Aqrate\Terminals\1024_TA_Triumph-Adler-UTAX\MyQKyoceraTerminal.exe – Notice: Number 1024 may vary based on installation.

5 Network Ports

NETWORK PORTS USED IN aQrate

This article describes network ports used in the aQrate system, including devices. The illustration below shows an overview of ports used by each component:



The following table shows details of each port used. Please note: The port number is the default number and may be changed by the system administrator.

Port number	Type	Sending	Receiving	Firewall rule direction on aQrate server	Detail
21	TCP	Device	aQrate server	Inbound	This port is used to transport scanned data from the device to the aQrate server when the FTP protocol is chosen (enabled by config.ini file). FTPS with AUTH TLS is supported.
49152-65535	TCP	Device	aQrate server	Inbound	These ports are used for FTP for actual file copy when the FTP protocol is chosen (enabled by config.ini file).
25	TCP	Device	aQrate server	Inbound	This port is used to transport scanned documents from the device to the aQrate server*
80	TCP	aQrate Server	License server	Outbound	This port is used to communicate with the license activation server. The license activation server's IP address is 202.214.28.72.
515	TCP	User PC/SJM/SPS	aQrate server	Inbound	LPR port used in the server to receive jobs from clients. We recommend that you do not change the port unless other services already use it, because the LPR port number used by client Windows PCs can only be changed by modifying the Windows registry.
515	TCP	User PC/SPS	Device	N/A	LPR port used to send jobs from clients to devices. We recommend that you do not change the port unless other services already use it, because the LPR port number used by client Windows PCs can only be changed by modifying the Windows registry.
631	TCP	TA Triumph-Adler Mobile Print app	aQrate server	Inbound	IPP (Internet Printing Protocol) port used to send jobs from TA Triumph-Adler Mobile Print to the server. You cannot change this port number.
717	TCP	TA Triumph-Adler Mobile Print app	aQrate server	Inbound	IPPS port used to send jobs from TA Triumph-Adler Mobile Print to the server. You cannot change this port number.
8631	TCP	User PC	aQrate server	Inbound	IPPS port used to send jobs from the client PC to the aQrate server.
8632	TCP	macOS/iOS/Android/Windows 10	aQrate server	Inbound	IPPS port used to send jobs from Airprint/Mopria to the aQrate server.
1433	TCP	SQL DB	aQrate SQL master server	Inbound	This port is used for communication between the SQL master server and SQL database. When the SQL database is installed on the same server as aQrate, the port does not need to be opened.
3050	TCP	aQrate master server	aQrate site server	Inbound	This port is used for communication with the database. In a standalone environment where the database is installed with aQrate on the same server, the port does not need to be opened. If the database is located on separate hardware or if a master-site server configuration is used, you must open this port on both the master and site servers for data replication purposes. This port is also used for job roaming.**

*The port is only required when using version 7.x Embedded or earlier. Version 8.x Embedded sends scanned documents using the FTP protocol.

**The port is not required when using the new central site.

Port number	Type	Sending	Receiving	Firewall rule direction on aQrate server	Detail
8080	TCP	Web/Embedded Terminal/aQrate server/SJM	aQrate server	Inbound	<p>This port is used for the following purposes:*</p> <ul style="list-style-type: none"> Web interface communication via browser Communication between Embedded Terminal and the server Job roaming for communication between site servers Communication between Smart Print services Communication between master and site server <p>This is a standard port, so if you want to set up secure communication, please use port number 8090</p>
8090	TCP	Web/Embedded Terminal/aQrate server/SJM	aQrate server	Inbound	This is the TLS v1.0/v1.2 communication layer of port number 8080.
8083	TCP	Web/aQrate server	aQrate SQL master server	Inbound	<p>This port is used for the following purpose:**</p> <ul style="list-style-type: none"> Web interface communication via browser for SQL master server Communication between the site server and SQL master server
8093	TCP	Web/aQrate server	aQrate SQL master server	Inbound	This is the TLS v1.0/v1.2 communication layer of port number 8083.
8081-8089	TCP	Embedded Terminal	aQrate server	Inbound	Ports open after adding a terminal package***
9093	TCP	EMB Lite	TA Triumph-Adler Provider	Inbound	This port is used between Embedded Lite terminals and TA Triumph-Adler Provider to provide authentication features. This port is secured with TLS v1.0/v1.2. TA Triumph-Adler Provider can only be installed along with the server.
9094	TCP	KX driver/TA Triumph-Adler Mobile Print	TA Triumph-Adler Provider	Inbound	This port is used between KX- Driver/Mobile Print and the server for authentication. It is secured with TLS v1.0/v1.2. You cannot change this port number.
9094	TCP	TA Triumph-Adler Provider	EMB Lite	Outbound	This port is used between Embedded Lite terminals and TA Triumph-Adler Provider to access devices. It is secured with TLS v1.0/v1.2. You cannot change this port number.
9095	TCP	TA Triumph-Adler Provider	EMB Lite	Outbound	This port is used between Embedded Lite terminals and TA Triumph-Adler Provider to provide Print & Follow features. This port is secured with TLS v1.0/v1.2. TA Triumph-Adler Provider can only be installed along with the server.
9097	TCP	TA Triumph-Adler Provider	EMB Lite	Outbound	This port is used between Embedded Lite terminals and TA Triumph-Adler Provider to receive log information notifications
9098	TCP	TA Triumph-Adler Provider	EMB Lite	Outbound	This port is used between Embedded Lite terminals and TA Triumph-Adler Provider to receive job status notifications
9099	TCP	TA Triumph-Adler Provider	aQrate server	N/A	This port is used between the main server and TA Triumph-Adler Provider. TA Triumph-Adler Provider can only be installed along with the server, so this port does not have to be opened.

*The port is not required when using version 8.x or later (the same port is used for http and https)

*The port is not required when using the new central server (the same port is used for http and https)

***Only one port is required when using aQrate and the new version (version 8.x Embedded). Otherwise, the ports for MyQ are used.

Port number	Type	Sending	Receiving	Firewall rule direction on aQrate server	Detail
9101	TCP	aQrate server	TA Triumph-Adler Provider	N/A	This port is used between the main server and TA Triumph-Adler Provider to provide user session services. You cannot change this port number.
10010	TCP	User PC	Embedded Terminal	N/A	This port is used to send jobs with Direct Print from the client to Embedded Terminal for local print spooling. You cannot change this port number.
10011	TCP	User PC	Embedded Terminal	N/A	This port is used to send jobs with Hold Print from the client to Embedded Terminal for local print spooling. You cannot change this port number.
10012	TCP	User PC	Embedded Terminal	N/A	This port is used to send jobs with Print & Follow from the client to Embedded Terminal for local print spooling. You cannot change this port number.
10013	TCP	User PC	Embedded Terminal	N/A	This port is used to send jobs with Delegated Print from the client to Embedded Terminal for local print spooling. You cannot change this port number.
10040	TCP	aQrate server	Embedded Terminal	Outbound	This port is used to send jobs with MPP(S) from the server to Embedded Terminal. You cannot change this port number.*
11108	UDP	Embedded Terminal	aQrate server	Inbound	This port is used for communicating with the device and applying settings. You cannot change this port number.
11108	TCP	aQrate server (Terminal Manager)	Embedded Terminal	Outbound	This port is used by Terminal Manager to communicate with Embedded Terminal. You cannot change this port number.
11112	UDP/TCP	SJM/SPS	aQrate server	Inbound	This port is used by Smart Job Manager and Smart Print Service to communicate with the aQrate server
11112	UDP/TCP	aQrate server	SJM	Outbound	This port is used by the aQrate server to send data to Smart Job Manager
9090	TCP	aQrate server	Device	Outbound	This port is used for remote printer setup of the device. It is called Enhanced WSD on the device. Please use 9091 for TLS v1.0/v1.2 communication. You cannot change this port number.
9091	TCP	aQrate server	Device	Outbound	This is the TLS v1.0/v1.2 communication layer of port number 9090. You cannot change this port number.
161	UDP	aQrate server	Device	Outbound	This is an SNMP v1/v2 port. It is used to check the device status and acquire counters from the device. You cannot change this port number.
443	TCP	aQrate server	Device	Outbound	This is an IPPS port used for secure printing between Embedded Terminal and the server. You cannot change this port number.
631	TCP	aQrate server	Device	Outbound	This is an IPP port used for secure printing between Embedded Terminal and the server. You cannot change this port number.
515	TCP	User PC/SPS	Device	N/A	LPR port used by to send a print job to the printer. We recommend that you do not change the port unless other services already use it, because the LPR port number used by client Windows PCs can only be changed by modifying the Windows registry.

*This port is used to send jobs in a highly compressed format from the server to Embedded.

Port number	Type	Sending	Receiving	Firewall rule direction on aQrate server	Detail
9100	TCP	aQrate server	Device	Outbound	This is the RAW port used to send jobs from server to the device. If you want to secure the jobs when sent from the server to the device, use an IPPS port. You cannot change this port number.
-	TCP	aQrate server	Device	Outbound	Some old devices only supports LPR for printing. For those machines, this port has to be opened. You cannot change this port number.
-	ICMP	aQrate server	Device	Outbound	This port is used to ensure the connection of devices. You cannot turn it off.

The following table shows default ports used to communicate with external systems such as SMTP or LDAP. Please note: Port selection depends on SMTP/LDAP server settings.

Port number	Type	Sending	Receiving	Firewall rule direction on aQrate server	Detail
25	TCP	aQrate server	E-mail server	Outbound	Port for SMTP protocol used to send outgoing e-mails from the server
465	TCP	aQrate server	E-mail server	Outbound	Port for SMTP over SSL protocol used to send outgoing e-mails from the server
587	TCP	aQrate server	E-mail server	Outbound	Port for SMTP over STARTTLS protocol used to send outgoing e-mails from the server
110	TCP	aQrate server	E-mail server	Outbound	Port for POP3 protocol used by the server to communicate with the e-mail server for jobs via e-mail.
995	TCP	aQrate server	E-mail server	Outbound	Port for POP3 over SSL protocol used by the server to communicate with the e-mail server for jobs via e-mail.
143	TCP	aQrate server	E-mail server	Outbound	Port for IMAP protocol used by the server to communicate with the e-mail server for jobs via e-mail
993	TCP	aQrate server	E-mail server	Outbound	Port for IMAP over SSL protocol used by the server to communicate with the e-mail server for jobs via e-mail
389	TCP	aQrate server	LDAP server	Outbound	Port used by the server to communicate with the LDAP server.
636	TCP	aQrate server	LDAPS server	Outbound	Port by the server to communicate with LDAP via the SSL server.

5 The TA/UTAX Commitment to TA/UTAX aQrate Security

TA/UTAX is monitoring the latest security vulnerability related information and taking security countermeasures against them.

Prior to releasing TA/UTAX aQrate, security diagnostic tests in development of TA/UTAX aQrate were conducted by a third party in order for customers to use TA/UTAX aQrate securely. TA/UTAX has confirmed from an objective point of view that there are no vulnerabilities affecting our products. The security diagnostic tests will also be conducted regularly in the future. If vulnerabilities are found, these will be immediately fixed.

This document is provided for informational purposes only. The content of this document are subject to change from time to time without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of TA/UTAX products or services. The information in this document is provided "as-is" without warranty of any kind, whether express or implied. Although care has been taken when compiling this information, TA/UTAX makes no representations or warranties about the accuracy, completeness or adequacy of the information provided herein, nor fitness for a particular purpose, and shall not be liable for any errors or omissions. The only warranties for TA/UTAX products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty.