e-BRIDGE CloudConnect

Systems and Functions White Paper

Revision History

Date	Version	Description	Author
01-28-2019	3.3	Updated supported MFD list. Updated regional data center hosting information.	TABS/DSE
09-29-2017	3.2	Minor update version for global release.	TABS/DSE
09-12-2016	3.1	Minor update version for global release.	TABS/DSE
02-09-2016	3.0	Update version for global release.	TABS/DSE

Trademarks

- Azure™, Internet Explorer, SQL Server™, and Windows are trademarks of Microsoft Corporation in the U.S. and other countries.
- Chrome™ browser is a trademark of Google Inc. in the U.S. and other countries.
- Firefox® is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Linux™ is a trademark of Linux Mark Institute in the U.S. and other countries.
- Oracle® is a trademark of Oracle Corporation in the U.S. and other countries.

Table of Contents

Table of Figures

1.0 Introduction

Toshiba e-BRIDGE CloudConnect is an integrated system of embedded and cloud-based applications that enable remote interactions between existing back-end business processes and our customer MFDs (multi-function MFDs) in the field. The system is primarily a service tool, designed to be used by Service Provider personnel to increase service efficiencies and create a tangible value-add for our customers. As such, there is no additional fee to our customers to be enrolled in the CloudConnect program.

The ultimate goal of the CloudConnect system is to improve overall customer satisfaction through the following set of goals:

- Enable a proactive service organization.
- Reduce multiple service calls.
- Reduce the number and time of onsite service calls.
- Automate service processes where possible.
- Enable consistent best practices across dealerships and geographies.
- Provide a platform to perform analysis of MFD data.

More specifically, the CloudConnect system enables service staff to provide better service to their customers in the following areas:

- Increased Uptime
  - Real-time alerts go to the Service Provider to update the status of MFDs.
  - Service technicians can set policies that make adjustments to internal MFD codes to control copy, scan, and other configuration settings.
  - Using the data sent from the MFDs, service staff will be better prepared for onsite service calls with correct parts and action plan for faster resolution.
- Reduced Customer Workload
  - MFD alerts are sent directly to the Service Provider, helping reduce customer help-desk burden.
  - Meter data updated daily is automatically transferred to various back-end systems.
  - Toner alerts can be monitored to provide automated supplies delivery.
- Keeping Customer MFDs Up-to-date
  - Firmware can be updated automatically, or purposely maintained and monitored at a customer-designated level. Updates can be scheduled for off-peak hours.
  - Remote Data Backup and Restore.
  - MFD configuration data/templates/settings/contacts can be maintained, stored, restored from the CloudConnect server.

2.0 System Overview

2.1 What is e-BRIDGE CloudConnect?

e-BRIDGE CloudConnect is an integrated system of embedded and cloud-based applications that provide functionality to support remote monitoring and management of Toshiba MFDs. It enables management of configuration settings through automated interaction. e-BRIDGE CloudConnect gathers service information from connected MFDs, including meter data, to speed issue diagnosis and resolution.

2.2 What Are the System Components?

e-BRIDGE CloudConnect is comprised of two main components:

- MFD component “ECC module” embedded in the MFD firmware.
- Hosted Application “e-BRIDGE CloudConnect”.

The hosted e-BRIDGE CloudConnect application is designed to allow interaction from other IT backend applications. These include Oracle for shipped MFD data, existing service systems for meter reads, help desk and service dispatch, and also future backend and mobile applications.

2.3 System Functional Overview

The following steps walk through the typical data flow and describe e-BRIDGE CloudConnect’s system functions:

1. The MFD initiates communication with e-BRIDGE CloudConnect and provides service data, error data, clone files, and log files through a secure Internet connection (SSL).
2. The data is received by a secure SQL database so it can be processed.
3. Data for each MFD is compared to its policy settings.

   A ***policy*** includes a list of parameters (rules) for incoming data as well as functions and actions to perform based on the data.
4. When data falls outside the parameters of the policy rule, it is a policy violation. When a policy violation occurs, an alert is triggered for the MFD:
   a. The violation is displayed on the Devices page on the e-BRIDGE CloudConnect portal.
   b. If the policy was written to trigger actions, the system executes the actions.

      Examples include: update a service code, monitor errors, set communication interval, or update firmware.
5. Updates (in the form of executable configuration files) are made available to the MFD.

6. The MFD interacts with e-BRIDGE CloudConnect to retrieve and execute the update, and then send an updated status to e-BRIDGE CloudConnect.

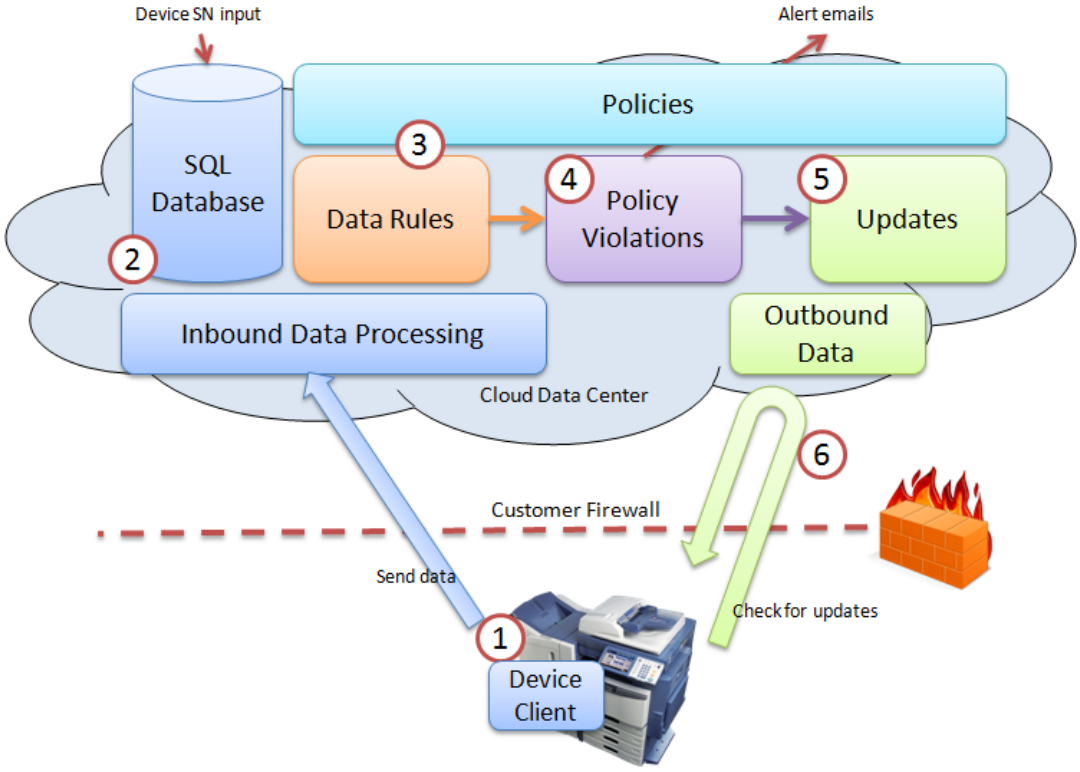

Figure 1: System Functional Overview

3.0 MFD Functions

3.1 Overview

The ECC module is an embedded service included in supported Toshiba MFDs that runs as a part of the MFD firmware. The primary function of the ECC module is to allow the MFD to communicate with e-BRIDGE CloudConnect, which serves to monitor MFD health and as necessary, provide updates to monitored MFDs.

The general MFD communication model is as follows.

- MFD initiates communication and contacts e-BRIDGE CloudConnect servers to check for updates.
- Download updates (if available).
- Updates are executed on MFD.
- MFD gathers service data and operation logs.
- MFD send data to e-BRIDGE CloudConnect servers.

3.2 Installation

e-BRIDGE CloudConnect does not require the installation of additional software components. The MFD functions are embedded in the latest versions of firmware. The user portal is Internet-based and available through commonly supported web browsers.

When an MFD is shipped, e-BRIDGE CloudConnect plugin functionality is disabled by default. To use e-BRIDGE CloudConnect functionality the plugin must be enabled by a Service Technician. Once enabled, the MFD reboots and runs through several system functions. After the NIC is initialized, the MFD attempts to register with e-BRIDGE CloudConnect.

An Installation Report is printed by the MFD to provide detail of the connection and registration status.

3.2.1 Supported MFDs

The ECC module that allows MFDs to communicate to e-BRIDGE CloudConnect is embedded in the following Toshiba e-STUDIO MFD series:

e-BRIDGE (eBX) MFDs:

- e-STUDIO 857 and 856 series
- e-STUDIO 6570C and 6550C series
- e-STUDIO 4540C series
- e-STUDIO 507 and 456 series
- e-STUDIO 5055C series
- e-STUDIO 2551C and 2550C series (HDD Models only)
- e-STUDIO 527S and e-STUDIO 407CS series
- e-STUDIO 307LP and 306LP series

e-BRIDGE NEXT (eBN) MFDs:

- e-STUDIO 7506AC and 7516AC series
- e-STUDIO 5005AC and 5015AC series
- e-STUDIO 2500AC and 2515AC series
- e-STUDIO 8508A and 8518A series
- e-STUDIO 5008A and 5018A series
- e-STUDIO 5008LP and 4508LP series

3.2.2 Supported Browsers

Browsers supported for use with e-BRIDGE CloudConnect include:

- Internet Explorer
- Firefox
- Chrome

Note: Internet Explorer requires Compatibility Mode to be disabled.

3.3 MFD Communications

Communication with the e-BRIDGE CloudConnect database is performed by the plugin on the MFD. Each MFD's Device Communication Settings determine what service data is collected and uploaded. These settings are controlled by the servicing dealer via the e-BRIDGE CloudConnect web portal. All MFD connections are logged at the MFD and in e-BRIDGE CloudConnect.

Note: To assist with compliance with local regulations, the MFDs default communication settings exclude collection of logs and address book data.

MFD service files, NIC configuration, and function list are collected and uploaded by default. This setting cannot be disabled until changes are made in the firmware.

The certificates the MFD uses for SSL communication are time stamped by the MFD. Scheduled actions taken by the MFD occur as per the MFD's date and time settings.

3.3.1 Communication Requirements

The MFD initiates all communications using a standard Internet protocol via a secure channel HTTPS over port 443. This method is similar to a web browser connecting to a secure website.

To communicate to e-BRIDGE CloudConnect, the following are required:

- The MFD must be able to access the Internet over port 443.
- The MFD serial number must be in the e-BRIDGE CloudConnect database.
- For firmware downloads from FTP, the MFD must be able to access the Internet through ports 20 and 21.
- The MFD must be registered and verified in e-BRIDGE CloudConnect.

Registration is a system function in which the MFD confirms that its model and serial number are an exact match with an existing record in the cloud. On the initial connection, a security protocol is used to register the MFD. Once the MFD is registered, e-BRIDGE CloudConnect provides a security token that the MFD uses on future connections.

Verification requires service personnel to login to e-BRIDGE CloudConnect and verify that an MFD's customer information is correct.

Process	Type	Performed by	Description
Registration	Automated	MFD	MFD confirms that its model and serial number are an exact match with an existing record in e-BRIDGE CloudConnect.
Verification	Manual, can be set to Automatic	Service Personnel	Service personnel confirms that a MFD's record in e-BRIDGE CloudConnect contains accurate customer information.

Figure 2: Registration and Verification Processes

Reasons for not being able to connect include the following.

- MFD IP address is being blocked and not allowed to access the Internet. You will need to request the customer to allow the MFD to access the Internet.
- The customer is using a proxy for Internet access. There are separate 08 codes to configure the MFD to communicate through a proxy server.
- The MFD serial number is not in the e-BRIDGE CloudConnect database.

3.3.2 Registration Process of a New Toshiba MFD

A new Toshiba MFD will, initially, send a registration request to North America cloud service. The North America cloud service will utilize the MFD's network external IP Address to determine the appropriate regional cloud service's URL for the registration. The MFD will retrieve this initial URL and attempt to register.

- If the registration is successful, then the URL of the regional cloud service is saved to the device for all communications.
- If registration is not successful, then the Toshiba MFD performs a Redirect URL process by attempting to communicate to each of the regional cloud service. This redirect routine occurs at every power up and ends at the last redirect regional cloud service or when the MFD has successfully registered.
- For eBN systems, the communication URL can be set via an 08 code to bypass the redirect registration process.

By design, the sequence in the redirect process is as follows:

- 1st Redirect URL attempt – North America
- 2nd Redirect URL attempt – Europe
- 3rd Redirect URL attempt – Asia Pacific

Note: It's important to allow all of the regional cloud services in the firewall and proxy in order to achieve a successful registration.

- North America:
  - edevice.toshiba-solutions.com
    - 157.55.252.141
  - eccwsi.toshiba-solutions.com
    - 157.56.28.169
- Europe:
  - gsidevice-eu.toshiba-solutions.com
    - 137.117.201.238
  - eccwsi-eu.toshiba-solutions.com
    - 104.40.159.11
- Asia-Pacific:
  - gsidevice-ap.toshiba-solutions.com
    - 13.75.159.193
  - eccwsi-ap.toshiba-solutions.com
    - 13.75.153.98

3.3.3 Communication Sequence and Data Sent

On start-up the MFD connects to e-BRIDGE CloudConnect after network services have been initialized. If the MFD fails to connect then up to three retries are attempted. If the connection is

unsuccessful the ECC module waits for the next scheduled communication cycle or power cycle, whichever comes first.

The following table details the communication sequence and data uploaded by the MFD:

Timing	Communication Sequence	Data Sent by the MFD
Initialization, reboot or power-cycle	• Registration • Check for updates • Download updates (skip if none) • Execute updates (skip if none) • Send updated data set	• Send 05/08/13 Code Settings (as an xml file) • MFD Clone Data (encrypted clone file)
Scheduled (at policy setting or off-hours)	• Registration • Check for updates • Download updates (skip if none) • Execute updates (skip if none) • Send updated data set	• 05/08/13 Code Settings (as an xml file) • MFD Clone Data (encrypted clone file) • Service files (CSV files) • Function List • NIC configuration page • MFD logs (print, scan, message)
Alerts (real-time)	• Registration • Send alert	• XML with code and text string

Figure 3: Communication Sequence and Data Sent by the MFD

3.3.4 Scheduled Communication (Communication Cycle)

During MFD registration, e-BRIDGE CloudConnect sets a default communication time for the MFD between 11:00 pm and 4:00 am (MFD time). MFD communication timing can be configured from the E-BRIDGE CloudConnect user portal for a specific time of day, or for an interval of time ranging from five to 60 minutes.

Communication is initiated daily at this time by the MFD. Communication times are automatically staggered to avoid network traffic issues.

The MFD checks for updates, executes available updates, and then uploads data specified in the Device Communication Settings.

3.4 Service Data

3.4.1 Gather Service Data

The ECC module collects the MFD state data and stores it initially on the MFD. The data sets include the following:

- 05/08/13 Code Settings (as an XML file).
- MFD Clone Data, including TopAccess settings (encrypted by the MFD).
- Service files (CSV files).

The ECC module has the ability to collect and send the following data; however these are turned off by default:

- MFD address book.
- Job Logs (print and scan).

3.4.2 Send Service Data

The MFD sends its state data to e-BRIDGE CloudConnect in a compressed .XML format file. The size of the file varies based on the length of logs retained on the MFD. Typically, a single compressed file is less than 6mb.

3.5 MFD Updates

There are several types of updates provided to the MFD:

- Configure a service code setting.
- Download a firmware package.
- Download a Toshiba embedded application.
- Download a Toshiba customized front panel User Interface design.

All types of update are in the form of an instruction set. For service code settings, the instruction contains the specific service code and associated value to be set. Firmware can be downloaded to the MFD from a Toshiba-hosted repository or another location (such as an FTP site) chosen by the service provider. The update instructions contain the location of the firmware files to download and time for when to install. Firmware packages include a digital signature to prevent unrecognized applications from being installed.

3.5.1 Download Updates

To check for updates, the ECC module sends a request over HTTPS to e-BRIDGE CloudConnect for available updates on every scheduled MFD-to-cloud communication, and on MFD power up.

If updates are available, the ECC module downloads the available packages and then applies the update packages to the MFD after the download is successfully completed.

For firmware updates, the ECC module receives the instruction to download the firmware files. The MFD commences downloading and when complete, either waits for the time instructed or installs immediately.

All downloads are performed in the background and are designed not to impede normal MFD functions.

3.5.2 Execute Updates

Once update instructions are downloaded, the MFD verifies the signature contained in the downloaded file before applying the updates.

Updates are applied immediately after download except in the case of a firmware update that is scheduled to install at a specific time.

The updates are typically applied without user intervention. In some cases, a firmware install may be prevented by MFD conditions.

Most updates are performed in the background. Some service code changes do require a reboot to take effect. For firmware updates, the MFD's front panel displays the message "Do not turn off the device" until the update has completed.

3.6 MFD Alerts

The MFD initiates communications to the cloud immediately – in near real time. The MFD sends the following data when a MFD alert occurs"

- MFD Identification (security token)
- Error Code
- Short Description of the Alert

e-BRIDGE CloudConnect saves the alert information and processes it based on policy settings. MFD service data is not sent to e-BRIDGE CloudConnect on alerts.

4.0 Web Portal Functions

The web portal provides user interface for service personnel to view, analyze, and act on data sent from enabled MFDs.

4.1 Functions

Service personnel have the following functions available to them:

- **Download Service Files** – download all or individual service files in .CSV format. The following are the available files.
- **View MFD Alerts** – all alerts sent from the MFD in the previous 24 hours are available.
- **Create/Apply Policy** – policies are used to configure and maintain MFDs. Policies can be applied to individual MFDs, or a fleet of MFDs.
- **Restore from Backup** – allows a MFD(s) to be configured to a state based on a clone file that gets saved in E-BRIDGE CloudConnect.
- **Create/Apply a Clone** – the system provides the capability to save a MFD clone file, and apply this saved file to other MFDs.

4.1.1 e-BRIDGE CloudConnect Mobile Functions

During login, mobile devices (cellular phones and tablets) are automatically directed to e-BRIDGE CloudConnect Mobile. e-BRIDGE CloudConnect Mobile enables users to easily access frequently used e-BRIDGE CloudConnect actions. Mobile user can:

- Search for MFDs (active, inactive and MFD's with errors/policy violations)
- Deactivate MFDs
- Apply Policy
- Remove Policy
- Restore From Backup

If necessary, mobile users can switch to the full e-BRIDGE CloudConnect website at any time.

4.2 Policies

Policies are used to create a near infinite number of attributes to monitor and configure a MFD or fleet of MFDs. They are organized into categories, and templates are provided to make the configuration of a policy fairly intuitive. These are the policy categories:

- Firmware Update
- Device Error Processing
- Backup
- Device Communication
- Custom

Additional policy categories/templates may be added in future releases.

5.0 Data and System Security

5.1 MFD – Cloud Communications

All communication between the MFD and e-BRIDGE CloudConnect are initiated by the MFD. By default all communication by the MFD is disabled. The service must be enabled on the MFD through a service code.

The MFD interfaces with the e-BRIDGE CloudConnect through standard Internet protocols. All status communications are over HTTPS, on port 443. The following table details the timing and sequence of MFD-to-cloud communications.

Timing	Communication Sequence	Data Sent by the MFD
Initialization, reboot or power-cycle	• Registration • Check for updates • Download updates (skip if none) • Execute updates (skip if none) • Send updated data set	• Send 05/08/13 Code Settings (as an xml file) • MFD Clone Data (encrypted clone file)
Scheduled (at policy setting or off-hours)	• Registration • Check for updates • Download updates (skip if none) • Execute updates (skip if none) • Send updated data set	• 05/08/13 Code Settings (as an xml file) • MFD Clone Data (encrypted clone file) • Service files (CSV files) • Function List • NIC configuration page • MFD logs (print, scan, message)
Alerts (real-time)	• Registration • Send alert	• XML with code and text string

Figure 4: Communication Sequence and Data Sent by the MFD

5.2 Data in the Cloud

After MFD data is received by the e-BRIDGE CloudConnect, it is processed against any policy applied to the MFD. The data is then stored either in file storage or Azure SQL database.

Data Set	Data types	Storage	Security Measures
Alert data	• Code and text string	• MS AzureSQL database	• Transmitted via SSL
Service Data	• MFD codes (XML) • Service files (CSV) • Clone files (proprietary)	• MS Azure “BLOB” storage	• Transmitted via SSL • Stored encrypted
User Data	• Email • Login ID • Password	• MS AzureSQL database	• Transmitted via SSL • Stored encrypted

Figure 5: Communication Sequence and Data Sent by the MFD

Standard IT practices apply to e-BRIDGE CloudConnect application operations. Toshiba has dedicated and separate development, staging, production applications. Access to the production system is restricted to operations staff. Database and application access is further separated and restricted. Toshiba follows strict release procedures for the deployment of any new production applications.

5.3 Data Center Cloud Hosting

The Toshiba e-BRIDGE CloudConnect application is deployed and run on Microsoft Azure cloud data centers in the following four regions.

- Americas (data center located in north-central United States, includes MFDs in North, Central, and South America)
- Europe (data center located in the Netherlands, includes MFDs in East Europe, West Europe, North Africa, and the United Kingdom)
- Asia Pacific (data center located in Australia, includes MFDs in East Asia, South Asia, Oceania, India, Middle-East, and South Africa)
- China (data center located in China, includes MFDs in mainland China)

Please refer to http://azure.microsoft.com/en-us/support/trust-center/ for the latest data security and compliance information.