TOSHIBA
Leading Innovation

e-BRIDGE CloudConnect

Remote Support

- Cloud based support service for monitoring devices.
- Handles device operation and status information.
- Comprehensive security - operational data is collected securely and reliably.
- All of this without any software to install - your Toshiba MFP does all the work.

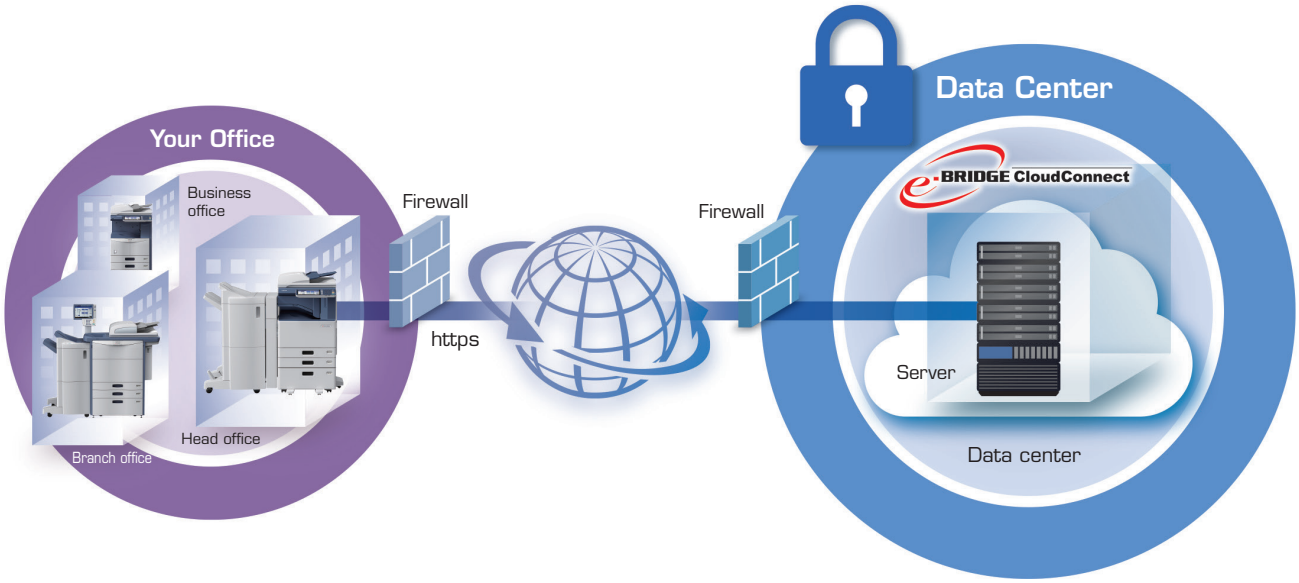
TOGETHER INFORMATION

MONITOR, CONFIGURE AND AUTOMATE

Toshiba e-BRIDGE CloudConnect offers comprehensive security and management for networked multifunction products (MFPs).

e-BRIDGE CloudConnect securely and reliably collects operation data transmitted from your MFPs over HTTPS/SSL connection. Only parties from contracted maintenance companies with valid permission can view the data.

- Cloud based support service for an end-to-end process for monitoring device communications
- Increase uptime with proactive device status alerts and remote diagnostics
- Reduce workload with scheduled meter readings and automated supplies delivery
- Keep machines up to date with the latest firmware and remote data back up
- Provide stability across your MFP fleet with regular, remote health checks



Activity Overview

Once connection to the server at the host site is established, the following can be monitored, set and saved to facilitate a remote repair or provide a visiting engineer with prior knowledge of any reported fault:

- **First Call Effectiveness**
  - Preparation by knowing device status before visit
- **Service Call Alerting**
  - Automated service policy management
  - Firmware updates
  - Detect and action process
- **Instruction for Data Backup**
  - Periodical communication
  - Download device settings
  - Automated upload data for backup
  - Remote restore of backup
  - Periodical communication (by manual trigger)
  - Automated updating out of hours
  - Backup and Restore
  - Device error processing

Operation Management

The equipment is operated and managed based on the system's security policy, in accordance with the ISO 27001 international standard for information security management.

- **ISO 27001-compliant data center**
  The server is carefully housed in a data center that is compliant with the ISO 27001 international standard, and that has passed evaluation under the information security management system (ISMS). A comprehensive system ensures nonstop operation—24 hours a day, 365 days a year.
- **Server authentication**
  A server authentication certificate issued by a third-party authenticating organization prevents server spoofing. The HTTPS protocol is used to prevent transmitted/received data leaks and tampering.

  e-BRIDGE CloudConnect uses Microsoft Azure as its cloud service. This means that security is constantly kept up to date, European device data is hosted in EU data center.

FLEXIBLE SUPPORT FOR YOUR SECURITY

Toshiba MFPs feature e-BRIDGE functionalty and support secure HTTPS protocol. e-BRIDGE CloudConnect allows for the safe handling of data such as the device operation status. It supports firewalls, proxy servers, and various configurations and authentications, providing flexible support for your security policies.

e-BRIDGE CloudConnect only handles the device operation status information. This includes data concerning charging and maintenance such as information on counter data (the number of sheets used, etc.), device failures, consumables replacements, and device settings and adjustments. Since e-BRIDGE CloudConnect does not handle actual document data, copy, fax, print and scan data will not be leaked to third parties.

Using the same principles used by client PCs, e-BRIDGE CloudConnect accesses secure data over a browser with HTTPS (server authentication and encryption). Data can only be sent from MFPs and access is limited to e-BRIDGE CloudConnect servers with valid authentication certificates. This provides excellent security.

The HTTPS protocol provides powerful security, ensuring that data is sent only from MFPs.

MFP contacts e-BRIDGE CloudConnect

MFPs also access e-BRIDGE CloudConnect when certain events are recognised, such as device failures or when consumables replacements are triggered.

MFP authenticates the server (the e-BRIDGE CloudConnect server's identity is confirmed) and communication is established using HTTPS

The MFP requests a server authentication certificate from e-BRIDGE CloudConnect. e-BRIDGE CloudConnect presents the server authentication certificate. The MFP compares the server authentication certificate received from e-BRIDGE CloudConnect with a certificate that has already been received from a certifying authority, to ensure that the certificate was issued by a valid third-party authenticating organisation.

HTTPS (encrypted) communication is established only if the server authentication certificate is valid. e-BRIDGE CloudConnect confirms that the remote device is a registered MFP before allowing the session to be established.

MFP data is transmitted and received under instruction of e-BRIDGE CloudConnect

The MFP encrypts and transmits necessary data (such as its current configuration) under instruction of e-BRIDGE CloudConnect. The MFP also receives encrypted configuration change data as needed from e-BRIDGE CloudConnect.

Communication ends

Once data transmission is complete, the MFP and e-BRIDGE CloudConnect terminate the connection, close the session, and end communication. MFPs do not allow access from outside once communication is complete. This allows for superior security.

SSL

To prevent server spoofing and to make sure data is transmitted to the correct server, e-BRIDGE CloudConnect features server authentication functionality that confirms whether the server to be accessed (e-BRIDGE CloudConnect) is the actual server that was specified. All transmitted and received data is encrypted to preserve its confidentiality and safety, and to protect against stealing, leaking, and tampering.

- HTTPS: HTTPS stands for "hypertext transfer protocol secure." It is a secured version of the HTTP protocol used for viewing websites.
- SSL: SSL stands for "secure sockets layer." SSL establishes communication only after verifying that a server is valid and has a server authentication certification installed. SSL also encrypts data before sending it.

FAQ

Q&A 1 Could copies, prints, faxes, or scans be leaked outside when using e-BRIDGE CloudConnect?

No. e-BRIDGE CloudConnect only handles device operation status information, so documents will never be leaked outside.

e-BRIDGE CloudConnect only handles data concerning charging and maintenance such as information on counter data (the number of sheets used, etc.), device failures, consumables replacements, and device settings and adjustments. This data is totally isolated from documents such as copies, faxes, and scans.

Q&A 2 Could copy, prints, fax, or scan counter data be leaked to or viewed from outside?

No. e-BRIDGE CloudConnect protects the counter data using server authentication, encryption, and an internally-developed system where data is transmitted only from inside.

These systems feature destination server authentication and encryption, while e-BRIDGE CloudConnect offers advanced security measures. e-BRIDGE CloudConnect also utilises an internally-developed system where data is transmitted only from MFPs to ensure that outside parties cannot break into MFPs from outside.

Q&A 3 How secure is the system?

e-BRIDGE CloudConnect uses HTTPS , a secured version of the HTTP protocol used for viewing websites.

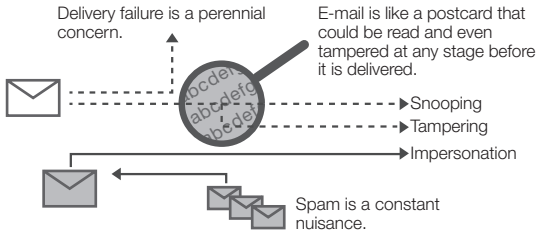
The device initiates a connection to the Service Cloud using a standard internet protocol via a secure channel HTTPS over port 443. This method is very similar to a web browser connecting to a secure website. All device connections are logged at the device and Cloud Connect connection. On the initial connection, a security protocol is used to register the device. Registration is a system function. Once the device is registered, the cloud provides a security token that the device uses on future connections.

Q&A 4 Why are e-mail addresses not used during communication between MFPs and e-BRIDGE CloudConnect?

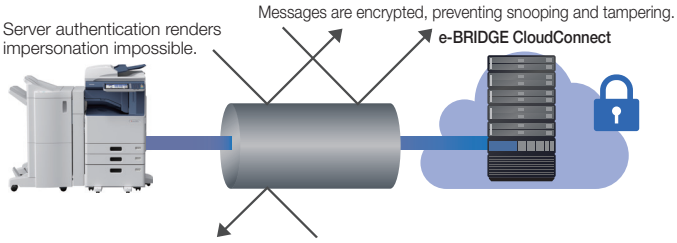
E-mail is vulnerable to impersonation, snooping, and tampering.

E-mail cannot authenticate the identity of the sender and is vulnerable to impersonation. Malicious third parties can also snoop or even tamper with e-mail. E-mail also carries the risks of delivery failure (as it is impossible to know if an e-mail has been received properly) and spam (unsolicited e-mail). e-BRIDGE CloudConnect therefore uses SSL during communication. Server authentication prevents impersonation, while HTTPS encryption prevents snooping and tampering. Finally, HTTPS sends data in real time so there is no risk of delivery failure or spam.

E-mail



e-BRIDGE CloudConnect



The problem of spam is avoided completely.

Because data is sent in real time, data can be exchanged surely and securely