TOSHIBA

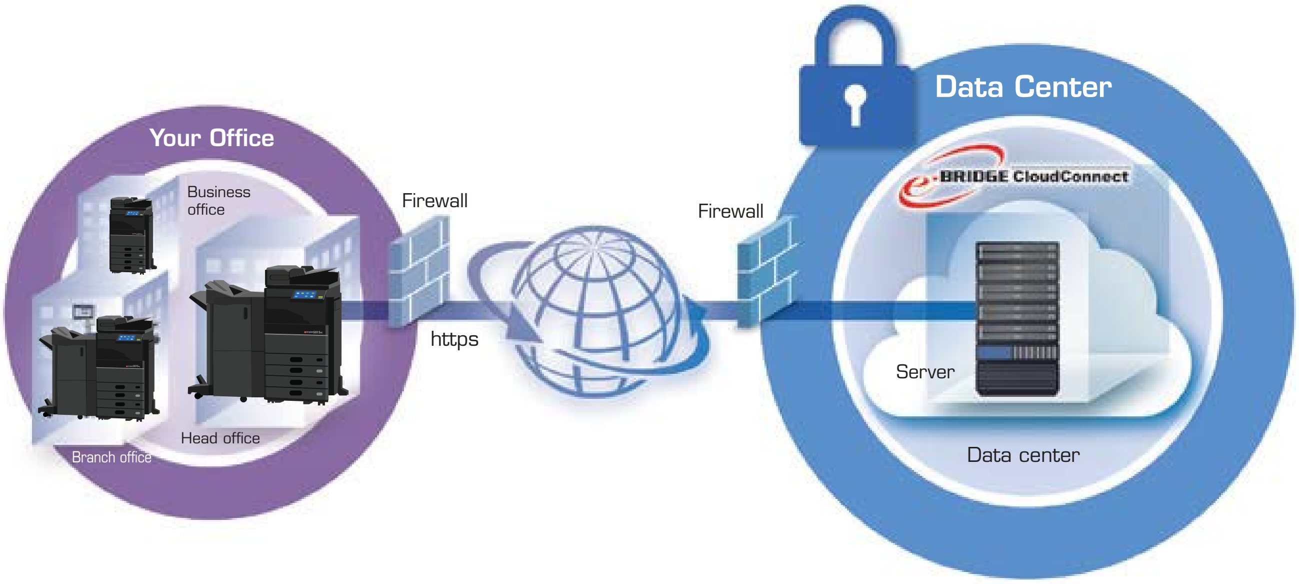
e-BRIDGE CloudConnect

WHITE PAPER

TOGETHER INFORMATION™

Toshiba e-BRIDGE CloudConnect offers comprehensive security.e-BRIDGE CloudConnect safely and reliably manages networked multi-function peripherals (MFP).

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



Toshiba MFPs

Toshiba multi-function peripherals (MFP) feature e-BRIDGE functionality and support the secure HTTPS protocol. e-BRIDGE CloudConnect allows for the safe handling of data such as the device operation status.

* Toshiba Australia is committed to obtaining ISO 15408—an international information security standard—for MFPs.
* e-BRIDGE CloudConnect does not support some MFP models.

Flexible support for your security policies

e-BRIDGE CloudConnect supports firewalls, proxy servers, and various configurations and authentications.

A secure design that does not handle transmitted, received, or copied data

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.

* On request, a service technician can set e-BRIDGE CloudConnect to permit or deny transmission.

Operation management in compliance with ISO 27001

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 organisation 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. Refer to the Microsoft Azure website for details.

Toshiba I.S. Corporation security check

e-BRIDGE CloudConnect also offers security checks conducted by Toshiba I.S. Corporation. This is done periodically to confirm the security of the system.

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

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

e-BRIDGE CloudConnect uses the same principles used by client PCs accessing 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.

1 MFP contacts e-BRIDGE CloudConnect

MFPs also access e-BRIDGE CloudConnect when certain events are recognised (such as during device failures or when it is time to replace consumables).

2 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 authetntication certificate. The MFP compares the server authentication certificate received from e-BRIDGE CloudConnect with a certificate that has already been 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 remove device is a registered MFP before allowing the session to be established.

3 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.

4 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/TLS

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.

DISCLAIMER NOTICE

The following notice sets out the exclusions and limitations of liability of TOSHIBA AUSTRALIA PTY LTD (including its employees, agents and sub-contractors) to any user ('User') of the e-BRIDGE CloudConnect.

1 The exclusion and limitations of liability referred to in this notice shall be effective to the fullest extent permissible at law. For the avoidance of doubt, nothing in this notice shall be taken to exclude or limit TOSHIBA AUSTRALIA's liability for death or personal injury caused by TOSHIBA AUSTRALIA's negligence or TOSHIBA AUSTRALIA's fraudulent misrepresentation.

2 All warranties, conditions and other terms implied by law are, to the fullest extent permitted by law, excluded and no such implied warranties are given or apply in relation to the system.

3 TOSHIBA AUSTRALIA shall not be liable for any loss, cost, expense, claim or damage whatsoever caused by any of the following: (a) use or handling of the system otherwise than in accordance with the manuals, including but not limited to Operator's Manual, User's Guide, and/or incorrect or careless handling or use of the system; (b) any cause which prevents the system from operating or functioning correctly which arises from or is attributable to either acts, omissions, events or accidents beyond the reasonable control of TOSHIBA AUSTRALIA including without limitation acts of God, war, riot, civil commotion, malicious or deliberate damage, fire, flood, or storm, natural calamity, earthquakes, abnormal voltage or other disasters; or (c) use in any operating environment or with settings other than those recommended by TOSHIBA AUSTRALIA.

4 Subject to paragraph 1, TOSHIBA AUSTRALIA shall not be liable to Customer for: (a) loss of profits; loss of sales or turnover; loss of or damage to reputation; loss of production; loss of anticipated savings; loss of goodwill or business opportunities; loss of customers; loss of, or loss of use of, any software or data; loss under or in relation to any contract; or (b) any special, incidental, consequential or indirect loss or damage, costs, expenses, financial loss or claims for consequential compensation; whatsoever and howsoever caused which arise out of or in connection with the system or the use or handling of the Product even if TOSHIBA AUSTRALIA is advised of the possibility of such damages.

TOSHIBA AUSTRALIA PTY LTD shall not be liable for any loss, cost, expense, claim or damage caused by any inability to use (including, but not limited to failure, malfunction, hang-up, virus infection or other problems) which arises from use of the system with hardware, goods or software which TOSHIBA AUSTRALIA has not directly or indirectly supplied.

Q&A 1 Could prints, copies, 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 print, copy, 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 an advanced security measures. e-BRIDGE CloudConnect also utilizes 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 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/TLS 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.

Q&A 4 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.

Q&A 5 What URL's do I need to allow for device access to e-BRIDGE Cloud Connect?

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.

The following web servers are contacted during the registration process in this sequence.

edevice.toshiba-solutions.com (157.55.252.141) skipped for AU.
gsidevice-eu.toshiba-solutions.com (137.117.201.238) skipped for AU.
gsidevice-ap.toshiba-solutions.com (13.75.159.193) used by AU.

The following web server is contacted for MFP meter collections.

eccwsi-ap.toshiba-solutions.com (13.75.153.98) used by AU.

Access will be required for all the above URL's.

Q&A 6 Where is the data centre hosted?

The Toshiba e-BRIDGE CloudConnect application is deployed and run on Microsoft Azure cloud data centre located in Australia.

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

Technical data is subject to change without prior notice. All company and/or product names are trademarks and/or registered trademarks of their respective manufacturers in their markets and/or countries. All rights reserved. We are constantly making efforts to deliver the latest status of data to our partners. Specifications for some models may change in the time between the production and the release of this documentation.