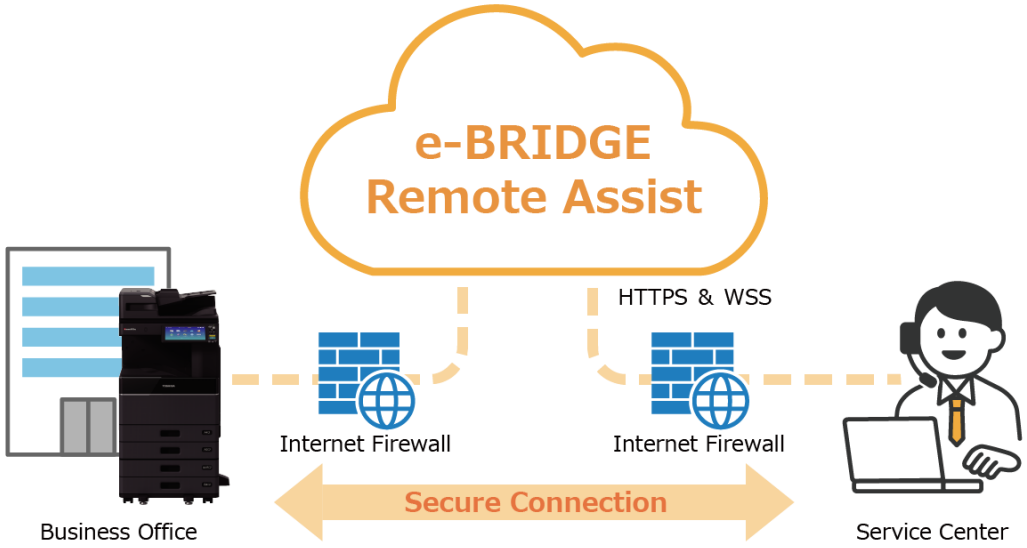
e-BRIDGE Remote Assist SECURITY GUIDE

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

e-BRIDGE Remote Assist provides safe and quick remote maintenance of your MFP from the service center. Only personnel from a contract maintenance company with a valid permit can perform remote maintenance.



Toshiba MFPs

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

* Toshiba TEC is committed to obtaining ISO 15408—an international information security standard—for MFPs.

* e-BRIDGE Remote Assist does not support some MFP models.

Flexible support for your security policies

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

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

e-BRIDGE Remote Assist uses VNC (Virtual Network Computing) technology and WSS (Web Socket over TLS) communication to perform secure and quick remote maintenance via the MFP operation panel. e-BRIDGE Remote Assist does not process actual document data, so copy, fax, print and scan data will not be leaked to third parties.

* On request, a service technician can set e-BRIDGE Remote Assist 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 organization prevents server spoofing. The HTTPS protocol is used to prevent transmitted/received data leaks and tampering.

e-BRIDGE Remote Assist uses Amazon Web Service as its cloud service. This means that security is constantly kept up to date. Refer to the Amazon Web Service website for details.

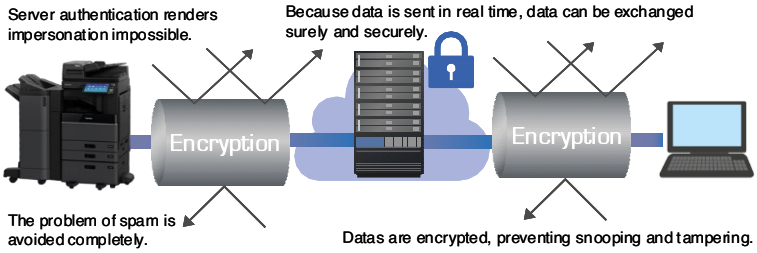
Toshiba I.S. Corporation security check

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

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

e-BRIDGE Remote Assist uses the same principles used by client PCs accessing secure data over a browser with HTTPS (server authentication and encryption) and WSS(WebSocket over TLS). Data can only be sent from MFPs and access is limited to e-BRIDGE Remote Assist servers with valid authentication certificates. This provides excellent security.

e-BRIDGE Remote Assist



SSL/TLS

To prevent server spoofing and to make sure data is transmitted to the correct server, e-BRIDGE Remote Assist features server authentication functionality that confirms whether the server to be accessed (e-BRIDGE Remote Assiste) 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 TEC CORPORATION (including its employees, agents and sub-contractors) to any user ('User') of the e-BRIDGE Remote Assist.

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 TEC CORPORATION's liability for death or personal injury caused by TOSHIBA TEC CORPORATION's negligence or TOSHIBA TEC CORPORATION'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 TEC CORPORATION 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 TEC CORPORATION 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 TEC CORPORATION.

4 Subject to paragraph 1, TOSHIBA TEC CORPORATION 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 TEC CORPORATION is advised of the possibility of such damages.

TOSHIBA TEC CORPORATION 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 TEC CORPORATION has not directly or indirectly supplied.

FAQ

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

No. e-BRIDGE Remote Assist uses server authentication and encryption to protect your communication data so that no data is leaked.

e-BRIDGE Remote Assist uses VNC (Virtual Network Computing) technology and WSS (Web Socket over TLS) communication to perform secure and quick remote maintenance via the MFP operation panel.

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

No. Since e-BRIDGE Remote Assist does not handle document data, the document will not be leaked to the outside.

e-BRIDGE Remote Assist only provides safe and quick remote maintenance of your MFP from the service center. Also only personnel from a contract maintenance company with a valid permit can perform remote maintenance.

Q&A 3 What happens to the remote service of e-BRIDGE Remote Assist if I forget to terminate it?

The e-BRIDGE Remote Assist remote service will automatically disconnect 60 minutes after you start the connection.

The e-BRIDGE Remote Assist remote service can be terminated from both the customer's MFP and the service center.
Reconnecting requires re-entering the authorization code into the customer's MFP.
In addition, the remote service of e-BRIDGE Remote Assist will be automatically disconnected 60 minutes after the connection is started.