TOSHIBA

e-BRIDGE SKY Suite™

Security Guide

* This service is not available under this name, e-BRIDGE SKY Suite™, in the European region.

OME220002A0

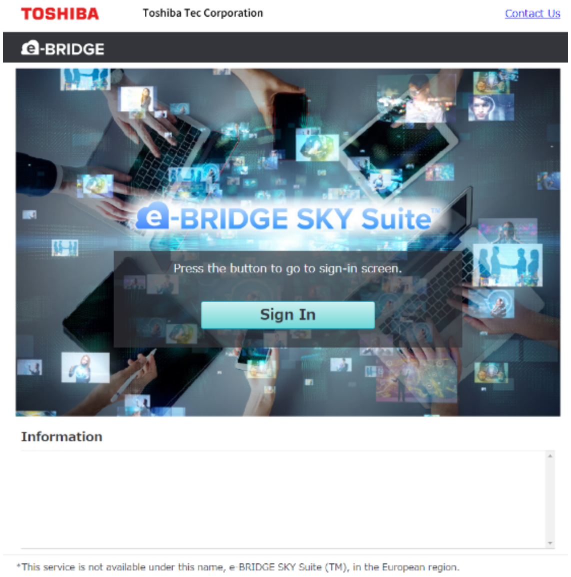
R2202220Y9601-TTEC

Ver01 F Issued in Oct. 2022

TOGETHER INFORMATION

e-BRIDGE SKY Suite™

To deal with problems faced in various business scenarios, we provide a solution by one-stop service. By using e-BRIDGE SKY Suite™ (hereafter called “this service”), you are able to use a service suitable for your problem in a one-portal site. You are also able to access and manage data and devices anytime and anywhere remotely. This will reduce cost and time, and thus operating effectiveness can be improved considerably.



TOSHIBA Toshiba Tec Corporation Contact Us

e-BRIDGE

e-BRIDGE SKY Suite™

Press the button to go to sign-in screen.

Sign In

Information

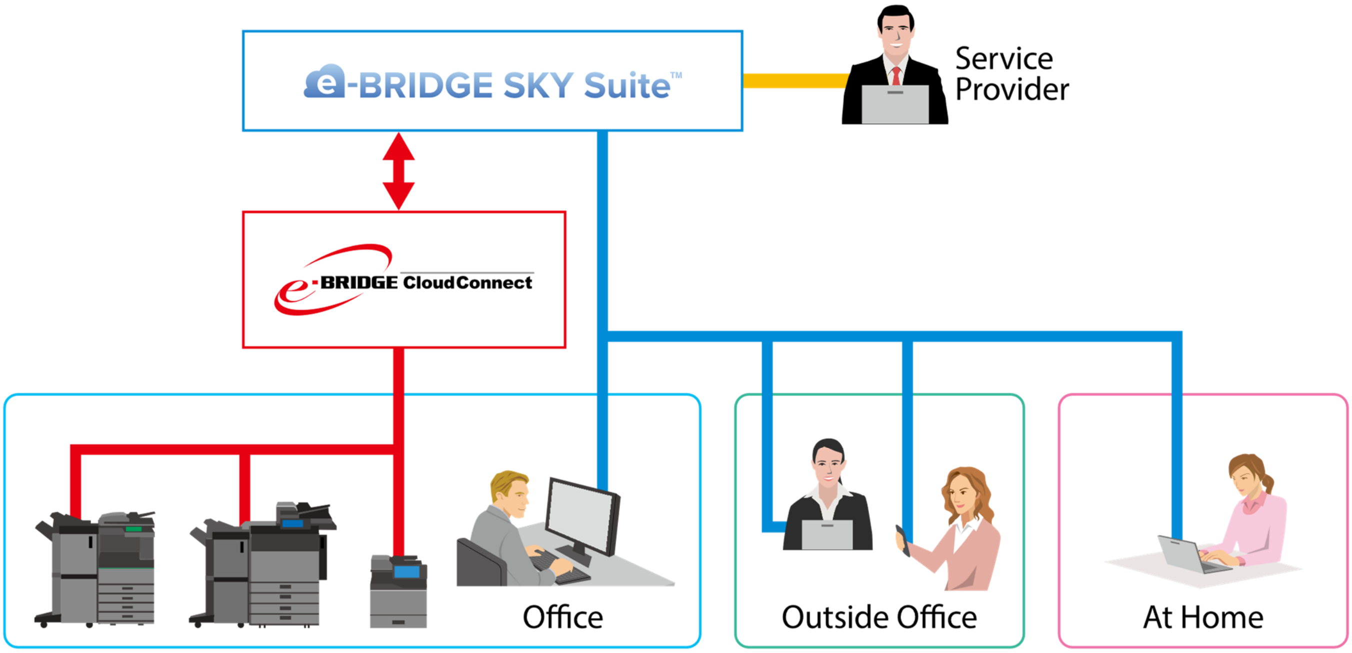
*This service is not available under this name, e-BRIDGE SKY Suite (TM), in the European region.

e-BRIDGE Meter Collector / e-BRIDGE Device Management Overview

These e-BRIDGE SKY Suite™ modules link with our current cloud based service platform e-BRIDGE CloudConnect and provide you with secure visibility and control of your Toshiba MFP fleet.

Using just a single dashboard you can see the status of any device, check usage counters and consumable levels along with being able to manage settings across your whole fleet.

* e-BRIDGE CloudConnect is a cloud system operated by Toshiba Tec Corporation (hereafter called “Toshiba Tec”), in order to collect operation information of users’ MFPs in a safe and secure manner.



Preface

This document describes the product security of this service at the time of the issue and has the only purpose of providing information. Users will be responsible for making decisions about the information in this document and the use of this service based on their own evaluation. Since the responsibility of this service to users is regulated by the agreement, this will not be changed by means of this document. Moreover, this document is subject to changes without notice.

Security Policy

The information security in this service is targeted to the information security basic policy regulated by Toshiba Tec and personnel information of users who use this service. We will operate the service with the utmost emphasis on maintaining the confidentiality of meta data (information related to MFPs operated in the field collected through this service) as the foundation of the business.

Responsibility Demarcation Points with Users

This service is an Saas cloud service configured by being based on Microsoft Azure, a cloud provider. Therefore, the demarcation points for the items are as below. In addition, necessary security measures are implemented within the scope of the provision of a provider of this service.

<table>
<tr><td colspan="4"><b>Data, Content</b></td><td>Responsibility: User
Subsidiaries, distributors</td></tr>
<tr><td colspan="4"><b>Application</b></td><td>Responsibility: Service provider (SaaS)
Toshiba Tec</td></tr>
<tr><td colspan="4"><b>Running time, Middleware</b></td><td rowspan="5">Responsibility: Cloud provider (PaaS)
Microsoft Azure</td></tr>
<tr><td colspan="4"><b>OS, Network</b></td></tr>
<tr><td><b>Computing</b></td><td><b>Storage</b></td><td><b>Database</b></td><td><b>Network</b></td></tr>
<tr><td colspan="4"><b>Domain</b></td></tr>
<tr><td colspan="4"><b>Region</b></td></tr>
</table>

Collected Data and Security

This service uses the operation status information of MFPs collected by the linked e-BRIDGE CloudConnect. This information contains the data regarding the usage fee and maintenance, such as counter data (number of used sheets of paper), device failure, consumables replacement, device settings and adjustment. Data collected from MFPs are encrypted by an HTTPS protocol and then can only be sent from MFPs to an e-BRIDGE CloudConnect server with valid authentication, resulting in the prevention of outside intrusion into the MFP.

■ Collected data

- Device information
  Serial number, model name, device explanation, others (MFP unique information)
- Counter information
  Print counter, scan counter, MFP type (B&W or color), other counters
- Consumables' information
  Toner cartridge remaining amount, drum cartridge status, other consumables' information
- Service-related information
- Device settings, error code, firmware version, other service-related information

Operation and Management of Cloud Service

■ Operation and management of ISO27001 compliance

This service is hosted in environments that have obtained ISMS (Information Security Management System) certification (ISO/IEC 27001).
In the near future we will also obtain certification to the ISO/IEC 27017 standard.

■ Security and compliance of Microsoft Azure

This service is hosted on Microsoft Azure, and thus the security of the data center is maintained at the highest standards. Microsoft Azure complies with numerous standards including ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP and ENS.
For further details, refer to the following URL for the Microsoft Azure website.
https://www.microsoft.com/en-us/TrustCenter/Compliance/

■ Periodic vulnerability audits

In order to ensure the utmost security of the system, Toshiba I.S. Corporation performs vulnerability audits on this service prior to release and on a regular basis.
WebInspect by Micro Focus and InsightVM by Rapid 7 are used as a vulnerability check tool to perform vulnerability assessments specific to web applications.

■ Monitoring of operation, malfunction and performance

This service collects and analyzes telemetry by using Azure Monitor to ensure the system is available and performing at its peak by proactively identifying and acting on potential problems in just moments.

■ Backing up of information

The back-up function provided by Azure is used to back up the database. The back-up data are all encrypted (AES256) and then stored in a storage location in Azure. Toshiba Tec will use those back-up data for the recovery when any trouble has occurred in this service; however, they will not be able to restore at the timing required by a contract user.

■ Time synchronization and storage of event logs

As for the time recorded in the event logs, its synchronization is also managed by an Azure management service. Moreover, appropriate logs required to maintain and manage the service are stored for up to 180 days by using Azure Monitor an Azure Application Insights. Users cannot obtain and browse their event logs. When browsing of event logs is required, contact Toshiba Tec (and its affiliates or subsidiaries, if applicable).

■ Disposal and reuse of the devices while keeping the security

This service is provided on a virtual environment configured by our contracted cloud service provider. Therefore, we do not have resources (devices, data storage, memory, files, etc.) which we will dispose of or reuse directly. We have confirmed that our contracted cloud service provider is properly disposing of or reusing resources in accordance with the contract.

Cloud Service Security

■ **User authentication**

Microsoft Azure AD B2C is used for user authentication of this service.

Microsoft Azure AD B2C is an ID management platform provided by Microsoft. By using OpenID Connect (OIDC), users can safely sign in to applications. In addition, this enables a single sign-on between multiple services offered, providing both user convenience and enhanced security.

■ Encryption of communication path

All user communications with this service are protected using HTTPS protocol supporting encryption at TLS1.2 or later only.

■ Server authentication

Server authentication certificate issued by a third-party certification organization prevents server spoofing.

Server authentication certificate (TLS/SSL certificates) uses OV authentication (corporate authentication certificate) issued by a third-party certification authority.

■ Network disconnection

To prevent security risks from cyber attacks and access to any important data, this service back end servers and database are disconnected from the internet by a virtual network (VNet).

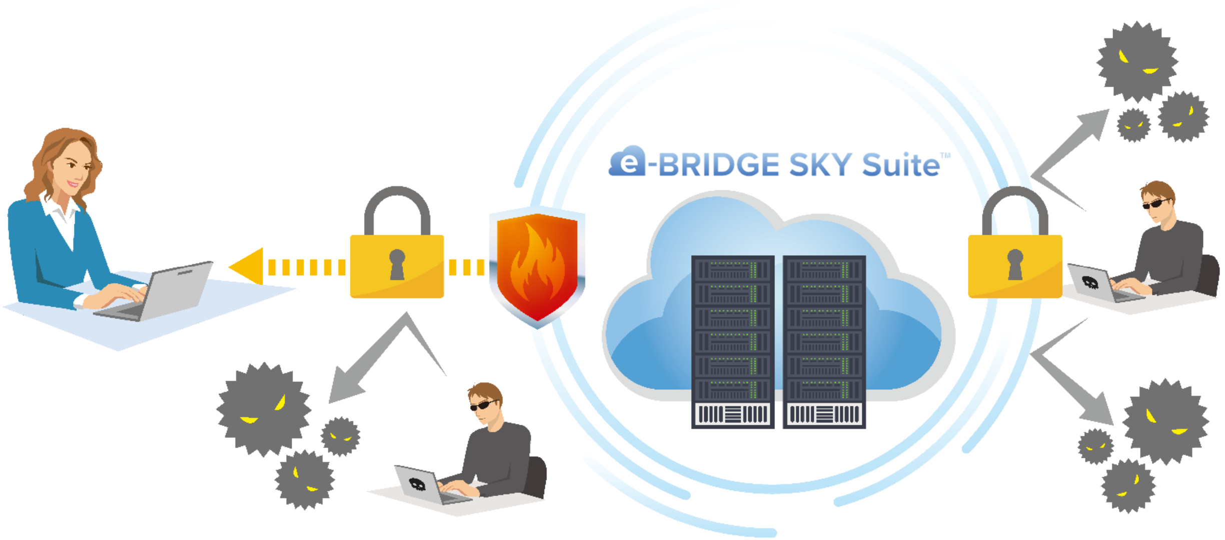
Thus, it is protected to prevent direct access to important data.

■ WAF (Web Application Firewall)

WAF (Web Application Firewall) minimizes risks by detecting and preventing attacks that exploit web application vulnerabilities, including SQL injection and cross-site scripting.

■ Malware countermeasure

This service introduces a Microsoft Defender virus countermeasure to protect the system from malware (malicious software), viruses and other threats. Even in the unlikely event that a threat is detected, appropriate measures can be taken to respond quickly and prevent information leaks.



FAQ

- **System Security**

  This service is hosted in environments that have obtained ISMS (Information Security Management System) certification (ISO/IEC 27001).

  By the end of 2022 we will have also obtained certification to the ISO/IEC 27017 standard.

- **Address of this service provider**

  The address of the head office of Toshiba Tec is as below.

  1-11-1 Osaki, Shinagawa-ku, Tokyo (Gate City Osaki West Tower)

- **Data storage location**

  Data for this service application are stored in Microsoft Azure cloud data centers in North America (U.S.A.), Europe (Netherlands) and Asia Pacific (Australia), depending on the region served.

  For details about the latest data security and compliance information, refer to the following URL.

  https://azure.microsoft.com/en-us/overview/trusted-cloud/

Trademarks

- Microsoft and Microsoft Azure, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- Other company names and precuts names in this document are the trademarks of their respective companies.

Copyright