TOSHIBA

e-BRIDGE CloudConnect

Assistenza remota

- Servizio di assistenza basato su cloud per il monitoraggio dei dispositivi.
- Gestione delle informazioni sullo stato e il funzionamento del dispositivo.
- Sicurezza globale: i dati operativi vengono raccolti in modo sicuro e affidabile.
- Tutto questo senza dover installare alcun software: il sistema MFP Toshiba gestisce tutte le operazioni.

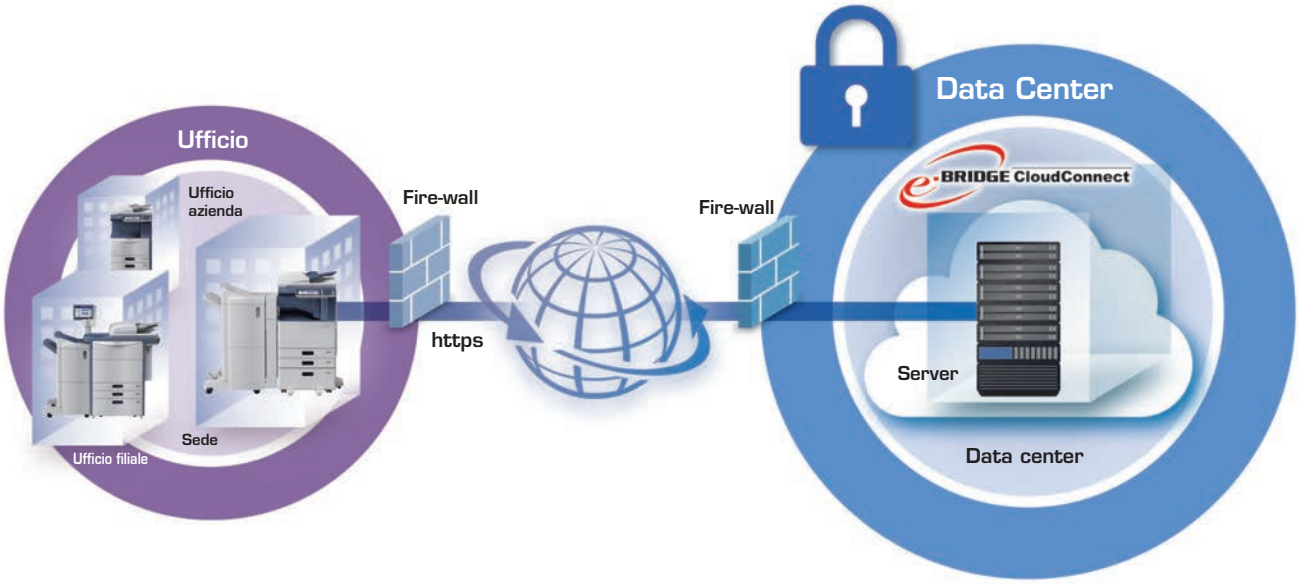
TOGETHER INFORMATION

MONITORAGGIO CONFIGURAZIONE E AUTOMATIZZAZIONE

Toshiba e-BRIDGE CloudConnect offre un sistema completo per la gestione e la sicurezza dei prodotti multifunzione (MFP) collegati alla rete.

e-BRIDGE CloudConnect raccoglie in modo sicuro e affidabile i dati operativi trasmessi dagli MFP utilizzando una connessione HTTPS/SSL. Solo i dipendenti autorizzati delle aziende incaricate della manutenzione possono visualizzare i dati.

- Servizio di assistenza basato su cloud per un processo end-to-end destinato al monitoraggio delle comunicazioni con il dispositivo
- Produttività migliorata grazie alla diagnosi remota e agli avvisi proattivi sullo stato del dispositivo
- Riduzione dei carichi di lavoro grazie alle misurazioni programmate e alla consegna automatizzata dei consumabili
- Aggiornamento dei dispositivi con l'ultimo firmware e il backup dei dati da remoto
- Stabilità della flotta di MFP garantita da regolari controlli da remoto



Descrizione dell'attività

Una volta stabilito il collegamento con il server, è possibile monitorare, impostare e salvare i seguenti dati per agevolare la manutenzione da remoto o per fornire ai tecnici che dovranno intervenire in loco informazioni utili in merito al guasto segnalato:

- **Efficacia della prima chiamata**
  - Preparazione basata sulle informazioni riguardanti lo stato del dispositivo, ricevute prima della visita
- **Avviso chiamata di assistenza**
  - Gestione automatizzata della politica di assistenza
  - Aggiornamenti del firmware
  - Processo di rilevamento e azione
- **Istruzioni per il backup dei dati**
  - Comunicazione periodica
  - Download delle impostazioni del dispositivo
  - Upload automatico dei dati per il backup
  - Ripristino del backup da remoto
  - Comunicazione periodica (attivata manualmente)
  - Aggiornamento automatico fuori orario
  - Backup e ripristino
  - Elaborazione degli errori del dispositivo

Gestione operativa

Il dispositivo è utilizzato e gestito in base alla politica di sicurezza del sistema conforme allo standard internazionale ISO 27001 per la gestione della sicurezza delle informazioni.

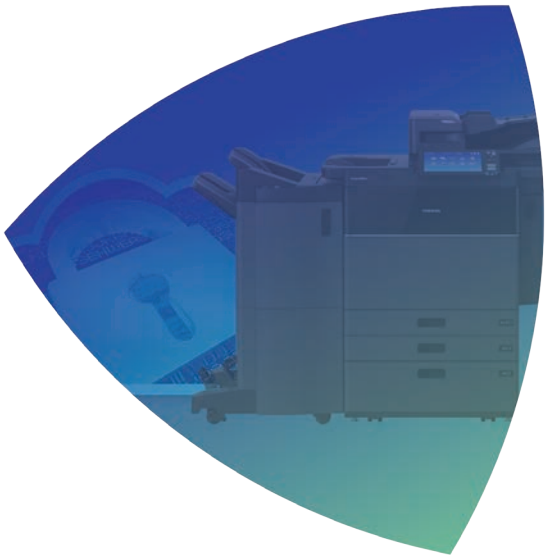
- **Data center conforme a ISO 27001**
  Il server è ospitato in un data center che è conforme allo standard internazionale ISO 27001 e che ha superato la valutazione ai sensi del sistema di gestione della sicurezza delle informazioni (ISMS). Un sistema globale garantisce un funzionamento ininterrotto: 24 ore al giorno, 365 giorni l'anno.
- **Autenticazione del server**
  Un certificato di autenticazione del server emesso da un organismo esterno attesta che l'organizzazione adotta misure atte a impedire lo spoofing del server. Il protocollo HTTPS consente di prevenire la diffusione e la manomissione dei dati trasmessi/ricevuti.

  e-BRIDGE CloudConnect utilizza Microsoft Azure come servizio cloud. Ciò significa che la sicurezza è costantemente aggiornata. I dati dei dispositivi europei sono ospitati in data center UE.

SUPPORTO FLESSIBILE PER LA SICUREZZA

Gli MFP Toshiba offrono la funzionalità e-BRIDGE e supportano il protocollo HTTPS. e-BRIDGE CloudConnect garantisce la gestione sicura dei dati, quali lo stato operativo del dispositivo. L'applicazione supporta firewall, server proxy e varie configurazioni e autenticazioni, garantendo un supporto flessibile per le policy di sicurezza.
e-BRIDGE CloudConnect gestisce solo le informazioni riguardanti lo stato operativo del dispositivo. Queste includono i dati riferiti ad addebiti e manutenzione, come ad esempio i dati dei contatori (numero di fogli usati, ecc.), le informazioni su guasti e sostituzioni dei consumabili, e le impostazioni e regolazioni del dispositivo. Poiché e-BRIDGE CloudConnect non gestisce i dati dei documenti, non esiste alcun rischio di divulgazione delle informazioni contenute in copie, fax, stampe e scansioni.
Utilizzando gli stessi principi adottati dai PC client, e-BRIDGE CloudConnect accede ai dati protetti tramite browser con HTTPS (autenticazione e crittografia del server). I dati possono essere inviati solo dagli MFP e l'accesso è limitato ai server e-BRIDGE CloudConnect con certificati di autenticazione validi. Ciò garantisce un'eccellente sicurezza.

Il protocollo HTTPS offre la massima sicurezza, garantendo che i dati vengano inviati solo dagli MFP.



MFP contatta e-BRIDGE CloudConnect

Gli MFP accedono a e-BRIDGE CloudConnect anche quando si verificano determinati eventi, come il guasto di un dispositivo o l'avvio del processo di sostituzione dei consumabili.

MFP autentica il server (l'identità del server e-BRIDGE CloudConnect viene confermata) e stabilisce la comunicazione utilizzando HTTPS

MFP richiede a e-BRIDGE CloudConnect un certificato di autenticazione del server. MFP confronta il certificato di autenticazione del server inviato da e-BRIDGE CloudConnect con un certificato ricevuto in precedenza da un'autorità certificatrice, per assicurarsi che il certificato sia stato emesso da un organismo esterno valido.
La comunicazione HTTPS (crittografata) viene stabilita solo se il certificato di autenticazione del server è valido. Prima di consentire l'avvio della sessione, e-BRIDGE CloudConnect verifica che il dispositivo remoto sia un MFP registrato.

MFP trasmette e riceve i dati attenendosi alle istruzioni di e-BRIDGE CloudConnect

MFP crittografa e trasmette i dati necessari (come la sua configurazione corrente) attenendosi alle istruzioni impartite da e-BRIDGE CloudConnect. MFP riceve anche i dati crittografati per la modifica della configurazione inviati da e-BRIDGE CloudConnect.

La comunicazione termina

Al termine della trasmissione dei dati, MFP ed e-BRIDGE CloudConnect interrompono la connessione, chiudono la sessione e terminano la comunicazione. MFP non consente l'accesso da dispositivi esterni una volta completata la comunicazione. Ciò contribuisce a incrementare la sicurezza del sistema.

SSL

Per prevenire lo spoofing del server e garantire che i dati siano trasmessi al server corretto, e-BRIDGE CloudConnect offre la funzionalità di autenticazione che verifica se il server cui si accede (e-BRIDGE CloudConnect) è quello effettivamente specificato. Tutti i dati trasmessi e ricevuti sono crittografati per proteggere la loro riservatezza e sicurezza e per impedirne il furto, la divulgazione e la manomissione.

- HTTPS: HTTPS è l'acronimo di "hypertext transfer protocol secure". È la versione protetta del protocollo HTTP utilizzato per visualizzare i siti web.
- SSL: SSL è l'acronimo di "secure sockets layer". SSL stabilisce la comunicazione solo dopo avere verificato che il server sia valido e abbia installato una certificazione di autenticazione del server. SSL crittografa inoltre i dati prima di inviarli.

FAQ

Q&A 1 Copie, stampe, fax o scansioni possono trapelare quando si utilizza e-BRIDGE CloudConnect?

No. e-BRIDGE CloudConnect tratta esclusivamente le informazioni sullo stato operativo del dispositivo, non esiste pertanto alcun rischio di divulgazione dei documenti.

e-BRIDGE CloudConnect gestisce solo i dati riferiti ad addebiti e manutenzione, come ad esempio i dati dei contatori (numero di fogli usati, ecc.), le informazioni su guasti e sostituzioni dei consumabili, e le impostazioni e regolazioni del dispositivo. Questi dati sono totalmente isolati dai documenti, come copie, fax e scansioni.

Q&A 2 I conteggi di copie, stampe, fax o scansioni possono trapelare o essere visualizzati da persone esterne all'azienda?

No. e-BRIDGE CloudConnect protegge i dati del contatore utilizzando l'autenticazione del server, la crittografia e un sistema sviluppato internamente in cui i dati vengono trasmessi solo dall'interno.

Questi sistemi prevedono la crittografia e l'autenticazione del server di destinazione, mentre e-BRIDGE CloudConnect offre misure di sicurezza avanzate. L'applicazione utilizza anche un sistema sviluppato internamente in cui i dati vengono trasmessi solo dagli MFP per garantire che nessuno possa accedere ai dispositivi dall'esterno.

Q&A 3 Quanto è sicuro il sistema?

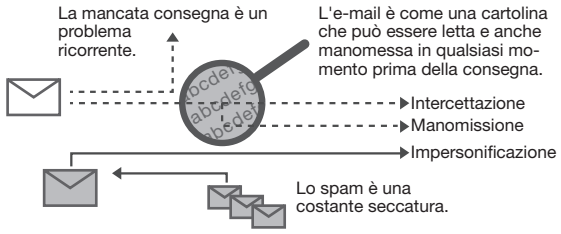
e-BRIDGE CloudConnect utilizza HTTPS, una versione protetta del protocollo HTTP utilizzato per visualizzare i siti web.

Il dispositivo avvia una connessione con il Service Cloud utilizzando un protocollo internet standard attraverso un canale sicuro HTTPS sulla porta 443. Questo metodo è molto simile a un browser web che si collega a un sito web sicuro. Tutte le connessioni del dispositivo sono registrate sul dispositivo e sulla connessione Cloud Connect. Durante la prima connessione, il dispositivo viene registrato utilizzando un protocollo di sicurezza. La registrazione è una funzione di sistema. Al termine della registrazione, il cloud fornisce un token di sicurezza che il dispositivo utilizzerà per le connessioni successive.

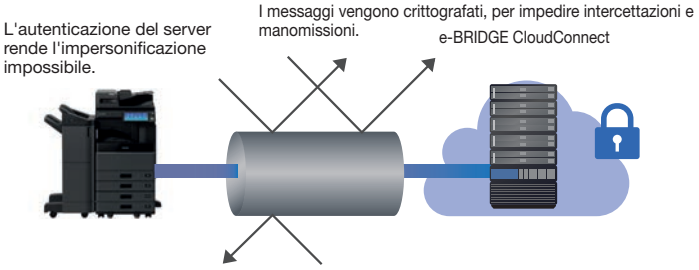
Q&A 4 Perché non si utilizzano gli indirizzi e-mail durante la comunicazione tra gli MFP ed e-BRIDGE CloudConnect?

Le e-mail possono essere impersonificate, spiate e manomesse.
La posta elettronica non è in grado di autenticare l'identità del mittente ed è pertanto esposta al rischio di impersonificazione. Terzi con intenti dolosi possono anche spiare o persino manomettere le e-mail. Le e-mail sono inoltre soggette al rischio di mancata consegna (non essendo possibile sapere se un messaggio è stato ricevuto correttamente) e di spam (e-mail indesiderate).
e-BRIDGE CloudConnect utilizza SSL durante la comunicazione. L'autenticazione del server previene l'impersonificazione mentre la crittografia HTTPS impedisce l'intercettazione e la manomissione. Infine, HTTPS invia i dati in tempo reale evitando il rischio di mancata consegna o di

E-mail



e-BRIDGE CloudConnect



Si evita il problema dello spam.

Poiché l'invio dei dati avviene in tempo reale, lo scambio è sicuro.