Xerox®
Connect App for Blackboard

Information Assurance Disclosure

BR25350
Document Version: 1.0 (October 2018).

Preface

Xerox® Connect App for Blackboard (BB) is a workflow solution that connects Xerox® Multifunction Printers (MFP) to a Blackboard Learn platform. Scanning documents to Instructor course folders is easy and convenient from Xerox® MFP devices without the need of a computer, servers, and third party scan equipment. This reduces time and cost while ensuring privacy and security.

1. Purpose

   The purpose of the Information Assurance Disclosure (IAD) is to disclose information for BB with respect to device security. Device security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® BB app relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and the Xerox® BB does not establish security for network environments where MFPs or the Blackboard Learn system is installed.

   This document does not provide tutorial level information about security, connectivity or Xerox® BB features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

2. Target Audience

   The target audience for this document is Xerox field personnel and customers concerned with IT security.

   It is assumed that the reader is familiar with the BB app; as such, some user actions are not described in detail.

3. Disclaimer

   The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

Contents

Note: The above table of contents is automatically created from text that is styled with Heading 1, Heading 2 and Heading 3 in the following pages (right-click on the table and select “Update Field”).

1. Description and Details

Overview

The Xerox® BB app provides two workflows.

- App setup
- Scan a document to a folder

Completing a workflow involves a combination of the following aspects described in detail below.

- App Hosting
- Device Authentication
- App Start Up
- App Setup
- Create a REST Integration in Learn
- Learn Cookie Disclosure Prompt
- Learn Authentication and Authorization
- Allow Learn Integration Prompt
- Course and Folder Selection
- Provide a Destination File Name
- Scanning

App Hosting

The Xerox® BB app is a ConnectKey App / EIP web application registered on a device and executes its functionality in the cloud.

All data communications in and out of the device and cloud components are encrypted over HTTPS using TLS 1.2.

Device Authentication

Device login: Prior to starting the Xerox® BB app, a device administrator authenticates using their device credentials. The device administrator must perform this step so that the BB app configuration settings can be viewed or changed.

The device login interaction is confined to the device login workflow, and the credential values provided are not interrogated by the BB app.

App Start Up

During startup of the BB app, the EIP browser runs the CK App HTML and JavaScript hosted on the device which fetches the App UI content from BB app endpoints hosted in the Azure App Service. The main page initialization script executes local HTTP calls to web services in order to obtain relevant details associated with the device and its capabilities.

The following app data is stored on the device, in browser storage, until the App is uninstalled from the device.

- Device serial number
- Device network MAC address
- Device User Administrator indicator
- Device Type indicator

App Setup

When using the app while signed into the device as a user with administrator privileges, the BB app displays the configuration settings related to the Blackboard Learn connection details, which is assigned to the device.

The following app data is stored on the device, in browser storage, until the App is uninstalled from the device.

- Blackboard Learn host
- Blackboard Learn HTTPS TCP port

The following app data is stored in the Azure App Database until periodic deletion is required.

- Device serial number
- Device network MAC address
- Blackboard Learn host
- Blackboard Learn HTTPS TCP port

Create a REST Integration in Learn

In order to use the BB app, the Blackboard Learn host must have a REST Integration registration entry associated with the BB app Application ID provided in the notification alert when running the app for the first time as a device administrator.

For more information on Blackboard Learn REST integration, please follow the link: https://community.blackboard.com/docs/DOC-1580-managing-rest-integrations-in-learn-the-rest-integrations-tool-for-system-administrators

Learn Cookie Disclosure Prompt

In order to use the BB app, the user must accept storing any HTTP cookie that originates from the Learn server. Whenever the Learn acceptance cookie is not found, the Learn OAuth2 workflow will prompt the user to accept a disclosure statement.

After the user accepts the statement, a disclosure acceptance cookie containing the string *true* is stored on the device in browser storage. The disclosure acceptance cookie is not flagged secure.

Cookie removal is triggered by specific device events. See Device Browser Cookies in section 3. Privacy for more details.

Learn Authentication and Authorization

User login: Once the BB app setup is completed, a Learn user can authenticate using their Learn account credentials. When using the app while signed into Learn having an institutional role of *Faculty* or *Student*, the BB app will display courses and course folders using the user's Learn authorizations once the user allows the app to integrate with Blackboard Learn.

The Learn login interaction is confined to the Learn login workflow. Although the user name is discoverable, the user's password cannot be interrogated by the BB app.

The following app data is stored on the device in browser storage as an authorization cookie. The authorization cookie is not flagged secure.

- Learn user's access token
- Learn session refresh token
- Learn user's randomized unique identifier

Cookie removal is triggered by specific device events. See section 4.1 Device Browser Cookies for more details.

The following app data is stored in process, in the Azure App Service, until the session terminates or is refreshed after expiring:

- Learn user's access token

Allow Learn Integration Prompt

In order to use the BB app, the user must allow the app to communicate with the Learn server using the dialog presented by Blackboard.

No user data is sent to or stored by the BB app during in this step.

Course and Folder Selection

At various steps in the application, the user may be prompted to make selections. This includes navigating Learn courses and corresponding folders. These lists are dynamic and driven by API calls to the BB app with the user's OAuth token.

The following app data is stored in process, on the device and in the Azure App Service, until the session terminates or a device timeout occurs:

- Learn user's randomized unique identifier
- Course Identifier
- Folder Identifier

Provide a Destination File Name

The user must provide an acceptable destination file name. The file name is stored in EIP browser memory during the session and in the Azure App Service until the session terminates.

In addition, the file name is persisted to a transaction log in the Azure App Service until periodic deletion is required.

Scanning

Scanned documents are securely transmitted to the Azure App Service using HTTPS TLS 1.2 from the device to the BB app and delivered in process, as a pass through, to the user's Learn course folder. This workflow can be executed multiple times per hour.

The following app data is stored in process, in the Azure App Service, until the session terminates or is refreshed after expiring:

- BB app system access token

The system access token is used when delivering scan output because the user access token does not permit users granted the institutional role of *Student* to upload content to course folders.

Unlike the user access token, the system access token permits the bearer to impersonate the Learn user associated with the REST Integration configuration item for the Xerox® BB app, which is designated in the institution's Learn System Administration panel.

See Learn Hosting in section 2. Security for more details.

The security of the scanned documents, after delivery to the Learn folder selected, is controlled by the Learn content system security settings and is not influenced by the BB app in any way.

2. Security

App Hosting

The Xerox® BB EIP app is hosted on the Microsoft Azure Network. Microsoft's Azure data center operations feature comprehensive information security policies and processes using standardized industry control frameworks, including ISO 27001, SOC 1, and SOC 2.

For a full description, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security

Learn Hosting

The Blackboard Learn system and network security is established and maintained by non-Xerox authorities.

For more information on Blackboard Learn authentication and authorization, please follow the link: https://community.blackboard.com/docs/DOC-4457-use-oauth-20-to-authenticate-with-blackboard-learn

For more information on Blackboard Learn REST integration, please follow the link: https://community.blackboard.com/docs/DOC-1580-managing-rest-integrations-in-learn-the-rest-integrations-tool-for-system-administrators

Secure Web Communications

All web communications are encrypted using TLS 1.2 over HTTPS.

Encryption

Except for securing the web communication, the BB app does not utilize other encryption technologies while working with the application data.

App Data

The file name provided by the Learn user is stored in the BB app transaction log.

3. Privacy

Device Browser Cookies

Cookies are stored on the device, in browser storage, until one of the following events occur.

- Device Logout
- Device Timeout
- Double Clear All
- Browser Restart
- Cycling the Browser from Disabled to Enabled
- App Exit

4. Ports

App

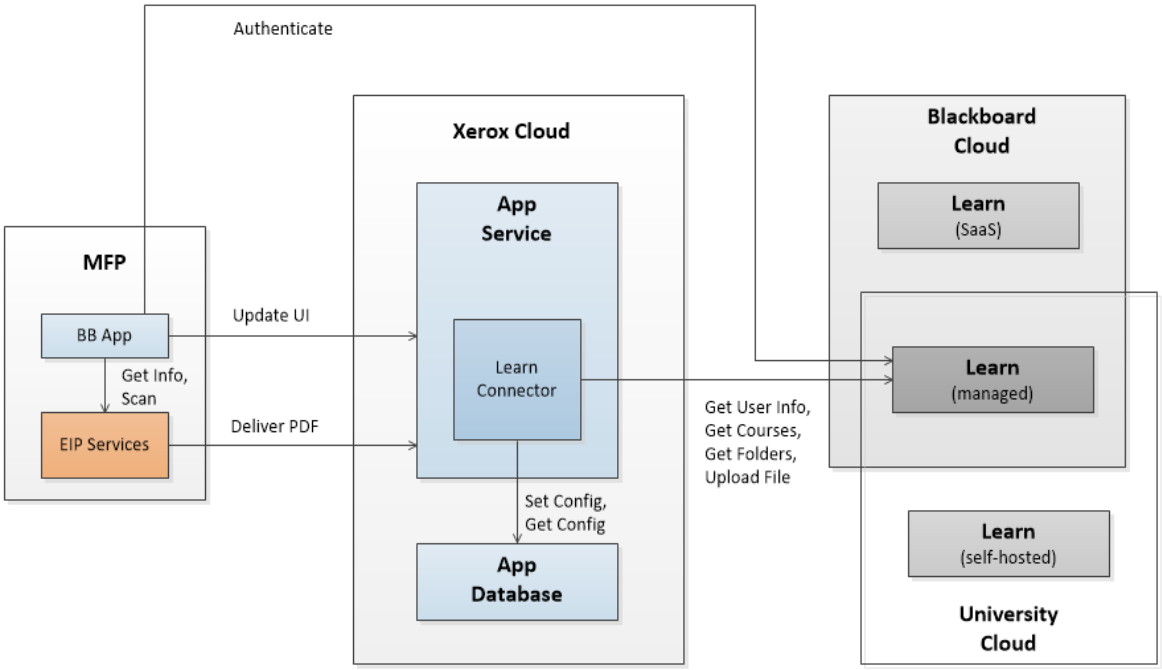
The Xerox® BB app requires the device to have Internet connectivity through HTTPS TCP port 443.

Blackboard Learn

The Xerox® BB app requires the institution’s Learn server to have Internet connectivity through the designated HTTPS TCP port set by the device administrator during the App Setup step.

5. Diagrams

Architecture



Workflow