WHITE PAPER

How to extend modern authentication to print devices

Table of contents

Modern authentication for a modern workplace

A new way of working requires a new security posture rooted in Zero Trust principles. One that allows businesses to manage sensitive data and meet strict compliance obligations. Today, IT leaders are looking to develop consistent authentication policies across all endpoint types.

This white paper explores how to extend modern authentication to print devices using HP Authentication Suite. We will dive into what it is, how it works, the business outcomes it supports.

Estimated reading time: 10 minutes

Shifting from perimeter to endpoint

Work has changed for good. It's not just about one main office anymore – it's also about thousands of offices of one. Employees need access to systems and tools from home, the office, and everywhere in between.

Supporting a new world of work requires a shift from protecting the perimeter to protecting individual devices using a "never trust, always verify" approach – the underlying principle of Zero Trust. We must assume that anything and anyone interacting on the network is inherently untrustworthy and must follow continuous verification to gain required access.

Today, a large segment of our device fleet is printers. Advanced multi-function printers (MFPs) play a key role in critical business workflows. As powerful IoT edge compute devices, they are handling some of our most sensitive company data. The question is, how are we integrating them within our Zero Trust model to help them stay protected?

Simplified modern authentication at the printer

HP Authentication Suite is a toolkit consisting of an authentication solution and a companion mobile app that provides a consistent and secure authentication experience for print devices. It supports a Zero Trust environment through two solutions:

HP AUTHENTICATION MANAGER | HP SECURE AUTHENTICATION

HP Authentication Manager

Bringing client-controlled identity management to print devices.

HP Authentication Manager allows organizations to link to their existing identity management system (e.g., Azure Active Directory), deploy an authenticating application to the printer through the HP Workpath environment, and authenticate users using a range of multi-factor authentication (MFA) solutions.

By integrating with an existing identity management system, HP Authentication Manager helps avoid duplication of user credentials, and provides high security standards with OAuth 2, OpenID Connect, and SAML 2 protocols. This means you get the security you need and the seamless user management experience you want.

HP Authentication Manager complements existing usage of proximity cards with a smartphone app that emulates the card itself. It deploys printer-based authentication that extends past simple pins, offering true conditional MFA using authenticator apps including Microsoft Authenticator, Google Authenticator, and HP Secure Authentication.

Organizations can also define and apply rules-based or scenario-based authentication requirements to deploy a set of authentication methods or combinations supporting badge/card replacement, conditional step-up authentication, strong knowledge factor, biometrics, FaceID, and tokens.

HP Secure Authentication

Enabling a modern authentication experience through a mobile authenticator app.

HP Secure Authentication emulates a Bluetooth proximity card or supports reader-less environments by allowing users to login using a QR Code through HP Authentication Manager.

Users can securely log into physical devices as well as all digital sites and services using just their smartphone, which replaces the need for expensive proximity cards and card reader hardware. They can also self-manage their authenticator and account for turnkey deployment and management.

Combined with the HP Authentication Manager, HP Secure Authentication lets you control user registration and authentication, supporting Single Sign-On (SSO) through OpenID Connect and SAML 2 tokens.

HP Secure Authentication app is available on both Google Play and Apple App Store.

How it works

Working with HP Authentication Manager is a seamless experience for users that's enabled by three stages.

Stage One:

LINKING TO THE ORGANIZATION'S IDENTITY MANAGEMENT SYSTEM

The organization first completes the application registration process. This enables HP Authentication Manager to communicate with their existing identity management system (e.g., Azure Active Directory), and confirm only active company users are permitted.

Further, the authorization tokens and MFA requirements used to log into the MFP, and other applications on the printer, are generated and managed through the organization's identity management system.

Stage Two:

REGISTERING USERS TO START THEIR SESSION

1. Users tap on a proximity reader with a card or capture the on-screen QR code using a smartphone.
2. Users are prompted to verify their identity by logging on with their existing identity management system.
3. If MFA is enabled, it will be integrated during the verification process.
4. Users link their MFA to their account.

Stage Three:

AUTHENTICATING USERS WHO ARE ALREADY LOGGED IN

1. Users tap on a proximity reader with a card or capture the on-screen QR code using a smartphone.
2. Physical tokens are referenced in the User Management console and rules of authentication are applied.
3. The necessary authentication prompts are presented, and the user authenticates to the printer. It is highly recommended to enable passwordless flow for the most user-friendly experience.

The main goal of the HP Authentication Manager is to authenticate a person to the printer and enable other applications on the MFP to login seamlessly using tokens generated and managed by the organization's identity management system.

In most scenarios, the printer users must be present at the printer and be authenticated within the network. Corporate users might have an RFID card, while small and mid-sized business customers may have a passcode, secret key, smartphone, username and password, or other authenticators.

While there are many methods, the goal of HP Authentication Manager is to facilitate the organization's workflow with minimal change when authenticating to the printer.

Bring modern authentication to your print devices

1

MODERNIZE IDENTITY MANAGEMENT AND SECURE ACCESS

Embrace mobile-driven authentication flows, eliminating the need for RFID cards or readers while helping to provide a secure and convenient experience for users.

2

STREAMLINE AUTHENTICATION EXPERIENCES

Implement a consistent authentication policy and robust security controls for a unified experience for the user across PCs and print devices.

3

MAINTAIN DATA PRIVACY, CONTROL, AND COMPLIANCE

Take control of authentication at the device level while enhancing your compliance posture with the flexibility to self-host the platform.

If you're ready to protect your endpoint devices with complete control, contact your HP representative about HP Authentication Suite today.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

©Copyright 2023 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

c08679508, June 2023