YubiKeys for Azure AD Passwordless Post Deployment

Introduction

The purpose of this document is to serve as a post-deployment checklist to validate all the settings in the “YubiKeys For Azure AD Passwordless Admin Deployment Guide” have been implemented to enable passwordless authentication in an Azure AD environment using a YubiKey. This document assumes you have met all the requirements in the pre-deployment.

Post Deployment Checklist

General Requirements	✓
Created a FIDO2 User Group	
Ensure combined security information registration is enabled for test user group	
Enabled FIDO2 Security Key Setting as an authentication method policy for test user group	
(OPTIONAL) If key restriction is enabled, YubiKey AAGUIDs are allowed	

Requirements for Azure domain joined only Windows 10 Login		✓
Enabled passwordless (FIDO2) security key sign-in into Windows 10 machines via **one** of the following options:		
	Created and installed provisioning package on Windows 10 machine	
	Enabled security key login for Windows 10 devices managed by Intune	
	Created and deployed a group policy object for Windows 10 devices	

Requirements for SSO into on-premise resources and hybrid Azure AD joined Windows 10 Login		✓
Configured an Azure AD kerberos server object on the Azure AD Connect server		
Enabled passwordless (FIDO2) security key sign-in into Windows 10 machines via **one** of the following options:		
	Created and installed provisioning package on Windows 10 machine	
	Enabled security key login for Windows 10 devices managed by Intune	

	Created and deployed a group policy object for Windows 10 devices	

References

1. https://support.yubico.com/hc/en-us/articles/360016913619
2. **Microsoft - Passwordless authentication options for Azure Active Directory:** https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key