



Kinect Sign for Cloud Environments

System Requirements

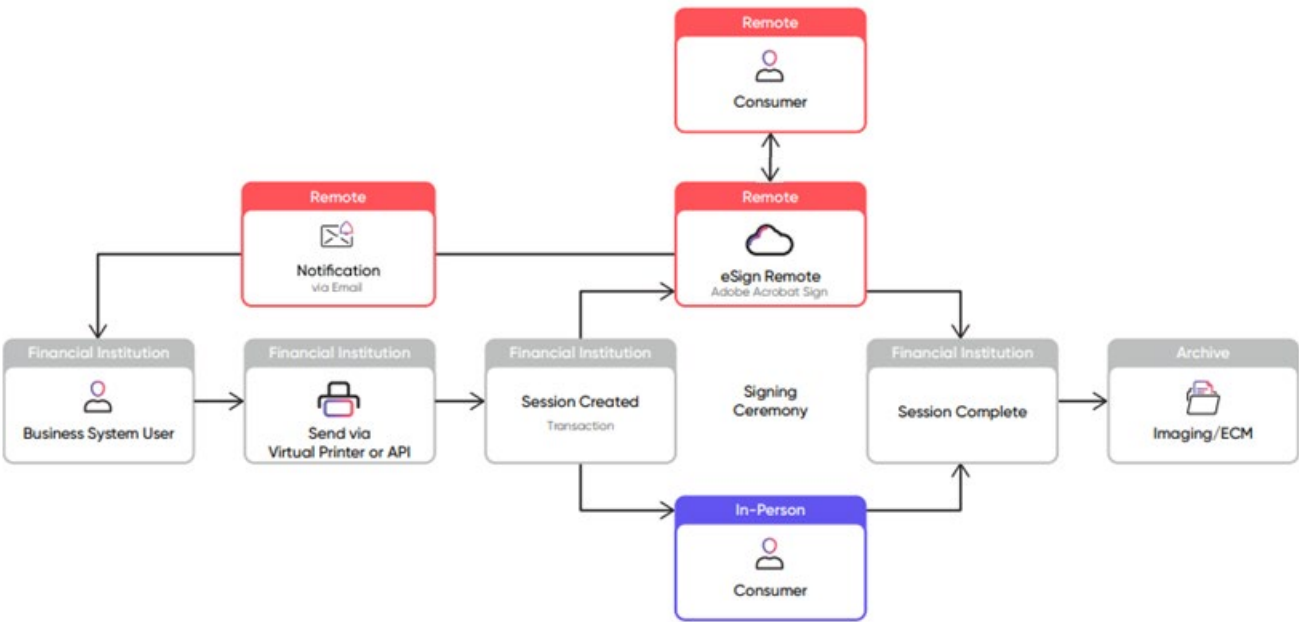
Overview

Kinect Sign is an eSignature platform used to power millions of “end-to-end” electronic transactions every month. Interfacing with virtually every business system used by financial institutions today, Kinect provides an easy-to-use eSignature experience for customers, while significantly transforming internal business processes and the way transactions flow across the institution. In addition, institutions can take advantage of SignPlus to get the same front-end eSignature capabilities as Sign, plus a business rules-based workflow engine.

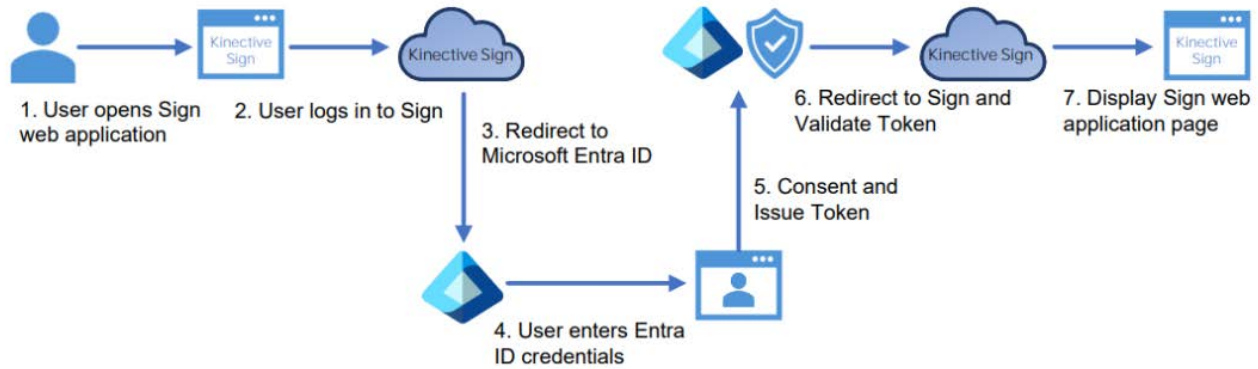
The Kinect Sign cloud service is fully managed by Kinect and runs on the Microsoft Azure platform as a Software as a Service (SaaS) solution to ensure scalability, security, and reduced management overhead for institutions. The utilization of Microsoft Entra ID (formerly Microsoft Azure Active Directory) provides centralized identity and access management, which streamlines user authentication and enhances security across systems. Microsoft Entra ID is a prerequisite for the Sign cloud environment and must be purchased separately.

Flow

Session Workflow



User Authentication with Microsoft Entra ID



Microsoft Entra ID

Requirements^{1,2,3}

- Microsoft Entra ID is a prerequisite for Kinect Sign cloud environments. Microsoft Entra ID is formerly known as Microsoft Azure Active Directory.
- Institutions are responsible for purchasing and managing their own Microsoft Entra ID account.
- Microsoft Entra ID premium licensing tiers (P1 and P2) and Microsoft Entra ID Free are supported.

Configuration

- This information must be provided by the institution:
 - Domain name associated with the institution's Microsoft Entra ID account
 - Email address of the institution's Microsoft Entra ID global administrator
- Multiple domains within a single Microsoft Entra ID account are supported.

Integration

- Kinect Sign integrates with Microsoft Entra ID using Microsoft Graph API to securely manage user identity and access.
- Before an institution can use Kinect Sign's cloud environment, Kinect sends a consent request to the institution's global administrator. This step ensures that Kinect Sign has the required permissions to perform secure authentication and access management while maintaining compliance with Microsoft's identity management protocols.
 - The consent request includes two Microsoft links: one link for Kinect Sign and one link for Kinect Sign client applications. The global administrator must click both links and accept the requested permissions to allow Kinect Sign to connect to the institution's Microsoft Entra ID account.
 - Once the institution's global administrator approves the consent request, only users within the institution's authorized domain are permitted to access Kinect Sign.

Data Security

- Kinect Sign receives access to basic user profile information, such as email address, manager, and user groups.
- Kinect Sign does not receive passwords or sensitive data from Microsoft.

1. For details about Microsoft Entra ID, refer to Microsoft's website: <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id>.
2. Institutions without a Microsoft Entra ID account should consult Microsoft Entra Plans and Pricing and contact Microsoft for any additional details: <https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing>.
3. Institutions interested in managing a Microsoft Entra ID Free account should request the Microsoft Entra ID Free reference guide from their Kinect representative.



Workstation Requirements

Hardware	General	• Intel Dual Core 3.0GHz, 4GB RAM • 20GB+ free disk space • Display resolution 1280 x 960 minimum
	Connectivity	• Sign Cloud Server
	Signing Devices^{1, 2, 3}	• iPad (iOS 14 or newer)⁴ • Topaz GemView Devices⁵ • Topaz LCD Signature Pads • Wacom Devices⁵ • Windows Touch-Enabled Devices (Windows Pro Tablets)
	Attachment Scanning	• ScanShell 3100D • Canon P-215/P-215 II • TWAIN scanner drivers are supported. Financial institutions are responsible for testing.
	Supported Cameras^{6, 7}	• Microsoft LifeCam • Built-In Cameras supported by Windows
Supported OS		• Windows 11 and Windows 10 (Professional or Enterprise)
Supported Web Browsers		• Google Chrome⁸ • Microsoft Edge⁸ • Mozilla Firefox⁸ • Internet Explorer mode in Microsoft Edge (Supported, Not Recommended)⁹
Software		• Net Framework 4.7.1 or later • Adobe Acrobat Reader is required for Internet Explorer mode in Microsoft Edge. • For all other web browsers, Adobe Acrobat Reader is not required.

1. For hardware inquiries and purchases, please contact your Kinective representative.
2. For Topaz devices, refer to the Topaz SigPlusExtLite User Installation Guide: https://www.topazsystems.com/software/SigPlusExtLite_UserInstall.pdf. For silent installations, refer to <https://www.topazsystems.com/silentinstallerform.html>.
3. Refer to the Adobe Acrobat Sign system requirements for details about remote signer requirements: <https://helpx.adobe.com/sign/system-requirements.html>.
4. iPads must be configured and fully functional on the institution's network before use. Sign is supported with the mobile browser experience only.
5. Recommended for the best consumer experience. Not supported on thin client configurations.
6. To use a camera with Google Chrome, Microsoft Edge, or Mozilla Firefox web browsers, HTTPS is required.
7. Other cameras may work. Financial institutions are responsible for testing.
8. Consult your Kinective representative to determine if there are any additional requirements for your integration.
9. Photos are not supported with Internet Explorer mode in Microsoft Edge.



Supported Thin Client Configurations

Citrix Virtual Apps and Desktops (XenApp and XenDesktop)	Server Citrix Virtual Apps and Desktops 7 2203
	Client - Via RDP: Thick client or WYSE Terminal running Windows Embedded OS Terminals - Via Citrix Receiver: Thick client or WYSE Terminal running Windows Embedded OS Terminals (Desktop sharing only) - Citrix Receiver on either thick client or XenDesktop device - Signatures supported with Citrix or Windows CDS (Citrix Device Service) only
VMware Horizon (VDI)	Server VMware Horizon 8 2203
	Client VMware Horizon on either thick client or a VMware Horizon device
Remote Desktop Services	Server Windows Server 2016, 2019, or 2022 (64-Bit) host configured for Terminal Services
	Client Thick client via RDP or any WYSE device running Windows Embedded OS Terminals



Ad Hoc Downloader Requirements

Ad hoc documents are documents sent directly from the Adobe Acrobat Sign application for remote signatures without using Kinective Sign. The Standalone Ad Hoc Downloader tool downloads the signed documents from Adobe Acrobat Sign (ad hoc documents) to a network location at the financial institution. If using the Standalone Ad Hoc Downloader, a dedicated server is required with SQL Server installed.

Note: As of Sign 23.1, the Standalone Ad Hoc Downloader is no longer required for web forms.

Dedicated Environment	A dedicated Windows Server (2016, 2019, or 2022)
SQL Server	SQL Server Standard or Express 2016 SP2, 2017, 2019, or 2022
Memory	4 CPU, 8GB RAM

Imaging Index Service Client

The Imaging Index Service Client is a component that downloads archived documents from Kinective Sign to the institution's Enterprise Content Management (ECM) system (also known as imaging system). The Imaging Index Service Client generates the required metadata for the ECM system. The Imaging Index Service Client is necessary based on the integration of Kinective Sign and the ECM system. Your Kinective representative will review the integration options to determine if this component is applicable to you.

Installation	- Institutions can download the Imaging Index Service Client from the Archive tab on the General Settings page in Kinective Sign. - Install on a workstation or server as discussed with your Kinective representative. - The eSign Imaging Client scheduled task will be created where the Imaging Index Service Client is installed. This task will download documents and perform indexing. - Imaging Index Service Client securely connects via HTTPS to Kinective Sign using an institution-specific token.
Configuration	Configure index fields and imaging system settings from the Imaging System Settings page in Kinective Sign as directed by your Kinective representative.
Software	.NET Framework 4.6.2 or higher is required on the workstation or server where the Imaging Index Service Client is installed.
Implementation	For additional information, refer to Kinective Sign online help.