

WhitePaper Azure



Datum: 12. März 2025

Dokument: D#90856.DE

Version: V2025.01.00

Copyright © by CodX Software AG, 6330 Cham (Schweiz)
Die Vervielfältigung oder Übersetzung, auch auszugsweise, ist ohne Genehmigung der CodX Software AG nicht gestattet. Alle Rechte nach dem Urheberrechtsgesetz bleiben der CodX Software AG vorbehalten.

Die Informationen und Abbildungen entsprechen der oben bezeichneten Version. Die CodX Software AG behält sich das Recht vor, Änderungen an den Angaben und Abbildungen in diesem Handbuch vorzunehmen.

CodX Software AG
Sinserstrasse 47
6330 Cham
Switzerland

+41 41 798 11 22
info@codx.ch
www.codx.ch

WhitePaper Azure

[Azure WhitePaper]

1. WhitePaper Azure

#SaaS #Azure

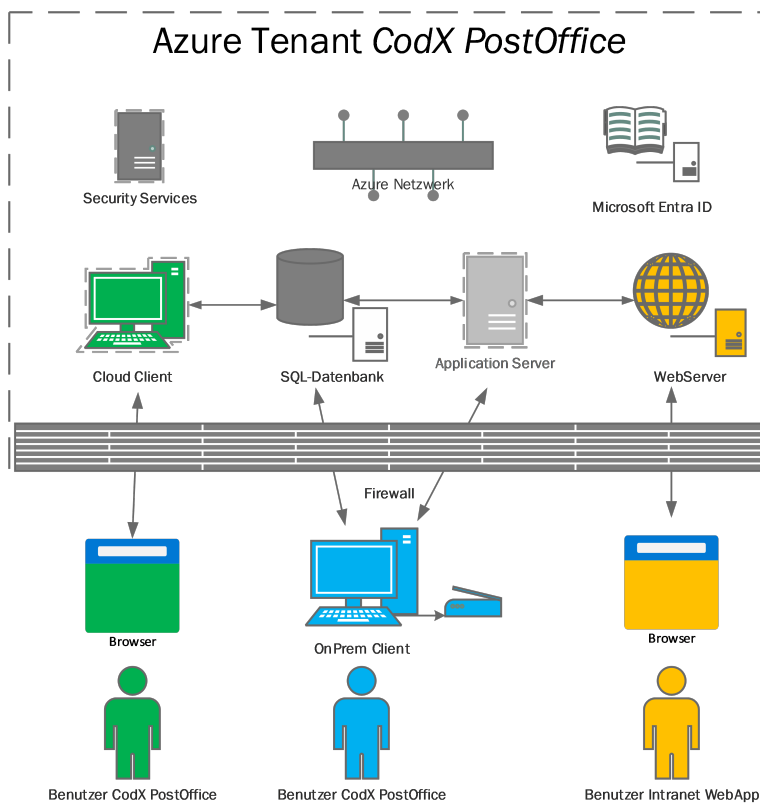
CodX PostOffice besteht aus verschiedenen Komponenten, welche im Azure-Umfeld in unterschiedlichen Konstellationen betrieben werden können.

Je nach Anwendungsfall und Datenmenge sind unterschiedliche Konstellationen möglich. Nachfolgend werden die Konstellationen nach Komponenten und typische Konstellationen beschrieben.

1.1. Azure Tenant

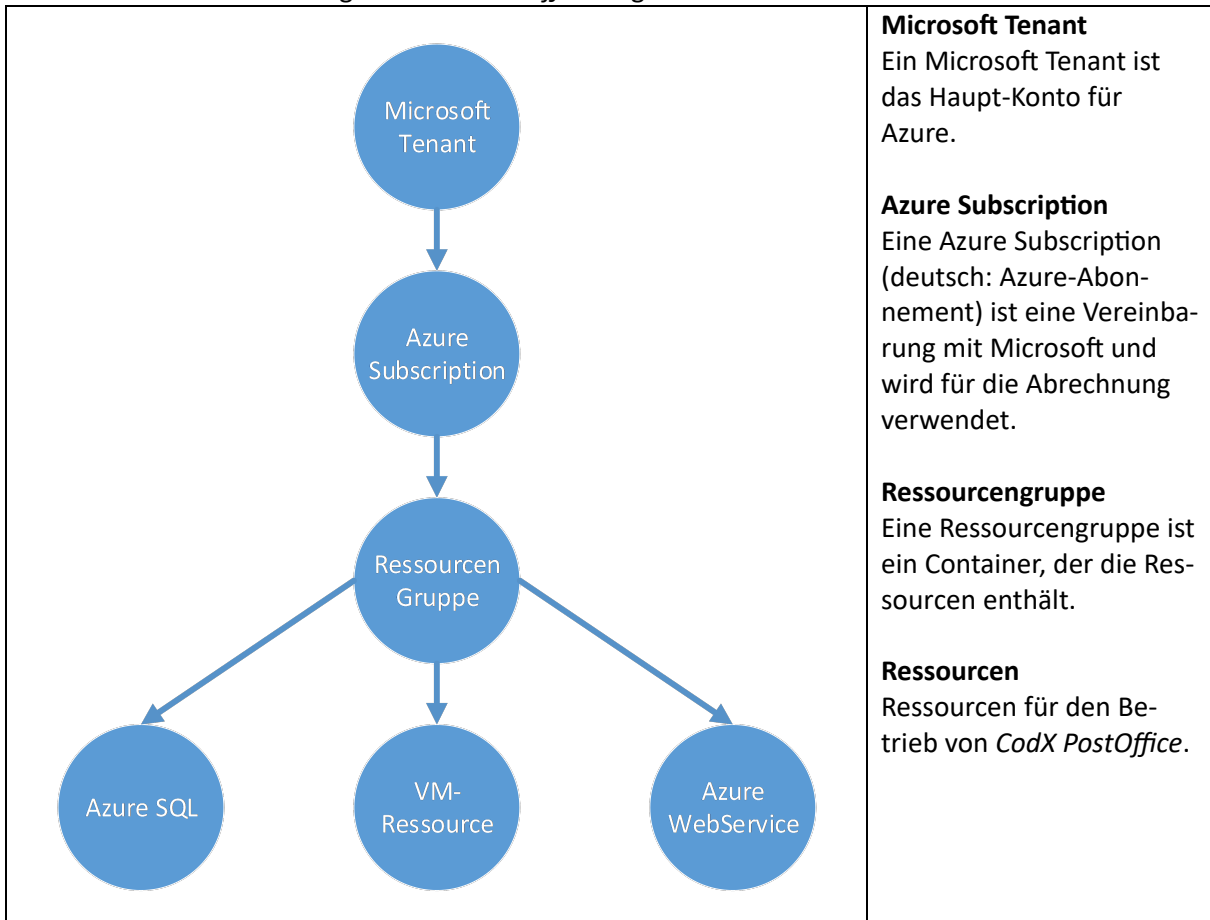
CodX PostOffice kann in einem Azure Tenant betrieben werden. Dabei kommen unterschiedliche Ressourcen von Azure zum Einsatz.

1.1.1. Architektur



1.1.2. Struktur Azure

Azure hat im Zusammenhang mit *CodX PostOffice* folgende Struktur:



1.1.2.1. Microsoft Tenant

Ein Microsoft Tenant ist das Haupt-Konto für Azure. Er stellt die logische Einheit dar, unter der die Benutzer, Anwendungen, Lizenzen und Daten einer Organisation zusammengefasst und verwaltet werden.

Für *CodX PostOffice* wird für jede Kundeninstallation eine separate Tenant eingerichtet. Im Spezialfall kann auch eine bestehende Tenant des Kunden eingesetzt werden.

1.1.2.2. Azure Subscription

Eine Azure Subscription (deutsch: Azure-Abonnement) ist eine Vereinbarung mit Microsoft zur Verwendung der Cloud-Plattformen oder -dienste, die für die Bereitstellung, Steuerung und Abrechnung verwendet wird.

Im Zusammenhang mit dem Hosting von *CodX PostOffice* wird nur eine einzige Azure-Subscription eingesetzt.

1.1.2.3. Ressourcengruppe

Eine Ressourcengruppe ist ein Container, der verwandte Ressourcen für eine Azure-Lösung enthält. Für das Hosting von *CodX PostOffice* wird nur eine Ressourcengruppe eingesetzt.



1.1.2.4. Azure SQL

Die Datenbanken von *CodX PostOffice* werden in Azure SQL installiert. Azure SQL ist ein Dienst von Azure und baut auf der SQL Server-Engine auf.

1.1.2.5. Azure VM

Für den Betrieb von *CodX PostOffice* kommen eine oder mehrere Azure VMs zum Einsatz. Auf einer dedizierten VM wird der Application Server von *CodX PostOffice* betrieben. Weitere VMs können als *Cloud Clients* betrieben werden.

1.1.2.6. Microsoft Entra ID

Für die Identifikation und Anmeldung wird für jede Azure Tenant *Microsoft Entra ID* eingesetzt. Entra ID wird verwendet, um die Ressourcen zu verwalten und zu schützen. Im Entra ID werden auch die Azure-Benutzer (named User) für *CodX PostOffice* eingerichtet.

1.1.2.7. Azure WebService

Die *Intranet WebApp* von *CodX PostOffice* wird auf einem Azure Web Service betrieben.

1.1.2.8. Azure Virtual Network

Azure Virtual Network ist ein Dienst, der den Grundbaustein für das private Netzwerk in Azure bereitstellt. Eine Instanz des Diensts (ein virtuelles Netzwerk) ermöglicht zahlreichen Azure-Ressourcentypen die sichere Kommunikation untereinander sowie mit dem Internet. Zu diesen Azure-Ressourcen gehören virtuelle Computer (VMs), Datenbank, usw.

1.1.2.9. Security Services

Zum Schutz und Überwachung der Ressourcen kommen diverse Services und Tools zum Einsatz. Das Kernstück bildet *Microsoft Defender for Cloud*. *Microsoft Defender for Cloud* ist eine cloudnative Anwendungsschutzplattform (Cloud-Native Application Protection Platform, CNAPP) mit einer Reihe von Sicherheitsmassnahmen und -methoden, die zum Schutz von cloudbasierten Anwendungen vor verschiedenen Cyberbedrohungen und Sicherheitsrisiken entwickelt wurden. Diese wird mit diversen Tools für die automatische Überwachung der Ressourcen ergänzt.

1.2. Datenbank

CodX PostOffice nutzt drei Datenbanken: *PostOffice*, *Image*, *Archiv*
Diese Datenbanken werden auf Azure SQL installiert.

1.2.1. Typische Konfiguration Azure SQL

Azure SQL kann je nach Anwendung entsprechend konfiguriert werden. Nachfolgend wird die empfohlene Standard-Konfiguration beschrieben:

Region:	Switzerland North (für Schweizer Kunden) Deutschland, Westen-Mitte (für deutsche Kunden)
Typ:	Elastischer Pool
Kaufmodell:	Virtueller Kern
Diensttarif:	Allgemein
Hardwaretyp:	Standard-Serie (Gen5)
Instanz:	2 virtuelle Kerne
Redundanz:	LRS
Zugang:	Im Normalfall private; Wenn OnPrem-Clients vorhanden, dann public



Backup:	PITR Standard; Kein LTR
---------	-------------------------

Die obenstehenden Konfigurationen können selbstverständlich auf die entsprechenden Bedürfnisse angepasst werden.

1.2.2. Backup

Datenbanksicherungen sind ein wesentlicher Bestandteil jeder Strategie für Geschäftskontinuität und Notfallwiederherstellung. Diese Sicherungen ermöglichen die Wiederherstellung der Datenbank bis zu einem bestimmten Zeitpunkt innerhalb der konfigurierten Beibehaltungsdauer.

Die Sicherungen von Azure SQL Datenbanken werden in kurzfristige (PITR) und langfristige (LTR) Sicherungen unterschieden.

1.2.2.1. Kurzfristige Sicherung (PITR)

Die kurzfristigen Sicherungen erfolgen automatisch und werden standardmässig für 7 Tage aufbewahrt. Dabei wird jede Woche eine vollständige Sicherung vorgenommen, alle 24 oder 12 Stunden eine differenzielle und bei Bedarf Transaktionsprotokollsicherungen etwa alle 10 Minuten. Die exakte Häufigkeit von Transaktionsprotokollsicherungen basiert auf der Compute-Grösse und dem Umfang der Datenbankaktivität.

Die Wiederherstellung erfolgt via Azure Portal, Azure CLI oder Azure PowerShell.

1.2.2.2. Langfristige Sicherung (LTR)

Wenn es gemäss Ihren Sicherheitsregeln erforderlich ist, dass Sicherungen über einen längeren Zeitraum verfügbar sind (bis zu 10 Jahre), können Sie sowohl für die Datenbanken die Langzeitaufbewahrung (LTR) konfigurieren.

Die langfristigen Sicherungen erfolgen in einen Speicher-Blob und verursachen dadurch weitere Kosten.

1.3. Application Server

Auf dem Application Server wird insbesondere der Service von *CodX PostOffice* betrieben. Der Service übernimmt alle Hintergrund-Prozesse von *CodX PostOffice*. Zudem ist der Service für die Konfiguration der Clients zuständig (Startup).

Der Service von *CodX PostOffice* auf einer dedizierten Azure VM betrieben. Dazu wird *CodX PostOffice* sowohl als Service, wie auch als Desktop-Applikation installiert.

Die Desktop-Applikation dient ausschliesslich für die Administration von *CodX PostOffice* und wird nicht von Benutzern von *CodX PostOffice* genutzt.

Der Zugriff auf den Application Server erfolgt über RDP. Dazu wird das Administratoren-Account der entsprechenden VM verwendet.

1.3.1. Typische Konfiguration VM für Application Server

Die VM für den Application Server kann je nach Anwendung entsprechend konfiguriert werden. Nachfolgend wird die empfohlene Standard-Konfiguration beschrieben:

Region:	Switzerland North (für Schweizer Kunden) Deutschland, Westen-Mitte (für deutsche Kunden)
Betriebssystem:	Windows 11
Typ:	Nur Betriebssystem



Tarif:	Standard
Kategorie:	Allgemein
Instanz:	A4 v2 4 Kerne; 8 GB RAM 40 GB temp. Speicher

1.3.1.1. Managed Disks

Tarif:	SSD Standard
Redundanz:	LRS
Grösse:	E15: 256 GB

1.4. Intranet WebApp

Die *Intranet WebApp* ist eine Komponente von *CodX PostOffice* für den Zugriff für Mitarbeiter auf ausgewählte Funktionen von *CodX PostOffice*.

Betrieben wird die *Intranet WebApp* auf dem *Azure Web Service*.

1.4.1. Typische Konfiguration Azure Web Service

Der Azure Web Service kann je nach Anwendung entsprechend konfiguriert werden. Nachfolgend wird die empfohlene Standard-Konfiguration beschrieben:

Region:	Switzerland North (für Schweizer Kunden) Deutschland, Westen-Mitte (für deutsche Kunden)
Betriebssystem:	Windows
Tarif:	Standard
Instanz:	S2: 2 Kerne, 3.5 GB RAM 50 GB Speicher

1.5. Client-Stationen

Die Benutzer arbeiten mit den Client-Stationen mit *CodX PostOffice*. Auf den Client-Stationen ist *CodX PostOffice* als Desktop-Version installiert. Je nach Einsatzgebiet kommt auch ein Service von *CodX PostOffice* zum Einsatz.

Es wird zwischen *Cloud Clients* und *OnPrem Clients* unterschieden.

1.5.1. Cloud Clients

Cloud Clients sind VMs, welche im Azure Tenant eingerichtet sind. Die Cloud Clients sind somit eine Ressource im Azure Tenant und unterliegen somit den entsprechenden Gegebenheiten bezüglich Management, Zugriff und Kosten.

Auf den entsprechenden VMs ist *CodX PostOffice* installiert. Damit steht praktisch der gesamte Funktionsumfang von *CodX PostOffice* zur Verfügung.

1.5.1.1. Zugriff auf Cloud Clients

Der Zugriff der Benutzer auf die Cloud Clients erfolgt wahlweise über AvD oder über einen Browser

Der Zugriff ist nur für Benutzer möglich, welche im Entra ID erfasst sind. Somit ist für den Zugriff auf die Cloud Clients auch ein entsprechender Azure-Benutzer notwendig.



1.5.1.2. Unterstützung von Hardware

Folgende Hardware von *CodX PostOffice* können mit Cloud Clients verwendet werden:

- Handscanner (Wedge)
- Labeldrucker

Unter Umständen müssen entsprechende Einstellungen vorgenommen und Treiber installiert werden.

1.5.1.3. Sicherheit

Die Cloud Clients werden so konfiguriert, dass der Betrieb von *CodX PostOffice* sicher betrieben werden kann und durch die Security Services geschützt und überwacht.

Allfällige Funktionen und Konfigurationen von Windows, welche nicht zwingend für den Betrieb von *CodX PostOffice* notwendig sind, werden deinstalliert oder gesperrt.

1.5.1.4. Typische Konfiguration VM für Cloud Client

Die VM für die Cloud Clients kann je nach Anwendung entsprechend konfiguriert werden. Nachfolgend wird die empfohlene Standard-Konfiguration beschrieben.

Die Leistungsfähigkeit der VMs ist abhängig von der Anzahl Benutzer, welche gleichzeitig auf *CodX PostOffice* zugreifen.

1.5.1.4.1. VM für 2 Sessions

Die empfohlene Konfiguration für eine VM für maximal gleichzeitige 2 Sessions sieht wie folgt aus:

Region:	Switzerland North (für Schweizer Kunden) Deutschland, Westen-Mitte (für deutsche Kunden)
Betriebssystem:	Windows 10/11
Typ:	Nur Betriebssystem
Tarif:	Standard
Kategorie:	Allgemein
Instanz:	A4 v2 4 Kerne; 8 GB RAM 40 GB temp. Speicher

1.5.1.4.2. Managed Disks

Tarif:	SSD Standard
Redundanz:	LRS
Grösse:	E15: 256 GB

1.5.1.4.3. VM für 5 Sessions

Die empfohlene Konfiguration für eine VM für maximal gleichzeitige 5 Sessions sieht wie folgt aus:

Region:	Switzerland North (für Schweizer Kunden) Deutschland, Westen-Mitte (für deutsche Kunden)
Betriebssystem:	Windows 10/11
Typ:	Nur Betriebssystem
Tarif:	Standard
Kategorie:	Allgemein
Instanz:	A8 v2 4 Kerne; 16 GB RAM 40 GB temp. Speicher



1.5.1.4.4. Managed Disks

Tarif:	SSD Standard
Redundanz:	LRS
Grösse:	E20: 512 GB

1.5.1.4.5. VM für 10 Sessions

Die empfohlene Konfiguration für eine VM für maximal gleichzeitige 10 Sessions sieht wie folgt aus:

Region:	Switzerland North (für Schweizer Kunden) Deutschland, Westen-Mitte (für deutsche Kunden)
Betriebssystem:	Windows 10/11
Typ:	Nur Betriebssystem
Tarif:	Standard
Kategorie:	Allgemein
Instanz:	A8m v2 8 Kerne; 64 GB RAM 40 GB temp. Speicher

1.5.1.4.6. Managed Disks

Tarif:	SSD Standard
Redundanz:	LRS
Grösse:	E30: 1024 GB

1.5.1.5. Hostpool

Für Installationen mit sehr vielen Benutzern kann der Hostpool aktiviert werden. Der Hostpool enthält mehrere VMs, welche bei Bedarf dazugeschaltet werden können.

Die aktiven Sessions werden auf die entsprechenden VMs im Hostpool zugewiesen, damit die Last gleichmässig verteilt ist.

Der Hostpool ist standardmässig nicht aktiviert.

1.5.2. OnPrem Client

OnPrem Clients sind lokale Arbeitsstationen beim Kunden vor Ort und in seinem lokalen Netzwerk. Diese werden vorwiegend für den Einsatz mit spezifischer Hardware, wie zum Beispiel Fachanlagen, Cx-LetterScan, OCR-Stationen oder Dokumentenscanner eingesetzt.

Die OnPrem Clients sind nicht Bestandteil der Azure Tenant und somit bezüglich Management, Zugriff und Kosten unabhängig.

1.5.2.1. Verbindung zur CodX PostOffice Azure Tenant

Die Datenverbindung vom OnPrem Client zur Azure Tenant erfolgt über das Internet.

Dies erfolgt im Detail über folgende Datenverbindungen:

Datenbank:	SQL-Datenbankverbindung über Port 1433, verschlüsselt.
Application Server:	HTTPS-Verbindung
Intranet WebApp:	HTTPS-Verbindung



Wahlweise kann für diese Verbindung auch ein VPN eingerichtet werden.

Die entsprechenden Zugriffe vom OnPrem Client ins Internet müssen vom Kunden freigeschaltet werden und die Internet-Bandbreite muss für den Betrieb von *CodX PostOffice Hosting* ausgelegt sein.

1.5.2.2. VPN: Microsoft Entra Private Access

#Security

Für den sicheren Zugang von den OnPrem Clients auf die Infrastruktur von Azure, kann optional 'Microsoft Entra Private Access' eingerichtet werden.

Dazu wird auf dem OnPrem Client den 'Microsoft Entra private network connector' und 'Global Secure Access Client' installiert. Dafür muss der OnPrem Client EntraID joined sein.

Die Einrichtung und Konfiguration von Microsoft Entra Private Access erfolgt im 'Microsoft Entra Admin Center'.

1.5.2.3. Sicherheit

#Security

Für die Sicherheit der OnPrem Clients ist der Kunde grundsätzlich selbst zuständig.

1.5.2.4. Systemanforderungen

Für die OnPrem Clients gelten die normalen Systemanforderungen für *CodX PostOffice*. Diese sind in der AdminDoc unter #SystemRequirement beschrieben.

1.6. Rollen für Benutzer

Es sind verschiedene Rollen für Benutzer vorhanden. Jeder Benutzer wird einer oder mehreren Rollen zugewiesen.

Rolle	Tätigkeiten / Rechte	Bemerkungen
IT-Admin	Administration der Infrastruktur. Kann Ressourcen bearbeiten usw.	Es kann mehrere Admin-Benutzer geben. Diese sind in Entra ID angelegt.
PO-Support	Administration von <i>CodX PostOffice</i> . Admin-Rechte auf VMs	Es kann mehrere PO-Support-Benutzer geben. Diese sind in Entra ID angelegt. Die Benutzer sind insbesondere Mitarbeiter vom Support von CodX Software.
PO-User	Betreiben von <i>CodX PostOffice</i> . Eingeschränkte Benutzerrechte auf VMs Die Benutzerrechte innerhalb von <i>CodX PostOffice</i> werden in <i>CodX PostOffice</i> selbst definiert (Modul <i>Zugriffsberechtigungen</i>).	Benutzer des Kunden (Entra ID).



2. Kontakt

Kontakt	<u>www.codx.ch</u> <u>info@codx.ch</u> <u>+41 41 798 11 22</u>
Postadresse	CodX Software AG Sinslerstrasse 47 6330 Cham Schweiz
Technischer Support	<u>https://support.codx.ch</u> <u>support@codx.ch</u> <u>+41 41 798 11 44</u>

