More4apps

ERP Cloud Toolbox

Architecture, Security and Data Privacy

Created By: Steve West

Creation Date: 1 May 2020

Version: 1.7

Version Date: 8 Feb 2022

1 Table of Contents

2 Purpose

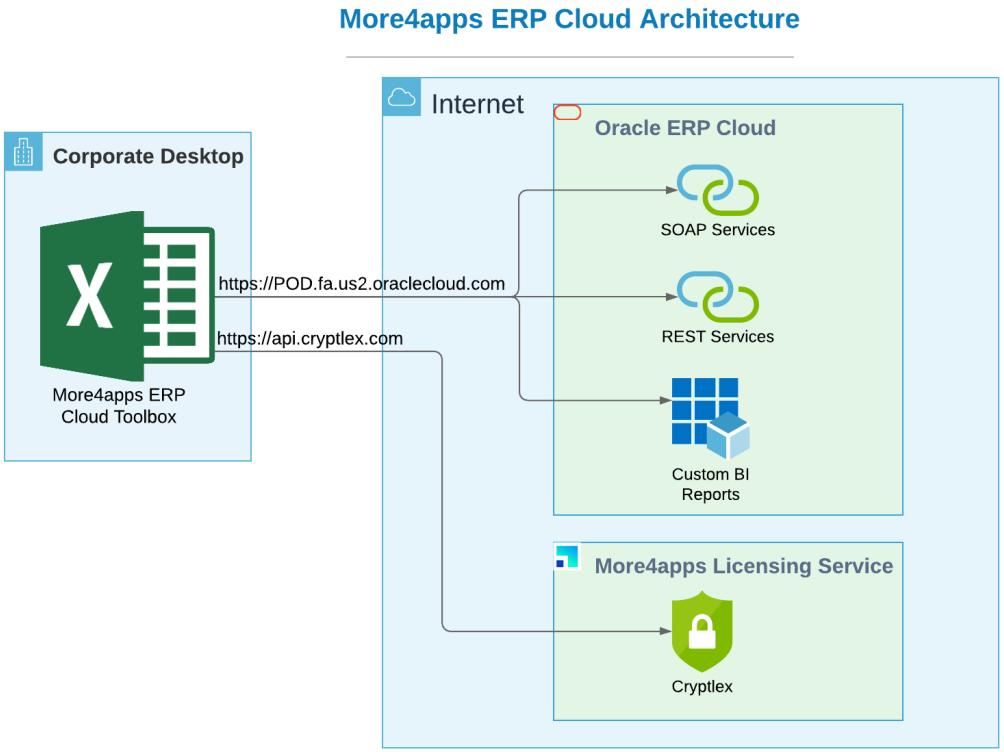
The More4apps ERP Cloud Toolbox enables end users to mass load data to Oracle ERP Cloud easily, quickly, and securely using Microsoft Excel on the desktop as the core user interface. This document describes the architecture of the products and explains the security and data privacy implications for organizations that implement our products.

3 Overview

More4apps ERP Cloud Toolbox for Excel utilizes secure Web Service communication with the Oracle ERP Cloud servers for all uploads and downloads. No additional software apart from Microsoft Excel and .Net Framework is required on the PC. There is full integration with the Oracle ERP Cloud authentication, SSO and security functionality:

- End users authenticate with their ERP Cloud username/password.
- End users cannot perform any more functions or get access to any more data than they can do through the standard Oracle ERP Cloud user interface.
- More4apps does not store, process, transmit or have access to any ERP Cloud data. The Toolbox utilizes Oracle's existing published and supported REST and SOAP Web Services to perform all uploads and downloads. This document explains the mechanics of this process.

3.1 Architecture Diagram showing Major Components



3.2 Architecture Description

- The end user authenticates to Oracle ERP Cloud from MS Excel using the standard authentication SSO login.
- The Excel template uses a .Net VSTO add-in to communicate with the REST and SOAP webservices in Oracle ERP Cloud to upload and download data (e.g.Standard Purchase Orders). Token (OAuth) authentication is used for all web service calls.
- LOVs are populated using either standard REST web services or custom BI reports.
- A call to our Licensing service (Cryptlex) is made at login to reserve a seat from the License for this instance.

4 Licensing

More4apps uses a Floating Concurrent licensing model. A License will entitle a customer to establish a maximum number of concurrent logins (Activations) to Oracle ERP Cloud from our products. An Activation lease time lasts for a minimum of 60 minutes, and a lease will expire after 60 minutes of inactivity.

5 Security

5.1 Data Encryption

All connections from Excel to the Oracle ERP Cloud web services and to the Cryptlex licensing service are encrypted by HTTPS. The encryption to Oracle ERP Cloud is managed by Oracle. The encryption to the Cryptlex licensing service is managed by Cryptlex. Both services employ TLS encryption technology with a private key of at least 2048 bits.

5.2 Authorization

The More4apps products use published Web Service API calls and as such respects all of the data and function authorization rules in Oracle ERP Cloud. End-users may have to be granted additional Roles in Oracle ERP Cloud in order to use the More4apps products.

5.3 Network access control

Oracle and the customer manage the network access between the client desktop and Oracle ERP Cloud. This connection can be a private VPN-protected connection or direct to the public Internet. The customer manages the network access to the Cryptlex server which is available on a standard HTTPS port on the public Internet.

5.4 Network Bandwidth and Latency

The customer is responsible for all internal network connections and Internet connectivity. More4apps will be responsible for ensuring the Cryptlex service is continuously available and will investigate and address any network issues.

5.5 Anti-Virus

The customer is responsible for ensuring anti-virus protection is installed on end user desktops. More4apps scans all software delivered to customers prior to making it available to minimize the risk of viruses, malware or other vulnerabilities embedded in the software.

5.6 Firewalls

Oracle and the customer are responsible for ensuring adequate firewalls are enabled on their respective networks. More4apps may require a firewall rule to be implemented by the customer to allow outbound calls to the Cryptlex web service from the end user's desktop **https://api.cryptlex.com** . There are no firewall implications between the client and Oracle ERP Cloud because the More4apps product calls standard Oracle published web services.

5.7 System Access Control and Password Management

End users authenticate with the standard Oracle ERP Cloud SSO login method. Oracle enforces security authentication and authorization rules through it's Cloud infrastructure. The customer is responsible for managing the end user credentials and password policy.
Access to the Cryptlex licensing service is verified via an encrypted API key embedded in the client software.
More4apps does not store or process any Oracle ERP Cloud passwords.

5.8 Data Management and Protection

The customer maintains control over and is responsible for the data residing in Oracle ERP Cloud. The customer is also responsible for and maintains control over the data that resides in the More4apps Excel Toolbox spreadsheets. More4apps has no direct access to any customer data and neither stores nor processes this data external to the customer infrastructure.

5.9 Security Incident Response

More4apps assumes that Oracle and the customer have their own respective Incident Response procedures if there are suspicions of unauthorized access to or handling of customer data, whether on Oracle hardware or on customer assets (desktops). More4apps is fully committed to participating in these Incident Response procedures if the threat involves the use of More4apps products or services.

5.10 System Resilience and Backups

Oracle is responsible for the resilience and availability of their ERP Cloud platform.
More4apps is responsible for the resilience and availability of the Cryptlex licensing platform.
Backups – Cryptlex is regularly backed up and mirrored and in the event of a DR situation the service can be restored within 3 minutes. There is no customer ERP data in Cryptlex, only licensing information (See Data Privacy and PII section below), therefore the impact to the customer is minimal, even if the Licensing system is completely lost. A downtime of the service will result in customer's inability to use the More4apps Excel templates until such time as the service is restored. Alternative methods of loading transactions into Oracle ERP Cloud such as the standard Oracle data entry forms would be unaffected.

5.11 Service Level Targets

Oracle's ERP Cloud availability target is 99.5%. Cryptlex (and thus, More4apps ERP Cloud Toolbox) availability target is 99.9%.

5.12 Monitoring

Oracle has comprehensive monitoring systems in place for the ERP Cloud platform. More4apps cannot directly monitor desktop Excel spreadsheets as More4apps has no access to customer environments. More4apps has processes in place to monitor the availability of the Cryptlex licensing service with alerts in place if the service experiences any issues.

5.13 Software Versioning

More4apps requires customers to keep up to date with released versions of the ERP Cloud Toolbox desktop software that match the version of Oracle ERP Cloud used by the customer. More4apps are not responsible for issues that arise from customers running versions of software that are configured for earlier or later releases of Oracle ERP Cloud.
More4apps has thorough change management procedures in place for all software development. The Release Process for More4apps's software includes comprehensive unit testing, system testing, integration testing and vulnerability testing in an automated Continuous Integration/Continuous Development (CI/CD) DevOps pipeline. Customers are notified of the availability of new releases and it is the customers responsibility to upgrade the installed software to match the Oracle ERP Cloud version. It is the customer's choice whether to upgrade to a new version if the new version is a feature or bug fix release within the same Oracle ERP Cloud version.

5.14 More4apps Support Policy

The subscription fee paid by the customer covers both use of the More4apps desktop products and support of the products for the period of the subscription. Customers visit the support site at https://more4apps.com/support. This is a 24/7 helpdesk with global coverage in all timezones. There is also a searchable database of solutions for customer self help.
Our support agreement is available here: https://more4apps.com/support

6 Data Privacy and PII (Personal Identifiable Information)

More4apps does not store any customer data on our servers other than what is collected by the licensing service for auditing and support purposes. More4apps does not store, process or transmit any ERP Cloud data outside of the client PC (Excel) and Oracle ERP Cloud.
The Licensing service (Cryptlex) stores the following attributes for every login to ERP Cloud through the More4apps Toolbox:

Required:

- Oracle ERP Cloud version
- More4apps Integrator version
- More4apps Add-in version
- Windows version
- Excel version
- BI Reports version
- Login time (Lease start time)
- Lease expiry time
  Lease last activity time
- Country
- City
- Machine name

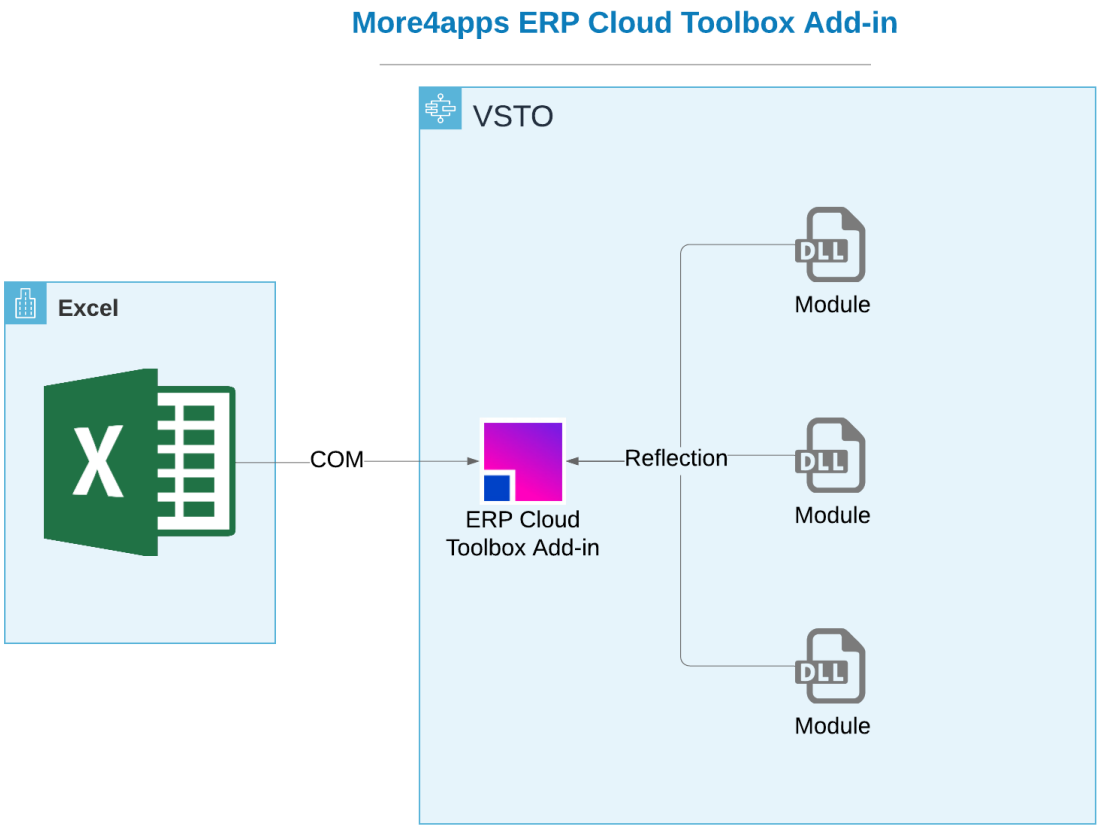
PII:

- IP address
- Oracle ERP Cloud username

These session attributes allow More4apps to better support our customers and also allows our customers to track the usage of the More4apps tools within the organization, analyze the usage of More4apps licenses, see who is using different versions of More4apps products etc. Upon request, the recording of the PII attributes can be turned off for individual licenses but organizations will lose the ability to analyze license usage down to individual users.

7 Client PC Architecture

The ERP Cloud Toolbox product is an Excel Visual Studio Tools for Office (VSTO) COM Add-in[1]. The Add-in is installed onto the client PC as the framework for hosting More4apps Modules.



7.1 Installation

- An Advanced Installer[2] setup executable is used to install the Add-in and Modules.
- Module installers check for a required Add-in version.
    - New Installation: The Add-in is downloaded and installed during the Module installation.
    - Existing Installation: The user is prompted to update the Add-in if it exists as an older version.
- The installation is user-level[3].

[1] "Office Add-ins platform overview - Microsoft Docs." 13 Feb. 2020, https://docs.microsoft.com/en-us/office/dev/add-ins/overview/office-add-ins. Accessed 12 May. 2020.
[2] "Advanced Installer." https://www.advancedinstaller.com/. Accessed 12 May. 2020.
[3] "Installation Context - Win32 apps | Microsoft ...." 31 May. 2018, https://docs.microsoft.com/en-us/windows/win32/msi/installation-context. Accessed 12 May. 2020.

    - The Add-in does not have machine-level rights and only user level registry values are created.
- Registry options are created under **HKEY_CURRENT_USER/Software/More4apps**. These are required for updates and Add-in/Module functionality.
- Registry options are created for the Add-in and per Module.
- Files are installed into a user specified location.

Once installed, the user is required to enable the Add-in via standard Microsoft mechanisms[4] .

7.2 Client Security

- The deployed Add-in code is obfuscated.
- Memory obfuscation has been implemented for runtime code.
- The Add-in is code signed via a More4apps digital signature.
    - A public key is available to add as a Trusted Publisher for Trusted Publisher enabled Excel security.
- Resources (Oracle BI Reports) have a detached GnuPGP[5] signature supplied which can be verified using the available More4apps public PGP key.
- The Add-in is compiled using Microsoft's Azure DevOps[6] CI/CD pipelines.
    - Security features are included as tasks and checks are automatically performed on new code.

7.3 Authentication Token

- The add-in calls public web services using token authentication.
- The Oracle Token Relay Service[7] is used to retrieve authentication tokens from user credentials.
    - User credentials **are not stored** within the Add-in runtime code or saved to file.
- The token is temporarily stored within memory & obfuscated until the application is closed.
- The Token Relay Service is called when the token is close to expiration, or a new session is required i.e. Excel is reopened. The expiration time is normally around 4 hours - if the token expires then the user is required to re-authenticate with ERP Cloud to obtain a new token.

---

[4] "Add or remove add-ins in Excel - Office Support." https://support.office.com/en-us/article/add-or-remove-add-ins-in-excel-0af570c4-5cf3-4fa9-9b88-403625a0b460. Accessed 12 May. 2020.

[5] "GnuPG." https://gnupg.org/. Accessed 12 May. 2020.

[6] "Azure DevOps Services | Microsoft Azure." https://azure.microsoft.com/en-gb/services/devops/. Accessed 12 May. 2020.

[7] "Configuring Client to Use Token Relay Service ... - Oracle Docs." https://docs.oracle.com/en/cloud/saas/sales-and-b2b-service/19d/fados/configuring-client-to-use-token-relay-service---sso-authentication.html. Accessed 12 May. 2020.

7.4 Modules

More4apps Modules represent the products that users interact with to perform business functions. i.e. Upload a Purchase Order or Invoice.

- Once a Module is installed with the Add-in, the Module is called via reflection and loaded into memory.
- The Module is loaded using a previously saved sheet template (which has sheet indicators) or when creating a new sheet via the New Sheet form.
- The Module uses the previously obtained authentication token to call any public web services or BI reports.