Digital Enterprise Platform

Whitepaper

unvired

Digital Delivered

unvired.com

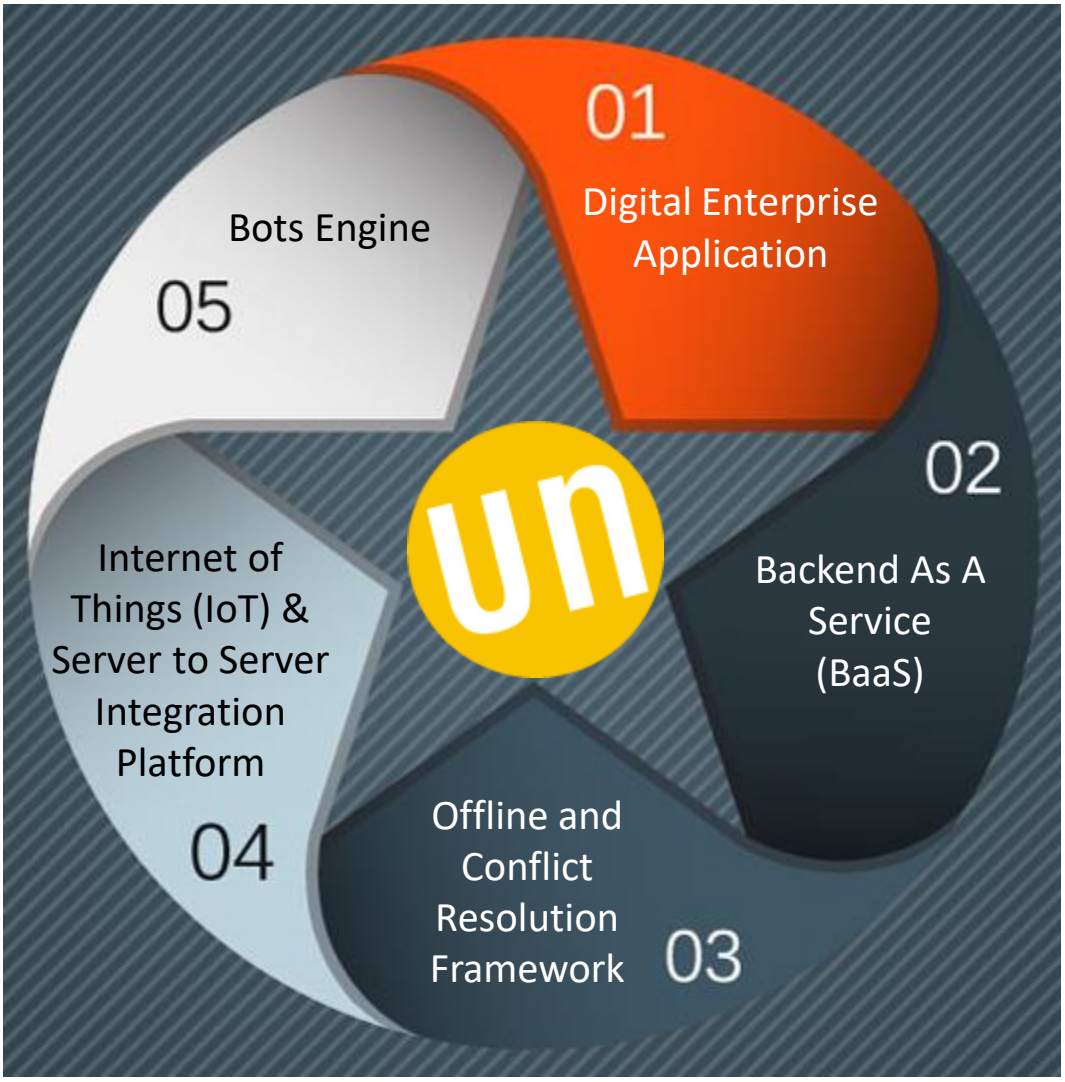
CONTENTS

CONTENTS

Overview

Digital Enterprise Platform (DEP) is a Low Code mobility, offline, digitization, and integration platform. DEP can either be used in its totality as a multi-utilitarian platform or as a specific use case platform.

The Digital Enterprise Platform helps connect business processes and data between 2 or more end systems / devices.



Use Cases

Mobile Applications

Definition:
DEP is a low code application platform that can be used to mobilize any business process from any enterprise system on any device (Android, iOS, Windows, HTML5).
Where?
A chemical manufacturing company based in Houston has used DEP to mobilize many business processes in Plant Maintenance and Warehouses on iPads. The customer uses offline mobile apps on iPads to access work orders, notifications inspection rounds, deliveries, compliance documents, and stock overview.

Digital Applications

Definition:
DEP enables digitization of documents, access to documents from anywhere (web, mobile), knowledge sharing, collaboration and data analytics helping customers convert to a Digital Enterprise. Paperless offices are a reality with DEP. Build rich HTML5 applications and deploy on web and/or mobile as hybrid apps with offline access (single code base).
Where?
Companies can digitize asset maintenance records and share them with technicians easily on mobile devices. Healthcare companies can digitize and enable secure access to healthcare records anytime anywhere. Doctors and nurses can share patient information securely and instantaneously electronically.

Backend As A Service (BaaS) or a Connector Framework

Definition:
DEP offers many enterprise connectors to systems like SAP, SharePoint, Oracle, Databases, file systems and systems based on web services. DEP works as a Backend As A Service (BaaS) to expose enterprise system data / processes as REST services to mobile and web. The REST services can contain complex business logic.

Use Cases

Contd.

BaaS continued…….Where?
A retail company based in Houston has used DEP to enable its custom retail software based on database stored procedures as REST services. The REST services expose delivery creation, inventory reconciliation, and new product addition. Schedulers in DEP are used to pick the latest changes in the product information in the retail system, and relay it to the applications that use the product information.

Offline and Conflict Resolution Framework

Definition:
DEP offers complete offline and conflict resolution framework for mobile apps. Mobile applications can use the offline functionality to store data and submit later. Mobile applications can use the conflict resolution to resolve data conflicts between enterprise systems and mobile devices.

Where?
A pharma company based in North America used DEP to build a mobile application for warehouse management with offline access and resolve conflict with goods issue.

Internet of Things (IoT) & Server to Server Integration Platform

Definition:
DEP enables data exchange between things and enterprise systems as well as between enterprise systems. DEP can be the common hub for integration across mobile devices, things, and enterprise systems.

Where?
A utilities company based in New Zealand is using DEP to integrate its GE Network Management System (NMS) with SAP ERP. The work orders that get registered in the NMS flow to SAP ERP and updates to the work orders in SAP ERP move to NMS via DEP.

Use Cases

Contd.

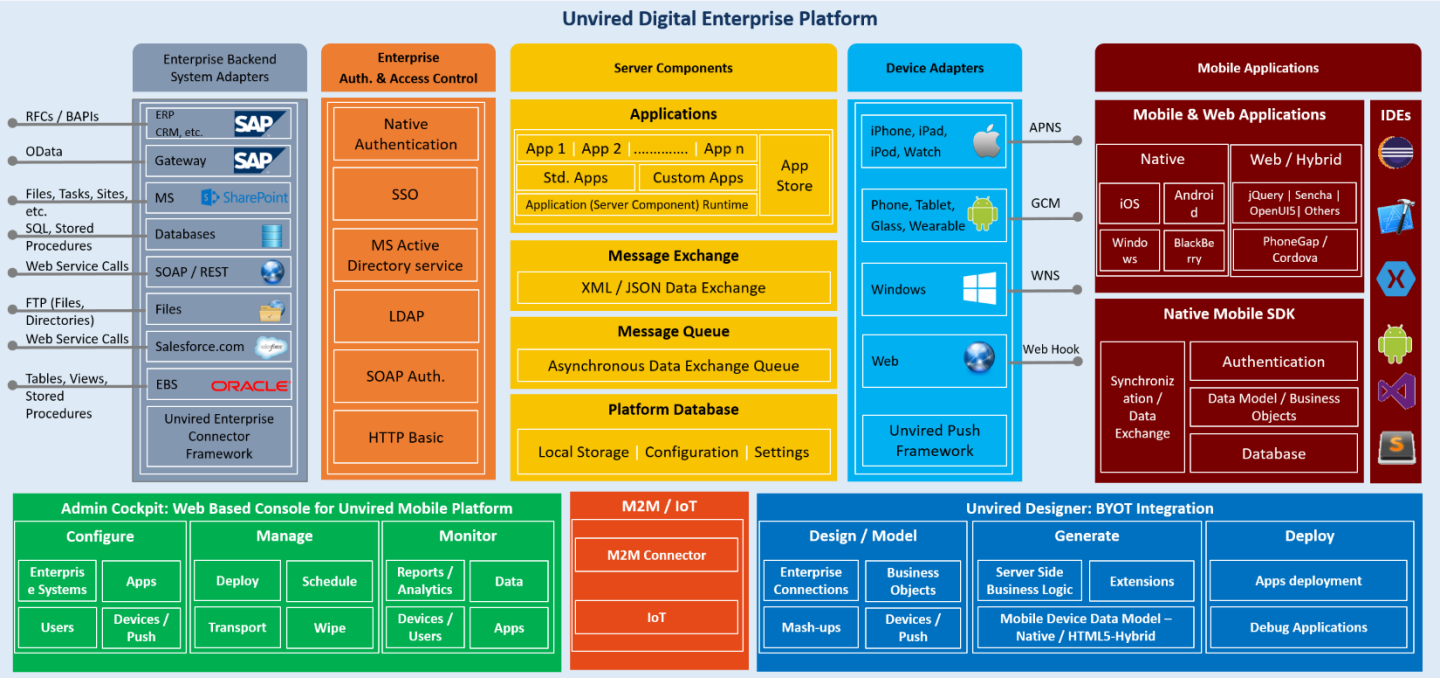
Bots for Business

Definition:
DEP offers a Bots engine that can be leveraged to orchestrate complex business logic as simple bots. Users can be alerted to External triggers or events and enabled to take instant actions.

Where?
Chyme is an Enterprise Bots and Messaging Platform that enables building Bots for Business in a simple drag and drop environment.

Visit https://chymebot.com for more details

Architecture

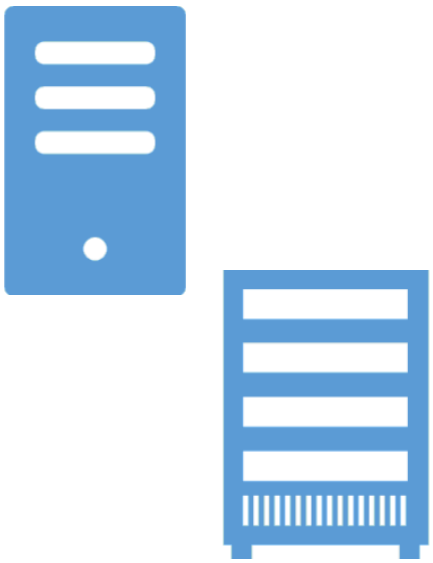


Digital Enterprise Platform – Editions

Cloud Edition

DEP runs on multiple clouds in an elastic mode (auto horizontal scaling). Customers with dynamic scaling requirements can run DEP on public cloud instances scaling them dynamically.

DEP runs on AWS, Google Compute Engine, MS Azure and IBM Cloud. DEP is also available for deployment in a Docker environment.



On-Premise Edition

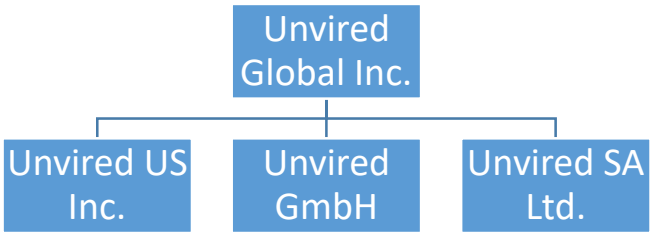
DEP runs in a controlled scaling (static instances) mode on-premise, in a data center and other software clouds. Static scaling is for customers whose peak load is predictable.

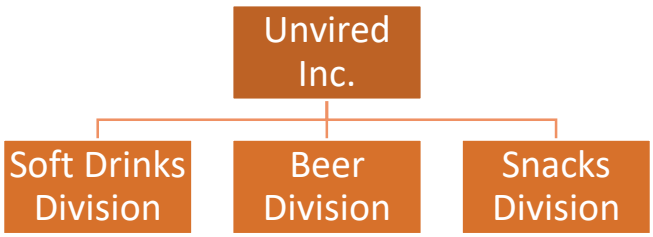
Note: On-premise edition supports high availability mode.

Centralization & Data Separation

Unvired Digital Enterprise Platform can be used as a centralized installation supporting a 2-level hierarchy for configuration and data separation. Examples:

- A global company can setup DEP as a centralized installation and configure the different regional companies as nodes of the centralized installation. Each company node can be supervised and managed separately. Data is also separated for each node.
- A company with multiple business departments can setup DEP as a centralized installation and configure the different departments as nodes of the centralized installation. Each department node can be supervised and managed separately. Data is also separated for each node.





Enterprise Connectors

Digital Enterprise Platform offers standard connectors to various enterprise systems out of the box. Unvired connectors can be either native or open based on the type of the system.

Enterprise connectivity is based on a connector framework. So connectivity can be extended to support any system in the world.

The different connectors are as follows:

SAP	SAP Gateway	MS SharePoint
Native integration with SAP. Use all SAP RFCs and BAPIs directly in DEP.	OData integration with SAP Gateway. Use OData services from SAP Gateway in the DEP.	Web service integration with Microsoft SharePoint Services to enable DMS services in DEP.

Web Services	Identity Mgmt	Database
Integration with all open systems via Web Services (both REST and SOAP).	Integrate with LDAP like Microsoft Active Directory for authentication.	Connect to any database using the database connector for direct table / view access or Stored Procedure access.

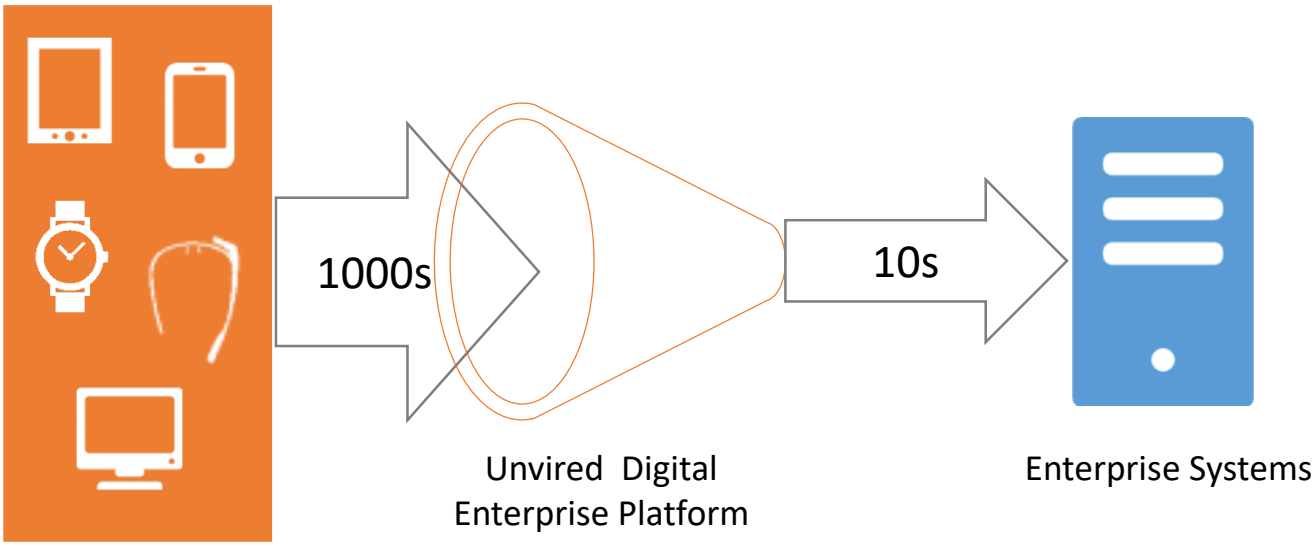
Oracle EBS	Salesforce.com	File Systems
Native integration with Oracle EBS. Use all PL SQL routines from Oracle EBS.	Integration with Salesforce.com web services (Enterprise and Partner).	File Transfer Protocol integration to access different file systems.

Enterprise Connectors

Contd.

Connection Management / Throttling

- Mobile devices in a company add additional load on the enterprise systems. Increase in mobile devices increase the load on enterprise systems. Enterprise servers cannot be scaled to handle hundreds of concurrent connections from mobile devices.
- Digital Enterprise Platform provides connection management for each enterprise system. For each system connections can be controlled and limited to a maximum number of connections.
- So for synchronous data exchange unavailability of connections will give an immediate error. For asynchronous data exchange the data is stored in the server and executed once the connections to the enterprise system becomes available.
- Connection management in DEP helps in scaling to a large number of users without stressing or resizing the enterprise systems.



Cross Platform

Digital Enterprise Platform supports all channels of access:

iPhone, iPad, Watch

Phone, Tablet, Wearables

Windows 8.+, Windows Mobile

Web

Build Once, Run Anywhere using the Unvired HTML5 / Hybrid SDK (mobile devices and web browsers alike)

Cross Platform

Contd.

App Types – Native, HTML5 / Hybrid and Web

Feature	Native Apps	HTML5 / Hybrid Apps	Web Apps
Unvired Client SDK – Manages Database, Data Model, Offline, Data Exchange, Conflict Resolution	Unvired Native SDK – Supports all Unvired Client SDK features	Unvired HTML5 SDK - Supports all Unvired Client SDK features (as good as native SDK)	Unvired Web SDK – Supports all Unvired Client SDK features with offline capability.
Cordova / PhoneGap	-	Cordova / PhoneGap – Unvired HTML5 SDK uses Cordova / PhoneGap under the hood	-
App Development	iOS - Objective C / Swift Android – Java Windows – C# .NET	JavaScript	
IDEs	Standard IDEs of each device iOS – Xcode Android – Android Studio Windows – Visual Studio	Any IDE	
User Interface	Standard for each device	Any responsive UI framework Ex: SAPUI5, OpenUI5, Bootstrap, etc.	
Database	SQLite Encrypted	SQLite Encrypted	Browser In Memory DB
Hardware Support Ex: Printer, Barcode, etc.	Whatever the device supports	Whatever Cordova / Phone Gap Supports	Whatever the browser supports
Xamarin Support	Yes. Xamarin can be used to build native apps once using C# .NET and run anywhere (on any device supported by Xamarin).	-	-

Devices

Hardware Integration

Printers, barcode readers, RFID readers, beacons and other hardware devices can be used in the mobile apps.

- For native mobile apps any supporting library from the hardware manufacturer or the operating system can be used directly in the app.
- For HTML5 / Hybrid apps hardware support is NOT restricted to PhoneGap / Cordova support. DEP's Hybrid model allows all hardware SDKs in the native layer to be exposed to the HTML5 layer. So all hardware integrations are possible.

Shared Devices

- Unvired Mobile apps can be used in a shared mode in a mobile device. If many users share a mobile device in a warehouse or a maintenance scenario (working shifts) it is possible to support multiple users to login to the app separately without affecting the data of the other users.
- All data is stored offline, preserved and available to the users when they login.
- One user's action on the device does not affect the status of the data of other users in the same app on the same device.

Application Management

Digital Enterprise Platform offers various features for application management:

- **User Management:** Manage users who are allowed to use the platform and the apps in the platform.
- **App Deployment:** Deploy applications to specific users controlling access to applications.
- **Device Enablement:** Enable applications on specific devices controlling access to applications on specific devices for users.

- **Auto and Administered Provisioning:** Deploy apps either in an administered mode to control access or enable auto provisioning based on specific checks to allow large scale deployments without any administration overhead.
- **Enterprise App Store:** Manage applications in the built-in app store and allow installations from the app store. See the section on Enterprise App Store for more details.
- **Device Tracking:** Track devices using apps on DEP to check device OS version, app version, last access date/ time, etc.
- **Location Tracking:** Switch on location tracking and track device location.
- **Remote Wipe:** Remotely wipe data in applications for specific users to protect company data in case of theft, job exit, etc.

Application Management

Enterprise AppStore

Enterprises do not want to expose internal applications on the public app store like Apple AppStore or Google Play Store. So DEP provides a built-in app store for companies to manage their applications.

- Enterprise AppStore offers the following features:
- List applications, screen shots and maintain app description to use as a catalog
- Maintain app icons for easy identification
- Maintain the app installable on the store
- Install applications from the app store on mobile devices

Security

Secure communication

All communication to the DEP server is sent over a secure HTTPS (Hypertext Transfer Protocol Secure) channel. It provides encrypted communication and secure identification of the DEP server. This is similar to the way data is exchanged between the browser and the bank website and is safe.

In addition, all credentials that are sent from mobile device are additionally encrypted (even though using https) using the Advanced Encryption Standard (AES) standard which is adopted by the US Government and is a trusted mechanism to secure data. The DEP encrypts the credentials that are exchanged using AES with 256 bits key which provides the highest security.

Each communication from the device to the DEP is further protected by a one time transaction token and ensures that transactions from trusted devices only are accepted and ensures impersonated data/transactions are not accepted by the platform.

Login to the Admin Cockpit is protected with Two-factor authentication

The DEP is administered and monitored by the Unvired Cockpit. The Unvired Cockpit can be accessed using a Secure HTTPS URL only. Further the login is protected with a two-factor authentication. This ensures that administrators need to know their password and additionally enter a one-time, time limited token to get access. The two-factor login ensures that the system cannot be accessed by unauthorized users.

Security

Contd.

Data partitioned and encrypted across companies / departments on the server

The data that is saved in the DEP is partitioned across customers so that data for each customer/ department is isolated. In addition the customer's data is encrypted using their own unique AES keys. All sensitive data including business content, system information, credentials etc. that are saved on the platform are encrypted using the AES algorithm with 256 bits key providing the maximum possible security.

The unique keys of the customer are encrypted with standard Public Key - Private Key cryptography and stored securely to ensure no unauthorized access is allowed.

Keys are stored on a server different from the platform server thus ensuring physical separation of the encrypted data and the keys.

Business content stored in DEP only until delivery to mobile device

The business content that is stored securely on the server is kept only until guaranteed delivery to the mobile device is completed. Once the mobile device acknowledges having received the message successfully, the data is discarded. This ensures that the business content is saved only as long as required and is never permanent.

Security

Contd.

Viewing of stored business content on the DEP server is protected with Two-factor authentication

The encrypted business content can be decrypted and viewed only by Super Administrator users. Further the Super Administrators are allowed access only after they validate successfully by entering a one-time, time limited token. The two-factor validation ensures that the data cannot be viewed by unauthorized users.

Data posted from the mobile device is protected with a One-Time token

The data that is posted from the mobile device to the server is additionally protected with a one-time token. The server validates this before accepting the message. This ensures that the data is originating from the trusted device and not an impersonation. Data which fails the one-time token check is rejected on the server and the mobile application clears itself preventing further use.

Audit logs on the DEP server.

Every critical and sensitive operation performed on the platform server is logged in the Audit log with the date / time of the operation and the administrator user who performed it. This provides complete track and trace functionality to check all changes performed on the system, by whom and when.

Single Sign On

DEP supports Single Sign On with SAP, based on web tickets.

Security

Contd.

Only trusted devices can connect to the DEP server.

The system is centrally administered using the Unvired Cockpit. Only trusted applications that have been uploaded to the platform can be used. Unvired users are typically managed and enterprise devices are assigned by the Administrator (although an unattended or automatic option is also available). Only such trusted users / devices can use the assigned applications affording complete security of enterprise data. Users who do not have access to the business functionalities any more can be disabled on the platform rendering the mobile application unusable.

Password protection on mobile applications

All mobile applications work with a centrally configured password policy. This ensures that access to the data and business functionality on the mobile device is available only to authorized and authenticated users.

For devices that support TouchID, security via TouchID (or equivalent) can also be enabled.

Data is stored encrypted and protected on the mobile device

The business content that is stored on the mobile device is always AES 256 encrypted and protected using native capabilities of the device. For example the data that is stored on an iOS device can only be read on that device and cannot be accessed outside.

Remote wipe of data on lost or compromised devices

DEP can wipe out the business content from devices that are lost or compromised. This is controlled centrally from the platform server and can be performed by the administrator. This ensures the additional safety of business content on the mobile devices.

Security

Contd.

HIPAA Compliance

HIPAA (Health Insurance Portability and Accountability Act of 1996) compliance is part of the DEP product roadmap.

Authentication Modules

- DEP supports multiple modes of user authentication for mobile applications:
- **Unvired User Id Access:** Login using the Unvired User Id configured in DEP.
- **Email Id Access:** Login using the email id associated with the Unvired User Id configured in DEP.
- **Microsoft Active Directory User:** Login using the Microsoft Active Directory User credentials.
- **SAP User:** Login using the SAP User credentials.
- **Custom Login:** Implement a custom module for user authentication.

Offline

Mobile Device Offline Access

Mobile applications that use the Unvired Client SDK has offline access by default. All data is stored in an encrypted SQLite database. Once data is obtained from the server or created on the device the data is saved in the device database.

The data that is saved in the device database can be submitted to the DEP server either automatically or on user decision.

- **Automatic Mode:** In the automatic mode data is submitted as soon as the data is saved if connectivity to the server is available. If connectivity is not available then the data is queued and send to the server as soon as connectivity is restored.
- **User Submission Mode:** User can decide to submit the data immediately (after saving) for an immediate response from the server. If connectivity is available then the data is submitted immediately to the server and response is available for user's immediate consumption. If there is no connectivity data can be stored and submitted manually later.

Server Offline Access

The DEP server also has built in offline capability. For e.g., if the SAP Gateway server is down for maintenance for an hour or so, DEP can store the messages that it receives from the device and then forward it to SAP Gateway as and when it is available. The benefit of this is that devices will NOT experience any errors and the whole process is transparent.

(**Note on SAP Gateway and Unvired Offline Access:** SAP Gateway is an online only tool. So scaling when a large number of users access SAP Gateway could be an issue as it passes through calls directly from caller to SAP backend. DEP can handle this by throttling calls to Gateway and SAP ERP / CRM / SCM / SRM and hence provide huge scalability when a large number of users need to access the system offline.)

SAP Gateway and SAP UI5 based apps can be made offline with DEP.

Conflict Resolution

Offline applications, by their nature, can lead to data conflicts between data in mobile apps and enterprise systems. DEP provides conflict resolution mechanism to resolve conflicts in data between the mobile apps and enterprise systems.

Conflicts can be resolved with the following rules:

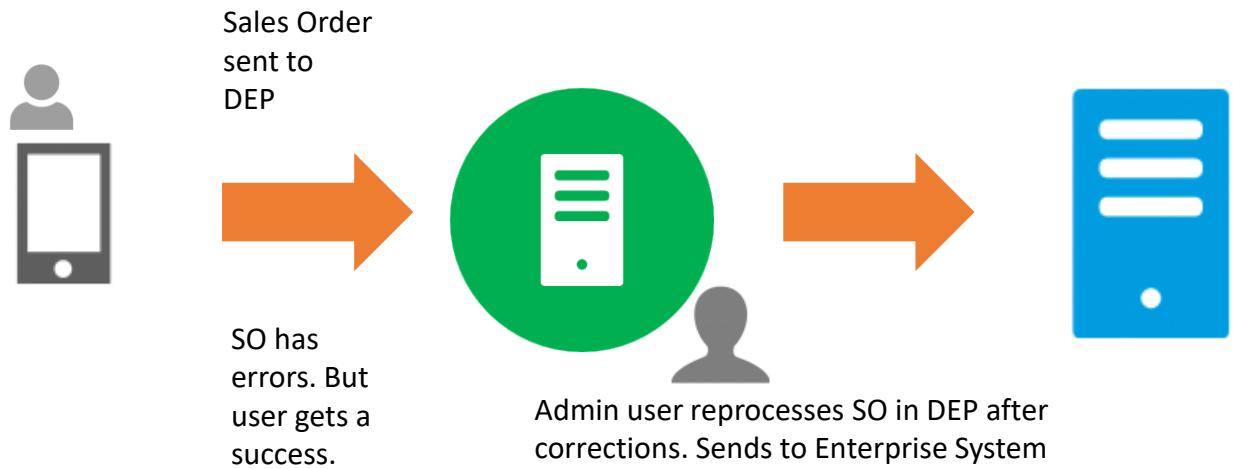
- **Server Wins:** Ensures that the latest update in the enterprise system overrides the mobile app data.
- **Client Wins:** Ensures that the latest update in the mobile app overrides the enterprise system data.
- **Custom Handling:** The conflicted data is given to the application for custom resolution. The application can implement an automatic resolution or provide a way to the user to choose the data that needs to be retained.

Error Console

Mobile application users, in many cases, do not want to be bothered about data / process failures in the enterprise system when the data is sent from the mobile app. In many cases the error are such that the mobile app user cannot resolve the issue immediately as there is dependence on a business rule in the enterprise system.

DEP provides a mechanism to store errored data in the Platform so that the errors can be resolved later by a business user / administrator without bothering the user. The business user / administrator can login to the Unvired Admin Cockpit, check the error console and reprocess after resolving the errors. This ensures that the data is not lost and the mobile app user is not bothered with error resolution.

Example: Sales executive created a sales order from the mobile app. Sales order failed in SAP as the material was not configured in the plant. The sales executive cannot resolve the material-plant issue but does not want to lose the sales order information. In this case the sales order is stored in DEP server and marked as an error. The sales executive is not bothered about error corrections. Later an SAP business analyst can set the plant for the material in SAP and then reprocess the sales order from the Error Console.



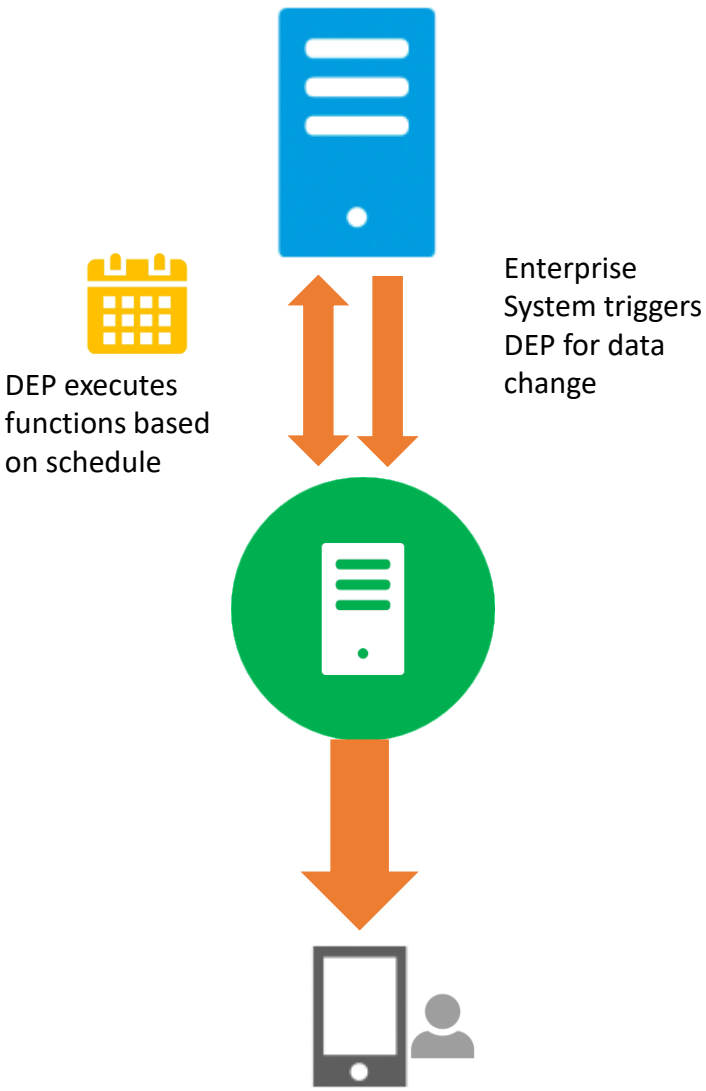
Schedulers & Triggers

Frequently it is required to take the data changes in the enterprise systems and push the data to the mobile applications so that the mobile app users do not have to query for the latest information.

DEP provides Schedulers and Triggers that can help to periodically get information from enterprise systems and push data to mobile apps or other enterprise systems.

Scheduler can execute specific functions periodically in the DEP based on configured schedules.

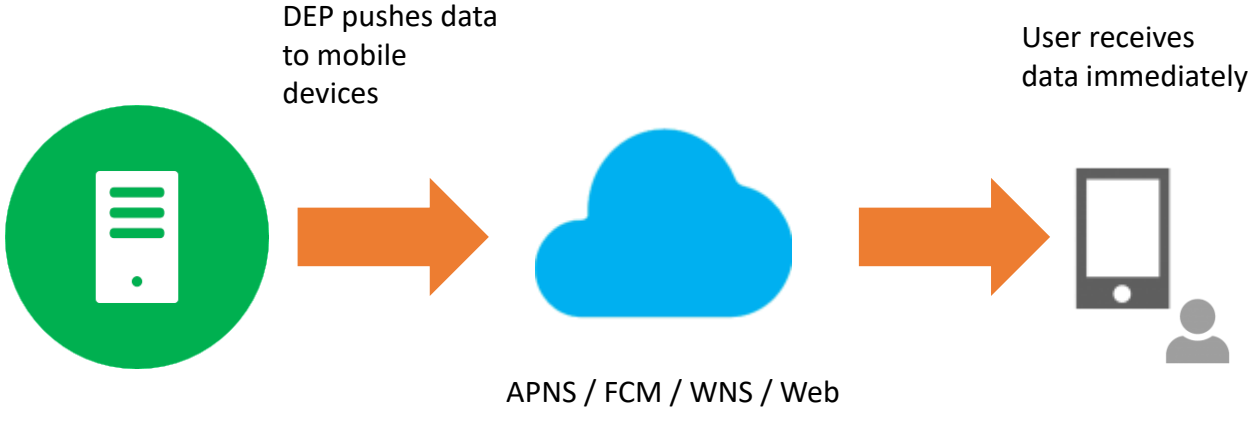
Triggers are APIs called from enterprise systems to for near real-time push of changed data across enterprise systems or from enterprise systems to mobile apps.



Data Push / Notifications

Digital Enterprise Platform supports data push / notifications to different mobile devices. Data push can be enabled with easy configurations.

- **Apple Push Notification Service (APNS):** APNS to push data to Apple devices (iPhone/iPad/Apple Watch).
- **Firebase Cloud Messaging (FCM):** FCM to push data to Android devices.
- **Windows Notification Service (WNS):** WNS to push data to Windows 8+ devices.
- **Browser Push:** Data push to the web app (cross browser) based on Server Side Event technology.



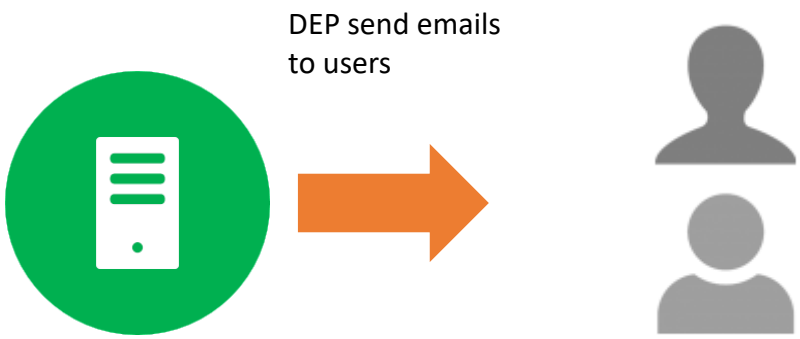
Attachments

- The Digital Enterprise Platform has a generic attachment module to support exchange of all kinds of attachments between enterprise systems or between enterprise systems and mobile apps.
- Both upload and download of attachments are supported.
- For download the attachments can be cached in the DEP to avoid round trips to enterprise systems for the same attachment used by multiple users.

E-mail Notifications

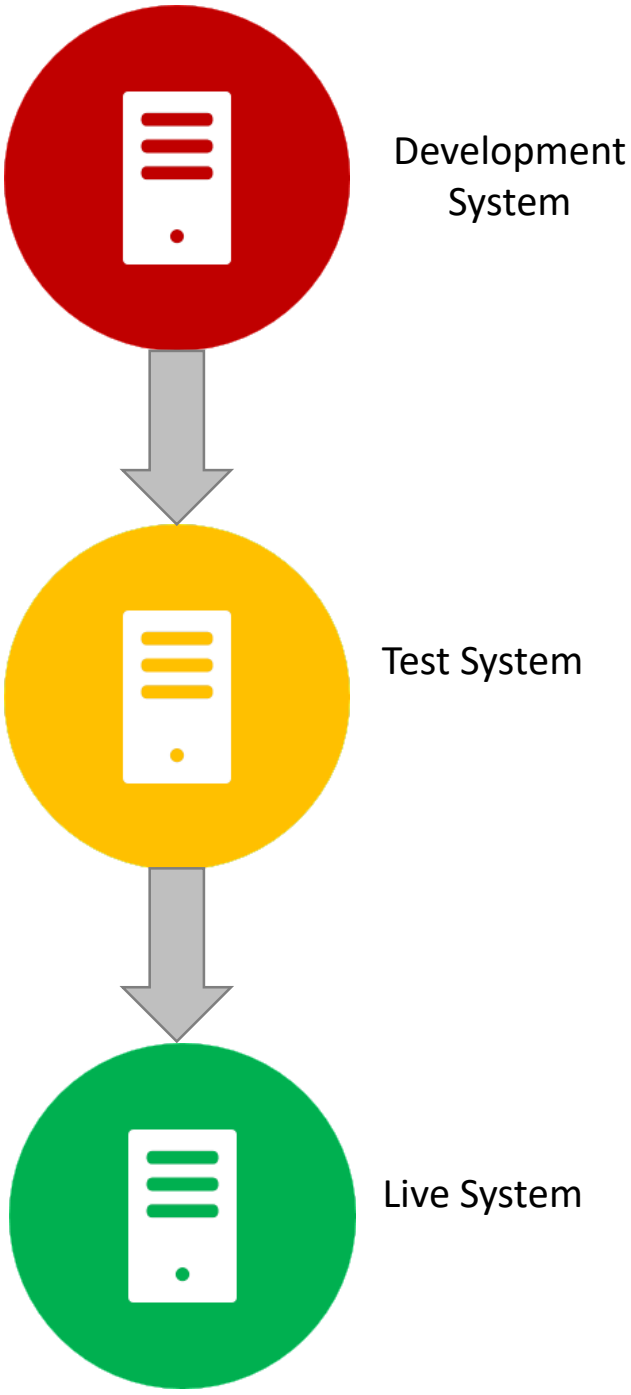
The Digital Enterprise Platform allows e-mail notifications to be sent to a group of people informing about:

- Important events
- Errors



Transport

- The Digital Enterprise Platform can be setup separately for development, quality and production / live usages.
- In such a landscape the applications can be transported or moved from one system to the other (development to quality to production in a 3 system landscape OR development to production in a 2 system landscape) easily using the built-in transport feature.
- This reduces manual application configuration / update errors.
- Transport automates the app movement while giving administrators control on when to move the apps.



Admin Cockpit

The Digital Enterprise Platform is administered using a web based app called Admin Cockpit that can be accessed from web browsers. Admin Cockpit offers:

- Configurations
- Management
- Monitoring
- Reporting

Reports

- DEP offers standard reports to check:
- App usage
- Device usage
- Data upload and download size
- Location tracking
- Data flow monitoring

Monitoring – Device

DEP allows data flowing between enterprise systems or between enterprise systems and mobile devices to be monitored for troubleshooting. Visibility of data can be turned off and on based on need. Typically in live / production systems data visibility is switched off.

Audit Logs

All configuration changes to the DEP and applications are logged for an audit trail. In a multi-administrator environment it is useful to know who did the changes and when the changes were made.

Technical Details

DEP is a Java Server application on IBM Redhat JBOSS. A typical fail safe configuration for a live system is as follows:

- Load Balancer
- At least 2 Instances of DEP (for fail safe) or a single instance (for non fail safe)
- Database with online replication (for failsafe) or a central database (for non fail safe) – MySQL, MS SQL, Oracle

Note:

- Unvired is an SAP Partner.
- DEP is certified by SAP to run on SAP NetWeaver and SAP S/4HANA.

Toolset

Unvired Designer

Unvired Designer helps to design, model and develop mobile applications. Unvired Designer is based on DEP. Unvired applications have 2 components:

- Server component residing on the DEP
- Mobile application (using the Unvired Mobile SDK) running on the mobile device or Web App (using the Unvired Web SDK) running on a browser or any other Server component (using the Unvired REST APIs)

Unvired Designer is a plugin to Eclipse IDE.

Thank You

unvired.com