ALESSA

Alessa Architecture Guide

JULY 11, 2024

About Alessa

Alessa is a compliance, controls monitoring and fraud prevention solution for banking, insurance, fintech, gaming, manufacturing, retail and more. With deployments around the world, Alessa allows organizations to quickly detect suspicious transactions, identify high-risk customers and vendors and decrease fraud risks that reduce profitability and increase costs. To learn more about how Alessa can help your organization ensure compliance to regulations, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at https://www.alessa.com.

Contents

Introduction

Alessa is software to screen and monitor customers and employees for financial services, such as banking, gambling, pay, and credit card use.

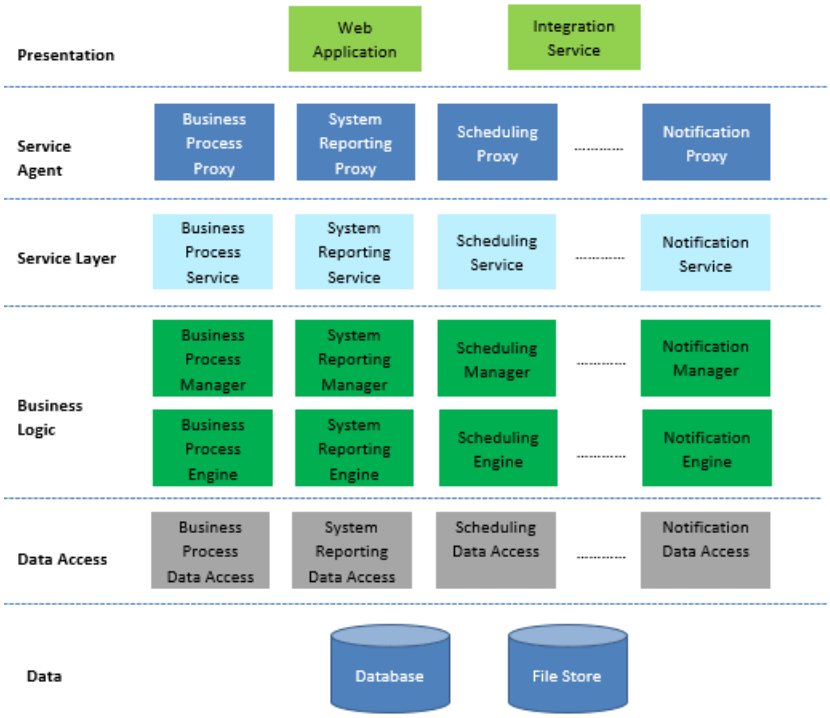
This document provides an overview of the Alessa architecture. It is for information technology (IT) specialists who install, configure, and maintain the application. It is for companies and organizations considering implementation of Alessa.

Components

Alessa is built on the Microsoft .NET platform and consists of the following components:

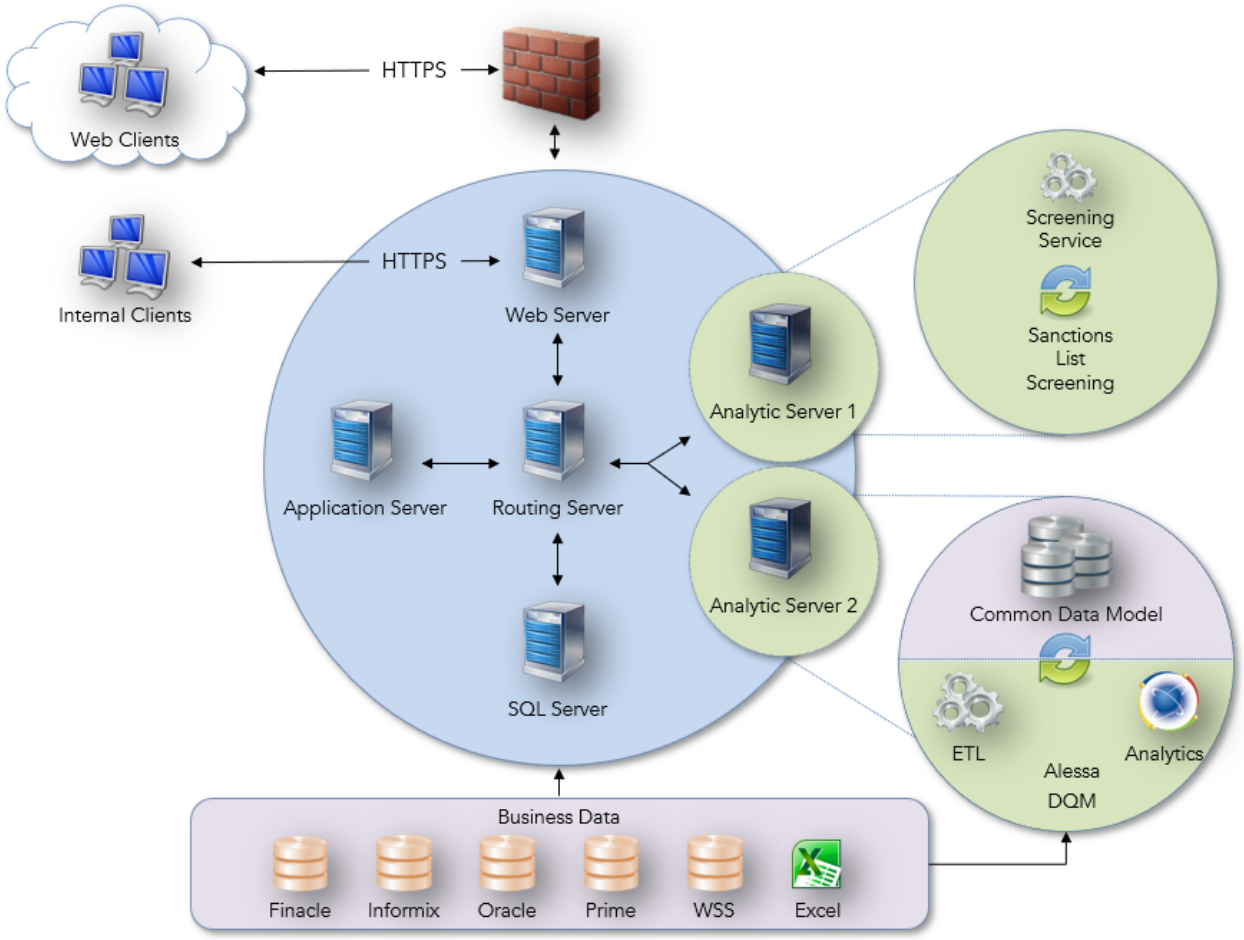
- Web Application Server
- Routing Server
- Application Server
- Analytic Engine Server
- Instance Manager

The figure shows a view of the Alessa architecture.



Topology

The deployment architecture is robust to tackle advanced deployment scenarios that can arise in an enterprise. It takes advantage of extended hardware resources to attain better performance in a distributed network environment. The figure shows a typical deployment of the application components on a network. Each Application Server, Routing Server, and Analytic Engine Server component can be installed on the same or separate machines.



The installation is done by a user who has rights on the domain to install each component on the server machine.

Installation can be done on-site or in the cloud.

Web Application Server

Alessa has a web-based interface. It is an ASP.NET 5.0 application running on Microsoft Information Systems (IIS).

The Web Application Server leverages the following technologies:

- Microsoft .NET Framework (4.8)
- EXT.JS
- EXT.NET
- JavaScript
- JGraph visualization library
- HTML 5
- CSS 3.0

Caching

The following information is stored in a cookie on the user's machine:

- The username of the last successful user to log in
- The locale of the last successful user to log in

Security

Alessa supports use of HTTPS for communication with the web server.

Routing Server

The Alessa Routing Server is an executable that is installed as a Windows service. The Routing Server contains several self-hosted Windows Communication Foundation (WCF) services that encapsulate the functionality needed for routing messages to other services. The routing server is the entry assembly for these services and acts as the central hub of Alessa.

The Routing Server leverages the following technologies:

- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (DTC)
- Microsoft .NET Framework (4.8)

The Windows service is the host for the WCF services listed in the table.

SERVICE	PLUGIN ASSEMBLY PATH	COMMENT
Notification	RoutingServices\NotificationService	Handles message events and interfaces with enterprise messaging systems (e-mail server, SMS service, MSMQ)
Publishing Subscription	RoutingServices\PublishingSubscriptionService	Handles event subscriptions and publishes events to subscribers as they occur. Provides a hub for remote inter-process communication.

Service	Plugin Assembly Path	Comment
Routing	RoutingServices\RouterService	Routes user requests to the appropriate service. Detects new services on the network when they become available for routing. Provides load balancing by routing user requests.

Application Server

The Alessa Application Server is an executable that is installed as a Windows service. It contains several self-hosted WCF services that encapsulate most of the user-centric business logic.

The Application Server leverages the following technologies:

- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (DTC)
- Microsoft .NET Framework (4.8)

The Windows service is the host for the WCF services listed in the table.

Service	Plugin Assembly Path	Comment
Process Management	ApplicationServices\ BPManagementService	Management service for business process features. Primary purpose is create, read, update, and delete (CRUD) functionality for processes, activities, controls, and result sets.
Membership	ApplicationServices\ MembershipService	Management service for authentication and authorization. Primary purpose is CRUD functionality for users, roles, and membership.
Notification Subscription	ApplicationServices\ NotificationSubscriptionService	Management service for notification events and user subscriptions. Primary purpose is CRUD functionality for notifications and message templates.
Workflow Engine	ApplicationServices\ WorkflowEngineService	Execute workflow jobs, including auto transitions, manual transitions, and overdue work items
Workflow	ApplicationServices\ WorkflowService	Management service for workflows. Primary purpose is CRUD functionality for workflows, teams, and templates.

Analytic Engine Server

The Alessa Analytic Engine Server is an executable that is installed as a Windows service. It contains a number of self-hosted WCF services that encapsulate the analytic engines supported by the solution.

The Analytic Engine Server leverages the following technologies:

- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (DTC)
- Microsoft .NET Framework (4.8)

The Windows service is the host for the WCF services listed in the table.

SERVICE	PLUGIN ASSEMBLY PATH	COMMENT
Data Analytic Engines	AnalyticEngineServices\ DataAnalysisEngineService	Management service for analytic engines. Primary purpose is engine configuration and task execution. This service hosts all analytic engine wrappers.
Parameters	AnalyticEngineServices\ ParameterManagementService	Management service for parameters used by the scripting engines. Primary purpose is create, read, update, and delete (CRUD) functionality for parameters.
Script Package	AnalyticEngineServices\ ScriptPackageService	Management service for script packages. Primary purpose is file management and versioning functionality for packages.
Task Management	AnalyticEngineServices\ TaskSchedulerService	Triggers the tasks that are scheduled to run scripts from packages. Primary purpose is CRUD functionality for tasks and triggering the analytic engine to execute a package script.

Instance Manager

An Alessa instance is defined by all of the components, such as the Application Server, Analytic Engine Server, Routing Server, Web Application Server, and licenses installed on the active computer.

The Alessa Instance Manager is software included that displays the Alessa instance on the active computer and lets you configure the Windows services installed by Alessa, deploy new application services, and deploy new data engines.

Software Compatibility Matrix

	Client	Web Application Server	Routing Server	Application Server	Analytic Engine Server	Database Server - Any 64-Bit Server OS
Browsers						
Firefox 68.x.x	✓					
Chrome 76.x.x.x	✓					
Operating Systems						
Windows Server 2022		✓	✓	✓	✓	
Windows Server 2016		✓	✓	✓	✓	
Databases						
Microsoft SQL Server 2022						✓
Microsoft SQL Server 2019						✓
Engines						
CaseWare IDEA Client 9.1.x, 9.2, 10.1.X, 10.2.X, 10.3, 11.1.1					✓	
Arbutus v5.53					✓	
ACL 9.1, 9.3, 10, 11					✓	
Programming Languages						
Python 3.6					✓	

Global Search

Alessa leverages the power of Elasticsearch to offer global search capability in the software interface to quickly and conveniently search work item data and metadata, such as assignees, comments, current states, and more. This feature allows users to locate work items, regulatory reports, and specific supporting information from any Alessa screen.

Security and Access Management

The Alessa security model has two levels.

- Message security level
- Application access level

Message security deals with how users access the application and the way services are accessed over the network. Alessa requires a user account to be registered before the user's first login. The user has to be authenticated at the application level by logging in. The user's network credentials are used to authenticate service requests. Administrators have the ability to enforce two-factor authentication for user accounts.

Application access security controls how users access different components (system objects) and features of the application. Permissions can be granted or denied for the configuration tools and each object created in the application, including reports, business process objects, scheduled tasks, and created business rules.

User Authentication Methods

Two-factor authentication can be applied.

Federated Identity Management

Alessa uses Shibboleth Service Provider to allow users stored in distinct identity management systems to use a single digital identity to access data or services. The Shibboleth Service Provider is a software solution that enables web applications like Alessa to process authentication requests using these identities. If your organization uses Federated Identity Management, you can use the Shibboleth Service Provider to authenticate to Alessa using your organization's Identity Provider.

Database Authentication

You can create user accounts that are stored in the Alessa database. When users log in to Alessa, their usernames and passwords are authenticated against the usernames and passwords in the Alessa database.

Windows Authentication

You can add users to Alessa from your company's Windows Active Directory. When the users are added, their Active Directory usernames and contact information are copied to the Alessa database. Users can then access Alessa using their Windows login credentials.

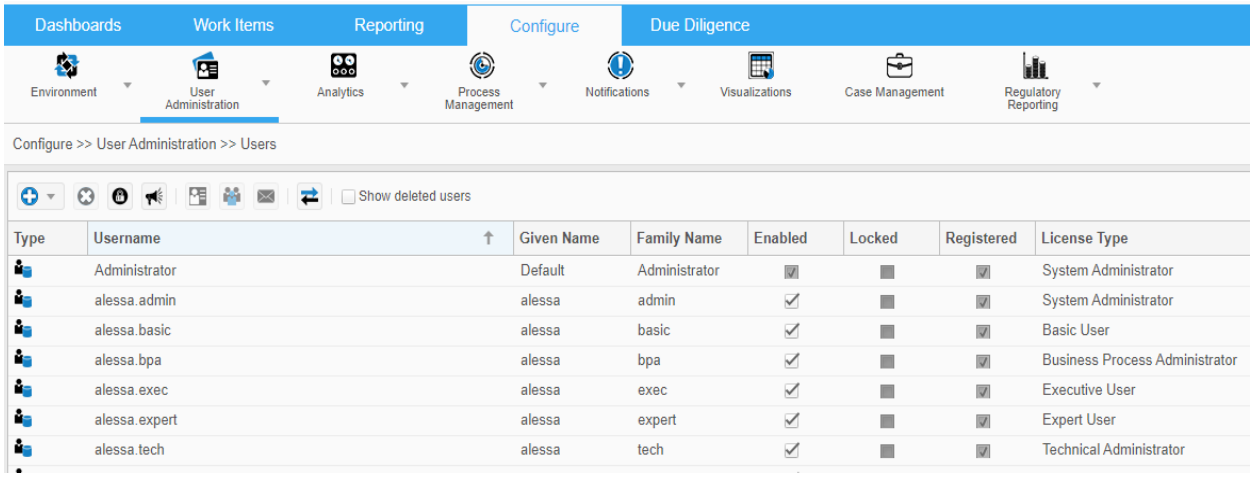
User Management

The following types of user accounts are possible:

- System Administrator
- Technical Administrator
- Business Process Administrator
- Expert User
- Basic User
- Executive User

Permissions to functions can be controlled, by account, account type, and roles.

Users are managed within Alessa from the User Administration page. System administrators can perform functions, such as creating, deleting, deactivating, and assigning required permissions to users. They can update user profiles and unlock user accounts when needed.



User Password Management

The Alessa password must be

- A minimum of eight characters
- A maximum of 128 characters

Passwords must contain at least one character from at least three of the following categories:

- Uppercase letters
- Lowercase letters
- Numbers (0-9)
- Non-alphanumeric characters (for example, @,#,$,*,&)

Passwords cannot

- Contain the username or any fragments or reverse fragments of three or more characters from the username (for example, the username Janebrown and password nworbe1)
- Be one of the last five passwords

The minimum and maximum lengths can be changed by contacting Alessa.

Data Security

The data encryption security level is configurable and can be modified post-installation/implementation. Alessa uses the Windows Communication Foundation (WCF) platform for all remote communication between software components. WCF is a Simple Object Access Protocol (SOAP) message-based distributed programming platform that provides a versatile and interoperable platform for exchanging secure messages based on the existing security infrastructure and the recognized security standards for SOAP messages.

Communication can be secured by using two forms of security, these being Transport Security and Message Security.

Transport Security mode uses a transport-level protocol, such as HTTPS, to achieve transfer security. This mode has the advantage of being adopted widely, available on many platforms, and less computationally complex. However, it has the disadvantage of securing messages only from point-to-point.

Message Security mode uses Web Services (WS) Security and other specifications to implement transfer security. Message security is applied directly to the SOAP messages and is contained inside the SOAP envelopes. Combined with the application data, it can be transport protocol-independent, more extensible, and ensures end-to-end security (versus point-to-point). It has the disadvantage of being several times slower than transport security mode because it must deal with the XML nature of the SOAP messages.

Data also can be secured at rest using existing encryption features in Microsoft SQL Server.

Data Integration

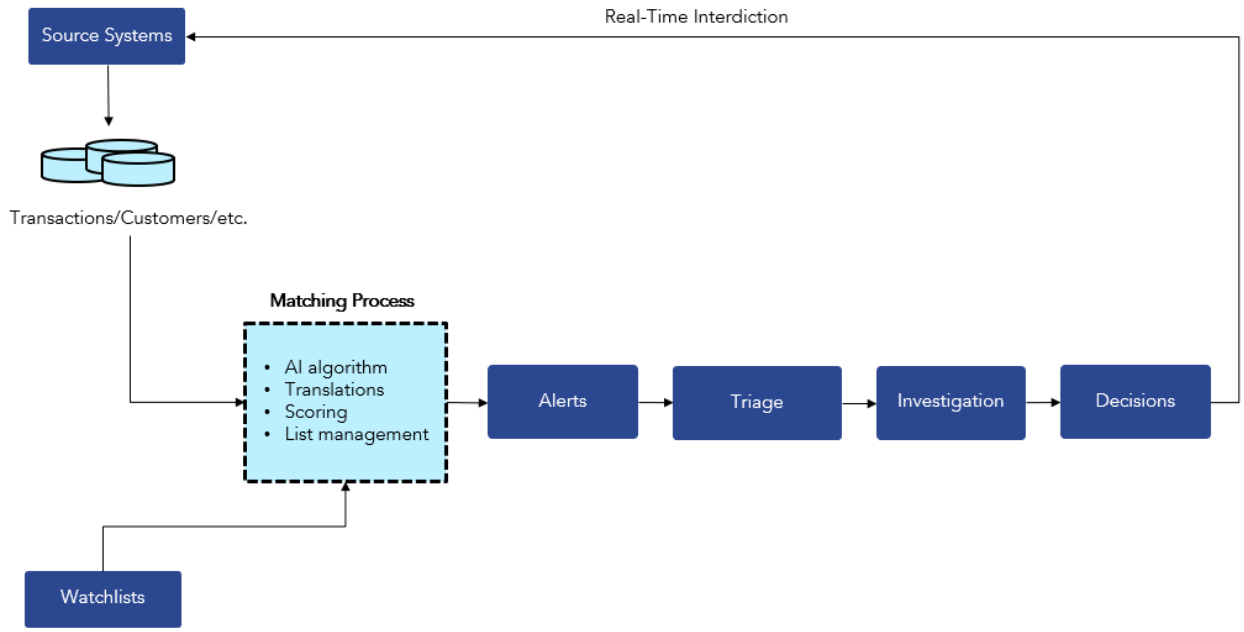
Alessa uses extract, transform, and load (ETL) tools to map and extract data from the source systems. Once extracted, the data analytics software processes the data and generates results.

Initial data access by Alessa to the core system is accomplished using the scripting engine's data import functionality, which can utilize either native database drivers or a generic Open Database Connectivity (ODBC) connection to the underlying database. After import, Alessa requires only read-only access to a company's data; it does not directly interact with core systems.

The scripting engines supported by Alessa can import data from any data source. These scripting engines support native drivers, such as Microsoft Access and SAP/AIS, and generic drivers, such as ODBC.

Data Flow

The figure depicts the data flow in the screening process in Alessa. Once alerts are generated, they are stored in the Alessa database, which is hosted on a Microsoft SQL Server.



Disaster Recovery Strategy

Alessa has a tiered architecture. As such, the backup and restoration for each layer is explained separately.

Application Layer Backup of Configuration Files

Following the configuration of Alessa at implementation, a full backup of the business processes located on the data Analytic Engine Server(s) is made by you. This is repeated for any changes to the business process configuration.

In the event of a loss of the server, Alessa can be installed, and the business process folder replaced by the backup file.

Recommended practices are

- Keep images of the data Analytic Engine Server(s) at an alternate site
- Back up business process files after configuration changes

If data loss occurs at this layer, the image can be restored and controls replaced in minutes.

Database Layer Backup

The second stage of a backup is the database backup. The database used is Microsoft SQL Server.

Alessa accommodates various database setups in its disaster recovery model where database clusters are mirrored synchronously in two separate locations, and backups are made and stored in a third location. Alessa supports native SQL functionality for disaster recovery, such as backups, log shipping, replication, and SQL clusters.

In this case, uptime is 99.99%, and data loss is zero. If one site goes down, the Application Server can be redirected to the mirrored database in seconds.

Document Revisions

Product Version	Document Version	Date	Description
5.5.3	1	14 April 2020	5.5.3 release
5.5.3	2	10 November 2021	Rebranded, minor edits, added Document Revisions section
5.5.3	3	29 December 2021	Updated template to Tier1 Financial Solutions, edited, restructured, added user account types to User Management section, replaced Software Conformance Matrix with Software Compatibility Matrix
5.5.3	4	20 December 2022	Rebranded
5.5.3	5	8 February 2024	Edited, added support for Windows Server 2022 and Microsoft SQL Server 2022, updated security classification, updated figures for consistent branding
5.5.3	6	11 July 2024	Edited, deleted Microsoft Server 2012, Microsoft SQL Server 2012, 2014, 2016, 2017 from Software Compatibility Matrix. Since v5.5.3.21, the minimum supported SQL version is 2017, and since v5.5.3.24, the minimum supported SQL version is 2019.