EASYVISTA™

White Paper Service Manager - SaaS

TABLE OF CONTENTS

Contents

Download the PDF file

INTRODUCTION

The purpose of this white paper is to help you understand:

- How EV Service Manager as SaaS can be integrated into your technical infrastructure technique.
- The SaaS environment provided as part of the EasyVista service.

Because individual constraints and technology choices make each client's infrastructure unique, every project will undergo a specific analysis during the pre-sales and/or installation phases.

PRODUCT GLOSSARY

EV Service Manager is based on:

- A **Front Office service** (Service Apps): Provision of a configurable services portal to your end users.
- A **Back Office service** (Service Engine): Provision of a more comprehensive product interface to your Back Office team in charge of dealing with incidents, changes, etc.

Depending on your project and how work is allocated between your end users (Portal) and your technical teams, either the Front Office or the Back Office part can dominate. The target architecture and integration into your infrastructure must take this allocation into account.

Other terms used

- **Environment**: Refers to EV Service Manager provided in a given version.
  - By default, you have a production environment. You can subscribe to additional environments (Qualification, Test, BI, etc.).
  - Different environments may have different versions.
- **Account**: Refers to an isolated Service Manager database (production account, test account, demonstration account).
  - Each account has a separate administrator.
  - The accounts in a single environment are all the same version.

OVERALL ARCHITECTURE

Access to EV Service Manager

The EV Service Manager service is accessible via four URLs (for a new installation) and two URLs (for an update):

- Demo tenant URL publishing apps (new installation).
- URL of the production tenant publishing the apps.
- URL of sandbox holder publishing apps (new installation).
- Service Engine URL.
- Through web services.

No other external access to the platform is authorized, such as:

- Access to the SQL database.
- Control of the servers that are part of the architecture.

It is possible to create a specific connection through your infrastructure using a VPN.

Accounts provided

Three accounts are provided:

- A production account.
- A sandbox account: This allows you to carry out integration or configuration tests before applying them to the production account.
- A demonstration account: This contains data and configuration examples.

All three accounts are based on the same infrastructure and therefore use the same version of EV Service Manager.

Components of different services

Service Engine

- **Web Front End**: In charge of processing http requests from users and returning HTML webpages.
- **Application Server**: In charge of processing business requests and providing the necessary data to the web server while taking into consideration the connected account and what that account is authorized to do and see.
- **Database Server**: In charge of storing data.

Service Apps

- **Web Front End**: In charge of processing http requests from users and returning HTML webpages.
- **Database Server**: In charge of storing data.

Adaptability to your constraints

Progressive scaling

The Service Manager architecture is scalable. It can be reviewed and modified based on changes in your requirements.

You can therefore start your project with a well-defined scope (modules used, number of users etc.) and extend it in line with your needs. This extension will be managed by our teams, working closely with you to ensure the process is as transparent as possible.

Security of your data in transit

To safeguard the confidentiality and integrity of data flows, we automatically install an SSL certificate on your platform.

If you wish to use your own domain name, you must provide us with a suitable SSL certificate that complies with our security requirements (no self-signed certificates, valid for at least the length of the contract, etc.).

On EasyVista servers, the SSL will be configured in compliance with our security requirements, i.e. not to accept protocols, ciphers, etc. that are known to be vulnerable:

- SSL v2, SSL v3, TLS v1.0, TLS v1.1.
- RC4, 3DES, etc.

Need for other environments

As well as the production environment, you can subscribe to additional environments to meet your organization's needs.

We recommend creating and maintaining at least one additional environment so that you can test changes before applying them to your production environment, in particular:

- Fixes or major changes to our products.
- Configuration changes to server components (Apache, PHP, SSL, etc.).
- Version upgrades or fixes to operating systems or server components.

Browsers

Suppliers

The browser market is constantly evolving, so please refer to our Supported browsers wiki page for an up-to-date list of compatible browsers.

Configuration

Pop-ups and JavaScript must be enabled and authorized for Service Apps.

The limit of the local cache and temp files must be adequate (> 10 MB).

If you are using the SSL protocol, you should check that the cache is authorized for the secure page.

Antivirus

On the client workstation, the local antivirus software should not check .JS (JavaScript) files systematically because this can lead to performance issues when displaying pages.

Miscellaneous

Our services do not require APPLET or ActiveX on the client browser.

Cookies

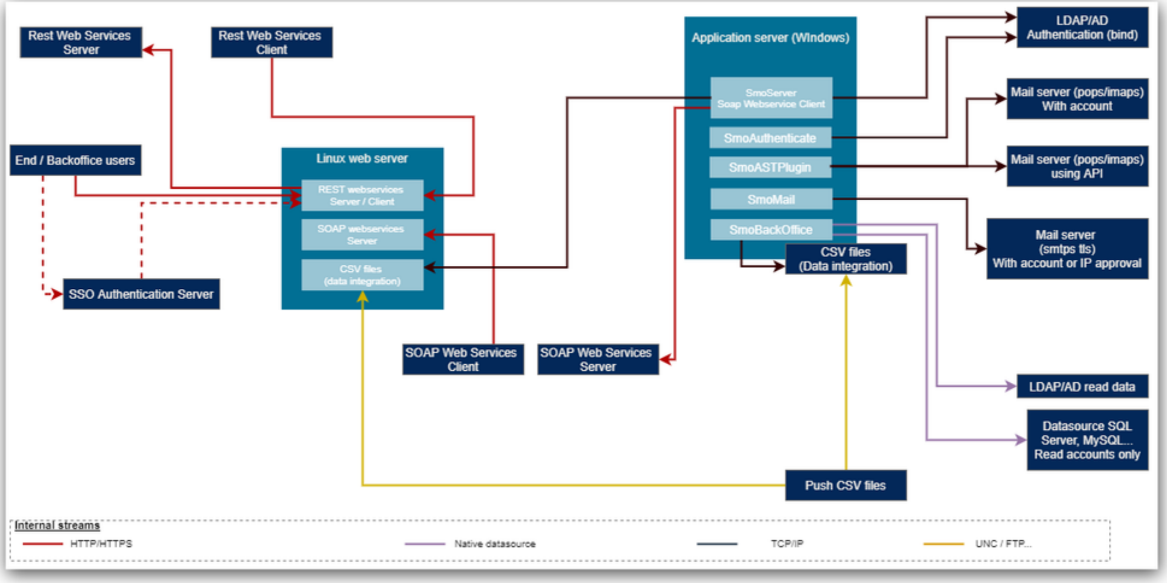
Our services use cookies to improve website functionalities and user experience. These cookies do not contain personal or sensitive data.

Your browser must authorize our services to create cookies.

FUNCTIONAL INTEROPERABILITY

Schematic diagram

The following diagram shows all possible interconnections between the Service Engine module and the information system.


Rest Web Services Server
Rest Web Services Client
End / Backoffice users
Linux web server
REST webservices Server / Client
SOAP webservices Server
CSV files (data integration)
SSO Authentication Server
SOAP Web Services Client
SOAP Web Services Server
Application server (Windows)
SmoServer Soap Webservice Client
SmoAuthenticate
SmoASTPlugin
SmoMail
SmoBackOffice
CSV files (Data integration)
LDAP/AD Authentication (bind)
Mail server (pops/imaps) With account
Mail server (pops/imaps) using API
Mail server (smtps tls) With account or IP approval
LDAP/AD read data
Datasource SQL Server, MySQL... Read accounts only
Push CSV files
Internal streams
HTTP/HTTPS
Native datasource
TCP/IP
UNC / FTP...

Overview

EasyVista.com may connect to your infrastructure in order to:

- Validate user IDs and passwords in your LDAP/AD directory.
- Authenticate users automatically using your corporate SSO system.
- Send emails directly from your internal email server.
- Data integration from your internal databases.

If your servers have a public IP address or are accessible via your EasyVista.com platform while limiting public access to it, these functionalities can be implemented in accordance with the service catalog conditions.

If your servers are not directly accessible from outside your network, you must implement a VPN connection to enjoy these functionalities.

Web services

REST and SOAP 1.2 provider

Our services are accessible as REST and SOAP 1.2.

REST and SOAP 1.2 client

The services can use external REST or SOAP 1.2 services.

E-mail

Sending e-mails

Service Engine and Service Apps must access you e-mail server to send e-mails to your users when handling incidents / changes.

The following protocols are supported: SMTP / SMTPS / SMTPS with TLS.

Automatic creation of tickets via e-mail

Service Engine must be able to access working email inboxes to which your users can send messages that will be automatically turned into tickets by the application.

The following protocols are supported:

- POP3 / POP3S.
- IMAP4 / IMAP4S / IMAP + TLS / IMAPS + TLS.
- Office 365: It corresponds to IMAP4 in modern authentication (XOAUTH2).
- Microsoft GRAPH: It uses Outlook REST API with modern OAUTH2.0 HTTPS authentication.

INTEROPERABILITY WITH YOUR INFRASTRUCTURE

Overview

EasyVista.com can connect to your architecture to:

- Integrate data coming from your platforms (LDAP, etc.).
- Validate the usernames and passwords of your users based on your LDAP/AD directory.
- Automatically authenticate your users through your company's internal SSO system.
- Send e-mails directly from your internal mail server.

If your servers have a public IP address or are accessible via your EasyVista.com platform while limiting public access to it, these functionalities can be implemented in accordance with the service catalog conditions.

If you servers are not directly accessible from outside your network, you must put in place a VPN connection to enjoy these functionalities.

VPN connection

A VPN connection is required if you would like EasyVista.com to be integrated into your infrastructure and your servers not to be accessible via a public IP address.

Bandwidth required

The bandwidth required depends on the traffic generated by the functionalities described above. The figures given are estimates designed to give you an idea of the resources necessary.

- Real-time processing:
  - Sending e-mails = <1 ko.
  - Validation of authentication by username/password = <1 kb.
- Asynchronous processes: These processes have no impact on what is displayed to the user and often run outside of working hours. They can therefore withstand any slowing due to insufficient bandwidth.
  - Retrieval of the directory from the database for importing into EasyVista.
  - Retrieval of e-mails received by technique support following the automatic creation of incidents (the size varies depending on the size of attachments).

Access to EasyVista is exclusively through an Internet connection and must not go through the VPN. If the client wishes to access EasyVista.com via the VPN rather than the standard Internet connection, the bandwidth of the VPN must be increased accordingly.

VPN connectivity pack

- Implementation services included in this pack:
  - Implementation of an IPSec VPN or point-to-point private VPN in accordance with the functionality and responsibility conditions outlined in this document.
- Services that can be ordered if this pack is purchased:
  - AD/LDAP authentication.
  - Scheduled import of AD/LDAP data.
  - Use of your e-mail server to send data.
  - Technical support agent.
  - Tridirectional SSO system (to be decrypted, the user credentials sent to EasyVista.com require an additional flow with your servers).
  - Read-only access to data through an SQL Server account for the purposes of creating reports.

VPN connection availability

Availability and responsibility in the event of maintenance vary depending on the technology used and the people involved.

If you want the backup platform to have exactly the same VPN service as the main site, you must configure a second VPN. Otherwise, in the event of a switch to the backup site, the running of EasyVista will automatically adapt to the new configuration (authentication no longer takes place through your infrastructure, but through the system built into EasyVista, etc.).

Choosing between IpSec VPN and point-to-point private VPN

Regardless of any restrictions that are part of your company's standards, the following criteria will help you to choose between the two solutions.

VPN type	Advantages	Disadvantages
IpSec	• Speed of set up (no line to configure; generally takes less than 2 days). • Costs less. • High security, even though data travels over the Internet.	Encrypted tunnel, but data does not travel over a private line.
Private point-to-point	• Maximum privacy. • Dedicated connection to access the EasyVista service instead of using standard Internet access.	• Cost of set up and use. • Line installation often takes over 4 weeks.

Front Office external flow matrix (Service Apps)

Source	Destination	Ports	UDP / TCP
Your users and functional administrators	Service Apps web server	443 (https)	TCP

Back Office external flow matrix (Service Engine)

Source	Destination	Ports	UDP / TCP
Your users and functional administrators	Service Engine web server	443 (https)	TCP

RESPONSIBILITIES DURING THE IMPLEMENTATION PHASES

Implementation phase	Description
Installation	• EasyVista installs and configures the environments, then creates the production and test accounts. • During this phase, the client or partner does not have access to the system. • Once installation is complete, the customer receives a document containing the connection information for the EasyVista site.
Implementation by the client	• The client/certified partner configures EasyVista as per their requirements. • The MyEasyVista admin console is available. • During this phase, the EasyVista.com backup and restoration system, as well as the monitoring and disaster recovery plan services, are not activated. • Once implementation is complete, the client asks our technical support service to launch the production phase.
Production	• The EasyVista.com backup and restoration system, as well as the monitoring and disaster recovery plan services, are activated, as are the associated alerts. • Backup and restoration operations for the production database via MyEasyVista is deactivated; the client/partner can no longer access the database. • The MyEasyVista management console allows backup and restoration operations to be carried out using the sandbox database, then the production database to be copied onto the sandbox database.

MIGRATION TO A MORE RECENT VERSION

Migration to a more recent version is part of the EasyVista.com service.

Responsibilities

The EasyVista CMC (Cloud Management Center) operations teams handle the migration to the new version following the standard migration process.

An information e-mail is sent letting you know that an update is available and providing you with a document outlining the new functionalities of the latest version.

Your teams must familiarize themselves with the new functionalities, train users and, if necessary, carry out any configurations as part of this new version.

If necessary, our advisors or certified partners are there to provide assistance and technical support.

Testing the new version

If you have a Qualification environment, our teams will first carry out the update in this environment, which will allow you to test it in accordance with your procedures (non-regression, new functionalities, etc.).

As part of the validation of a minor version, a temporary acceptance platform will be made available to you upon request if you do not have a Qualification environment. This temporary platform is provisioned for a period of three weeks with the functional configuration of the application but without the SSO and the flows impacted by the VPN.

Once this version has been validated by our teams, you can schedule migration to your production environment.

Note: It is not possible to have two Service Engine versions in the same environment.

Special case of migration from versions prior to Oxygen to versions Oxygen and above

As part of migration to the Oxygen version, a temporary acceptance platform will be made available to you, even if you do not have a Qualification environment. This temporary platform is provisioned for a period of three weeks with the functional configuration of the application but without the SSO and the flows impacted by the VPN.

Installation in your production environment

Migration phase	Standard duration	Description
Update availability		Update availability for a Service Engine version as SaaS is usually the same as for updates for on-premise clients.
Migration of your Qualification environment	1 day	• Client: Technical support receives a request to update your Qualification environment to the new version. • EasyVista CMC: • Sets a date for the update. • On the scheduled date: • Updates the Qualification environment in accordance with the current version of your production environment. • Updates the Qualification environment in accordance with the new Service Engine version. • Sends you an e-mail to confirm migration of the Qualification environment to the new version.
Validation	Variable	• Client: Validation process and testing of new functionalities. **Caution**: Changes made to the test platform are not kept when migrating to the production environment.
Planning migration of the production environment	1/2 day	• Client: When you are ready (processes validated, users trained, etc.), ask our technical support service to update the production environment. • EasyVista CMC: • The date and time for the migration are set after consulting you.
Migration of the production environment	Between 2 and 4 hours (depending on the size of the database)	• Client: Users must be informed that the production environment will be unavailable during the migration phase. • EasyVista CMC: On the scheduled date: • Backup of your databases before migration. • Migration to the new version. • Testing of the migration. • An e-mail is sent to the client informing them that migration is complete. • The production environment is re-opened.

CUSTOMIZING THE EASYVISTA.COM SERVICE

Login pages and CSS customization

Two login pages are provided by default: the first for the production account, the second for the test account.

This page follows the standard EasyVista login page format. You can modify it by adding colors and logos of your choice. The customizations possible are described in the EasyVista.com deployment guide.

More advanced customization is also possible upon request.

See Customizing Service Engine CSS style sheets.

Implementing scheduled data integrations

By default, it is possible to implement scheduled data integrations based on .CSV files provided to EasyVista (by uploading them to an FTP site dedicated to your platform).

If you have subscribed to the VPN option, it is also possible to integrate data for which the source is accessible in your infrastructure.

Adding fields, views and tables to the standard data template

You can request the addition of fields, views and tables to the Service Engine data template via MyEasyVista or via technical support. These additions will be implemented after technical validation by our teams and consultation with you on the implementation period.

TECHNICAL MAINTENANCE OF THE ENVIRONMENTS

Platform security

Default security

Our platforms are configured to reduce security risks to a minimum through:

- Automatic access restriction (*None by default* policy).
- IPS/IDS to detect malicious access.
- Anti DDOS to reduce the risk of unavailability.
- Antivirus to ensure system integrity.

Vulnerability tests

Vulnerability tests are carried out weekly on all platforms by our partner Qualys.

Maintenance of operational conditions

To enable us to keep your platforms in optimal condition, three hours of technical maintenance are scheduled each month. Amongst other things, this allows us to update operating systems and components used.

> Note: These hours are not automatically used, just as required.

These hours are not included when calculating the platform's unscheduled production downtime. They are determined:

- Either automatically by our teams based on your observed activity to minimize the impact on your users (at night, on Saturdays).
- Or in liaison with you if you wish to choose a specific timeslot from those available (at night, on Saturdays).

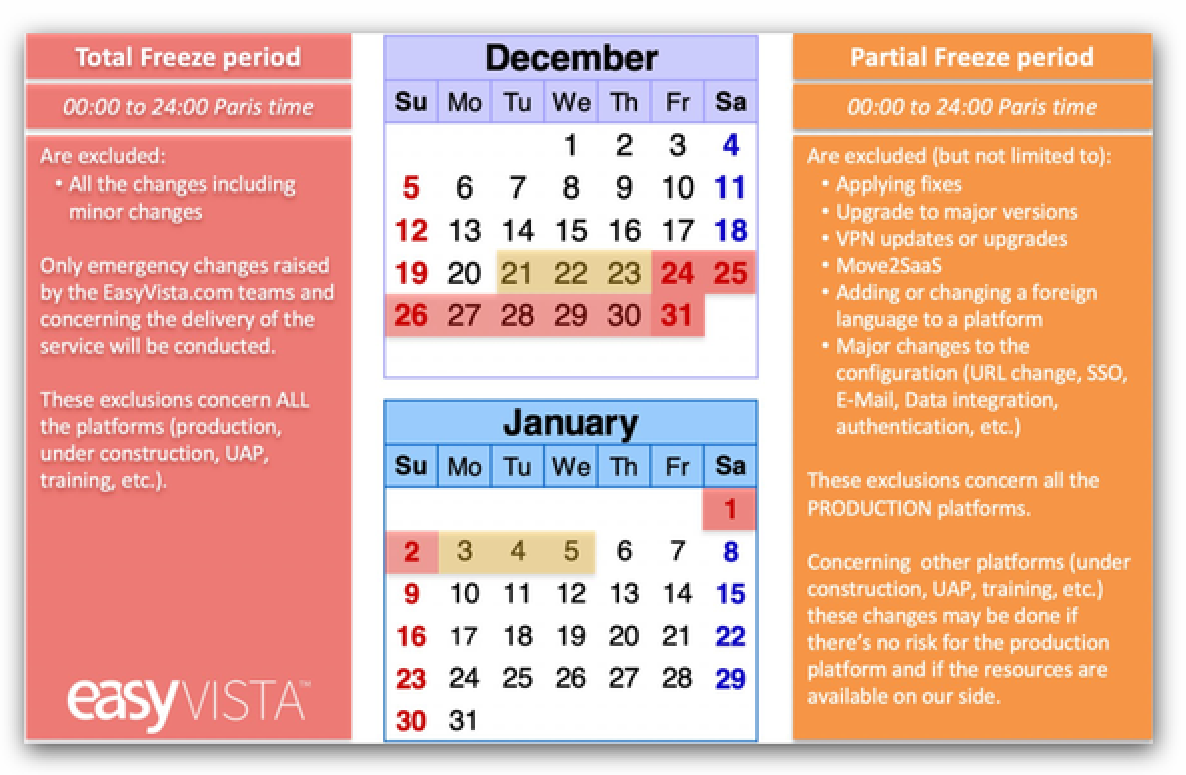
When an operation is scheduled, an information e-mail is sent to you stating the date, time and duration of the operation.

Annual frozen period

A frozen period is automatically implemented in the last week of the calendar year N, and the first week of the calendar year N+1.

During this period, the number and type of changes authorized on production platforms is limited.

example



Total Freeze period

00:00 to 24:00 Paris time

Are excluded:

- All the changes including minor changes

Only emergency changes raised by the EasyVista.com teams and concerning the delivery of the service will be conducted.

These exclusions concern ALL the platforms (production, under construction, UAP, training, etc.).

easyVISTA™

December

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

January

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Partial Freeze period

00:00 to 24:00 Paris time

Are excluded (but not limited to):

- Applying fixes
- Upgrade to major versions
- VPN updates or upgrades
- Move2SaaS
- Adding or changing a foreign language to a platform
- Major changes to the configuration (URL change, SSO, E-Mail, Data integration, authentication, etc.)

These exclusions concern all the PRODUCTION platforms.

Concerning other platforms (under construction, UAP, training, etc.) these changes may be done if there's no risk for the production platform and if the resources are available on our side.

USER AUTHENTICATION

Division of roles

Authentication and authorization

For Service Engine and Service Apps, we distinguish between:

- Authentication: Confirmation of the identity of the person trying to connect.
- Authorization: What the person identified has the right to do on Service Engine and Service Apps.

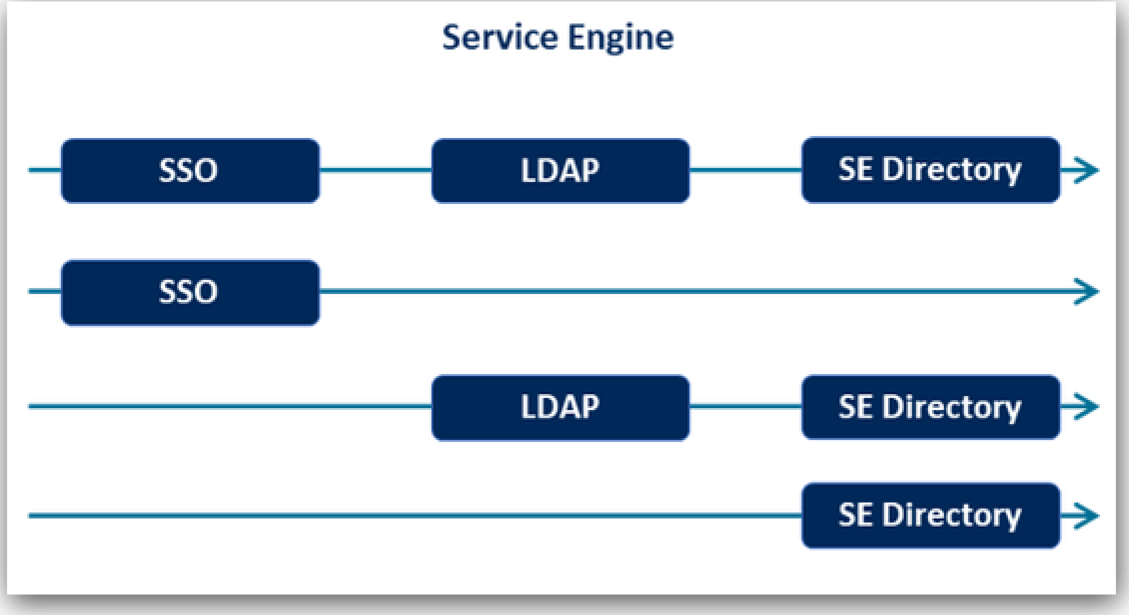
User authentication

Service Engine has the following means of authentication:

- Authentication via the application's internal employee database.
- Authentication via your LDAP/AD directory(ies).
- Authentication via an SSO compatible with our services.

The processing order for authorizations is as follows:

1. Identification based on SSO.
2. If step **1** is unsuccessful, authentication via login/password based on your LDAP/AD directory(ies).
3. If step **2** is unsuccessful, authentication via login/password based on the Service Engine internal directory.



Service Engine internal authentication can be deactivated. However, if you use Service Engine as a web service provider, authentication is performed via the Service Engine internal directory or LDAP authentication.

You can use several directories (or branches of the same directory) to authenticate your users. In this case, authentication will be performed by testing the directories in the order given.

Authorization of users

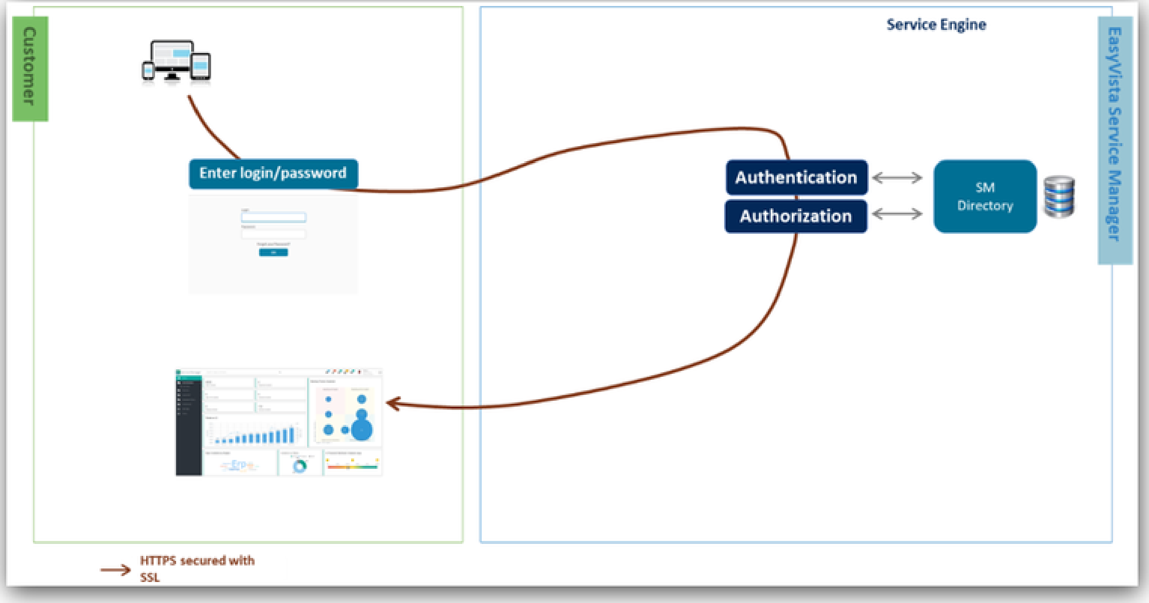
Once identified, the determination of what the user has the right to do and on what will be based on:

- Service Engine: profiles (what the user can create) and domains (what the user can see).
- Service Apps: Application groups that will define the accessible applications and the role associated with the user of each of these applications.

Service Engine - Internal authentication

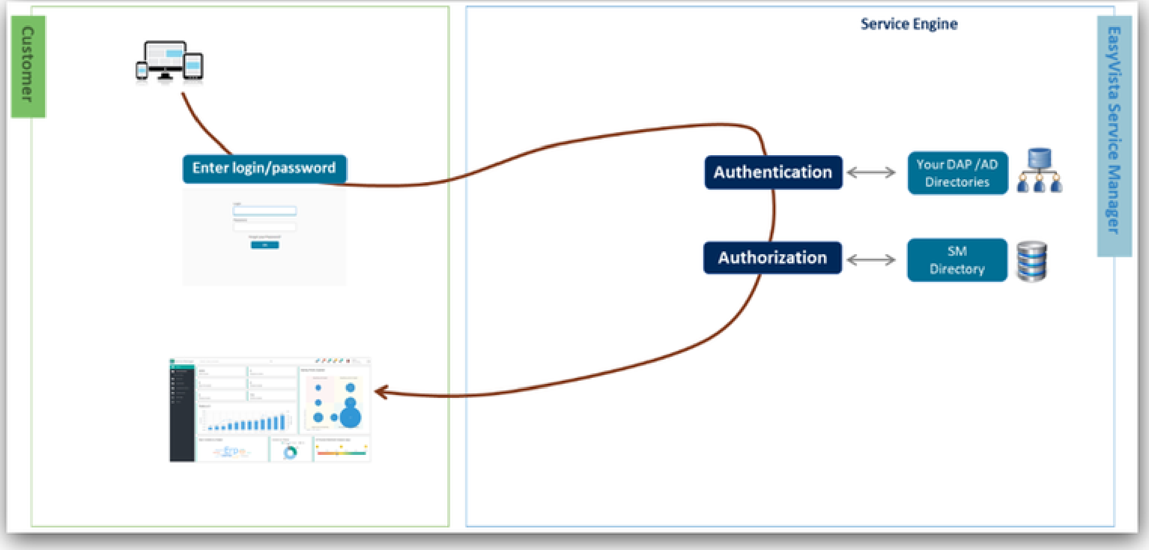
Passwords are stored in the form of a hash (non reversible).

A policy for the length and formation can be set.



Service Engine - Authentication via LDAP/AD servers or trees

Service Engine authentication can be based on several different LDAP/AD trees.



Service Engine - SSO (Single Sign On)

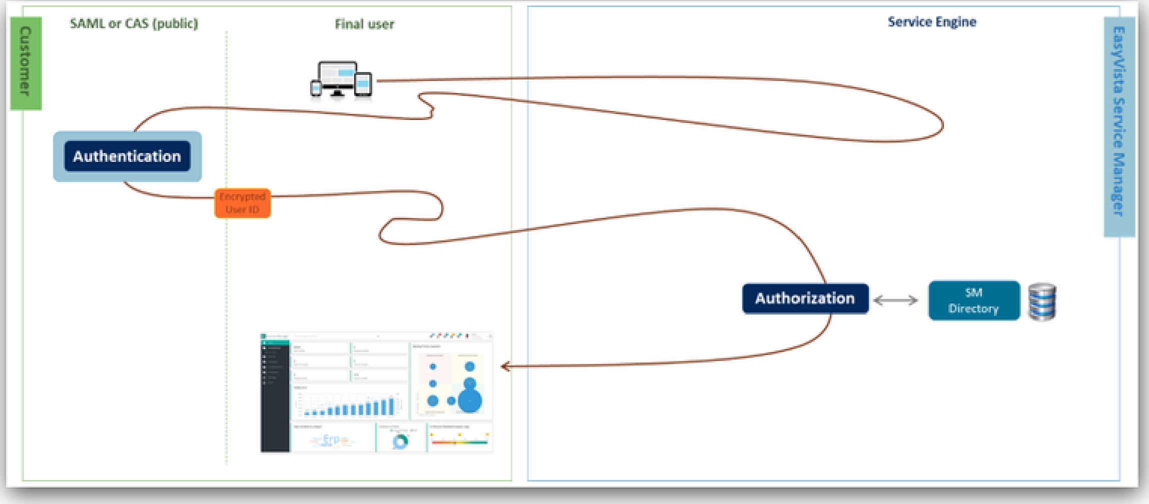
Introduction

Service Engine can authenticate users by providing identify information via our systems. The following systems are supported:

- SAML and ADFS.
- CAS.

SSO via SAML/ADFS or CAS

Your identity unifier is configured in our services so that user identification is provided upon initial connection to our services.



Systems supported but not recommended

If you have an IIS server somewhere on your network, it can be used to port the identity of your user to our services.

Caution: This is not SSO, but "identity porting" *(The user's identity is retrieved and transferred to our services through an encrypted header)*. You should consider this functionality as an easy connection for users, but in no way a completely secure solution compared to true SSO systems like SAML/ADFS or CAS which include multiple protections like:

- Derived unique key per transaction.
- Key exchange.
- Refusal of unsolicited responses.
- Impossible to perform "man in the middle" attack.
- Restriction of systems authorized to perform authentication and limited scope of accessible information.
- Traceability and alerts.

What's more, these systems rely on the fact that the user has already been identified at the network level. As a result, this will not work if our services must be accessed via a public network (which is the case for mobile applications, unless they use a VPN to simulate an internal network presence).

Identification systems specific to your company

Any identification system specific to your company can be analyzed to see how it can be used by our services (particularly in terms of availability, accessibility and security).

The analysis, development and implementation of this type of authentication will be billed separately based on their complexity.

Systems not supported or maintained

Note: This section concerns all the identification methods not previously mentioned.

Systems that require the installation of additional components on our platforms are not authorized (SSPI module, Kerberos module, etc.).

Service Apps - Authentication

Users are designated by their login.

Once identified by an EasyVista approved identity provider, the user can be looked up in the Service Engine directory using the login associated with their Employee form in the Service Engine directory.

If several EV Service Manager users share the same login, they will access the same user account in Service Apps.

AUTHORIZATION MANAGEMENT

Service Engine

In Service Engine, a user is allocated:

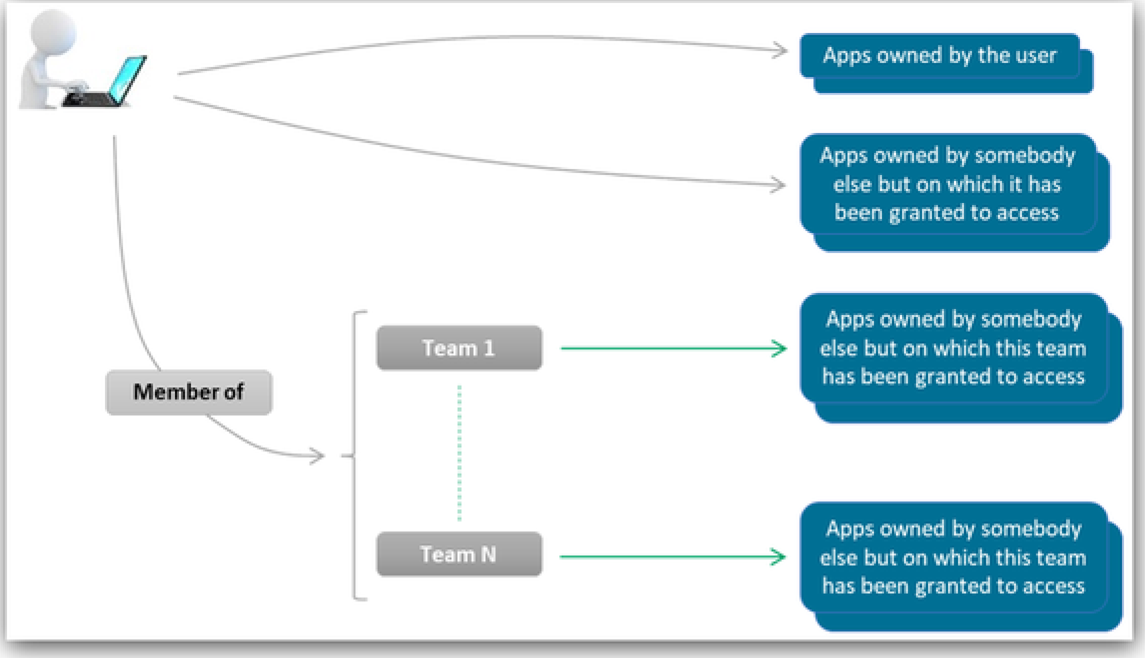
- A unique profile: This determines what the user has the right to do with all the data they have access to.
- One or more domains: These determine the scope of the date that the user has the right to access (for example, a geographical area, a type of machine with several entities, etc.).

Service Apps

How are access rights to an application granted?

A Service Apps user can be belong to several groups and have access to:

- Applications directly, because they own or have been given the right to use them.
- Applications through the teams they belong to that have the required access rights.


Apps owned by the user
Apps owned by somebody else but on which it has been granted to access
Member of
Team 1
Team N
Apps owned by somebody else but on which this team has been granted to access
Apps owned by somebody else but on which this team has been granted to access

How are teams identified in the Service Apps directory?

In the Service Apps directory, teams are identified by their name.

These Service Apps team names are linked to the English names of Service Manager groups.

OPTIONAL PACKS

Premium backup pack

Implementation services included in this pack:

- An incremental backup is performed every hour on the production account.
- A full backup of your production account, copied to one of your FTP servers, is made available to you every month.

Additional pack for document storage

This pack allows you to expand the storage capacity dedicated to documents accompanying the knowledge base, CMDB (Configuration Management Database), requests, contracts, equipment, etc.

The size of the database is not taken into account in the calculations.

On-premise EasyVista to EasyVista.com pack

Implementation services included in this pack:

- Migration of your current database to the latest Service Engine version.
- An EasyVista.com platform is provided with your data to validate the migration.
- Once you have evaluated the platform, the definitive migration of your database to EasyVista.com can be scheduled and implemented.

MYEASYVISTA

EasyVista provides you with an admin console that allows you to perform the following operations:

- Access contract details and status, including license utilization patterns.
- Check the availability metrics of your EasyVista.com platform so you can ensure that the cloud service level agreement (SLA) is adhered to.
- Carry out maintenance activities:
  - Database management, including restoration, backup and transfer.
  - EasyVista upgrade.
  - Functional recipe of the platform by you.
  - EasyVista service restart.

- Anticipate and assess high-impact events, then take action to avoid unnecessary downtime:
  - Availability metrics.
  - Size of databases.
  - Utilization rate and system activity.
    - Number of users connected.
    - Interaction details.
    - Utilization of the page and activity assistant.
    - Potential system errors.

- Rationalize and improve service delivery:
  - Understand which services are the most requested and the most problematic.
  - Identify the least used services.

SERVICE COMMITMENTS

EasyVista.com

Service availability

This service is available **7 days a week and 24 hour a day** outside of the maintenance periods specified below.

We guarantee 99.9% availability (calculated over a quarter, excluding scheduled maintenance periods).

Scheduled maintenance periods must not exceed 2 hours per month.

Performance

EasyVista servers are sized that the production performance of web pages meets our standards.

The load time varies depending on the page type and configuration. In 90% of cases, it is under 2 seconds.

The benchmark times are measured as an output from the EasyVista platform using the product's internal functions (ShowStack=simple). These measurements can be taken from any workstation.

Regular measurements are also taken by automated systems on the benchmark platforms and the EasyVista teams are alerted in the event of a problem.

If necessary, technical support can provide you with a procedure to follow to check for the most frequently encountered problems:

- Different use of the interface (too many lines displayed on screen in *List* mode, for example).
- Identification of components likely to slow down page loading on client workstations (browser cache configuration, antivirus, etc.).
- Analysis of traffic between client workstation and the EasyVista platform to detect any problems (proxy, etc.).

Subsequently, further actions to help you identify contextual performance problems are suggested for a fee.

Platform monitoring

The platform is automatically monitored by various tools for this purpose. Alerts are also automatically sent to the EasyVista CMC team.

Aspects covered by monitoring are:

- The data integration process.
- The users connected to the service.
- The workload coming from application services.
- The slowest requests executed on the platform.
- The use of disk space allocated under the contract.

Availability of the service, IP addresses and the database is automatically checked every 30 seconds.

Data backup

Databases linked to the production account are backed up according to the following schedule:

- Full daily backup, kept for 5 days.
- Incremental backup performed every hour.
- Potentially, transfer of a monthly database backup to one of our FTP servers.

The database linked to the sandbox account is not automatically backed up, but the client/partner can perform backups on request and restore them via MyEasyVista (it is possible to keep up to 5 different backups for an account and replace them as you see fit).

Data restoration request

All data restoration requests must be made by opening a request in MyEasyVista or through technical support, specifying the desired date and time for the restoration.

To restore your production platform's database, a service interruption is required.

Restoration phase	Description
Backup retrieval	Depending on the age of the backup and the restoration requested: • <=48 hrs: immediate availability, performed in under 2 hours. • > 48 hrs: 24 hours.
Restoration	• The date and time of the restoration are agreed with you. • The production platform is stopped. • The active database is backed up. • The requested database is restored. • Production is restarted. • The entire operation generally takes under an hour.

Batch processing

The import of inventory data is carried out between 6 pm and 6 am (Brussels/Copenhagen/Paris/Madrid time zone), and not immediately during the day.

If your teams work outside of these standard periods in the Brussels/Copenhagen/Paris/Madrid time zone, these periods can be moved to the times when your platform is inactive.

The integration of data specifically for your project must be scheduled so as not to disrupt your users.

Technical infrastructure

The EasyVista.com environments are hosted by providers meeting the following standards:

- Tiers 3+ or 4.
- ISO 27001, SOC2 certifications.
- Data storage locations that meet your legal requirements.

EasyVista service continuity

Automatic monitoring services are implemented on all the platform components. Dedicated teams are responsible for managing any anomalies detected and, if necessary, restoring good service.

Monitoring process

Phase	Action	Description
1	Detection	• 1st human assessment of the incident to determine whether it is indeed a problem. • If genuine alert, switch to phase **2**.
2	Information about the detection	• The relevant person at the partner/client is informed of the alert and its consequences, and receives an initial estimate of potential downtime. • Information e-mails are sent regularly to give the partner/client a progress report until the situation is resolved.
3	Resolution	Corrective measures implemented.
4	Information about the resolution	The partner/client is informed that service availability has been restored.
5	Analysis	• Information gathered (logs, screenshots, etc.) about the problem. • Information sent to EasyVista CMC teams who will determine whether the problem is likely to recur.

Priority is given to service restoration; analysis of the problem's causes takes second place if it takes too long.

For each monitoring incident, an incident ticket is created.

Aspects not included in service continuity

Anomaly	Corrective measure
Unexpected use of our SMTP server	• We strongly recommend that you use your own SMTP enterprise server for the EasyVista platform rather than our EasyVista.net SMTP server. • This is so that, when EasyVista sends e-mails to your end users from our EasyVista.net domain but using sender accounts from your domain, there are no delays and e-mails are not marked as spam. • For example, users who open an incident receive a confirmation e-mail from an account such as *backoffice@your_corporate_domain.com*. This account is in fact easier to identify and recognize than *donotreply@easyvista.net*. • In any case, there is a risk that your e-mail system considers this e-mail as spam and blocks or rejects it temporarily (greylists it), because the IP address of the EasyVista.net SMTP platform that appears to be the actual sender is not identified in the MX record of your DNS for *your_corporate_domain.com*. • For this reason, we cannot guarantee that e-mails will be immediately transmitted in the order they were sent, or that they will even be delivered. The only way to avoid this risk is to use your own SMTP server, either directly if it's accessible externally, or via a VPN connection if not.

Continuity of the monitoring service

Various sites are qualified and configured for the physical and logical administration of the host platform. If the main administration site becomes unavailable, our teams are transferred to a secondary site to prevent any interruption in platform monitoring.

Disaster recovery plan

In the event of prolonged downtime of the main site, a secondary site is available.

- Recovery point objective (RPO) = 2 hours.
- Recovery time objective (RTO) = 4 hours.

If the disaster recovery plan has to be triggered, the following measures will be taken:

Phase	Action	Description
1	Detection	Internal detection and confirmation of problem.
2	Decision	Based on the information provided and the possible downtime estimated, the CEO or the CTO decides to implement the disaster recovery plan.
3	Downtime notification	Management at the partner/client concerned are sent an e-mail informing them that the disaster recovery plan will be implemented and what the consequences in terms of downtime will be.
4	Integration/configuration	The secondary site is configured as the main site.
5	Notification of disaster recovery plan site availability	Management at the partner/client receive an e-mail informing them that the secondary site is available and providing links to access it.
6	Correction	The problem that required implementation of the disaster recovery plan is corrected on the main site.
7	Notification/schedule	An e-mail is sent to the client to inform them that the correction has been performed on the main site and to schedule restoration of the client platform on this site.

The priority is to restore availability of the Service Manager interface.

Return of data

At the end of the contract, data is returned to the client on DVD, in the form of an SQL Server backup of the Service Engine database in the version used by the hosted platform at that time. This backup includes the configuration database associated with the production account and acceptance account.

The backups in our possession are then destroyed once the client has confirmed safe receipt and reading of this data.

The following are not included by default but can be requested for a fee:

- Delivery in any other format or on any other media.
- Assistance in using and understanding this data.
- Integration of this data into a third party tool.
- Backups of test databases (sandbox).