White Paper
Self Help - SaaS

TABLE OF CONTENTS

Contents

Download the PDF file

PRESENTATION

The purpose of this white paper is to help you understand how the SaaS-based Self Help can be integrated within your technical environment.

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

PRODUCT GLOSSARY

Self Help is based on three main functions:

- A presentation function for procedures and the virtual agent.
- An edition function for procedures and the virtual agent.
- A Self Help Studio thick client installed on the workstations of writers in charge of procedures.

Depending on your project, the edition and presentation functions may be hosted on a single machine or they may be hosted on different machines. The target architecture and integration within your infrastructure must take this into consideration.

OVERALL ARCHITECTURE

Access to Self Help

You can access the service:

- Via a URL in the following format: *https://xxxxxx.ezvsaas.com*.
- Via web services.

No other external access to the platform is authorized, including:

- Access to the database.
- Remote control of servers in the architecture.

Components of different services

A Self Help platform may be made up of one or more servers.

Depending on the operating requirements and constraints of the project, the architecture may be affected by the following:

- Segregation of roles (edition, presentation or test).
- Load balancing among presentation servers or among server roles.

Each server on the platform can support the following functions:

- A presentation function for procedures and the virtual agent.
- An edition function for procedures and the virtual agent.

Single server platform

All functionalities are supported on the same machine.
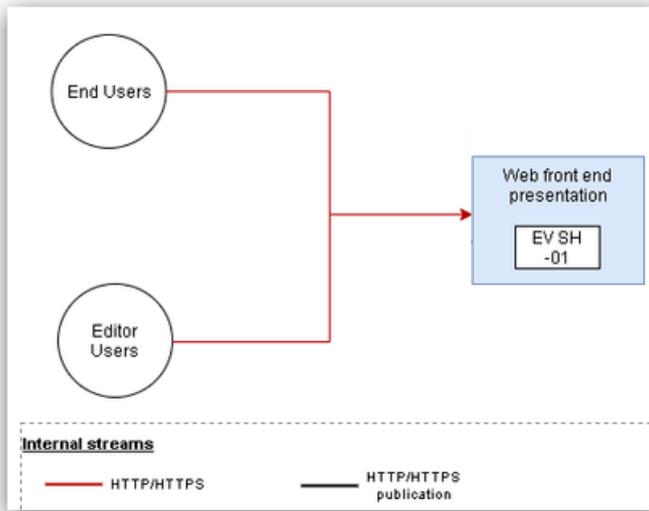
Multi-server platform

The configuration below is used to dedicate one machine on the platform to the following:

- Edition and testing of procedures.
- Configuration and testing of the virtual agent.

This machine will be in charge of publishing the configurations on presentation servers.
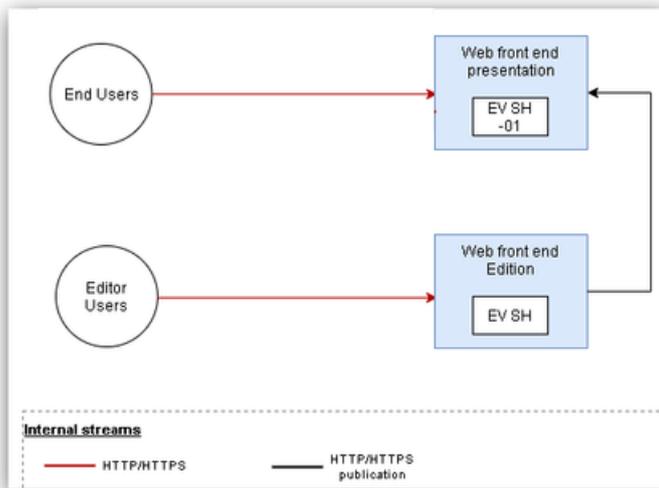
Adaptability to your constraints

Progressive scaling

The Self Help architecture is scalable. It can be reviewed and modified based on changes in your requirements. You can start your project with a basic architectural model and review it subsequently, for example, when the number of concurrent users increases.

The diagram below shows a few examples of the possible presentation server architectures.

Security of your data in transit

To safeguard the confidentiality and integrity of data flows, an SSL certificate will systematically be installed on your platform.
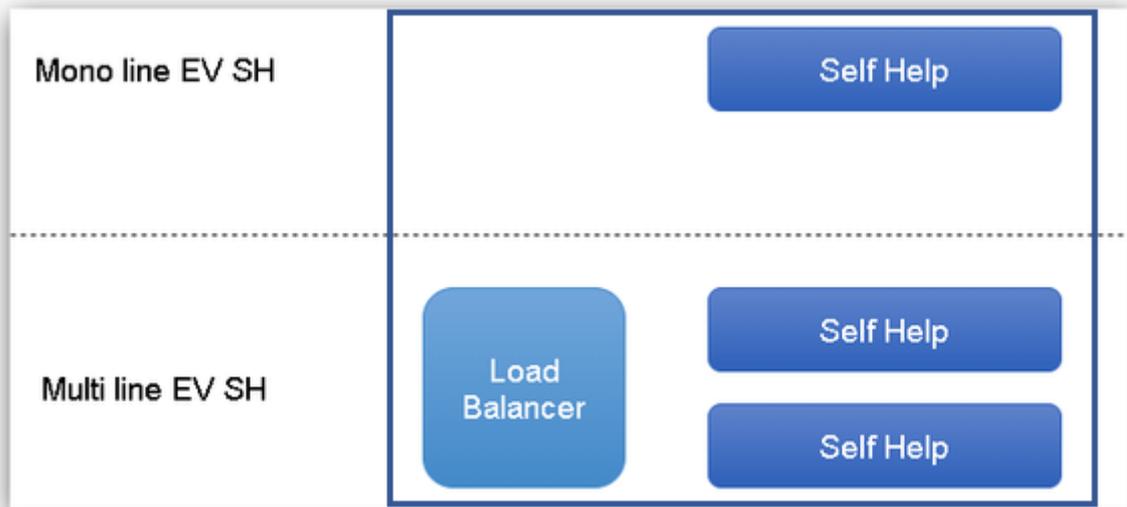
If you wish to use your own domain name, you must provide us with a suitable SSL certificate that complies with our security requirements (no self-signed certificates, valid for at least the length of the agreement, etc.).

On EasyVista servers, the SSL layer 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

Besides the production environment, you can purchase 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 such as Apache, Tomcat, SSL, etc.
- Version upgrades or fixes to the operating system or server components.

Browsers

Suppliers

Because the browser market is constantly evolving, please refer to our Supported Web Browsers wiki page for an up-to-date list of compatible browsers.

Configuration

Pop-ups and JavaScript must be enabled and authorized for Self Help.

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.

Others

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

Cookies

Our services use cookies in order 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.

Configuration of the client workstation for writers

Self Help Studio is a Java/Eclipse RCP application that runs in connected mode in https (port 443) on TCP/IP on the central edition server. The only infrastructure required is Java Virtual Machine 1.8 shipped and installed with the Studio.

Hardware configuration:

Prerequisites	
OS	Windows 7 and later
CPU	Intel core i3 or higher (or AMD equivalent)
Web browser	For standard skins delivered with the software, the following browsers are supported: • Google Chrome 70 • Firefox version 63.0 • Edge 42 • Internet Explorer 11
Memory	4 GB
Disk space	1 GB

The Studio can be connected to the edition server via a corporate proxy.

FUNCTIONAL INTEROPERABILITY

Schematic diagram

The diagram below displays interoperability with Self Help.
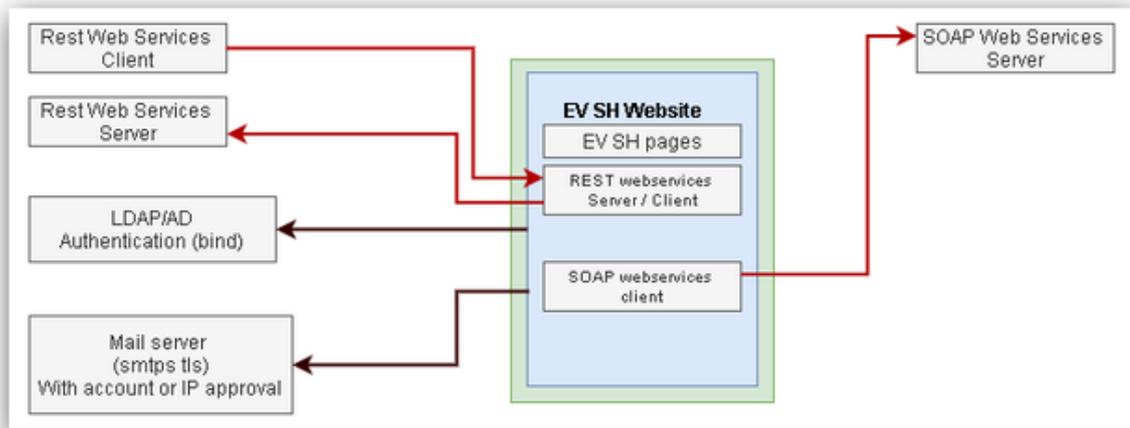
Overview

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.

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 provider

Our services are accessible using REST.

SOAP 1.2 and REST client

The services can use external REST or SOAP 1.2 services.

Email

Self Help must access your email server to send emails to users.

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

Interoperability with EasyVista Service Manager

Self Help communicates with Service Manager via https/http flows for the following functionalities:

- At the end of Self Help procedures, tickets are created via REST or SOAP in Service Manager.
- Self Help Extractor: from Service Manager to Self Help in https to consolidate procedures in the knowledge base.
- From Service Apps, to present Self Help procedures in https.

Interoperability with all other tools

Self Help communicates with your tool via https/http flows for the following functionalities:

- At the end of Self Help procedures, tickets are created via REST or SOAP in your tool.

VPN connection

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 of emails = <1 KB
- Validation of authentication by login/password = <1 KB

Access to Self Help is performed exclusively via an Internet connection and not through the standard VPN integrated with the platform.

If the customer wants access via the VPN and not via a standard Internet connection, the VPN bandwidth must be scaled accordingly.

A VPN connection is required if you want to integrate EasyVista.com within your infrastructure and if you do not want your servers to be accessible via a public IP address.

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 the pack is purchased:
    - AD/LDAP authentication.
    - Use of your email server to send data.
    - Three-way SSO system. User credentials sent to EasyVista.com require an additional flow with your servers in order to be decrypted.

VPN connection availability

Availability and responsibility in the event of maintenance depend 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. If this is not the case and if you switch to the backup platform, EasyVista will run automatically using the new configuration. Authentication will no longer be performed via your infrastructure, but via the authentication system integrated within EasyVista.

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	• Quick implementation, no line to configure, generally takes less than two days • Lower cost • High-level security even if data travels over the Internet	Encrypted tunnel but data does not travel over a private line
Point-to-point private	• Maximum privacy • Dedicated connection to access the EasyVista service instead of using standard Internet access	• Cost of implementation and use • Line installation often exceeds four weeks

External flow matrix

Source	Destination	Ports	UDP / TCP
Your users	Presentation server	443 (https)	TCP
Your functional administrators	Edition server	443 (https)	TCP
Edition server	Presentation server	443 (https)	TCP
Presentation server	EV SE Web front-end	443 (https)	TCP
Presentation server	EV SA Web front-end	443 (https)	TCP
EV SE Web front-end	Presentation server	443 (https)	TCP

RESPONSIBILITIES DURING IMPLEMENTATION PHASES

Implementation phase	Description
Installation	• EasyVista will install and configure the environments and then create the production and test accounts. • During this phase, the customer or partner will not have access to the system. • Once installation is complete, the customer will receive a document containing information for logging in to the EasyVista website.
Implementation by the customer	• The customer or authorized partner will configure EasyVista based on their requirements. • During this phase, the EasyVista.com backup and restoration system, monitoring services and disaster recovery plan services will not be enabled. • Once implementation is complete, the customer can ask our Technical Support team to start the production phase.
Production	• The EasyVista.com backup and restoration system, monitoring services and disaster recovery plan services, as well as the corresponding alerts, will be enabled.

MIGRATION TO A MORE RECENT VERSION

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

Responsibilities

The EasyVista CMC (Cloud Management Center) operational teams will perform the migration to the new version based on the standard migration process.

An email will inform you that an update is available and send you 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 required, our consultants or authorized partners are there to provide assistance and technical support.

Testing the new version

If you have a qualification environment, our teams will first upgrade this environment. This will enable you to test it according to your procedures, e.g. non-regression, new functionalities, etc.

Once this version has been validated by our teams, you can schedule the migration of your production environment together with our teams.

Note: You cannot have two Self Help versions in a given environment.

Installation in the production environment

Migration phase	Standard duration	Description
Availability of the upgrade		The availability of Self Help upgrade versions is usually identical for both SaaS-based and on-premises customers.

Migration of the qualification environment	1 day	• Customer: Technical Support receives a request to upgrade your qualification environment to the new version.
		• EasyVista CMC:
		 • Schedule a date for the upgrade.
		 • On the scheduled date:
		  • Upgrade the qualification environment based on the current version of your production environment.
		  • Upgrade the qualification environment based on the new Self Help version.
		  • Send the customer an email to confirm the migration of the qualification environment to the new version.

Validation	Variable	• Customer: Validation process and testing of new functionalities **Caution**: Modifications made to the test environment will not be kept when migrating the production environment.
Scheduling of the migration of the production environment	0.5 day	• Customer: Once you are ready, i.e. the process is validated, users are trained, please ask our Technical Support team to upgrade the production environment. • EasyVista CMC: • The date and time of the migration will be arranged together with you.
Migration of the production environment	From 2 to 4 hours	• Customer: Users must be informed that the production environment will be unavailable during the migration phase. • EasyVista CMC: On the scheduled date: • Back up databases prior to migration. • Perform migration to the new version. • Test the migration. • An email will inform the customer that migration is complete. • The production environment is once more available.

TECHNICAL MAINTENANCE OF ENVIRONMENTS

Platform security

Default security

Our platforms are configured to minimize security risks:

- Automatic access restriction (*None by default* policy)
- IPS/IDS for detecting malicious access
- Anti-DDOS for reducing risks of unavailability
- Antivirus to ensure system integrity

Vulnerability tests

Vulnerability tests are run weekly by our QUALYS partner on all platforms.

Maintenance of operational conditions

To enable our teams to keep your platforms in optimal condition, three hours of technical maintenance are scheduled monthly, during which the operating systems and components used are upgraded.
Note: The time spent on maintenance may vary as required.

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

- Automatically by our teams based on observed activity in order to minimize impact on your users, e.g. at night, on Saturdays.
- Jointly with you if you want to select a specific time slot from those available, e.g. at night, on Saturdays.

When an operation is scheduled, an email will inform you of the date, time and duration of the operation.

Yearly blackout period

A blackout period is systematically scheduled for the last week of calendar year Y and the first week of the calendar year Y+1.

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

example

USER AUTHENTICATION

Role distribution

For Self Help, we differentiate:

- Authentication: Confirmation of the user identity that is logging in.
- Authorization: Rights of the logged-in user in Self Help.

User authentication: Self Help with Service Engine

Self Help provides the following authentication methods:

- Authentication using the application's internal employee database.
- Authentication via Service Engine.

The authentication methods supported by Service Manager are as follows:

- Authentication using the application's internal employee database.
- Authentication via your LDAP/AD directory.
- Authentication via an SSO system compatible with our services.
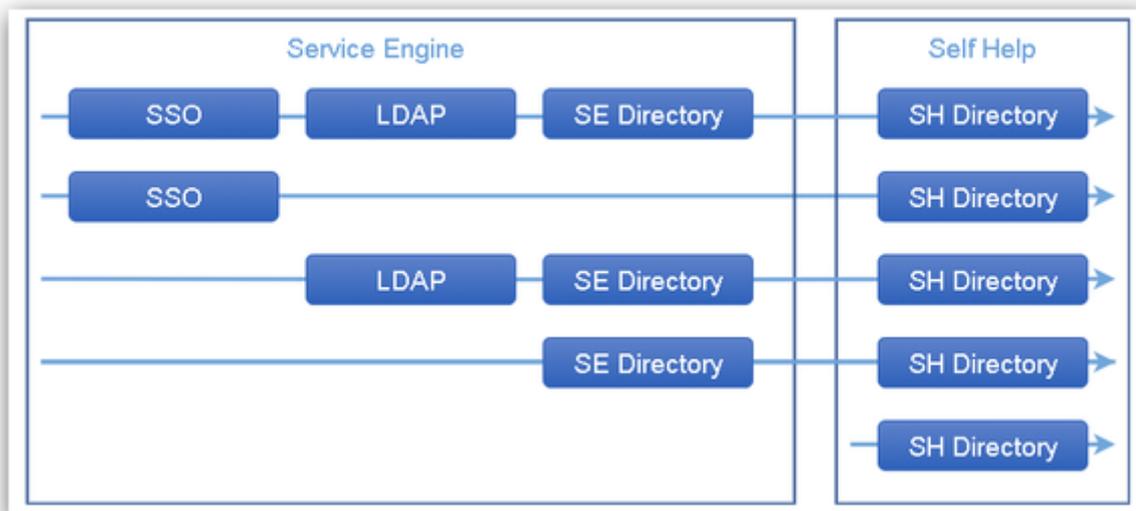
User authentication: Self Help without Service Engine

Self Help can be connected to another tool without Service Engine.

Self Help provides the following native authentication methods:

- SSO SAML as client of your SSO system.
- Authentication on LDAP servers via a bind.
- Authentication using the application's internal employee database.

Self Help   - Internal authentication

Passwords are stored in a hash (non-reversible).

In the Self Help directory, users are identified by their login which is also used for authentication. This means that each login can only be used once to identify a given user.

Self Help   - Trusted Provider based on Service Engine

Self Help can use Service Engine to authenticate the user and perform first-level authorization.

In this case:

- Authentication is managed by Service Engine based on the methods configured, i.e. internal authentication, multi LDAP/ AD, SSO.
- Service Engine also performs first-level authorization. Users are known and active with a language defined, etc.
- Once users are validated by Service Engine, Self Help accepts and adds them to its local database if required.

The following information is sent by Service Engine so that Self Help can automatically populate its internal directory and rights management system:

- Full name of the employee.
- Employee login.

Only one Trusted Provider can be associated with Self Help.

AUTHORIZATION MANAGEMENT

Self Help

Self Help ensures secure access to the entire application as well as secure access to each project.

Access to the application

An account on the Self Help server is required. This account must be associated with one or more domains, directly or assigned to a member of a user group.

The application is accessed via a login window.

Access rights

Only administrators can access all of the functionalities in the *Administration* module.

Access rights are defined for each project, e.g. administration, modification, duplication, execution, and are specific to each writer.

Virtual agent

Users

User authorizations for communicating with the virtual agent (access to the virtual agent's Self Help project procedures) are managed in the group to which the user belongs.

User groups can be created using various criteria, e.g. department, location, level of skill, etc.

Writers

Writers are usually subject knowledge experts. They write and publish procedures.

- They are authorized to work on the virtual agent's Self Help projects based on their read, write and publish rights. See Access rights management.
- They are supervised by the Knowledge Manager.
  - The role of this person is to ensure the uniformity of the virtual agent's Knowledge Base, ensuring that each procedure is written in the same way in compliance with the style guide.
  - The Knowledge Manager also makes sure that the topics covered by the virtual agent fall within the functional scope.

OPTIONAL PACKS

Additional pack for document storage

This pack enables you to expand the storage capacity for documents attached to procedures.

The size of the database is not taken into consideration in the calculation.

On-premises 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 will be scheduled and performed.

SERVICE COMMITMENTS

EasyVista.com

Service availability

This service is available 24/7 apart from the maintenance periods defined below.

We guarantee an availability rate of 99.9% calculated over a quarter, excluding scheduled maintenance periods.

Scheduled maintenance periods must not exceed two hours per month.

Performance

EasyVista servers are sized to ensure that web display performance in the production environment meets our standards.

Loading times vary depending on the page type and configuration. In 90% of cases, it is under two seconds.

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:

- Non-standard use of the interface, e.g. too many rows displayed in *List* mode.
- Identification of components likely to slow down page loading on client workstations (browser cache configuration, antivirus, etc.).
- Analysis of traffic between client workstations and the EasyVista platform to detect problems, e.g. proxy, etc.

Other actions to help you detect context-specific performance issues are available on a fee-paying basis.

Platform monitoring

The platform is automatically monitored by different tools. Alerts are also automatically sent to the EasyVista CMC team.

Aspects covered by monitoring are as follows:

- Data integration process.
- Users connected to the service.
- Workload from application services.
- The slowest requests run on the platform.
- Usage of disk space allocated per agreement.

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

Data backup

Databases linked to the production account are backed up according to the frequency below:

- Full daily backup, stored for a period of five days.
- Incremental backups run hourly.
- If required, transfer of a monthly database backup to one of your FTP servers.

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 two hours - > 48 hrs: 24 hours

Restoration	- The date and time of the restoration are arranged together with your teams.
	  - 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.

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, for restoring the smooth running of the service.

Monitoring process

Phase	Action	Description
1	Detection	• First human assessment of the incident to determine whether it is indeed a problem. • If it is a genuine alert, proceed to phase **2**.
2	Information regarding the detection	• The relevant partner or customer contact is informed of the alert and its consequences, and receives an initial estimate of potential downtime. • Progress reports are sent regularly by email to the partner or customer until the situation is resolved.
3	Resolution	• Corrective measures implemented.
4	Information regarding the resolution	• The partner or customer is informed that the service is now available.
5	Analysis	• Information collected on the problem, e.g. logs, screenshots, etc. • 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 corporate SMTP server for the EasyVista platform instead of our EasyVista.net SMTP server. • This is to ensure that there are no delays and that emails are not marked as spam when EasyVista sends emails to your end users from our EasyVista.net domain using sender accounts from your domain. • For example, users who open an incident will receive a confirmation email from an account such as *backoffice@your_corporate_domain_name.com*. This account is easier to identify and recognize than *donotreply@easyvista.net*. • In any case, your email server may consider this email to be spam and block or reject it temporarily (greylisting), 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_name.com*. • For this reason, we cannot guarantee that emails will be immediately transmitted in the order they were sent, or that they will even be delivered. The only way to eliminate this risk is to use your own SMTP server, either directly if it is accessible externally, or if it is not, via a VPN connection.

Continuity of the monitoring service

Various sites are qualified and configured for the physical and software 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 is 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 may decide to implement the disaster recovery plan.
3	Downtime notification	An email will inform partner or customer managers that the disaster recovery plan will be implemented and describe the consequences in terms of downtime.
4	Integration/Configuration	The secondary site is configured as the main site.
5	Notification of disaster recovery plan site availability	An email will inform partner or customer managers that the secondary site is available and provide 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 email will inform the customer that the correction has been performed on the main site and schedule restoration of the customer platform on this site.

The priority is to restore the availability of the Self Help interface.