Matrix42 Cloud Services

EgoSecure Data Protection 15 as Cloud Solution

Contents

1 Introduction

This document describes the functionality of Matrix42 EgoSecure (ES) Data Protection version 15 as a cloud solution using the same product platform as On-Premise and differing only in product usage.

2 Components

The following table shows the differences in the individual components between the on-premise and cloud solution.

2.1 EgoSecure Bundles

Component	On-Premise	Cloud
EgoSecure Access Control	●	●
EgoSecure Secure Audit	●	●
EgoSecure Secure Audit – Shadow Copy	●	○
EgoSecure Application Control	●	●
EgoSecure Removable Device Encryption	●	●
EgoSecure Local Folder Encryprion	●	●
EgoSecure Cloud Encryption	●	●
EgoSecure Network Share Encryption	●	●
EgoSecure Full Disk Encryption	●	●
EgoSecure Pre-boot Authentication	●	●
EgoSecure Permanent Encryption	●	●
EgoSecure IntellAct Automation	●	●
EgoSecure Insight Analysis	●	●
EgoSecure Antivirus	●	●
EgoSecure Tools	●	●
EgoSecure DLP (Deep Content Analysis)	●	●

● possible, ◗ partly possible, ○ not possible

2.2 Supported Addons

Component	On-Premise	Cloud
E-Mail Encryption	●	●
Mobile Encryption	●	●
Cloud-Connect Server (CCS)	●	●

● possible, ◗ partly possible, ○ not possible

2.3 Supported Operating Systems

Component	On-Premise	Cloud
Windows	●	●

● possible, ◗ partly possible, ○ not possible

3 Use of the cloud service

3.1 Accessing the cloud service

Access to the Cloud Service is via the EgoSecure Management Console and an SSL connection via port 443. Access to the Matrix42 Cloud Service via the Remote Desktop Protocol (RDP) and to the file system is not possible for either consultants or customers. Only the Matrix42 Cloud Operations Team and Matrix42 Support are eligible. Consequently, no changes can be made at the file level. It is also not possible to access the database or the SQL server to read or manipulate data. The following table shows the different access options.

Method	On-Premise	Cloud
EgoSecure Console (SSL)	●	●
RDP	●	○
File access	●	○
SQL Server	●	○
Matrix42 Marketplace Apps	●	●

● possible, ◗ partly possible, ○ not possible

3.2 SSL certificate and domain

The domain name (FQDN) of the customer environment is assigned by Matrix42 as subdomain of "m42cloud.com" in the scheme "egosecure000.m42cloud.com". The subdomain can be freely chosen on customer request depending on availability. The corresponding SSL certificate for a secure connection via SSL is also provided and managed by Matrix42. Customer domains or certificates are not possible because they are not managed by Matrix42 Cloud Operations. The following table shows the differences to On-Premise.

Method	On-Premise	Cloud
Customer's own SSL certificate	●	○
Self-signed SSL certificate	●	○
Own FQDN	●	○

● possible, ◗ partly possible, ○ not possible

3.3 EgoSecure Agent

The connection of the EgoSecure Agent takes place in the polling interval, i.e. the agent reports to the EgoSecure Cloud Service after a specified time window. The time window can be defined via the EgoSecure console and is 60 minutes by default.

3.4 EgoSecure Secure Audit, IntellAct Automation and Insight Analysis

The Secure Audit, IntellAct Automation and Insight Analysis functions record various activities on the client via the EgoSecure Agent and can be displayed within the EgoSecure console for evaluation. This information is held for 30 days in the cloud service and then exported. The export is maintained for a further 60 days and can be downloaded from Matrix42 Support at the customer's request.

3.5 E-Mail connection

Matrix42 EgoSecure Cloud Services have pre-configured an SMTP server for outbound email by default. The transmission of data is encrypted via a TLS connection. It is not possible for customers to access the SMTP server and make settings. From the customer's point of view, a separate mailbox must be integrated to receive e-mails. For the connection, the options available in the product standard can be used without restriction. Customers can use their own SMTP server to send e-mails.

4 Authentication

The authentication of users in Matrix42 EgoSecure takes place in different ways, but is only possible on the basis of the Matrix42 EgoSecure internal management structure. The following chapters describe the different scenarios. The following table shows all authentication options.

Method	On-Premise	Cloud
AD-Authentication	●	○
AAD-Authentication	●	●
ES internal Domain	●	●

● possible, ◗ partly possible, ○ not possible

4.1 Microsoft Azure Active Directory (AAD)

The connection of an AAD enables the synchronization of directory objects and directory structure and can be configured via the EgoSecure console. This allows administrative user accounts to be linked to an AAD user account.

4.2 ES internal Domain

Importing users and computers into a Matrix42 EgoSecure Cloud Service is done by automatically registering and adding objects by the EgoSecure Agent when the agent is installed or when an unknown user logs into EgoSecure's own management structure (Own Directory). The objects are created on the server in a structure tree that has the domain name as root. OUs and groups can be created and filled/linked with objects for better clarity.

4.3 Single Sign-on (SSO)

Users must authenticate to the EgoSecure console independently of the Windows logon. SSO is therefore not available.

5 Integration

Method	On-Premise	Cloud
Matrix42 Service Management	●	◗
PROVAIA by PRESENSE	●	●
Macmon Network Access Control (NAC)	●	○
PRTG	●	○

● possible, ◗ partly possible, ○ not possible

5.1 Matrix42 Service Management

Matrix42 EgoSecure can be connected to Matrix42 Service Management via Matrix42 Workflow Studio when both are on the same network. If, for example, Matrix42 Service Management is operated in the customer network and Matrix42 EgoSecure Data Protection is purchased from the cloud, no connection is currently possible. This also applies in the reverse case. If both software solutions are in the Matrix42 cloud or in the customer network, a connection is possible without problems.

5.2 Workflow Studio Integration

With the Matrix42 Workflow Studio, processes can be carried out automatically in a single operation. For example, when data access anomalies, applications, or suspensions are detected, tickets or incidents can be automatically created in the Matrix42 Service Desk.

5.3 PROVAIA by PRESENSE

The connection to the data gateway of PRESENSE can be made by specifying the XML report certificates and activating the respective filter in EgoSecure Access Control.

5.4 PRTG

The integration with PRTG from Paessler is only possible for clients, not for the EgoSecure Cloud Service.

6 API access

Matrix42 EgoSecure does not currently offer an external management interface. For configuration changes, the EgoSecure Management Console is provided as an executable application.

7 Customizings

For Matrix42 EgoSecure there is no customizing option.

8 Glossary

Term	Explanation
AD	Active Directory (AD) or Active Directory Domain Services (ADDS) is a directory service Microsoft has developed for Windows domain networks. It stores information about members of the domain, including devices and users, verifies their credentials and defines their access rights. The server running this service is known as a domain controller. A domain controller is contacted when a user logs on to one device or accesses another device on the network.
AAD	Azure Active Directory (AAD) is Microsoft's cloud-based identity and access management service and can share information with other services based on SAML 2.0 or OAuth 2.0.
ADFS	Active Directory Federation Services (ADFS), a software component developed by Microsoft, can run on Windows Server operating systems to allow users single-sign-on access to systems and applications across corporate boundaries. ADFS can interact with other SAML 2.0 compliant federation services as a federation partner.
HTTP/S	The Hypertext Transfer Protocol (HTTP) is a stateless protocol for transmitting data on a network. In the Hypertext Transfer Protocol Secure (HTTPS) the data is transmitted between web servers and web browsers encrypted.
OAuth2	Open Authorization (OAuth) 2.0 is an open protocol and provides specific authorization processes for web applications, desktop applications, mobile phones and smart devices.
SAML2	Security Assertion Markup Language (SAML) 2.0 is an XML framework for sharing authentication and authorization information and provides capabilities to describe and transmit security-related information.
Single Sign-on	Single Sign-on (SSO) allows users to use other services they are entitled to without logging in again after one-time authentication.
TLS	Transport Layer Security is a hybrid encryption protocol for secure data transmission on the internet and a further development of the Secure Sockets Layer (SSL) protocol.

9 Abbreviations

Abkürzung	Bedeutung
AAD	Azure Active Directory
AD	Active Directrory
ADFS	Active Directory Federation Services
CA	Certificate Authority
ES	EgoSecure
FQDN	Fully Qualified Domain Name
HTTP/S	Hypertext Transfer Protocol/Secure
LAN	Local Area Network
OAuth	Open Authorization
OLEDB	Object Linking and Embedding, Database
RDP	Remote Desktop Protocol
SAML	Security Assertion Markup Language
SASM	Software Asset & Service Management
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign-on
TLS	Transport Layer Security

Effective: March 2020