FORTINET | SECLORE

DEPLOYMENT GUIDE

Seclore Email Auto Protector and Fortinet FortiMail

Seclore Email Auto Protector and Fortinet FortiMail

1. Introduction

This document explains how to deploy and configure Seclore Email Auto Protector with Fortinet FortiMail for automatic protection of emails and attachments.

2. Introduction to Seclore Rights Management

Seclore Rights Management protects sensitive information regardless of device or location. Whether a file is on a server, in an email, on a mobile device, or copied to a USB memory stick unintentionally left behind in an airport, unauthorized users will not be able to access the information. Since usage policies stay with the file, Seclore enables organizations to securely adopt the cloud, BYOD, and external collaboration.

Seclore makes it easy to centrally define, associate, enforce, modify, and audit granular file usage permissions including:

WHO can access the file?
User or Groups Within or Outside the Organization

WHAT can they do with it?
View, Edit, Print, Copy Content, Take Screen Grabs, Work Offline

WHEN can they do it?
Automatic File Expiry, Date and Time Ranges, Number of Days from First Access

WHERE can they do it?
Specific Computers or Devices, Specific IP Address

3. Extend Your Email Security with Seclore Email Auto Protector

Seclore Email Auto Protector, a key part of Seclore Rights Management technology, allows you to: Seclore Email Auto Protector, a key part of Seclore Rights Management technology, allows you to:

- Secure and track your emails—even when sent to other domains
- Automatically add protection to emails and attachments being sent or received without relying on the end user
- Control how the authorized recipient can use the attachment (view, edit, cut/paste, print)
- Track the use of emails and individual attachments
- Expire or revoke emails sent (undo) or forwarded to the wrong recipient by mistake or malice

4. How Does It Work?

User creates an outgoing email or there is an incoming email sent by a user outside of the enterprise domain. In both outgoing and incoming email scenarios, the email is received by the email service. The email service will then route the email to FortiMail, which based on certain criteria and sensitivity of the email will insert an X-Header in the email and relay the email to the Seclore Email Auto Protector component. The Seclore Email Auto Protector acts as a Mail Transfer Agent (MTA)and allows for organizations to set up protection rules to automatically apply usage controls to emails and attachments in the background without human intervention. The process is completely transparent to the email sender.

Email is sent by a user

Email Server or Cloud Service receives email

FortiMail inserts X-Header in the email

Email Auto-Protector checks if any rules are met

Recipients receive protected email that is protected and trackable

5. Components Required

1. **FortiMail**—Secure Email Gateway for inspecting emails
2. **Seclore Policy Server**—Seclore Policy Server is the central unified policy server engine responsible for key and policy management
3. **Seclore Identity Manager and OpenDJ**—User repository for storing and managing external user identities
4. **Seclore Lite Online**—Document rendering engine for accessing protected documents in an agentless manner via a browser
5. **Database**—Database instance to store user activities, policy definition
6. **Seclore Email Auto Protector**—Seclore MTA for auto protecting emails and attachments based on rules

6. Deployment Requirements

6.1. Server Requirements

Server Role	OS Requirements
Seclore Policy Server	Windows 2012 R2 / 2016 / 2019
Seclore Identity Manager and OpenDJ	
Lite Online	
Database (MSSQL 2012–2017 OR Oracle 12c, 18c, 19c)	Windows 2012 R2 / 2016 / 2019
Seclore Email Auto Protector	RHEL 7.4 x64 and above OR CentOS 7.4 x64 and above

6.2. Deployment Options

- On-premises
- On-cloud

7. Components—System Requirements and Prerequisites

7.1. Seclore Policy Server

7.1.1. Server Requirements

- OpenJDK 11.0.1
- Tomcat 9.0.13Secure and track your emails—even when sent to other domains

7.1.2. Prerequisites

- Policy server should be accessible from the local enterprise network as well as internet
- Valid SSL Certificate
- Policy Server License (customer specific)
- One Active Directory user (password set to never expire) for AD integration for user authentication.
- Connectivity to SMTP Gateway to send emails using the enterprise email system
- Connectivity to Database, Windows AD, OpenDJ and Lite Server

7.2. Seclore Policy Server

7.2.1. Server Requirements

- OpenJDK 11.0.1
- Tomcat 9.0.13

7.2.2. Prerequisites

- Connectivity to OpenDJ service
- Connectivity to SMTP Gateway to send emails using the enterprise email systems

7.3. OpenDJ Server

7.3.1. Server Requirements

- OpenJDK 11.0.1
- Compatible with OpenDJ 2.6.2

7.4. Seclore Lite Online Server

7.4.1. Server Requirements

- Connectivity to Database and Policy Server
- Apache HTTP server

7.4.2. Prerequisites

- Connectivity to Database and Policy Server
- Apache HTTP server

7.5. Seclore Policy Server

7.5.1. Server Requirements

- CentOS 7.4 (x64) and above OR RHEL 7.4 (x64) and above

7.5.2. Prerequisites

- No other application should be running on port, 8080, 8005 (reserved for tomcat), 9999 (reserved for milter)
- Internet connection is mandatory

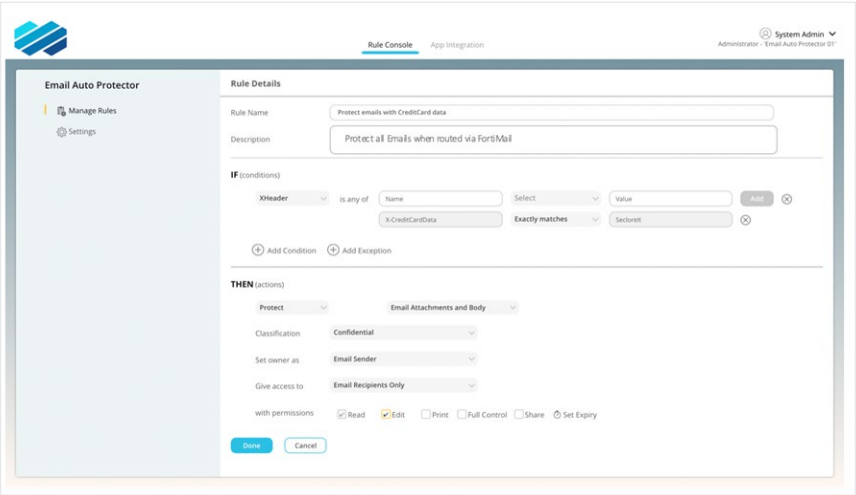
8. Seclore Email Auto Protector—Architecture

The diagram below depicts an overview of the Seclore MTA architecture.

- Mail received from email server is sent to Postfix via SMTP port **25**
- Postfix will send this email to Milter, which is listening on port **9999** before processing
- Milter will forward this email to web service running on port **8080**
- Web service will process this email and apply Seclore Protection by contacting Policy server and returns the updated email to Milter
- The updated email will be sent back to Postfix via Milter

9. Seclore Email Auto Protector—Architecture

1. Log in with System Admin credentials in the Seclore Policy Server Console
2. Go to More > App Integrations
3. Click to Add a new “Enterprise Application” for Email Auto Protect
4. Post definition, click on “Manage Enterprise Application”
5. Click on “Add New Rule”



10. Seclore Email Auto Protector Rule Configuration (Admin user)

Please refer to the FortiMail Deployment Guide for instructions and configuration for configuring X-Headers and routing/relaying the email to the Seclore Email Auto Protector component.

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.