



Microsoft® Forefront™ Online Protection for Exchange

Microsoft



Forefront Online Protection for Exchange

Forefront Online Protection for Exchange

Electronic messaging is mission critical but remains vulnerable to a growing array of threats. Viruses, worms, denial-of-service attacks, spam, and the need to satisfy a growing set of regulations all make effective message management increasingly difficult.

Microsoft offers solutions to help companies combat these threats, including hosted services for email filtering, and encryption. Microsoft® Forefront® Online Protection for Exchange provides enterprise-class reliability for messaging security and management. This service can help your organization by protecting against spam and malware, encrypting data to help preserve confidentiality, and maintaining access to email during and after emergency situations.

Forefront Online Protection for Exchange

can help you simplify the administration of your messaging environments. The hosted online services model requires no hardware or software installation, minimizes up-front investment, and provides a predictable payment schedule through a subscription-based service.

As one of the Microsoft® Online Services, Forefront Online Protection for Exchange provides a layer of protection features deployed across a global network of secure data centers. It creates a security-enhanced message stream to and from your on-premises, hosted, or Microsoft® Exchange Online messaging environment.

How it Works

To help ensure high availability, Forefront Online Protection for Exchange utilizes a global network of state-of-the-art, fully redundant, load-balanced data centers. Servers in the data centers are load-balanced from site to site and from server

to server. After domain validation, with a simple mail exchange (MX) record configuration change, Forefront Online Protection for Exchange can be up and running quickly. FOPE requires no hardware or software to install, manage, and maintain, and enables customers to satisfy company policy and regulatory compliance requirements for e-mail. The network of data centers at key sites along the Internet backbone help ensure that in the unlikely event that one data center is unavailable, traffic can be easily routed to another data center. In addition, Microsoft algorithms analyze and route message traffic between data centers to help ensure secure and timely delivery.

Service Level Agreements

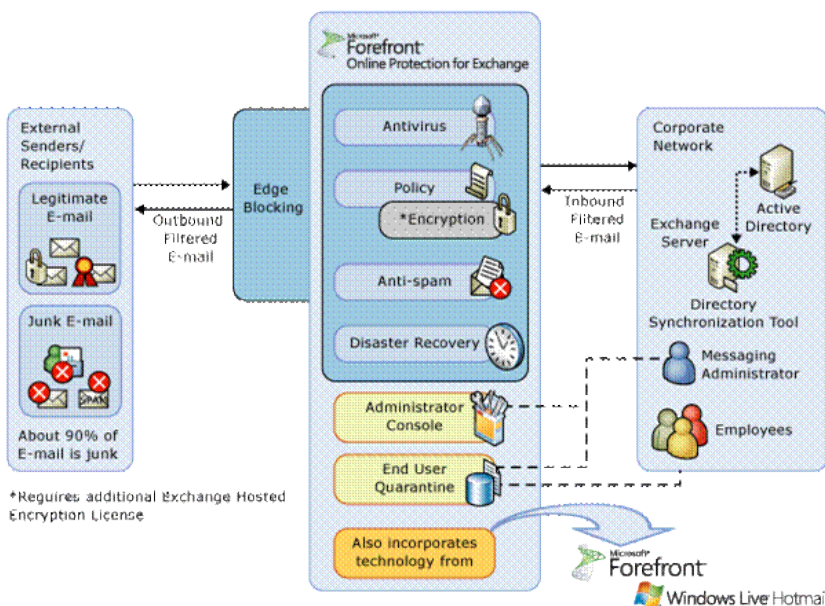
Forefront Online Protection for Exchange comes with financially backed SLAs covering network uptime, virus and spam detection and false positives ratio. These SLAs include:

Network infrastructure

- Network uptime: 99.999%
- Email delivery: Average delivery commitment of less than one minute

Filtering accuracy

- Virus Blocking: 100% protection against all known email viruses
- Spam Capture: Capture of at least 98% of all inbound spam emails
- False Positive Ratio: False positive commitment of less than 1 in 250,000 emails



Features and Benefits

Enterprise-Class Reliability

- Scales to meet the needs of virtually any enterprise
- Helps ensure that no email is lost or bounced during disaster recovery
- Helps provide high availability through strategically located, load-balanced data centers
- FOPE Datacenters are managed by GFS and our datacenters are SAS 70 Type II and ISO 27001 certified. (FOPE as a service is also ISO 27001 certified)

Active Protection

- Offers multi-layered, real-time anti-spam and antivirus defenses
- Helps eliminate threats before they reach the corporate firewall
- Assists with policy enforcement and meets most compliance requirements
- Helps keep unwanted email from reaching your corporate network using Active Directory® synchronization

Simplified Management

- Simplifies your IT environment by reducing the need for in-house email security servers and applications
- Saves time on anti-spam management, freeing up network and server resources
- Starts with a simple MX record change
- Helps reduce up-front capital investment
- Offers a predictable, subscription-based payment
- Lowers total cost of ownership compared with on-premises solutions

Security-based Messaging

- Protects virtually everywhere and provides access from virtually anywhere
- Integrates and extends security across the enterprise
- Simplifies the security experience and manages compliance

Hybrid Messaging Protection

- Provides a unified interface for managing messaging security for both Forefront Online Protection for Exchange and Microsoft Forefront Protection 2010 for Exchange Server messaging security

Comprehensive Customer Support

- Customer support is available 24/7 via phone and e-mail, including international translation services for all customers at no additional cost.
- Implementation Project Managers (IPMs) available for qualifying accounts for the first 90 days to answer complex questions.

Solutions Overview

Forefront Online Protection for Exchange

- **Multi-engine virus and spam filtering**
With its multiple filtering engines and an around-the-clock team of anti-spam experts, Forefront Online Protection for Exchange virtually eliminates spam from inboxes, helping to provide bandwidth for legitimate corporate use. Forefront Online Protection for Exchange combats known and unknown threats by integrating its anti-virus engines at the API level, providing timely virus definition updates and sophisticated heuristics.
- **Active content, connection and policy-based filtering**
A highly customizable filter helps you comply with corporate policies and government regulations.
- **Forced TLS Option**
By creating a Forced TLS rule in the policy filter, you can help ensure that sensitive email is encrypted during transport. Forced TLS enforces transport layer security (TLS) between your outbound message transfer agent (MTA) and your recipient's MTA.

Fast Message Trace and Reporting

Fast reporting and the Message Trace tool give you insight into your email environment by retrieving the status of any message that Forefront Online Protection for Exchange processes—in real time. You can quickly find out whether the service received a message and whether it scanned, blocked, or delivered the message.

Disaster Recovery

If the destination email server becomes unavailable for any reason, Forefront Online Protection for Exchange helps to ensure no email is lost or bounced by automatically queuing email for up to five days, attempting to deliver it every 20 minutes.

Microsoft Exchange Hosted Encryption

- **Policy-based encryption from sender to recipient add on service**
Because encryption at the gateway is based on policy rules, end users can send and receive encrypted messages directly from their desktops in the same way that they would send regular, unencrypted messages. All messages that meet the rules of the policy are automatically encrypted, without end users having to change anything.
- **Identity-based Encryption (IBE) technology uses a common ID for public key**
IBE automatically binds the recipient's identity to the public key, eliminating the need for managing certificates.
- **Zero Download Messenger—web-based decryption and encrypted replies**
Zero Download Messenger provides secure, web-based decryption with encrypted replies for any mail recipient messages—with no need to train end users or install software.

Additional Resources

- <http://www.microsoft.com/fope>
- FOPE Privacy Statement - <http://go.microsoft.com/fwlink/?LinkID=138500>