Microsoft® Office 365™ and Zix™ Email Encryption

A NATURAL FIT

By ZixCorp
www.zixcorp.com

THE POWER OF EVERYONE

INTRODUCTION

IT managers and decision makers are being pressured from all sides to find ways to safely migrate to cloud-based services. Corporate management has expectations of significant operational cost savings, and key vendors have been investing heavily to move their longstanding on-premises solutions to hosted versions of the same. Understanding the technical implications and business risks of a migration is crucial for a smooth transition.

For many IT organizations, internally deployed and managed Microsoft® products form a stable foundation for service provision. For them the Microsoft Office productivity suite for document creation and collaboration is a given, as are Microsoft Outlook and Microsoft Exchange for email communication.

Gartner has recommended that “all organizations should evaluate cloud email services prior to an on-premises upgrade” and went so far as to say that “by YE20 [Gartner] believes at least 50% of Exchange deployments will be in the cloud.”

As Microsoft pours huge investments into their cloud-based Office 365™ offering and the business case for migration becomes clearer and more compelling, remaining questions for the IT decision maker shift to when to migrate and how to ensure adjunct capabilities continue to meet organizational needs and service level agreements.

Although Internet-based email is ubiquitous and very well understood, many organizations have not yet established good email encryption practices with their business partners and clients. This results in significant risks, notably in regulated businesses such as finance and healthcare where privacy breaches can expose organizations to litigation and fines.

Zix™ customers have long understood the benefits of encrypted email, but those who are considering a migration to Office 365 will need to understand the deployment models and considerations.

In that context, this paper will explore how Zix™ Email Encryption integrates seamlessly with Office 365 while supporting a number of alternative deployment approaches.

zix Office 365

Zix Email Encryption integrates seamlessly with Office 365 while supporting a number of alternative deployment approaches.

BACKGROUND

The Simple Messaging Transfer Protocol, SMTP, is a proven workhorse. Originally designed in the early 1980's, it has become the backbone of what we now know as business email with only minor updates over the years. Technology market research firm The Radicati Group estimates that 100 billion business emails are sent and received each day, many of which are transported over SMTP to reach their destination.

A core concept of SMTP is the mail exchanger record or 'MX record'. In this model a sending mail server will examine the recipient's email address and then use the global Domain Name System (DNS) to look up the appropriate destination server address for mail delivery. That information is stored in the DNS in the form of an MX record. The sending mail server can then open a connection with the destination mail server and deliver the message.

Organizations can also use the flexibility of this approach to redirect inbound or outbound messages through intermediary services like spam filtering, anti-virus, compliance, archiving, and email encryption by publishing different MX record information. Most mail servers are also flexible enough to allow messages to be routed differently based on destination, sender, or message content. Many IT professionals refer to the resulting paths that messages follow in and out of the organization as 'mail flow.'

The following sections provide an overview of mail flow as it relates to Zix Email Encryption and how it works with the mail flow feature area of Office 365 and Exchange Online.

100 BILLION

business emails are sent and received each day.

—The Radicati Group, Inc.

DEPLOYING ZIX EMAIL ENCRYPTION WITH OFFICE 365

Using Office 365 in any organization requires some changes to mail flow to route messages inbound and outbound through Exchange Online instances in Microsoft data centers. As an example, standard techniques such as Group Policies can be used to provision and configure desktop Outlook installations to use the Exchange Online instances assigned to an organization by Microsoft prior to decommissioning on-premises Exchange installations.

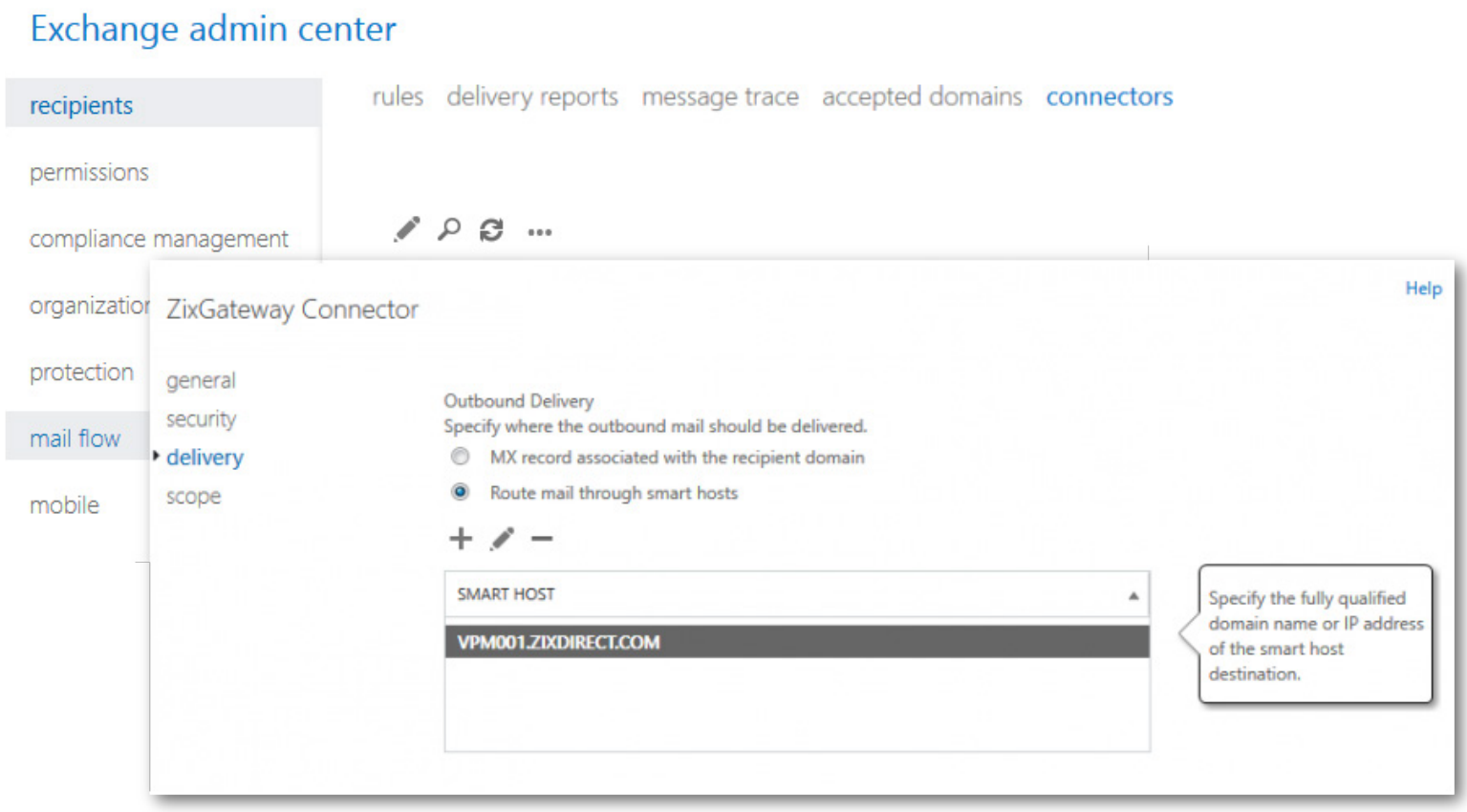
To take advantage of Zix Email Encryption capabilities in an Office 365 deployment, mail flow must be securely routed between the organization's Exchange Online instances and ZixGateway instances.

There are a wide range of deployment scenarios that can be accommodated in an integrated solution. In the majority of cases, the primary integration tasks are:

- Configure an Outbound Connector from Office 365 to the ZixGateway instance using Microsoft's Exchange Admin Center
- Add an MX Record to point to the ZixGateway instance for inbound encrypted messages using standard DNS tools
- Configure ZixGateway to accept mail relayed from the Office 365 subnets using Zix administration interfaces.

The Office 365 mail flow settings are available in the Exchange Admin Center from the Exchange link under Admin.

A Zix Deployment Coordinator will provide assistance with planning deployment scenarios such as staged migrations or hybrid combinations of on-premises and hosted products.



ZIX EMAIL ENCRYPTION

Since the company's founding in 1998, Zix Email Encryption has been designed on a Software-as-a-Service (SaaS) architecture with a clear focus on simplifying secure email for organizations and providing the best possible experience for both the sender and receiver.

A significant solution of Zix Email Encryption is ZixGateway®, a policy-based email encryption service for privacy and compliance. Installed at the periphery of an organization's network, ZixGateway automatically scans outbound email for sensitive information based on defined corporate policies. If sensitive information is identified, it can be either blocked or sent encrypted. Automatic scanning provides peace of mind for companies protecting sensitive information. It also provides a transparent experience for employees, who can continue to conveniently click "send" without worry or extra steps.

Much like Office 365 is a hosted version of the Exchange 2013 software named Exchange Online, ZixGateway can be deployed as a fully hosted solution.

KEY MANAGEMENT

Once the message is encrypted, key management is one of two core challenges remaining for a successful email encryption solution.

Finding and managing the keys needed to encrypt is complex and time-consuming when an organization is communicating with individuals and organizations outside of its control.

To eliminate these difficulties, ZixCorp developed ZixDirectory®, a hosted and shared email encryption community. ZixDirectory includes tens of millions of members and increases at approximately 100,000 members per week. Its automated key management reduces the typical cost and complexity associated with email encryption solutions and saves wasted hours spent setting up and exchanging keys. ZixDirectory also safeguards against expired keys and certificates by providing centralized distribution among all members.

ZixGateway provides peace of mind for companies with sensitive data and an easy, transparent experience for employees.

BEST METHOD OF DELIVERY

The second core challenge of email encryption is secure delivery. There are a number of delivery approaches, such as TLS encryption of SMTP traffic, S/MIME, and OpenPGP, that are all well-documented, standards-based options to encrypt email. In addition, encrypted email can be delivered through secure web portals ("pull").

Unlike web browsing where a clear security technology emerged very early in the form of the SSL/TLS protocol for encrypted delivery of web content, none of the above technical approaches have become the de facto encryption approach for secure delivery of email.

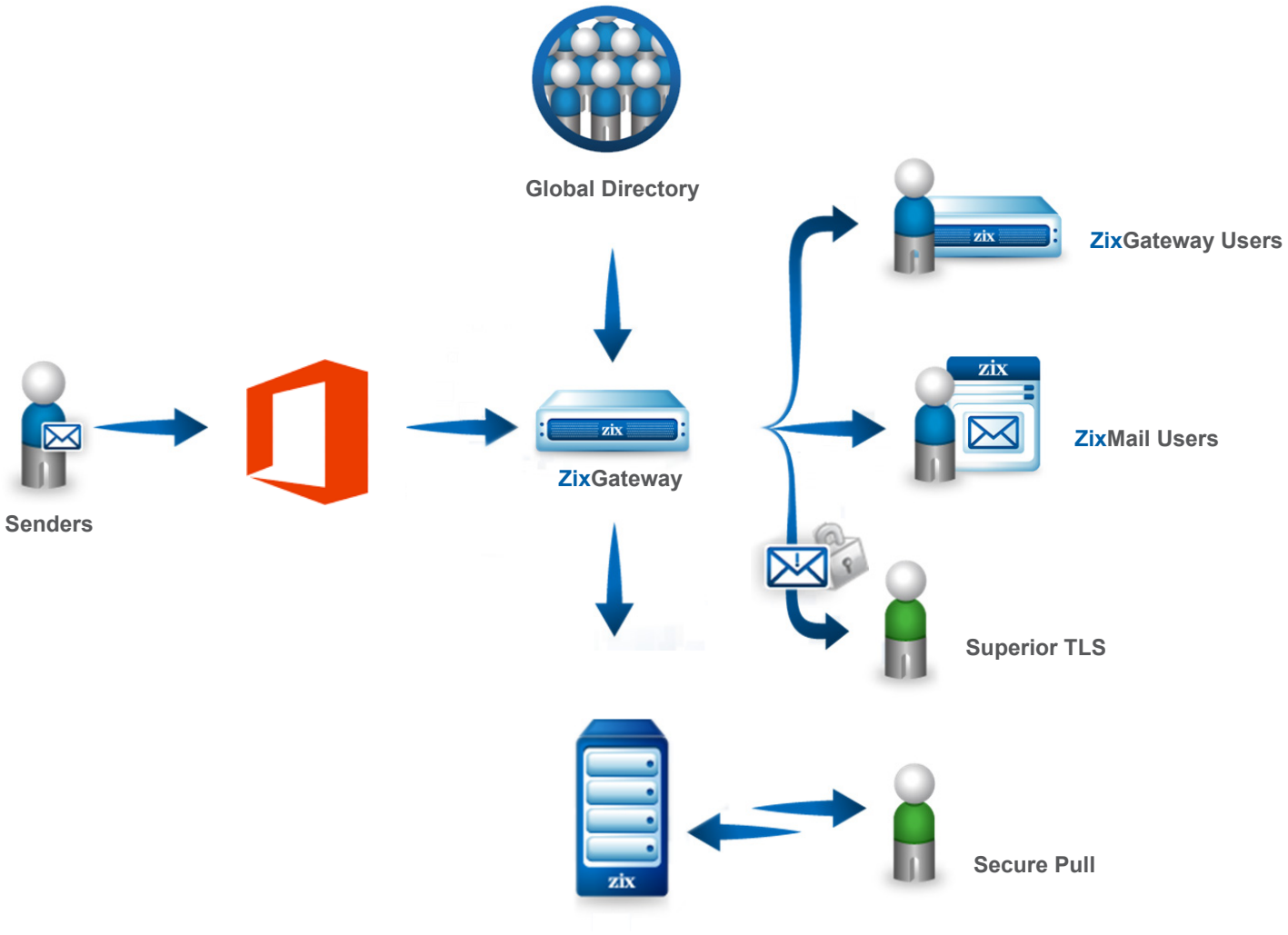
As a result, knowing which delivery method will be successful for a particular recipient organization or individual is very difficult. ZixCorp addresses this challenge with the Best Method of Delivery℠.

Best Method of Delivery offers the industry's most robust options for receiving encrypted email and automatically determines the most secure and transparent method of sending your message. If the recipient sits behind ZixGateway, the message is sent transparently to the person's inbox, so that no extra steps or passwords are needed to read and reply to the encrypted email. On average, more than one-third of our customers' recipients receive their encrypted email messages transparently.

If the message cannot be delivered through ZixGateway, then the encrypted email will be delivered through ZixMail®, a one-click desktop email encryption solution, or via mandatory TLS.

Recipients who do not have email encryption or TLS capabilities can receive encrypted email through ZixPort®. ZixPort is a pull technology that provides a secure portal for delivering sensitive information to customers and partners. It can be branded and integrated into your corporate portal. All of these options combine to create the Best Method of Delivery, and secure reply is available to all recipients to avoid exposure of sensitive information in responses.

ZIXCORP'S BEST METHOD OF DELIVERY



ENCRYPTION FOR MOBILE USERS

Mobile users on IOS, Android, and Windows Phone devices are equally well served as senders and recipients of Zix Encrypted Email. ZixGateway can automatically encrypt messages based on message content, subject, or attachment. This means mobile users do not need to take any action; the experience is secure and seamless when sending messages from mobile devices.

Depending on the delivery method, recipients of Zix Encrypted Email may receive messages in different formats on their mobile devices. If the recipient sits behind ZixGateway or a TLS connection, the experience is once again seamless and transparent – no extra steps or passwords are required. For recipients without Zix Email Encryption, the experience is as easy as accessing encrypted email from the desktop. ZixMobility, a feature of ZixPort, optimizes layouts designed for the user's environment, maximizes the user's screen and removes any cumbersome steps to ensure the recipient can access and reply from any device, anywhere, anytime.

ZIXCORP LEXICONS

With ZixGateway deployed into an organization's Office 365 environment, a wide range of email encryption scenarios become possible. Among them, email encryption policies can be configured to ensure:

- any email and attachments containing protected health information (PHI) are encrypted,
- any email and attachments containing social security numbers or financial information are encrypted, or
- all email between specific business associates and regulators are encrypted.

To accurately identify PHI, financial information, social security numbers, and other sensitive information, ZixCorp has developed a number of lexicons. Each lexicon consists of comprehensive sets of terms, phrases, expressions and pattern masks which can be used to automatically examine email subject lines, message bodies, or attachments. The more widely used standard lexicons include Healthcare, Financial, SSN, Health Research, Profanity, and State Regulatory Requirements. Each lexicon has the flexibility to be customized to suit particular customer situations.

ZIXDATA CENTER

To support Zix Email Encryption, ZixCorp built and maintains ZixData Center™, a state-of-the-art facility with SysTrust/SOC3 certification and SOC2 accreditation in the areas of security, confidentiality, availability and integrity. The ZixData Center is also PCI Level 1, DSS V2.0 certified. The facility is staffed 24 hours a day with operations personnel constantly monitoring the facilities, networks, systems, and applications. It has a track record of consistent 99.999% availability, and service availability levels are guaranteed to customers through our service level agreements (SLAs).

The ZixData Center has satellite data centers in Austin, Texas, and the United Kingdom. These facilities share service back-up and distributed service delivery roles with the main facility.

SUMMARY

Organizations looking to ensure the success of their Office 365 migration are carefully planning every aspect of their projects to reduce risk. Email encryption capabilities should not be overlooked in those plans.

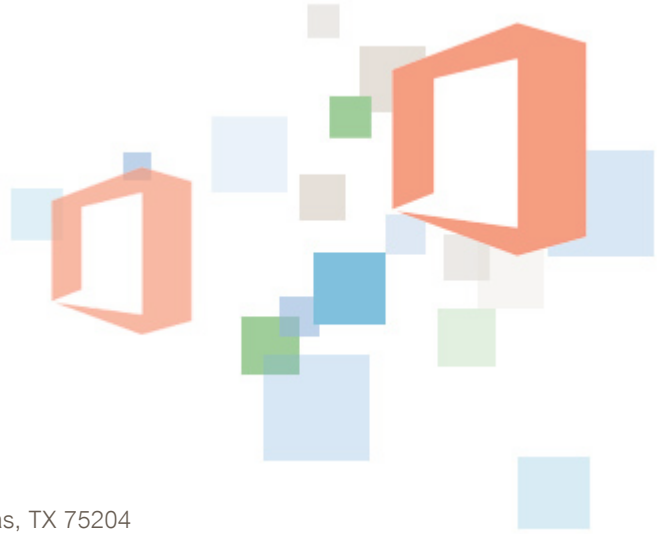
ZixGateway enables a low-risk, straightforward integration with Office 365, leveraging readily accessible and broadly used configuration settings.

To take advantage of this, organizations should consider including the integration of Office 365 with Zix Email Encryption as a part of their migration plans. In this way they can provide the benefits of an easy to use email encryption solution for their users while reducing the organization's IT management costs through the use of well-established hosted providers for both email and email encryption.

ABOUT ZIXCORP

ZixCorp is a leader in email data protection. ZixCorp offers industry-leading email encryption, a unique email DLP solution and an innovative email BYOD solution to meet your company's data protection and compliance needs. ZixCorp is trusted by the nation's most influential institutions in healthcare, finance and government for easy to use secure email solutions. ZixCorp is publicly traded on the Nasdaq Global Market under the symbol ZIXI, and its headquarters are in Dallas, Texas. For more information, visit www.zixcorp.com.

zix Office 365



Zix Corporation . 2711 N. Haskell Avenue . Suite 2300, LB 36 . Dallas, TX 75204
Phone 866 257 4949 . sales@zixcorp.com . www.zixcorp.com