



End of Exchange 2003 - Decision Guide

HOW TO USE THIS GUIDE

On April 8, 2014, Microsoft will end extended support for Exchange 2003.

Business technology has changed dramatically since 2003. Mobile devices are now powerful and pervasive, Bring Your Own Device (BYOD) is a reality in most businesses, and people have new expectations from their email, calendar, and messaging environments. Newer Microsoft Exchange platforms have kept pace with these changing expectations. Although Exchange 2003 has remained a stable platform for business email, it is a product of a technologically simpler time.

And now, its time has come. On April 8, 2014, Microsoft will end extended support for Exchange 2003.

This means that Microsoft will no longer issue security patches. Businesses that are still running Exchange 2003 beyond this date will face security risks.

Business and IT leaders who are using Exchange 2003 must make a decision by April 8th: accept the risk and do nothing, or migrate to a newer version of Exchange. This report explores the benefits, costs, and risks for all three options facing these leaders:

1. Remain on Exchange 2003
2. Upgrade to on-premise Exchange 2010 (or Exchange 2013)
3. Migrate to cloud-based Exchange 2010 (or Exchange 2013)

NOTES FOR YOUR DISCUSSION

OPTION 1: REMAIN ON EXCHANGE 2003

To date, many businesses have made a sensible decision to continue with Exchange 2003. But the fact that Microsoft is ending extended support for Exchange 2003 changes the risk profile of that decision.

Benefits: Doing nothing requires no investment and no change in the user experience. It is the path of least resistance, which can be appealing to a time-constrained IT team.

Costs: IT organizations face increased support costs as they troubleshoot problems for ten-year-old technology without patches, bug fixes, or phone support from Microsoft. In addition, third-party developers who create solutions involving Exchange will stop developing for this unsupported version, which limits IT's ability to access new innovations. Most importantly, the potential for lost productivity increases as Exchange security vulnerabilities are detected and remain unpatched.

Risks: The end of extended support raises the risk profile of Exchange 2003 in at least three ways.

- + Because Microsoft will stop creating security patches, hackers can exploit any vulnerabilities they find, increasing risk of data breaches.
- + Running unpatched software may violate regulatory compliance requirements and standards.
- + Exchange 2003 lacks the security and availability features offered in other versions, such as email encryption, disaster recovery features, and integrated archiving and eDiscovery.

Key Considerations: Ask yourself these questions when considering remaining on Exchange 2003.

- + What is the cost of running Exchange without any support from Microsoft?
- + Which additional initiatives (e.g. BYOD, real-time collaboration) are jeopardized by not running a newer version of Exchange?
- + Are the additional security and compliance risks acceptable? Do the Exchange 2003 users ever send or receive regulated data (PII, PHI, credit card data, etc.)?
- + Are business users willing to forgo ten years' worth of advances in email and collaboration?

Additional Resources:

[Exchange 2003: What happens when the clock stops?](#)

NOTES FOR YOUR DISCUSSION

OPTION 2: UPGRADE TO ON-PREMISE EXCHANGE 2010 OR 2013

Another option is to upgrade an on-premise Microsoft Exchange deployment to Exchange 2010 or Exchange 2013.

Benefits: Recent versions of Exchange simplify administration and improve availability and resiliency. Mobile users benefit from an enhanced OWA interface and a consistent interface across the PC, browser, and phone or tablet.

Costs: A successful Exchange upgrade typically requires the services of specialized Exchange migration consultants, as well as significant IT time and budget that detract from other IT initiatives.

In addition, this upgrade will be much more complex than simply upgrading licenses and installing servers. That's because Microsoft Exchange 2010 and 2013 have fundamental differences from 2003 and necessitate an upgrade to the surrounding network. Other costs include:

- + Network topology upgrades and investments
- + Network and datacenter security investments
- + Uptime planning and failover systems design
- + Equipment upgrades (server, data storage, etc.)
- + New software and support licenses
- + Increased management costs of a more complex technology environment

NOTES FOR YOUR DISCUSSION

OPTION 2: UPGRADE TO ON-PREMISE EXCHANGE 2010 OR 2013

Any additional changes to the environment will incur significant costs. For example, adding Lync or SharePoint functionality requires a major investment of time and effort. Voicemail integration is difficult to set up and maintain. Integrating further services, such as email archiving and disaster recovery, will increase the overall investment and amplify the ongoing management burden.

Risks: The lengthy and difficult upgrade process risks draining IT focus from other, more strategic business initiatives. In addition, a complex and time-consuming migration increases the possibility of errors that could lead to downtime, bounced messages and lost data.

Key Considerations: Ask yourself these questions when considering upgrading to on-premise Exchange 2010 or 2013.

- + What equipment changes are needed to create a new environment for Microsoft Exchange?
- + What datacenter investments are required to provide sufficient availability and failover?
- + What network infrastructure changes are necessary to provide appropriate security and performance?
- + Does the IT team have the time and resources for a major software deployment? Which other IT initiatives will they defer to upgrade the email environment?
- + Do you want to add other related services, such as email archiving or disaster recovery, or integrate email with voice mail, Microsoft Lync, or SharePoint? Each of these integrations will increase the total IT resource commitment.

NOTES FOR YOUR DISCUSSION

OPTION 3: MIGRATE TO CLOUD-BASED EXCHANGE 2010 OR 2013

Companies can avoid the labor costs and capital investments of an on-premise upgrade by migrating to cloud-based Exchange. The choice of the right cloud Exchange provider is important to your cost/benefit/risk equation. The right cloud provider will eliminate downtime risk, keep costs low and deliver on the promise of a reliable, secure and integrated cloud environment for Microsoft Exchange.

Benefits: Your business will see productivity gains from the advances in Microsoft Exchange, including better mobility, security, availability and administrative features. The Exchange hosting provider owns and maintains all of the equipment, eliminating the need for up-front capital investments. As a result, your internal IT team can focus on core or differentiating technologies rather than 'baseline' technologies like email. Of course, each hosted Exchange provider is different, with varying levels of investment in network and datacenter infrastructure.

The right hosted Exchange service should scale easily to support remote offices, a contingent workforce, business growth and service enhancements. The right cloud provider should offer IT a high level of control over the Exchange environment while making it easy to manage licenses, users and additional services.

Costs: Costs shift from capital expenditures to operating expenditures through a predictable subscription fee based on usage. All licensing and equipment costs are absorbed into the subscription fee. Unlike an on-premise deployment, the business itself does not have to invest in network infrastructure changes, server upgrades, storage, or redundant datacenter infrastructure.

The right cloud provider should offer full migration and onboarding services for no additional cost. Businesses with limited IT staff availability should beware of cloud providers who either charge extra for migration and onboarding services, or require customers to hire migration consultants. It is worth noting that Microsoft does not certify migration services for any Microsoft partner, making it difficult to identify the right migration specialist to hire. The consequences of a poor migration can be significant.

NOTES FOR YOUR DISCUSSION

OPTION 3: MIGRATE TO CLOUD-BASED EXCHANGE 2010 OR 2013

The right cloud provider should offer full migration and onboarding services for no additional cost. Businesses with limited IT staff availability should beware of cloud providers who either charge extra for migration and onboarding services, or require customers to hire migration consultants. It is worth noting that Microsoft does not certify migration services for any Microsoft partner, making it difficult to identify the right migration specialist to hire. The consequences of a poor migration can be significant.

Risks: The risk profile of every cloud provider is different. Lack of control over the Exchange environment is one potential risk. A good provider should offer a robust control panel that provides a similar overall level of Exchange control as an on-premise solution, while making it easy to deploy additional users and services.

The risks inherent in the migration itself will depend on whether migration is performed by the provider or a third party – and on that provider’s experience with Exchange 2003 migrations.

Businesses should evaluate hosting providers for relevant standards, audits and regulations while also understanding the provider’s privacy policies and the impact they may have on valuable data. Some providers guarantee that data is never stored in locations outside of US legal jurisdiction, while others may maintain a loophole that allows data to move outside the primary storage region to other countries – which govern your data with different laws.

Key Considerations: Ask yourself these questions when considering migrating to cloud-based Exchange 2012 or 2013.

- + Does the provider include full migration services? Do they have a proven track record?
- + What levels of support does the provider offer during and after the migration?
- + What service levels of availability are guaranteed in Service Level Agreements (SLAs)?
- + Does the provider offer certifications/audit reports for compliance with security and data protection standards and regulations?
- + What is the provider’s privacy policy? Where will your valuable data be stored?

Additional Resources:

[24 Questions to ask About Migration to Exchange in the Cloud](#)

NOTES FOR YOUR DISCUSSION

ABOUT INTEGRA'S HOSTED MICROSOFT EXCHANGE SERVICE

Integra is a premier provider of cloud services to small and medium-sized businesses. Integra provides full migration to Hosted Exchange 2010/2013 at no cost. Integra offers 99.999 percent uptime guarantee as part of the most stringent Service Level Agreements in the industry.

In addition to its Hosted Exchange services, Integra offers a number of other fundamental business tools—including traditional and IP voice services; data networking and Internet; and a variety of affordable, powerful business bundles designed to meet the requirements of companies both large and small. You can conveniently manage and control all of these services through our integrated control panel.

CONTACT US ▶ (877) 953-7747

ABOUT INTEGRA™

Integra is one of the largest facilities-based providers of communication and networking services in the western United States. We connect businesses of all sizes with advanced technology solutions in 35 metropolitan markets. Integra owns and operates an enterprise-class network consisting of a 5,000-mile long-haul fiber-optic network, and over 3,000 miles of metropolitan fiber and a nationwide IP/MPLS network.

www.integratelecom.com