RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: SPO3-W03

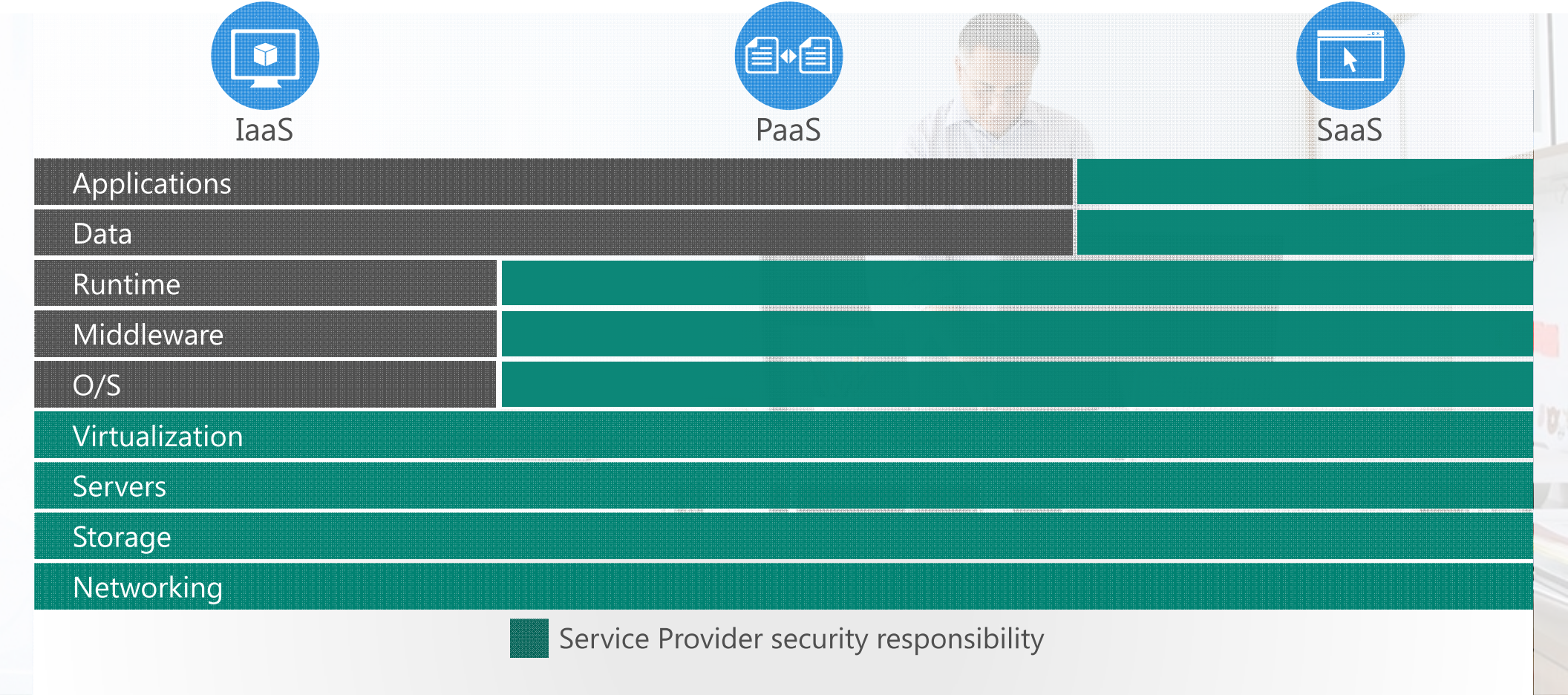
Enterprise Cloud: Advancing SaaS Security and Trust

Chang Kawaguchi

Principal Group Engineering Manager,
Office 365 Security Microsoft

Security without compromising experience

Techniques for securing the data should be specific to the type of cloud service



Common concerns about the cloud

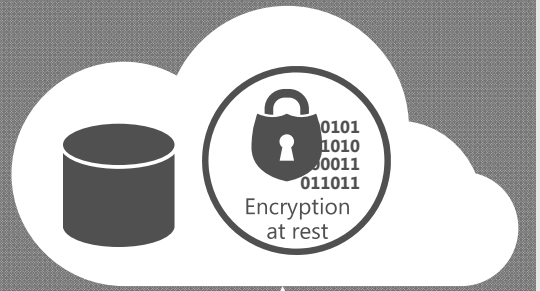
Is my content **safe** in your data centers?

Who has **access** to my organization's content in the service?

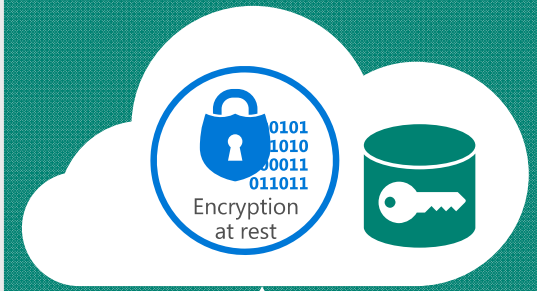
What **visibility** do I have into the **activity** on my content in the service?

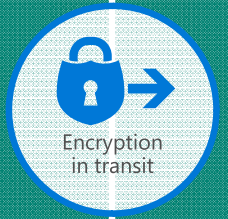
Can I **encrypt** everything so that it's not possible for you to have access to my content?

Encryption Options



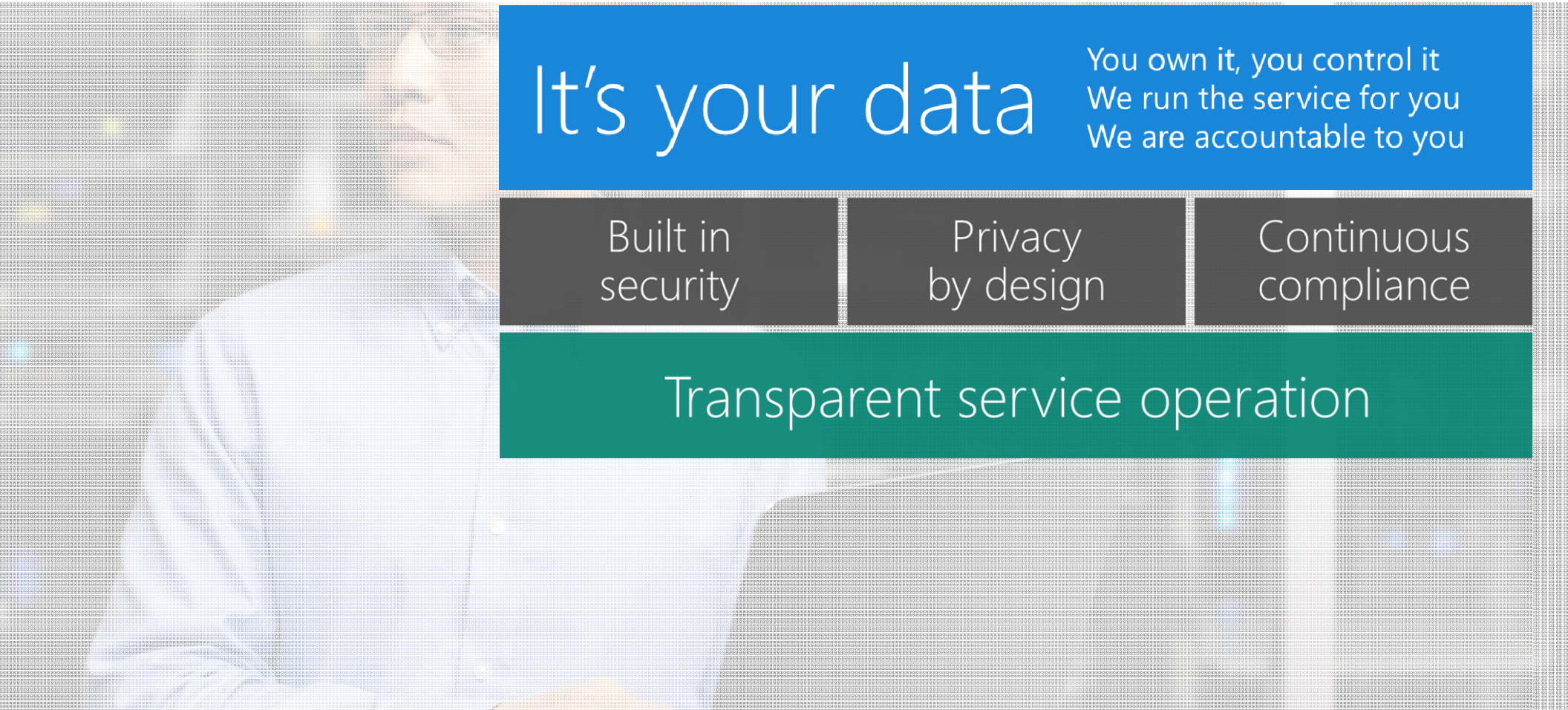
Data Loss Prevention ✖
Search ✖
Insights ✖
General content analysis ✖





✔ Data Loss Prevention
✔ Search
✔ Insights
✔ General content analysis

Cloud principles



Defense in depth approach

100101 011010 100011 011011 Content	Gain transparency
Physical security	Access control
Network	Intrusion and vulnerability detection
Host	Configuration management
Application	Securing and access control
Admin	Account management

Independently verified to meet key standards –
ISO 27001, SSAE 16 (SOC 1) Type II and (SOC2) Type II only), FISMA

Security strategy beyond defense

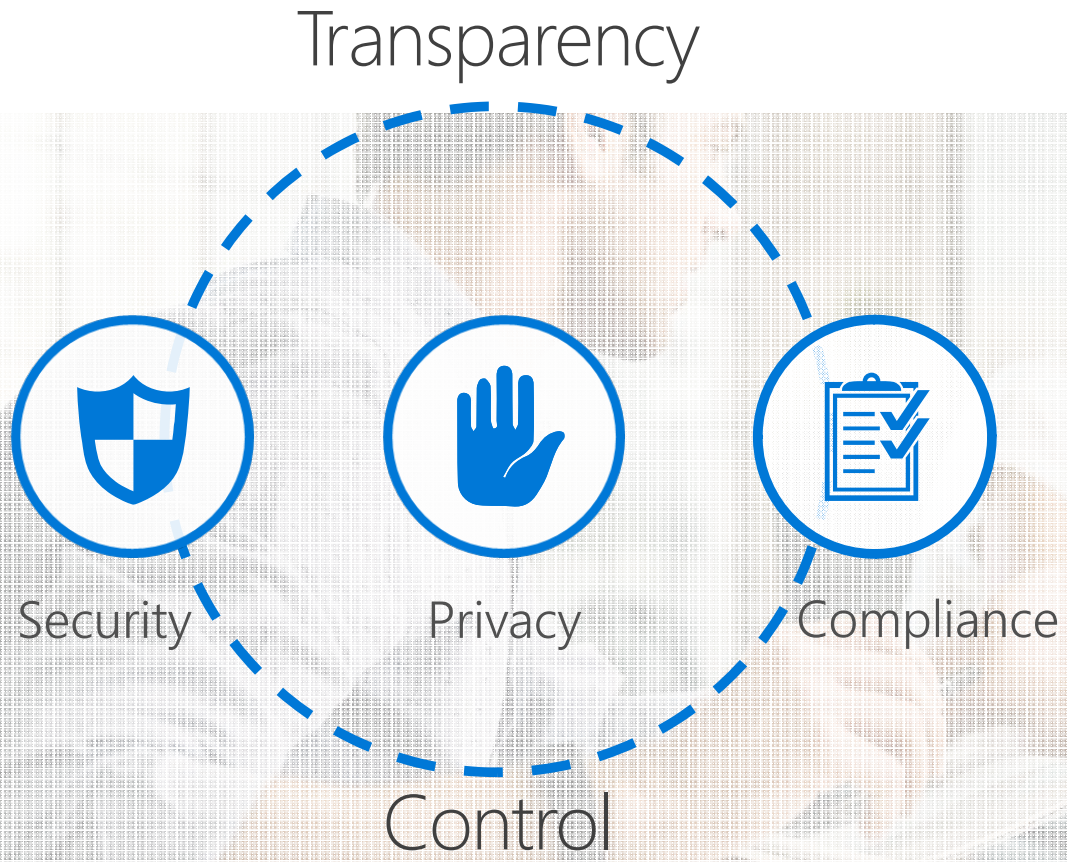
Red teaming

- Our own Office 365 pen testers test our services
- Simulate outsider and insider attack scenarios
- Strict Rules of Engagement (“do no harm”)
- Practice incident response

Bug bounty

- External security researchers hunt for vulnerabilities
- Compensated for significant valid vulnerabilities if found
- Enable customers to run their own vulnerability assessments

Earning and maintaining customers' trust

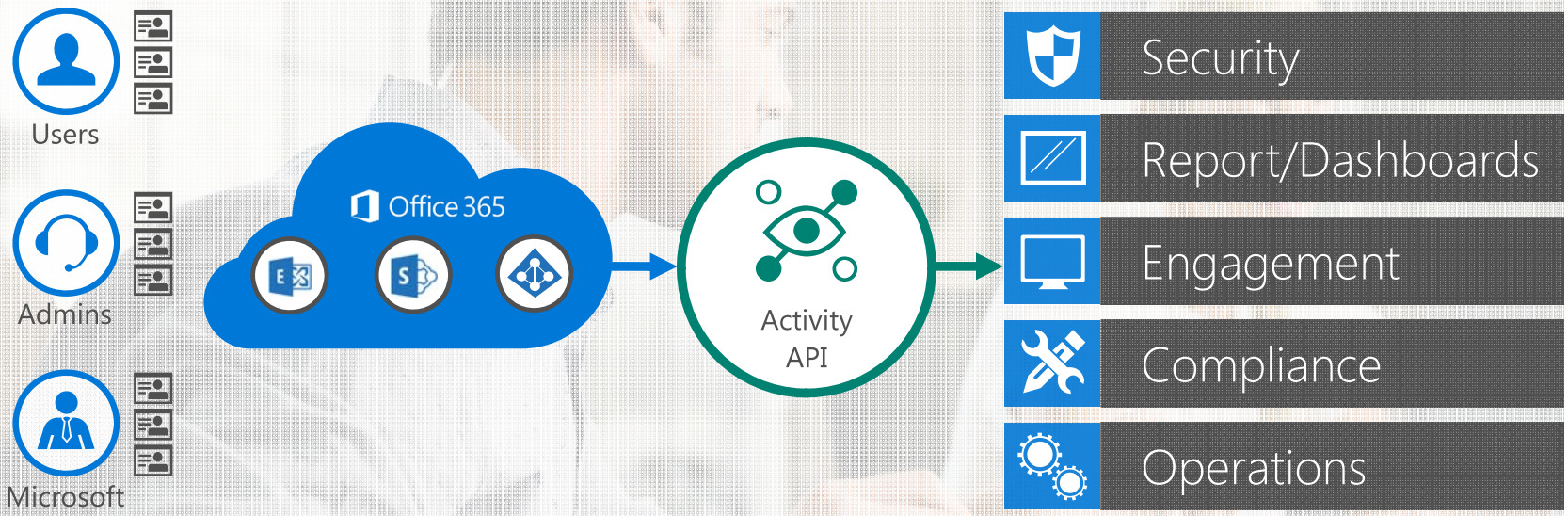


In the world of SaaS, it is through **transparency** and **control** that we earn and maintain customers' trust

Investments we announced yesterday are a significant step in this direction

Building transparency and control

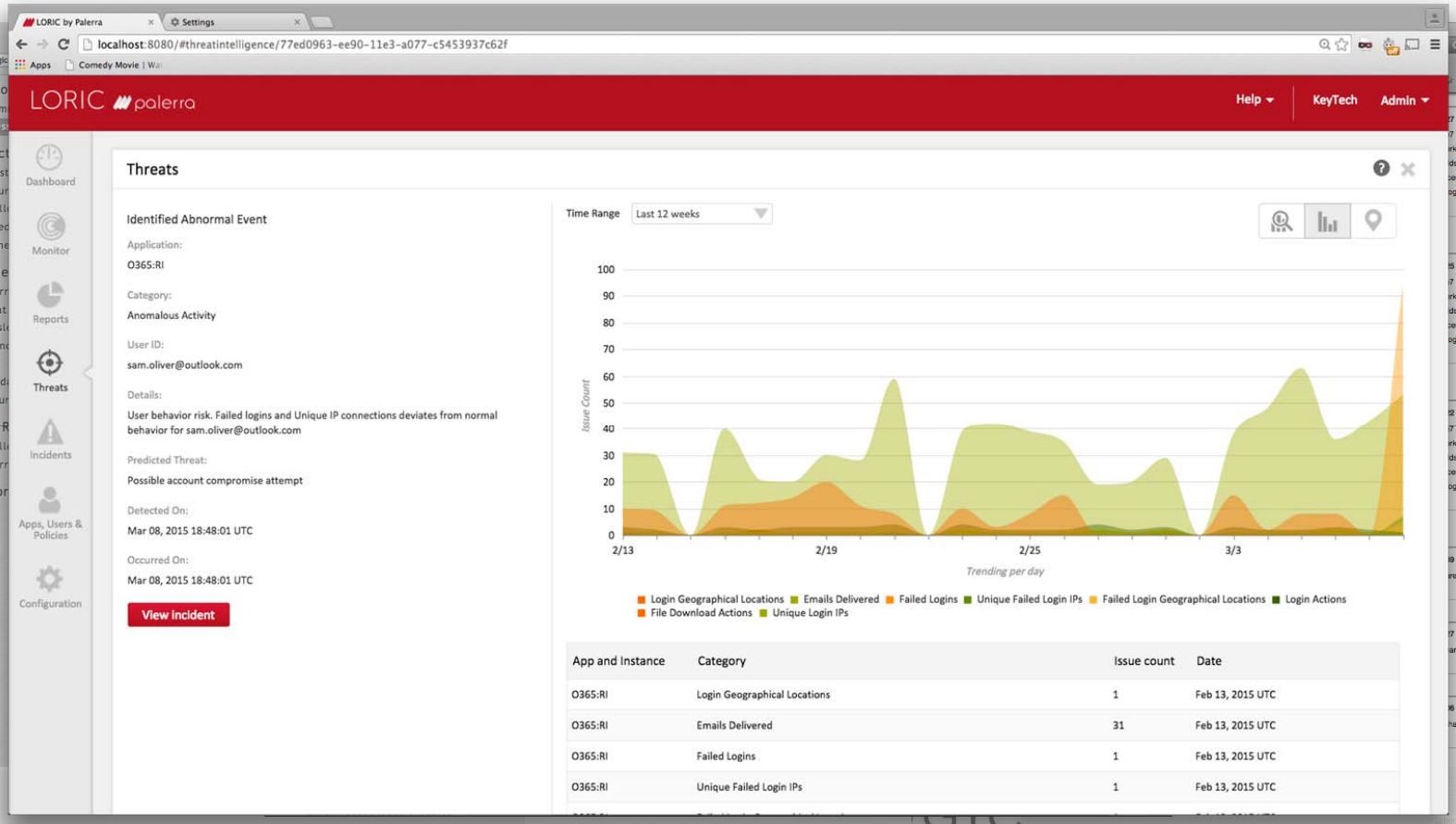
Security & compliance signals



ISVs

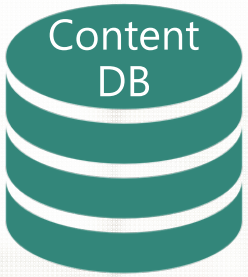
RAPID7
palerra
sumologic
ALERTLOGIC
CloudLock
BetterCloud
logentries
AvePoint
cogmotive
VARONIS
netskope
skyhigh
druva
LogRhythm

ISV Partner Integrations

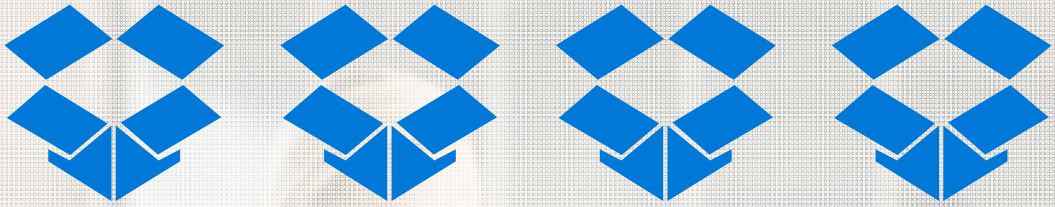


palerra

Content level encryption at rest in SharePoint



Azure
containers

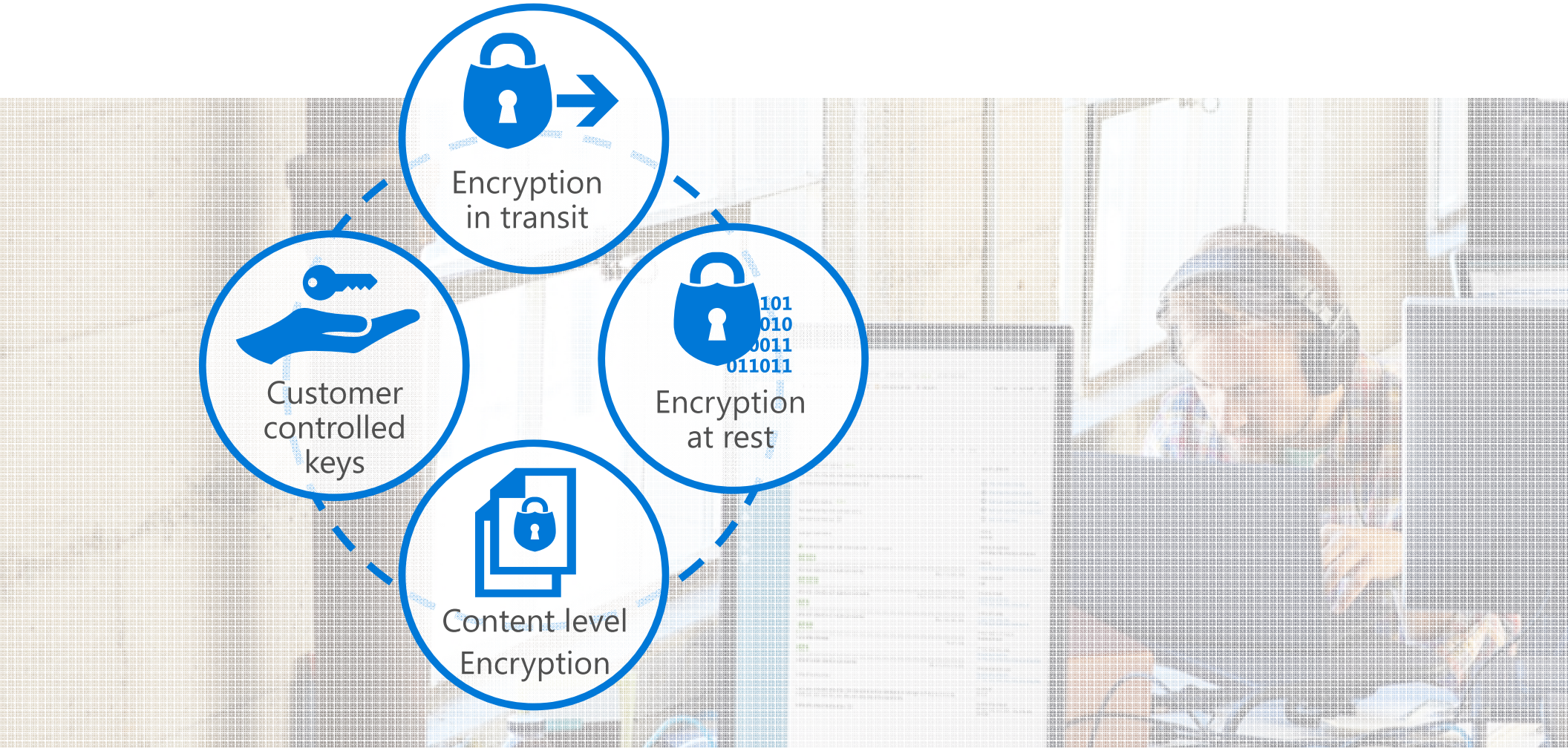


Disk level encryption at rest in Exchange

Content level encryption at rest in Exchange

Customer controlled keys in Exchange

Control: Encryption with customer control



Transparency and control: running the service

Most operations are automated

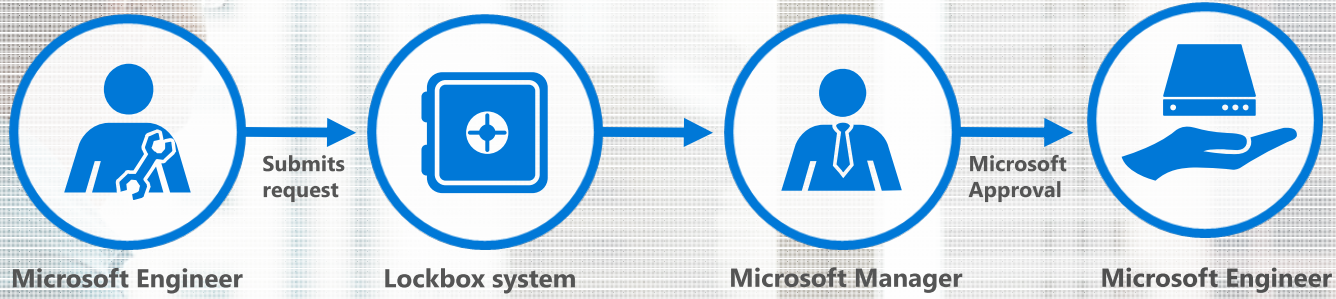
Data Center operations do not require access to customer content

Rare occasions where humans need access to run data center operations

Humans have to meet clearance requirements and require 2 factor auth to request access

Any access is highly controlled with multiple levels of approval using Lockbox

Lockbox



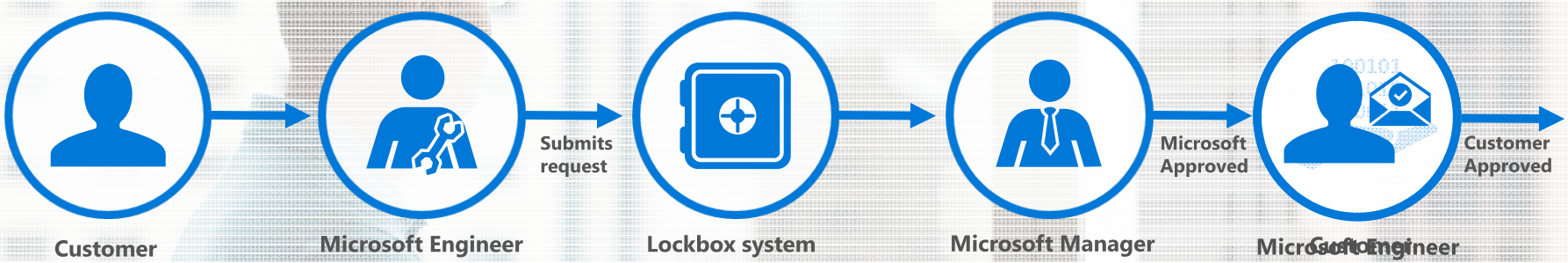
Scoped, least privileged access

Just-in-time access for limited duration

Audit logs for all access

Customer Lockbox

Now we want to extend Lockbox approval to you for human access to customer content



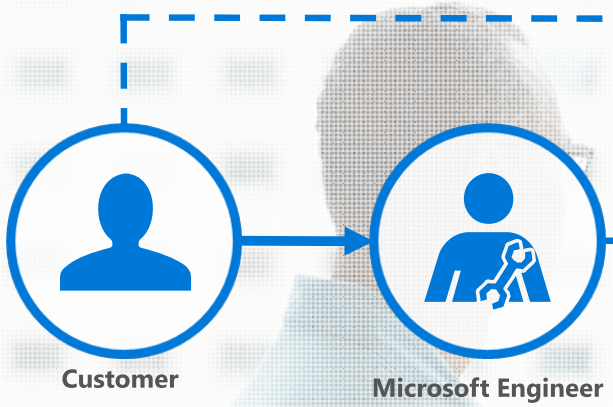
Customer controls authorization of Office 365 personnel access

Customer Lockbox

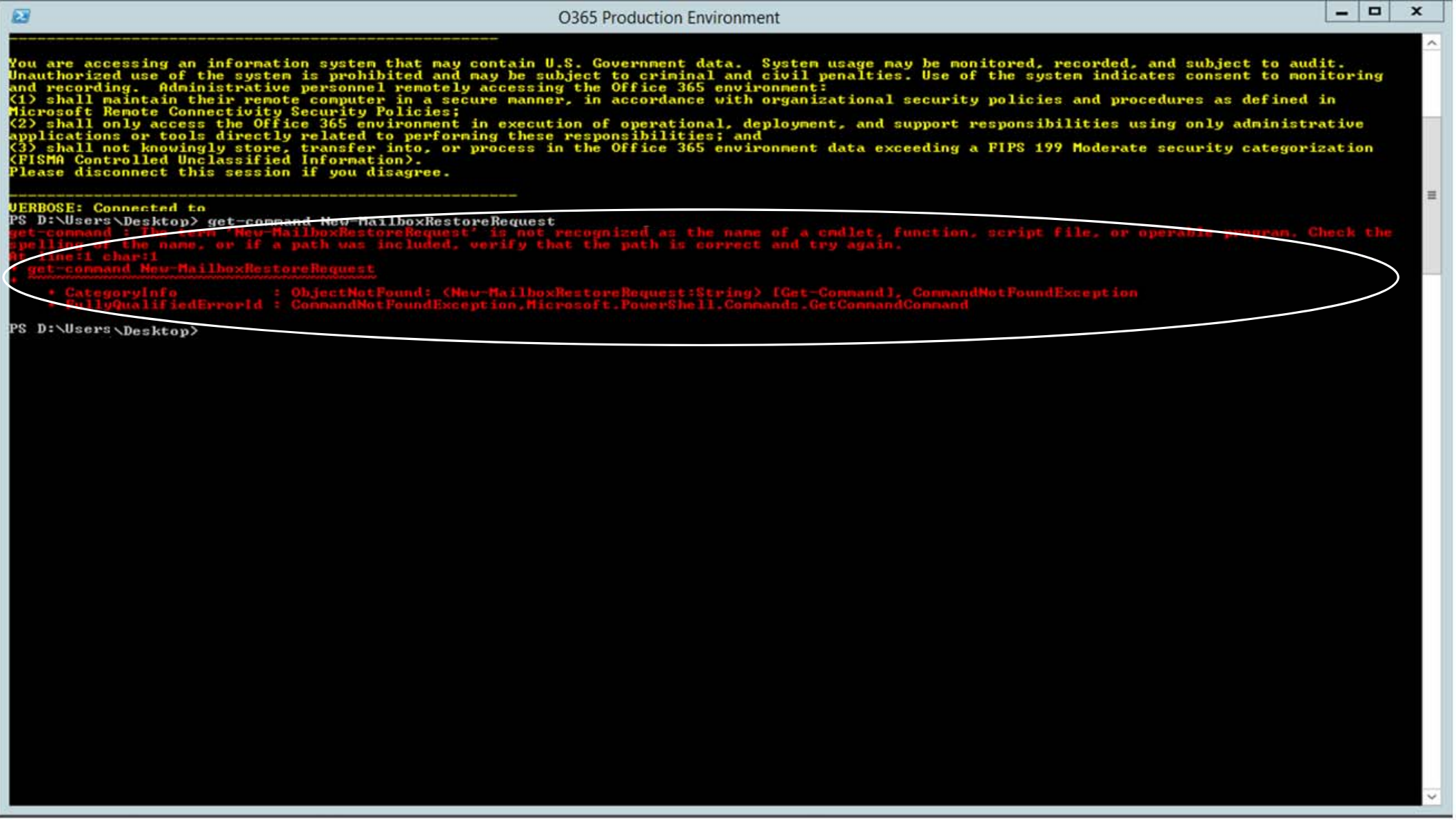
It's your data

You own it, you control it

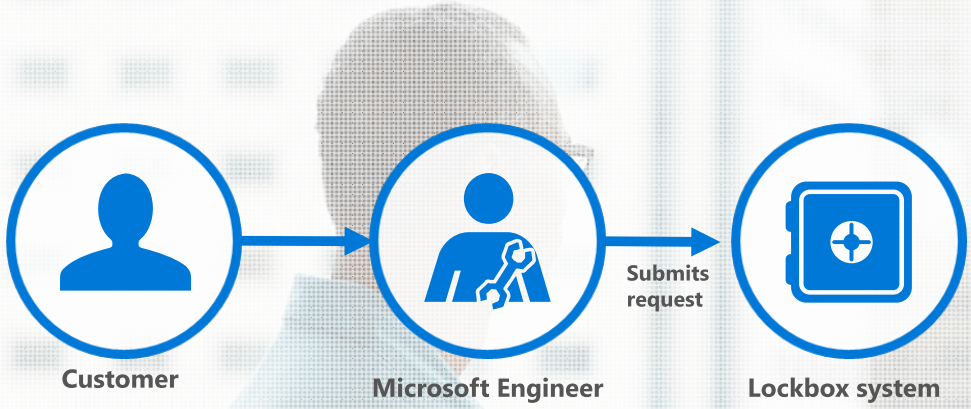
Customer Lockbox flow

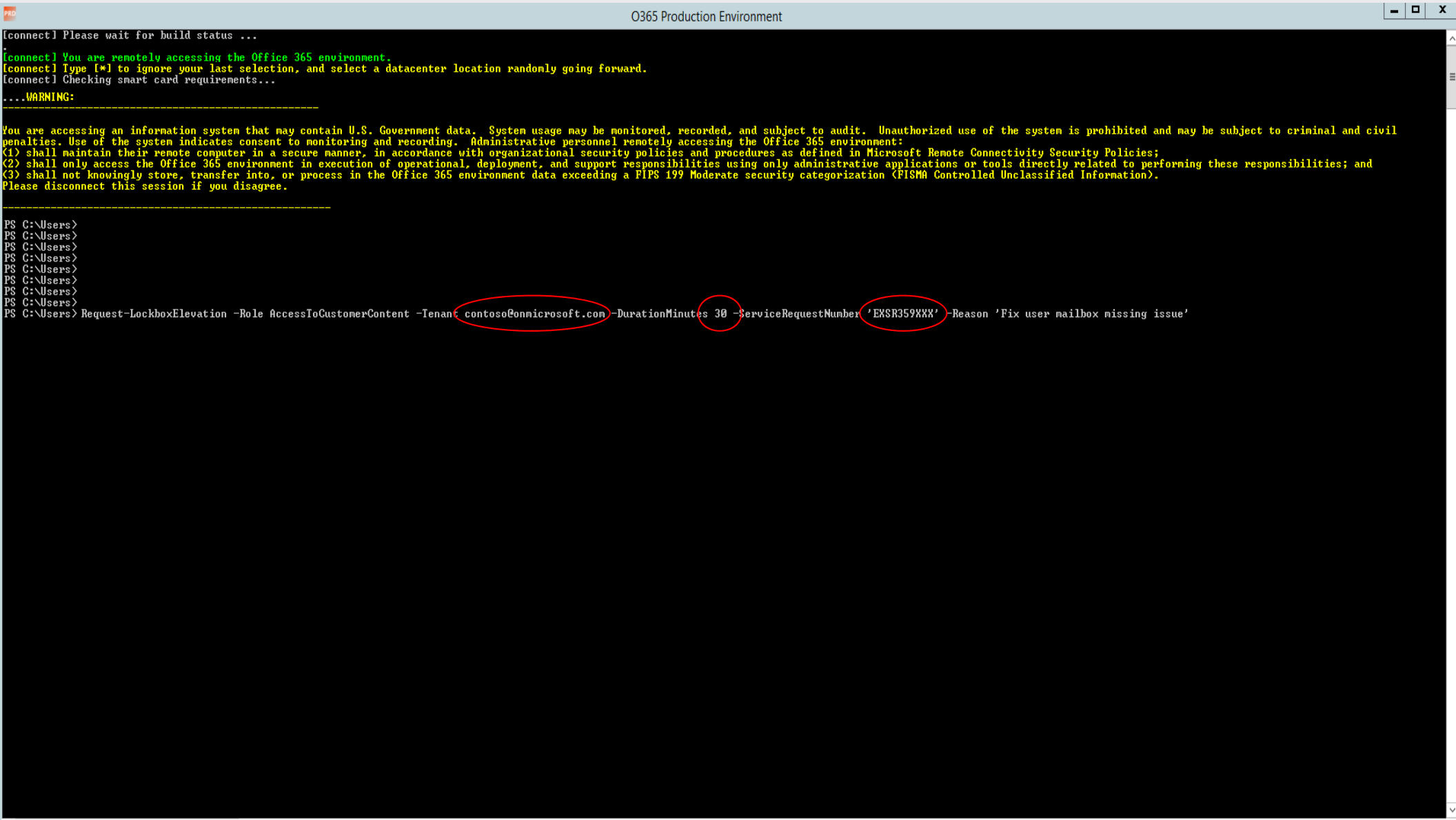


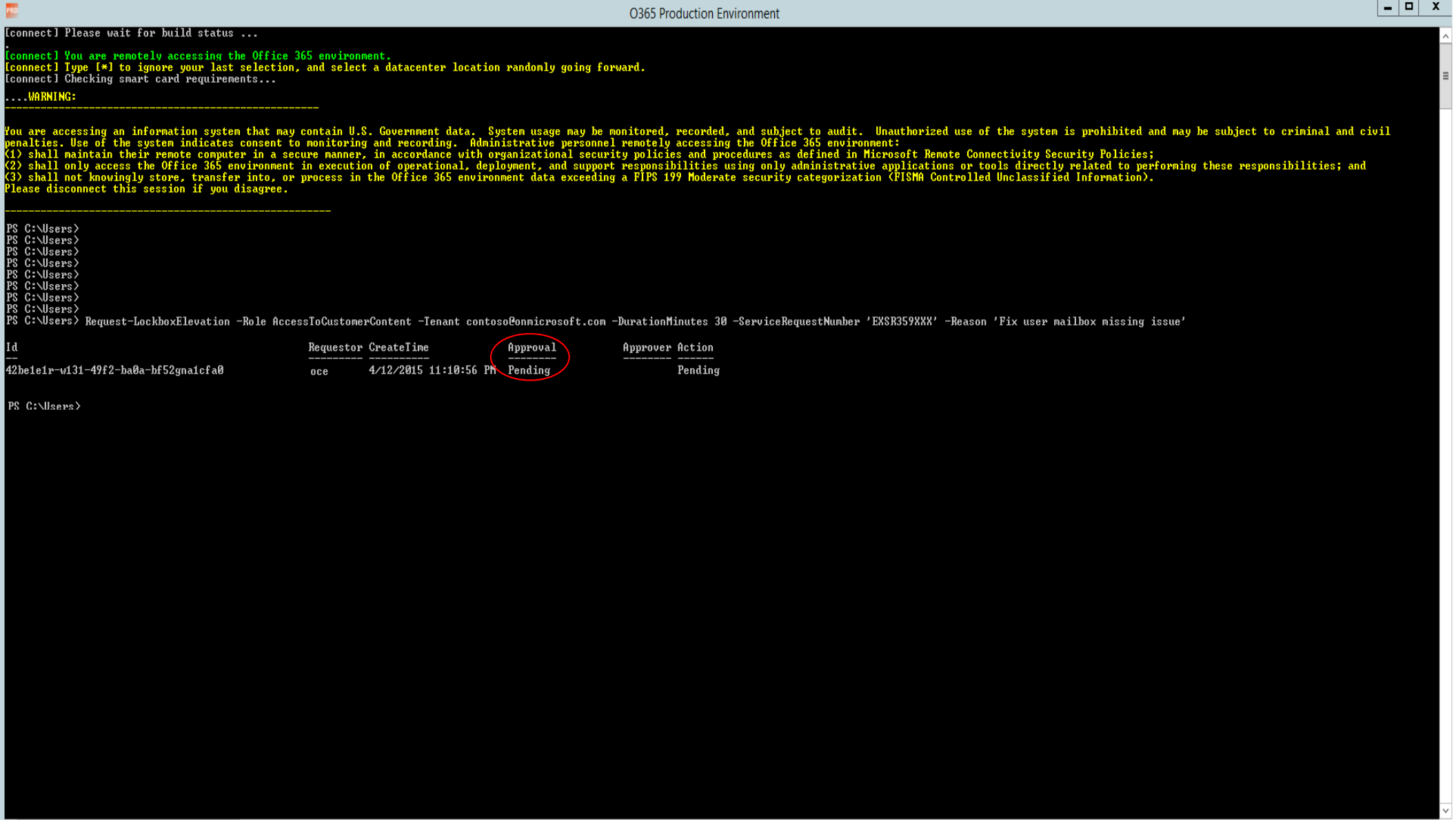
Service Request# EXSR359XXX
[Status: Active] Help!
User's mailbox,
Need access to customer content to fix this issue
not listed in soft deleted or removed mailboxes

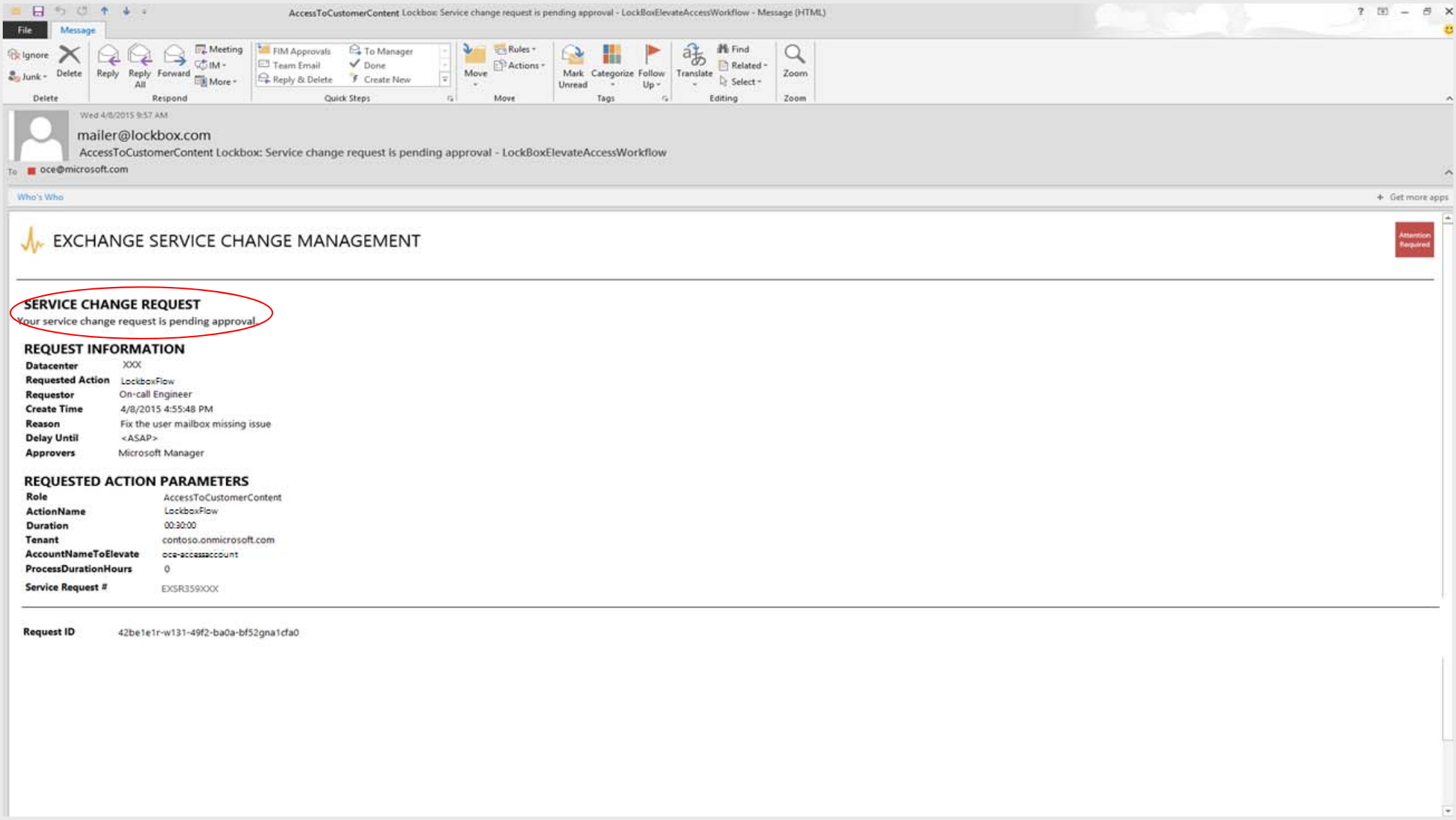

O365 Production Environment
You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit.
Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring
and recording. Administrative personnel remotely accessing the Office 365 environment:
(1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in
Microsoft Remote Connectivity Security Policies;
(2) shall only access the Office 365 environment in execution of operational, deployment, and support responsibilities using only administrative
applications or tools directly related to performing these responsibilities; and
(3) shall not knowingly store, transfer into, or process in the Office 365 environment data exceeding a FIPS 199 Moderate security categorization
(FISMA Controlled Unclassified Information).
Please disconnect this session if you disagree.
VERBOSE: Connected to
PS D:\Users\Desktop> get-command New-MailboxRestoreRequest
get-command : The term 'New-MailboxRestoreRequest' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ get-command New-MailboxRestoreRequest
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : ObjectNotFound: (New-MailboxRestoreRequest:String) [Get-Command], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException,Microsoft.PowerShell.Commands.GetCommandCommand
PS D:\Users\Desktop>

Customer Lockbox flow

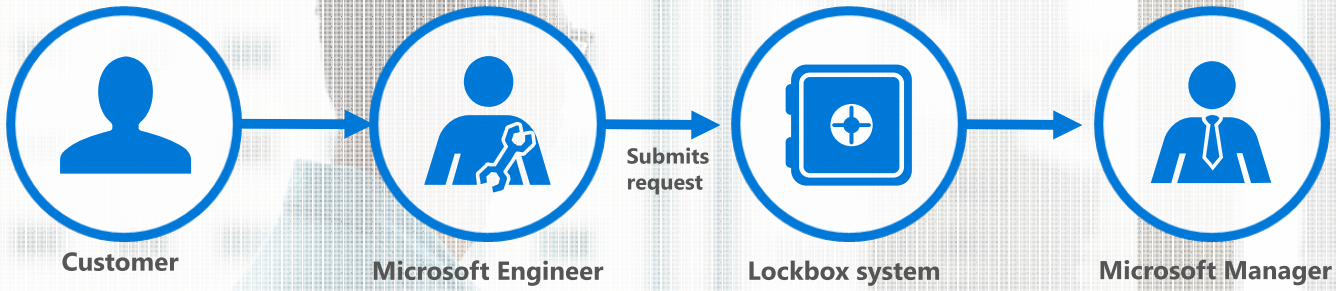


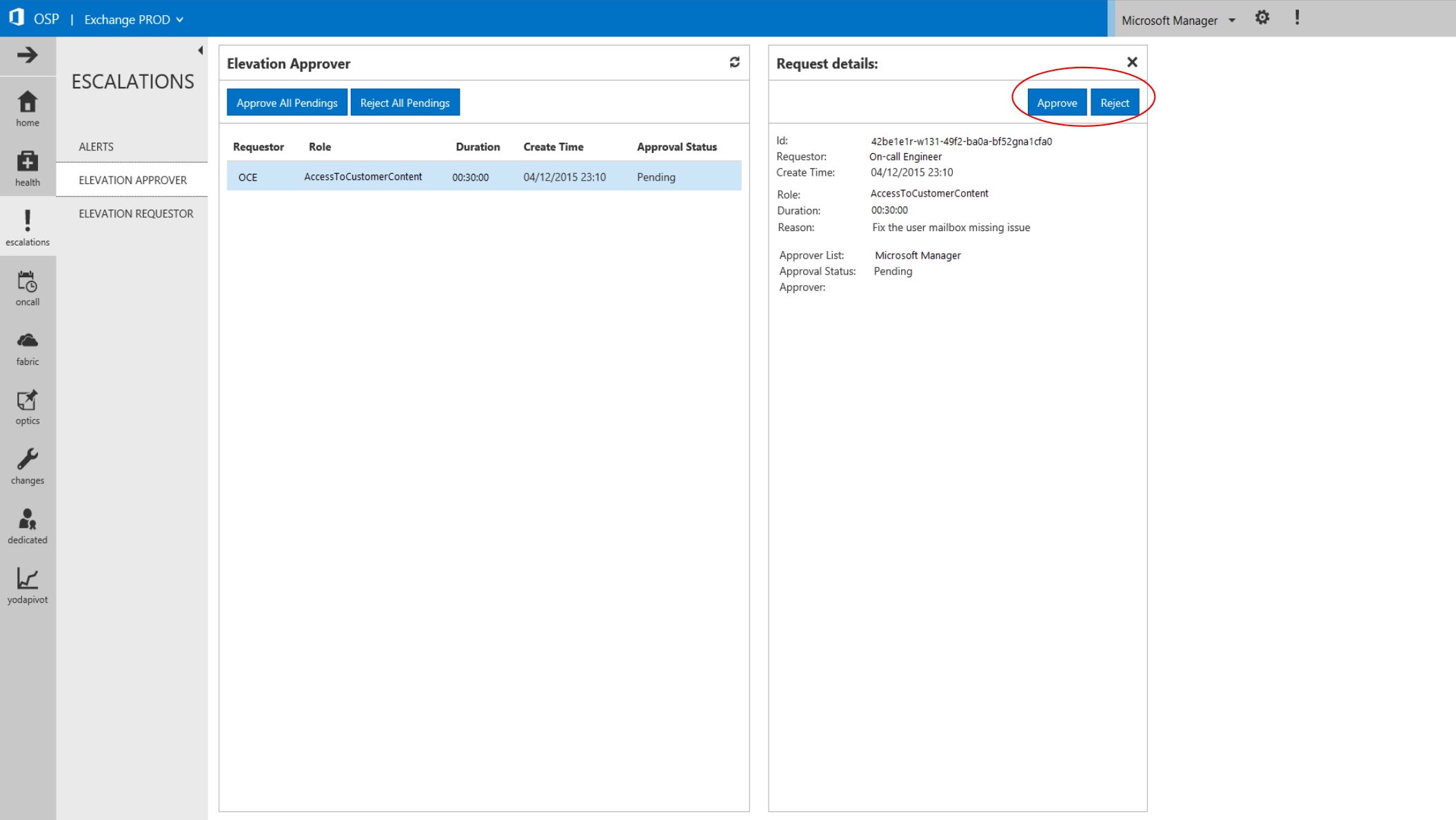

O365 Production Environment
[connect] Please wait for build status ...
.
[connect] You are remotely accessing the Office 365 environment.
[connect] Type [*] to ignore your last selection, and select a datacenter location randomly going forward.
[connect] Checking smart card requirements...
....WARNING:
You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring and recording. Administrative personnel remotely accessing the Office 365 environment:
(1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in Microsoft Remote Connectivity Security Policies;
(2) shall only access the Office 365 environment in execution of operational, deployment, and support responsibilities using only administrative applications or tools directly related to performing these responsibilities; and
(3) shall not knowingly store, transfer into, or process in the Office 365 environment data exceeding a FIPS 199 Moderate security categorization (FISMA Controlled Unclassified Information).
Please disconnect this session if you disagree.
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users> Request-LockboxElevation -Role AccessToCustomerContent -Tenant contoso@onmicrosoft.com -DurationMinutes 30 -ServiceRequestNumber 'EXSR359XXX' -Reason 'Fix user mailbox missing issue'

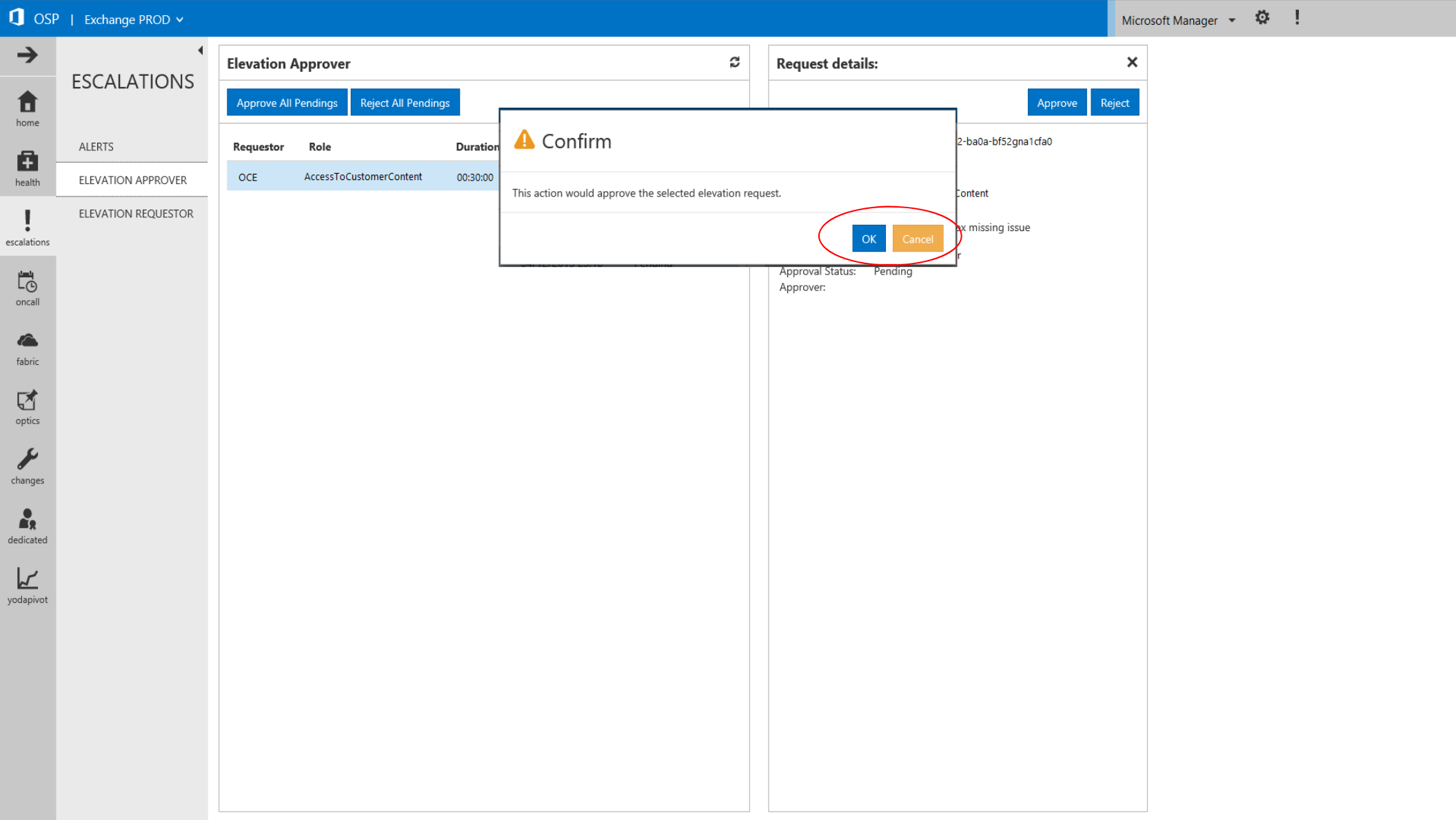

O365 Production Environment
[connect] Please wait for build status ...
.
[connect] You are remotely accessing the Office 365 environment.
[connect] Type [*] to ignore your last selection, and select a datacenter location randomly going forward.
[connect] Checking smart card requirements...
....WARNING:
You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring and recording. Administrative personnel remotely accessing the Office 365 environment:
(1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in Microsoft Remote Connectivity Security Policies;
(2) shall only access the Office 365 environment in execution of operational, deployment, and support responsibilities using only administrative applications or tools directly related to performing these responsibilities; and
(3) shall not knowingly store, transfer into, or process in the Office 365 environment data exceeding a FIPS 199 Moderate security categorization (FISMA Controlled Unclassified Information).
Please disconnect this session if you disagree.
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users> Request-LockboxElevation -Role AccessToCustomerContent -Tenant contoso@onmicrosoft.com -DurationMinutes 30 -ServiceRequestNumber 'EXSR359XXX' -Reason 'Fix user mailbox missing issue'
Id Requestor CreateTime Approval Approver Action
42be1e1r-w131-49f2-ba0a-bf52gna1cfa0 oce 4/12/2015 11:10:56 PM Pending Pending
PS C:\Users>

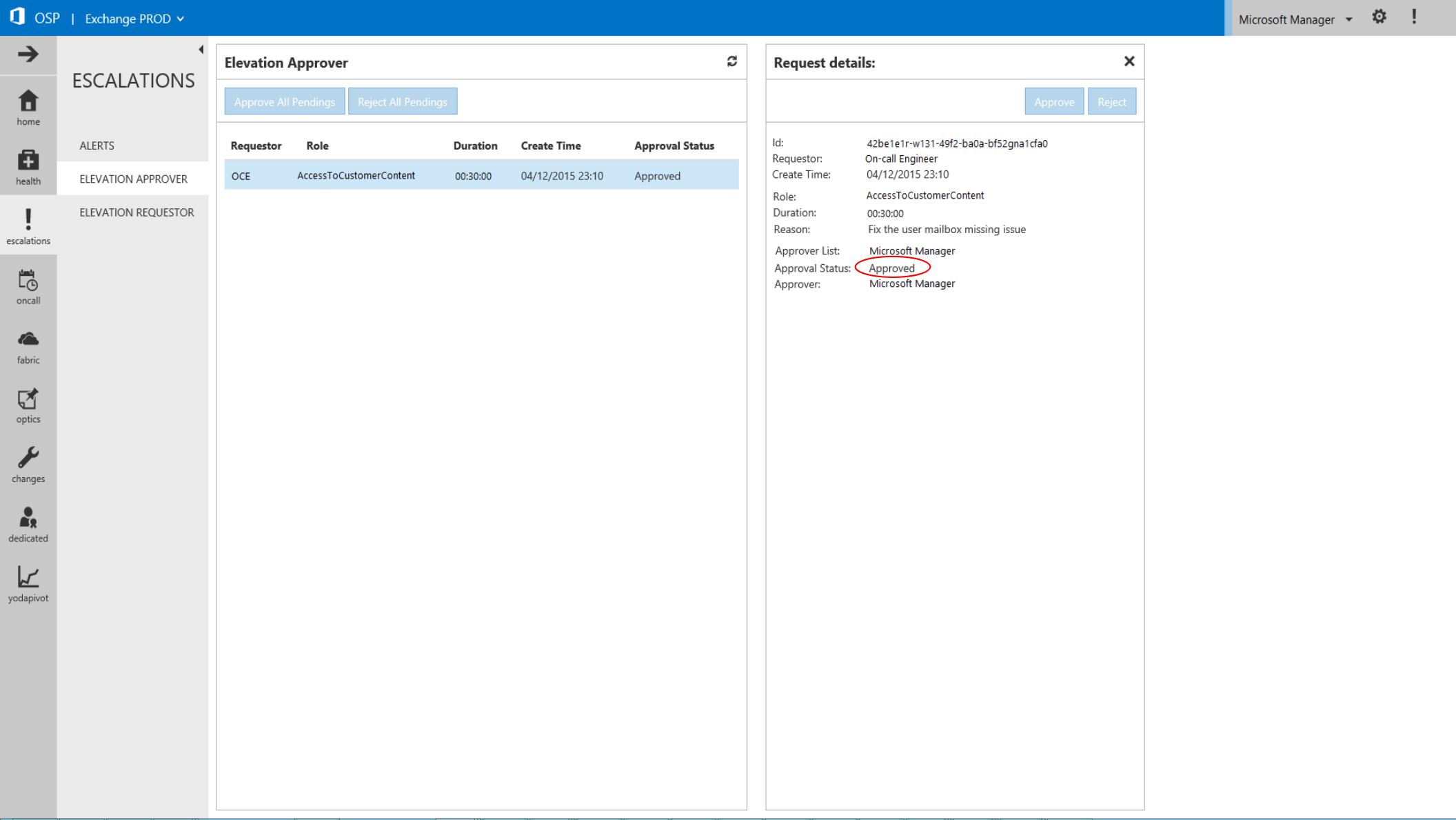

AccessToCustomerContent Lockbox: Service change request is pending approval - LockBoxElevateAccessWorkflow - Message (HTML)
File
Message
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
IM
More
Respond
FIM Approvals
Team Email
Reply & Delete
To Manager
Done
Create New
Quick Steps
Move
Rules
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
Zoom
Wed 4/8/2015 9:57 AM
mailer@lockbox.com
AccessToCustomerContent Lockbox: Service change request is pending approval - LockBoxElevateAccessWorkflow
To oce@microsoft.com
Who's Who
Get more apps
EXCHANGE SERVICE CHANGE MANAGEMENT
Attention Required
SERVICE CHANGE REQUEST
Your service change request is pending approval.
REQUEST INFORMATION
Datacenter XXX
Requested Action LockboxFlow
Requestor On-call Engineer
Create Time 4/8/2015 4:55:48 PM
Reason Fix the user mailbox missing issue
Delay Until <ASAP>
Approvers Microsoft Manager
REQUESTED ACTION PARAMETERS
Role AccessToCustomerContent
ActionName LockboxFlow
Duration 00:30:00
Tenant contoso.onmicrosoft.com
AccountNameToElevate oce-accessaccount
ProcessDurationHours 0
Service Request # EXSR359XXX
Request ID 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0

Customer Lockbox flow




OSP | Exchange PROD
Microsoft Manager
ESCALATIONS
home
health
escalations
oncall
fabric
optics
changes
dedicated
yodapivot
ALERTS
ELEVATION APPROVER
ELEVATION REQUESTOR
Elevation Approver
Approve All Pendings
Reject All Pendings
Requestor
Role
Duration
Create Time
Approval Status
OCE
AccessToCustomerContent
00:30:00
04/12/2015 23:10
Pending
Request details:
Approve
Reject
Id: 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0
Requestor: On-call Engineer
Create Time: 04/12/2015 23:10
Role: AccessToCustomerContent
Duration: 00:30:00
Reason: Fix the user mailbox missing issue
Approver List: Microsoft Manager
Approval Status: Pending
Approver:


OSP | Exchange PROD
Microsoft Manager
ESCALATIONS
home
health
escalations
oncall
fabric
optics
changes
dedicated
yodapivot
ALERTS
ELEVATION APPROVER
ELEVATION REQUESTOR
Elevation Approver
Approve All Pendings
Reject All Pendings
Requestor
Role
Duration
OCE
AccessToCustomerContent
00:30:00
Request details:
Approve
Reject
2-ba0a-bf52gna1cfa0
Content
x missing issue
Approval Status: Pending
Approver:
Confirm
This action would approve the selected elevation request.
OK
Cancel


OSP | Exchange PROD
Microsoft Manager
ESCALATIONS
home
health
escalations
oncall
fabric
optics
changes
dedicated
yodapivot
ALERTS
ELEVATION APPROVER
ELEVATION REQUESTOR
Elevation Approver
Approve All Pendings
Reject All Pendings
Requestor
Role
Duration
Create Time
Approval Status
OCE
AccessToCustomerContent
00:30:00
04/12/2015 23:10
Approved
Request details:
Approve
Reject
Id: 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0
Requestor: On-call Engineer
Create Time: 04/12/2015 23:10
Role: AccessToCustomerContent
Duration: 00:30:00
Reason: Fix the user mailbox missing issue
Approver List: Microsoft Manager
Approval Status: Approved
Approver: Microsoft Manager

Wed 4/8/2015 9:57 AM

mailer@lockbox.com

AccessToCustomerContent Lockbox: Service change request is approved - LockBoxElevateAccessWorkflow

To oce@microsoft.com

Who's Who + Get more apps

EXCHANGE SERVICE CHANGE MANAGEMENT

Attention Required

REQUEST APPROVED

Your Service Change Request has been approved by Datacenter approver. Pending approval from Tenant admin.

REQUEST INFORMATION

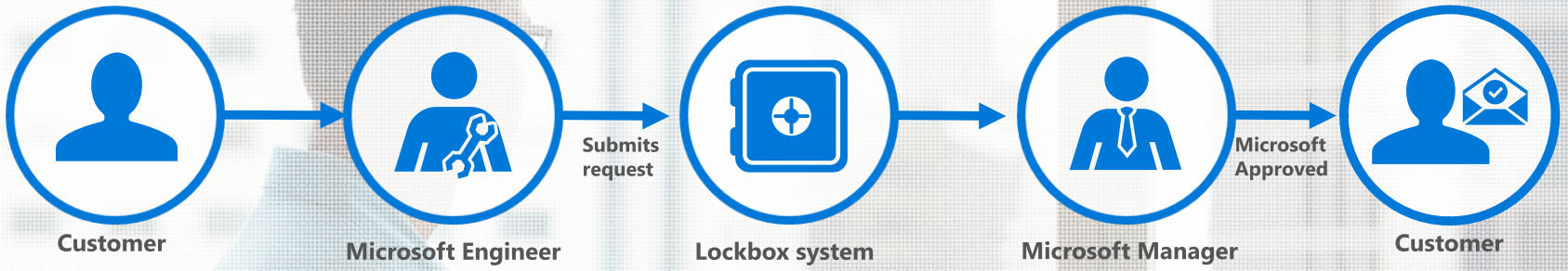
Datacenter	XXX
Requested Action	LockboxFlow
Requestor	On-call Engineer
Create Time	4/8/2015 4:55:48 PM
Reason	Fix the user mailbox missing issue
Delay Until	<ASAP>
Approvers	Customer

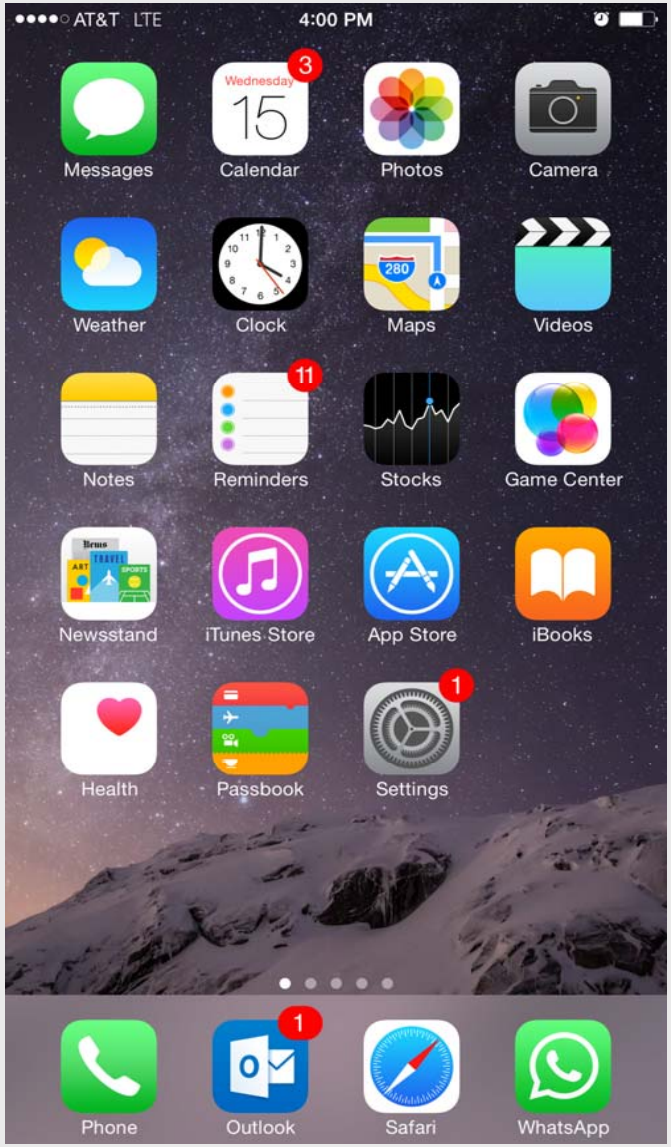
REQUESTED ACTION PARAMETERS

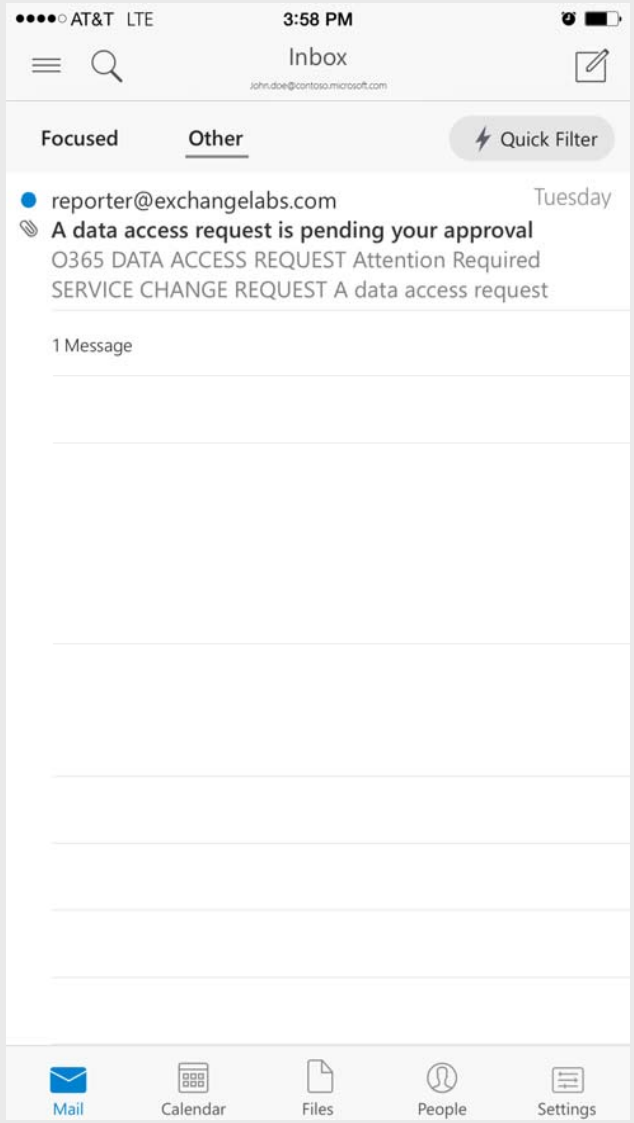
Role	AccessToCustomerContent
ActionName	LockboxFlow
Duration	00:30:00
Tenant	contoso.onmicrosoft.com
AccountNameToElevate	oce-accessaccount
ProcessDurationHours	0
Service Request #	EXSR359XXX

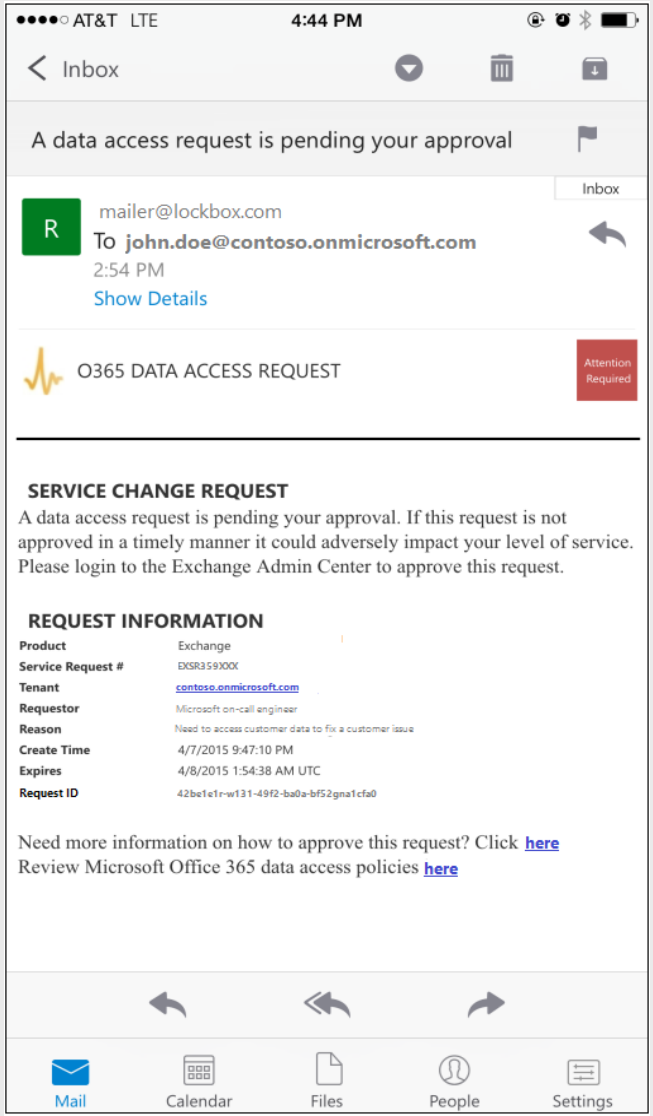
Request ID 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0

Customer Lockbox flow




AT&T LTE
4:00 PM
Messages
Wednesday
15
3
Calendar
Photos
Camera
Weather
Clock
280
Maps
Videos
11
Notes
Reminders
Stocks
Game Center
Newsstand
iTunes Store
App Store
iBooks
1
Health
Passbook
Settings
1
Phone
Outlook
Safari
WhatsApp


AT&T LTE
3:58 PM
Inbox
Focused
Other
Quick Filter
reporter@exchangelabs.com
Tuesday
A data access request is pending your approval
O365 DATA ACCESS REQUEST Attention Required
SERVICE CHANGE REQUEST A data access request
1 Message
Mail
Calendar
Files
People
Settings


●●●●○ AT&T LTE
4:44 PM
Inbox
A data access request is pending your approval
Inbox
R
mailer@lockbox.com
To john.doe@contoso.onmicrosoft.com
2:54 PM
Show Details
O365 DATA ACCESS REQUEST
Attention Required
SERVICE CHANGE REQUEST
A data access request is pending your approval. If this request is not approved in a timely manner it could adversely impact your level of service. Please login to the Exchange Admin Center to approve this request.
REQUEST INFORMATION
Product Exchange
Service Request # EXSR359XXX
Tenant contoso.onmicrosoft.com
Requestor Microsoft on-call engineer
Reason Need to access customer data to fix a customer issue
Create Time 4/7/2015 9:47:10 PM
Expires 4/8/2015 1:54:38 AM UTC
Request ID 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0
Need more information on how to approve this request? Click here
Review Microsoft Office 365 data access policies here
Mail
Calendar
Files
People
Settings

Office 365

Sign in with your work or school account

john.doe@contoso.onmicrosoft.com

••••••••••••••••••

Keep me signed in

Sign in

Can't access your account?

Your work or school account can be used anywhere you see this symbol. © 2015 Microsoft Legal Privacy Feedback

Hi, John.

Install Office on your PC

Word Excel PowerPoint Outlook OneNote

Got a Mac? Sign in to Office 365 on your Mac to install.

Smartphone or tablet? Get Office on your devices
Learn how to set up email and Office 365 apps on your device

Install now

Language: English
Change language
Troubleshoot installation

Collaborate with Office Online

Mail Calendar People Newsfeed OneDrive Sites Tasks

Delve Word Online Excel Online PowerPoint Online OneNote Online Admin

Office 365 admin center «

Search users, admin tasks and

DASHBOARD
SETUP
USERS
COMPANY PROFILE
CONTACTS
SHARED MAILBOXES
MEETING ROOMS
GROUPS
DOMAINS
PUBLIC WEBSITE
BILLING
EXTERNAL SHARING
SERVICE SETTINGS
REPORTS
SERVICE HEALTH
SUPPORT
PURCHASE SERVICES
MESSAGE CENTER
TOOLS
ADMIN
Exchange
Lync
SharePoint
Compliance
Azure AD
Bing Places for Business

Welcome to Office 365!

Watch the video to get an overview
Set up your services
Download your software
Get information on Yammer

Watch the video to get started quickly

Service overview

Service health
No service issues

Data access requests
1 request(s) pending

Service requests
No open service requests

Inactive email users
0 users have not signed in for 30 days or more.

Mail protection
13 messages received, 0 processed by filtering.

Message center
1 new message in the past 7 days

Included services

Current health

Exchange	No issues
Identity Service	No issues
Lync	No issues
Office 365 Portal	No issues
Office Subscription	No issues
Rights Management Service	No issues
SharePoint	No issues
Yammer Enterprise	No issues

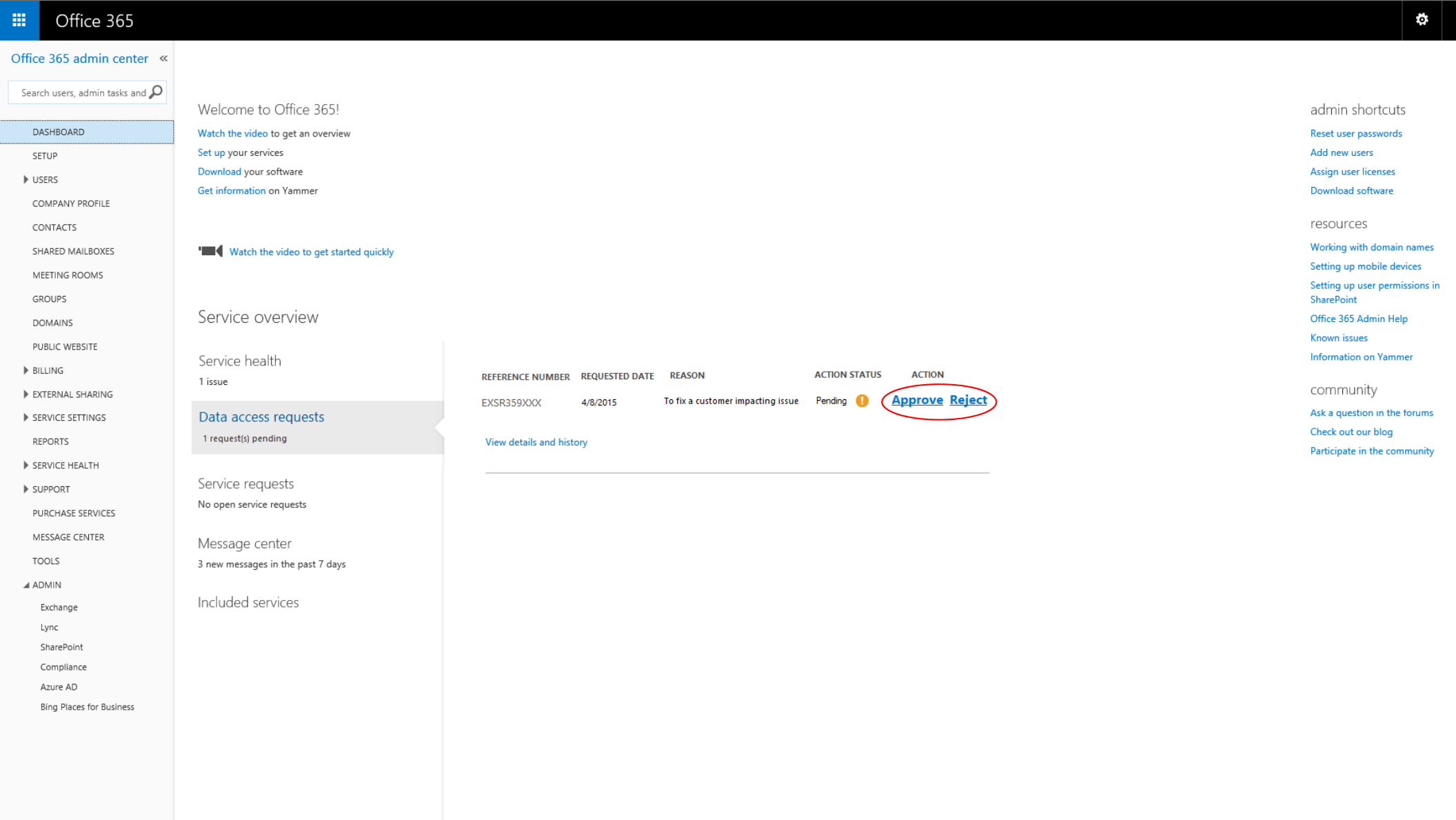
View details and history

Planned maintenance
No planned maintenance scheduled.

admin shortcuts
Reset user passwords
Add new users
Assign user licenses
Download software

resources
Working with domain names
Setting up mobile devices
Setting up user permissions in SharePoint
Office 365 Admin Help
Known issues
Information on Yammer

community
Ask a question in the forums
Check out our blog
Participate in the community


Office 365
Office 365 admin center
Search users, admin tasks and
DASHBOARD
SETUP
USERS
COMPANY PROFILE
CONTACTS
SHARED MAILBOXES
MEETING ROOMS
GROUPS
DOMAINS
PUBLIC WEBSITE
BILLING
EXTERNAL SHARING
SERVICE SETTINGS
REPORTS
SERVICE HEALTH
SUPPORT
PURCHASE SERVICES
MESSAGE CENTER
TOOLS
ADMIN
Exchange
Lync
SharePoint
Compliance
Azure AD
Bing Places for Business
Welcome to Office 365!
Watch the video to get an overview
Set up your services
Download your software
Get information on Yammer
Watch the video to get started quickly
Service overview
Service health
1 issue
Data access requests
1 request(s) pending
Service requests
No open service requests
Message center
3 new messages in the past 7 days
Included services
REFERENCE NUMBER
REQUESTED DATE
REASON
ACTION STATUS
ACTION
EXSR359XXX
4/8/2015
To fix a customer impacting issue
Pending
Approve
Reject
View details and history
admin shortcuts
Reset user passwords
Add new users
Assign user licenses
Download software
resources
Working with domain names
Setting up mobile devices
Setting up user permissions in SharePoint
Office 365 Admin Help
Known issues
Information on Yammer
community
Ask a question in the forums
Check out our blog
Participate in the community

Office 365 admin center «

Search users, admin tasks and

DASHBOARD
SETUP
USERS
COMPANY PROFILE
CONTACTS
SHARED MAILBOXES
MEETING ROOMS
GROUPS
DOMAINS
PUBLIC WEBSITE
BILLING
EXTERNAL SHARING
SERVICE SETTINGS
REPORTS
SERVICE HEALTH
SUPPORT
PURCHASE SERVICES
MESSAGE CENTER
TOOLS
ADMIN
Exchange
Lync
SharePoint
Compliance
Azure AD
Bing Places for Business

Welcome to Office 365!

Watch the video to get an overview
Set up your services
Download your software
Get information on Yammer

Watch the video to get started quickly

Service overview

Service health
1 issue

Data access requests
1 request(s) pending

Service requests
No open service requests

Message center
3 new messages in the past 7 days

Included services

DATA ACCESS REQUESTS

ARE YOU SURE YOU WANT TO APPROVE THIS DATA ACCESS REQUEST?

YES NO

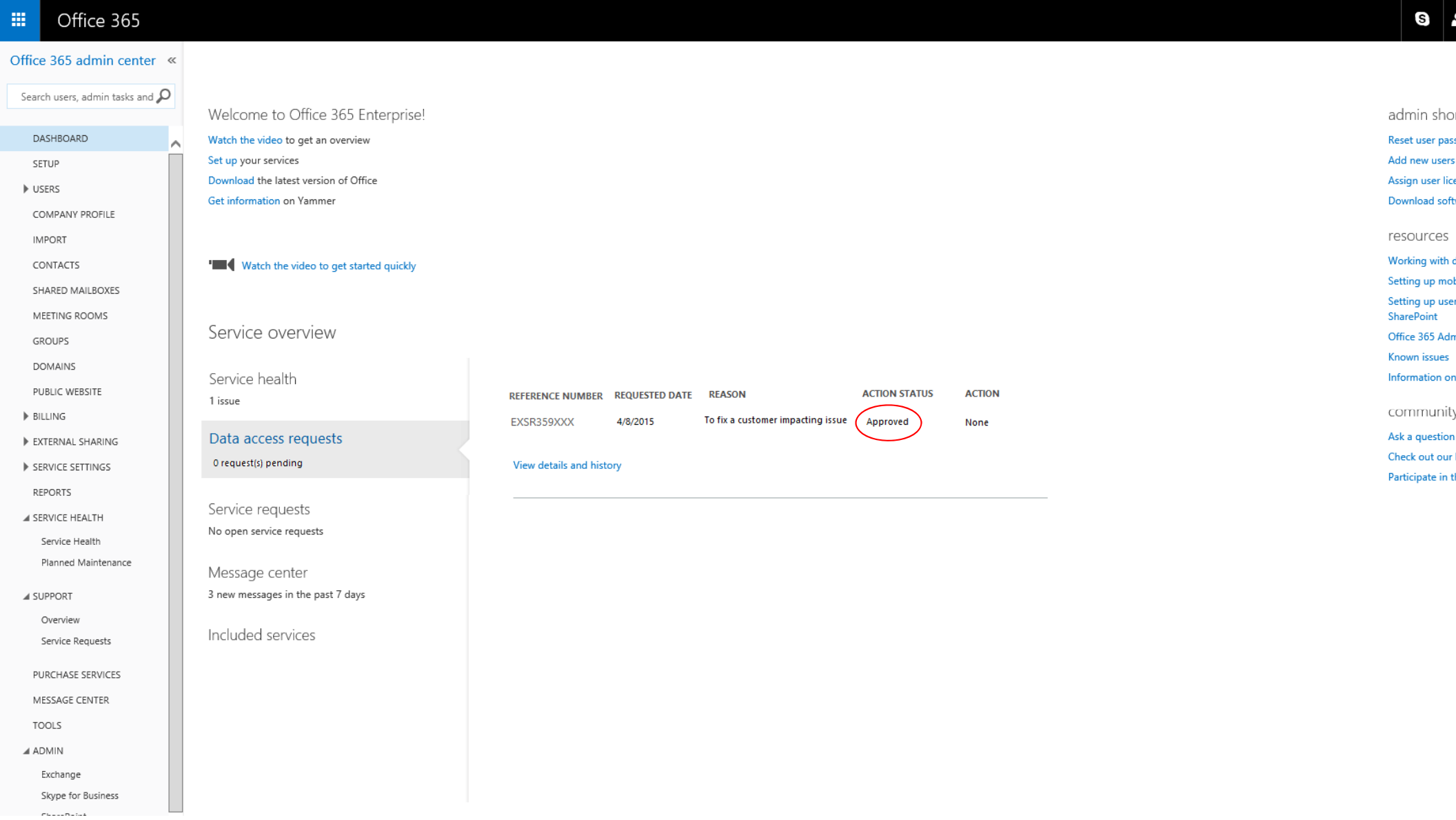
ACTION

Approve Reject

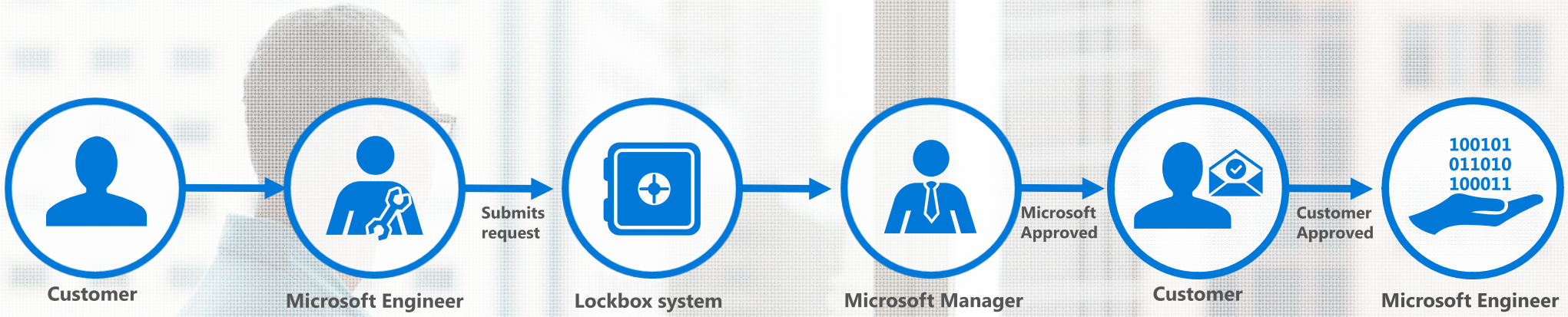
admin shortcuts
Reset user passwords
Add new users
Assign user licenses
Download software

resources
Working with domain names
Setting up mobile devices
Setting up user permissions in SharePoint
Office 365 Admin Help
Known issues
Information on Yammer

community
Ask a question in the forums
Check out our blog
Participate in the community


Office 365
Office 365 admin center
Search users, admin tasks and
DASHBOARD
SETUP
USERS
COMPANY PROFILE
IMPORT
CONTACTS
SHARED MAILBOXES
MEETING ROOMS
GROUPS
DOMAINS
PUBLIC WEBSITE
BILLING
EXTERNAL SHARING
SERVICE SETTINGS
REPORTS
SERVICE HEALTH
Service Health
Planned Maintenance
SUPPORT
Overview
Service Requests
PURCHASE SERVICES
MESSAGE CENTER
TOOLS
ADMIN
Exchange
Skype for Business
Welcome to Office 365 Enterprise!
Watch the video to get an overview
Set up your services
Download the latest version of Office
Get information on Yammer
Watch the video to get started quickly
Service overview
Service health
1 issue
Data access requests
0 request(s) pending
Service requests
No open service requests
Message center
3 new messages in the past 7 days
Included services
REFERENCE NUMBER
REQUESTED DATE
REASON
ACTION STATUS
ACTION
EXSR359XXX
4/8/2015
To fix a customer impacting issue
Approved
None
View details and history
admin sho
Reset user pass
Add new users
Assign user lice
Download soft
resources
Working with
Setting up mob
Setting up user
SharePoint
Office 365 Adm
Known issues
Information on
community
Ask a question
Check out our
Participate in t

Customer Lockbox flow



Wed 4/8/2015 9:57 AM

mailer@lockbox.com

AccessToCustomerContent Lockbox: Service change request action has completed - LockBoxElevateAccessWorkflow

To oce@microsoft.com

EXCHANGE SERVICE CHANGE MANAGEMENT

Attention Required

ACTION EXECUTED SUCCESSFULLY

Your account has been provisioned for AccessToCustomerContent

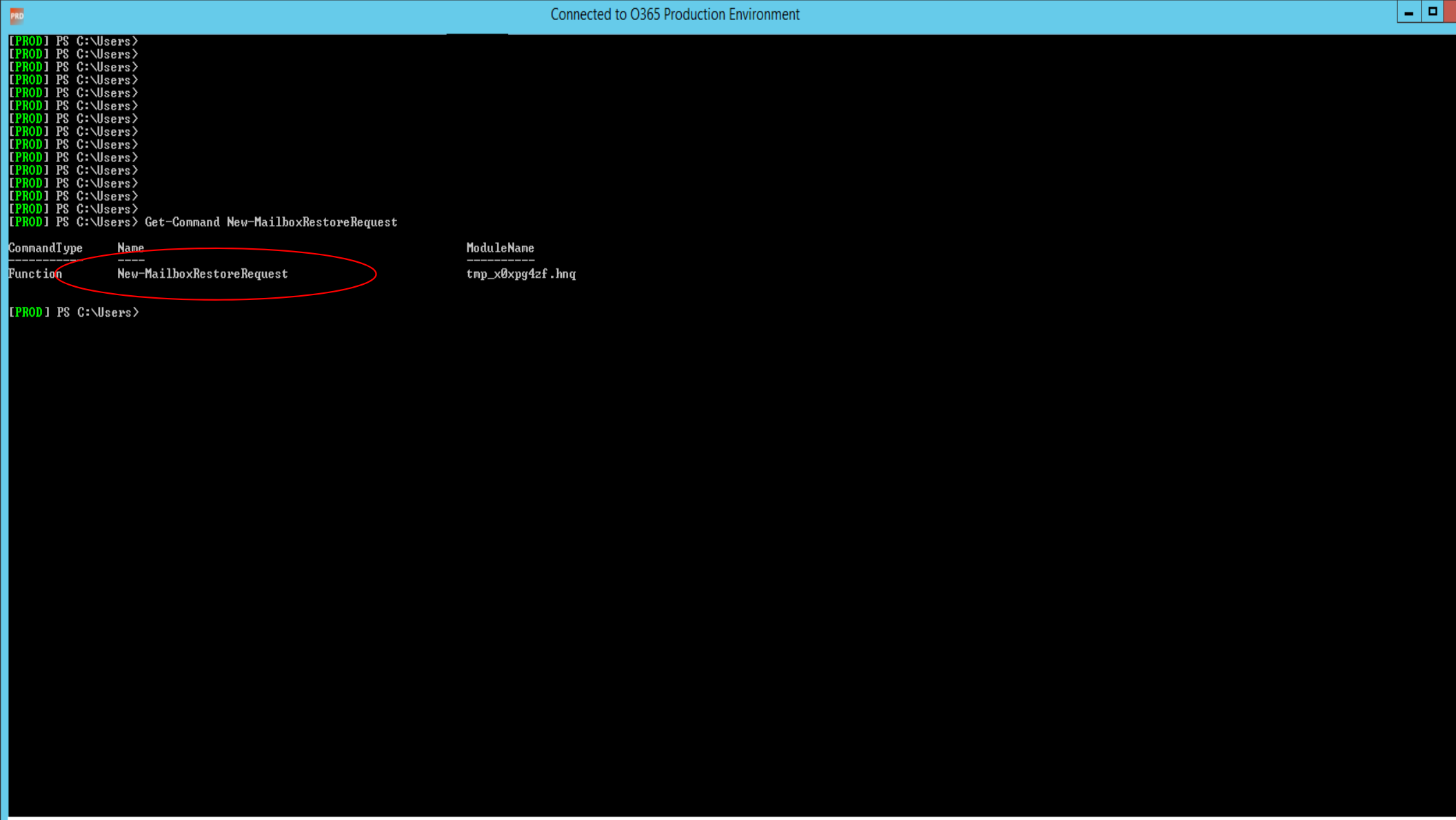
REQUEST INFORMATION

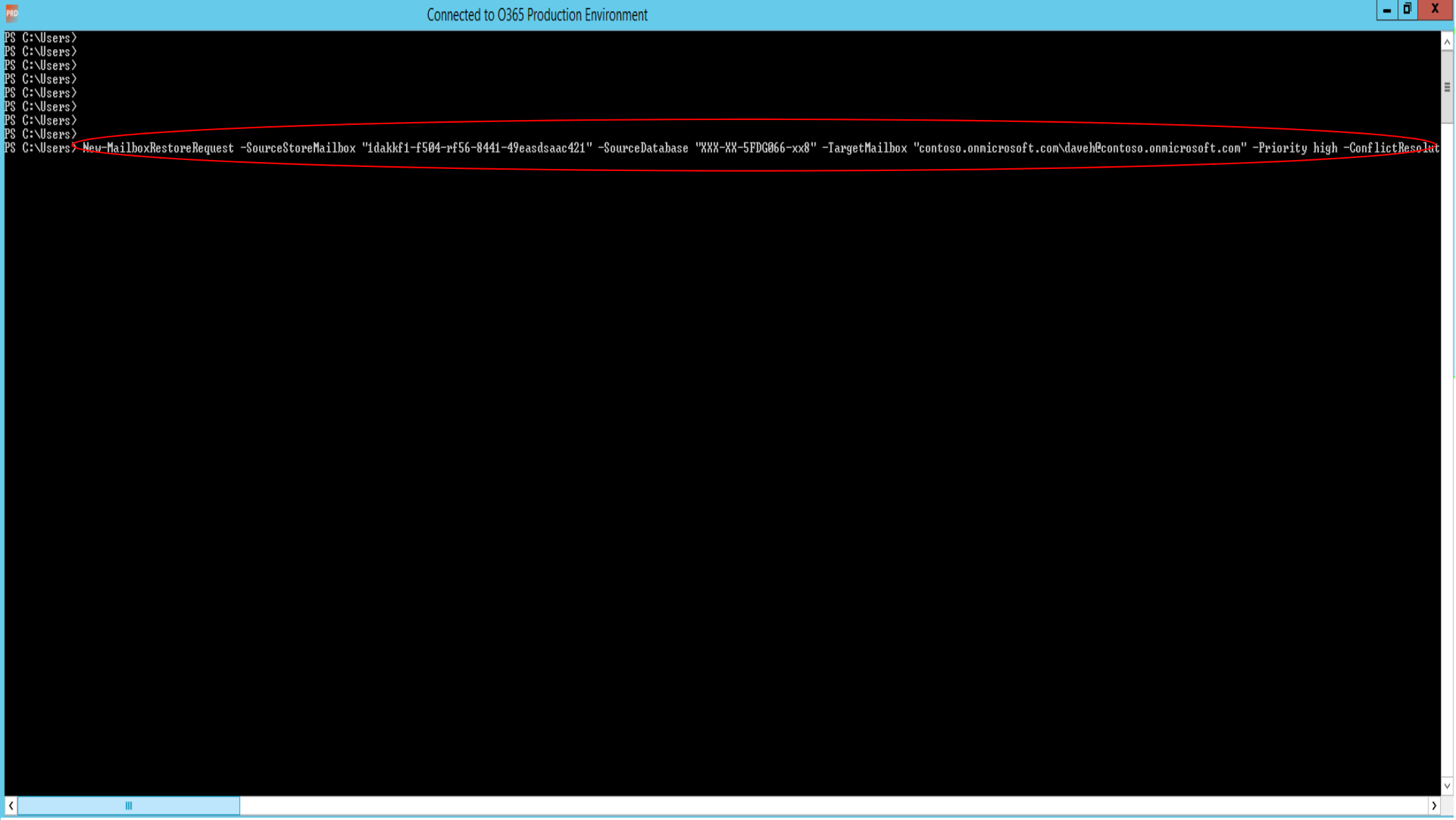
Datacenter	XXX
Requested Action	LockboxFlow
Requestor	On-call Engineer
Create Time	4/8/2015 4:55:48 PM
Reason	Fix the user mailbox missing issue
Delay Until	<ASAP>
Approvers	Microsoft Manager

REQUESTED ACTION PARAMETERS

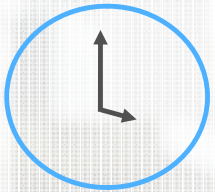
Role	AccessToCustomerContent
ActionName	LockboxFlow
Duration	00:30:00
Tenant	contoso.onmicrosoft.com
AccountNameToElevate	oce-accessaccount
ProcessDurationHours	0
Service Request #	EXSR359XXX

Request ID 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0


Connected to O365 Production Environment
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users>
[PROD] PS C:\Users> Get-Command New-MailboxRestoreRequest
CommandType Name ModuleName
Function New-MailboxRestoreRequest tmp_x0xpg4zf.hnq
[PROD] PS C:\Users>

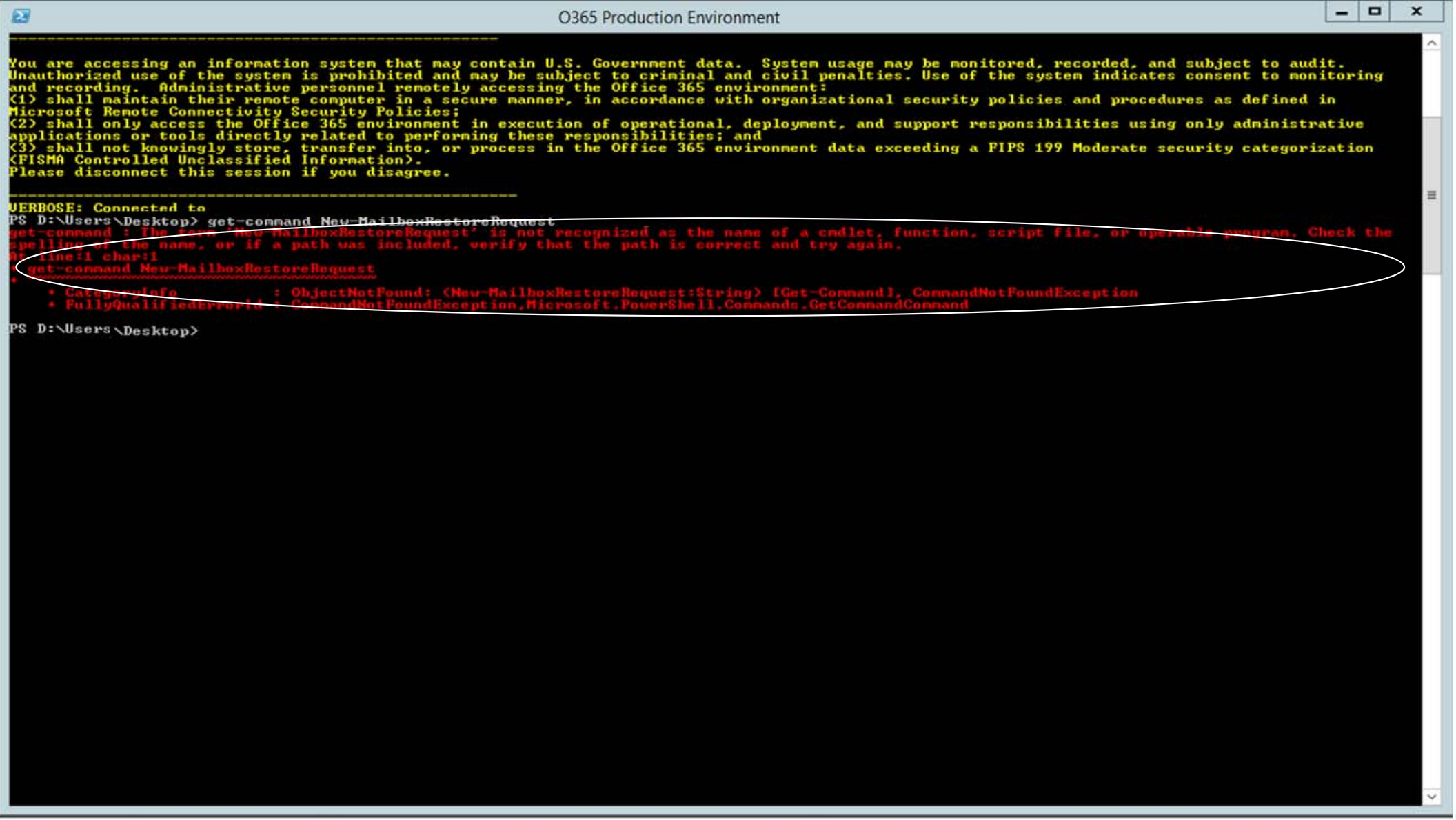

Connected to O365 Production Environment
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users>
PS C:\Users> New-MailboxRestoreRequest -SourceStoreMailbox "1dakkf1-f504-rf56-8441-49easdsaac421" -SourceDatabase "XXX-XX-5FDG066-xx8" -TargetMailbox "contoso.onmicrosoft.com\daveh@contoso.onmicrosoft.com" -Priority high -ConflictResolut

Customer Lockbox flow



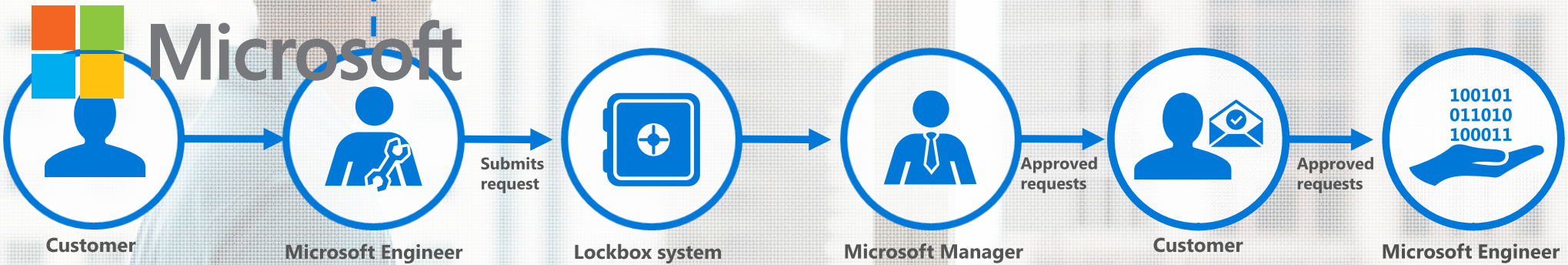
Elapsed Time

00:30:00 Minutes


O365 Production Environment
You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit.
Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring
and recording. Administrative personnel remotely accessing the Office 365 environment:
(1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in
Microsoft Remote Connectivity Security Policies;
(2) shall only access the Office 365 environment in execution of operational, deployment, and support responsibilities using only administrative
applications or tools directly related to performing these responsibilities; and
(3) shall not knowingly store, transfer into, or process in the Office 365 environment data exceeding a FIPS 199 Moderate security categorization
(FISMA Controlled Unclassified Information).
Please disconnect this session if you disagree.
VERBOSE: Connected to
PS D:\Users\Desktop> get-command New-MailboxRestoreRequest
get-command : The term 'New-MailboxRestoreRequest' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
get-command New-MailboxRestoreRequest
+ CategoryInfo : ObjectNotFound: (New-MailboxRestoreRequest:String) [Get-Command], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException,Microsoft.PowerShell.Commands.GetCommandCommand
PS D:\Users\Desktop>

Customer Lockbox flow

Service Request# EXSR359XXX [Status: Closed]
Lockbox Request# 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0
Role Requested CustomerContentAccess

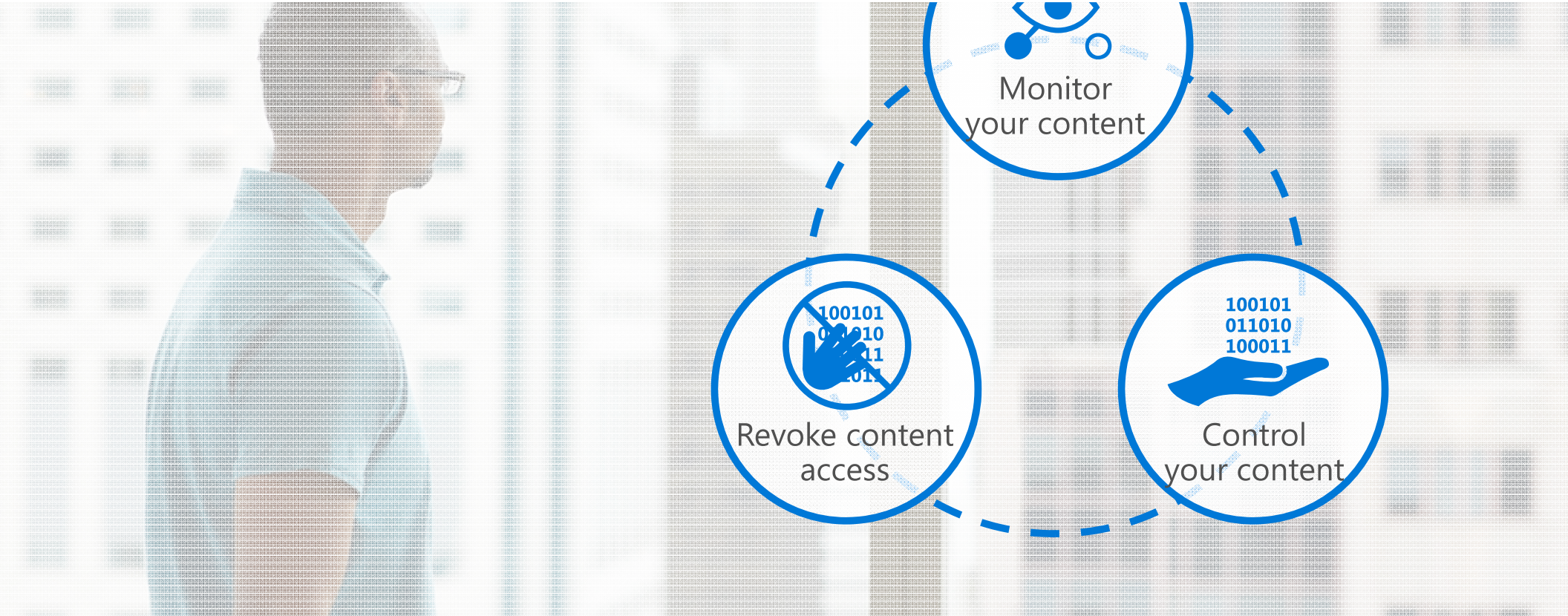


Scoped, least privileged access

Just-in-time access for limited duration

Audit logs for all access

Trust = transparency + control



Q&A

© 2015 Microsoft Corporation. All rights reserved.

Appendix