nordic infrastructure conference 2017

The premium event for IT-professionals

Feb. 1-3rd in Oslo Spektrum

Andy Malone MVP

CEO: Quality Training (Scotland) Ltd

Andrew.malone@quality-training.co.uk

Follow me on Twitter @AndyMalone

Andy Malone

(United Kingdom)

Microsoft MVP (Enterprise Security)
Microsoft Certified Trainer (20 years)
Founder: Cybercrime Security Forum
Worldwide Event Speaker
Author: The Seventh Day
www.AndyMalone.org

Lesson 1 The Trust Vs Knowledge Theory

Common Cloud Misconceptions

- My current computer systems will work just as well in the cloud as they do today
- It is easy to change from one cloud provider to another whenever I want to
- One vendor is more secure than another
- Vendors Cannot Access User Data
- Being in the Cloud Ensures my Privacy!
- Most users are brand loyal and will always stick to one vendor
- All Data is encrypted

Common Cloud Frustrations

- At Mercy of Vendors Security Policy
- Easy to Migrate Data in, but Difficult to Migrate out
- Users unsure on how to encrypt / Decrypt data
- How can users Backup Encryption Keys
- Vendors often Vague about Where Data in Stored.
- 85% Vendors Based in USA

Common Cloud Frustrations

- Difficulty to decipher the encryption terms cloud vendors use to describe their security
- Doing so would require discrimination between
- Transport encryption
- Data encryption
- Metadata encryption
- Encryption at rest vs. in motion & then most importantly Evaluating key management & access

I don't
trust words,
I TRUST
ACTIONS.

What do these Vendors Have in Common?

SPIDEROAK

Zero Knowledge Systems

"We don't know the names of your files, the names of your folders, the date they were created or last modified or accessed, their size, their checksums or hashes...in short we know nothing about your data except how much you store."

Lesson 2 Azure & the Brick Wall Theory

Azure Security = The Brick Wall Theory

Azure Information Protection

Azure Security Portal

BitLocker Disk Encryption

Azure Security Troubleshooter

Azure Security Documentation

Container Security

Multi Factor Authentication

Azure Forensics

Azure Security Health Monitoring

Azure AD Connect Health

Azure AD Privileged Identity Management

Hybrid Management

Microsoft Anti Malware For Cloud Services & Virtual Machines

Azure Key Vault

Azure AD Identity Protection

Azure Business Continuity

Traditional Security is not working

Data in Transit at Risk!

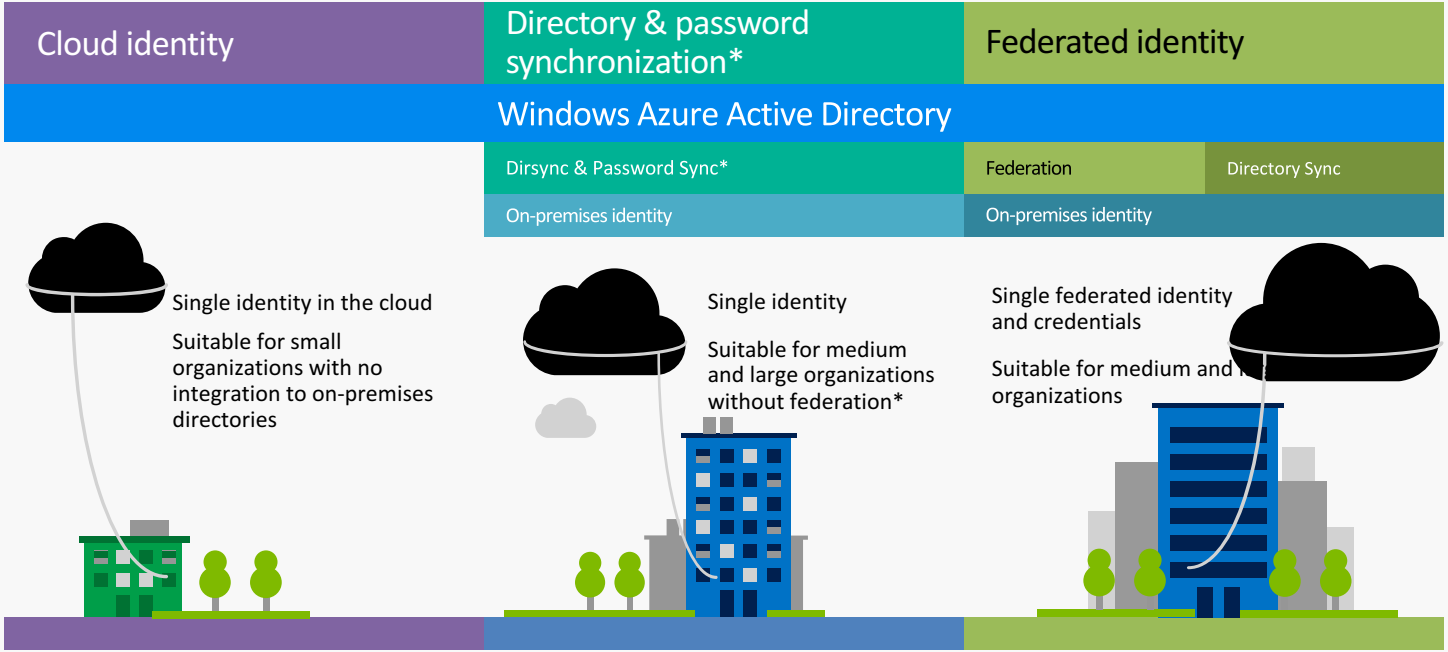
How is Microsoft Addressing the Problem?

Lesson 3 Identity is the New Control Plane

Identity has its Challenges …

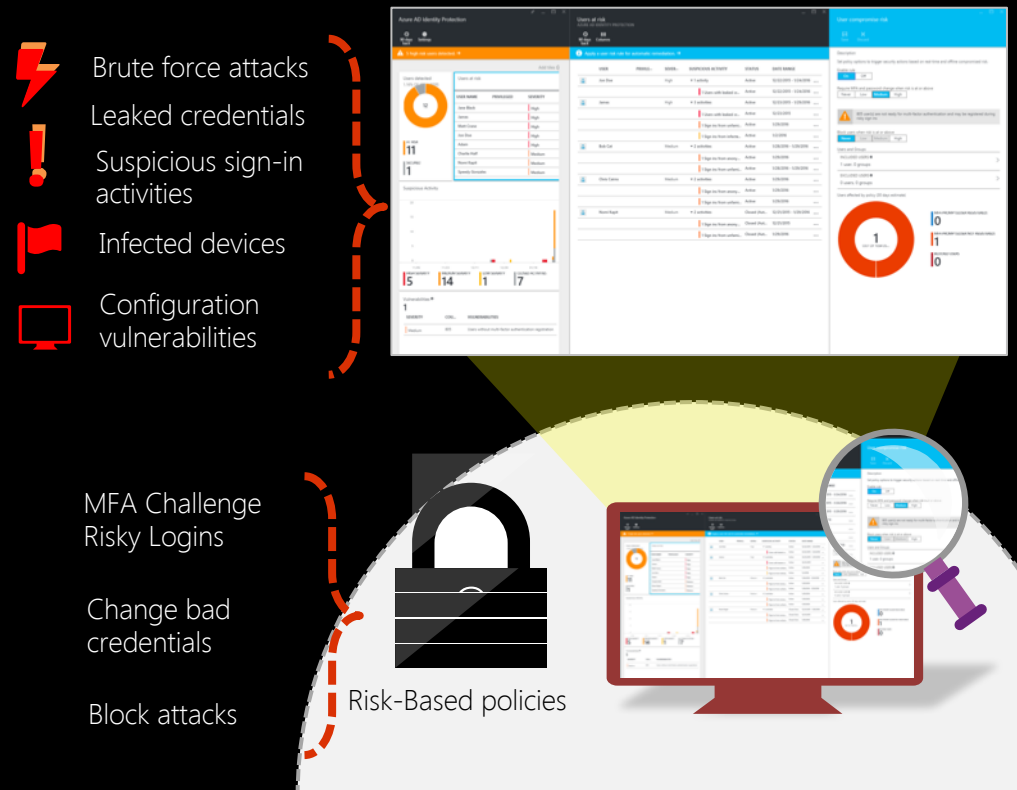
- Managing and controlling identity and user access
- Encrypting communications and operation processes
- Securing networks
- Managing threats
- Governess & Compliance
- Law Enforcement

Identity is the new Control Plane …



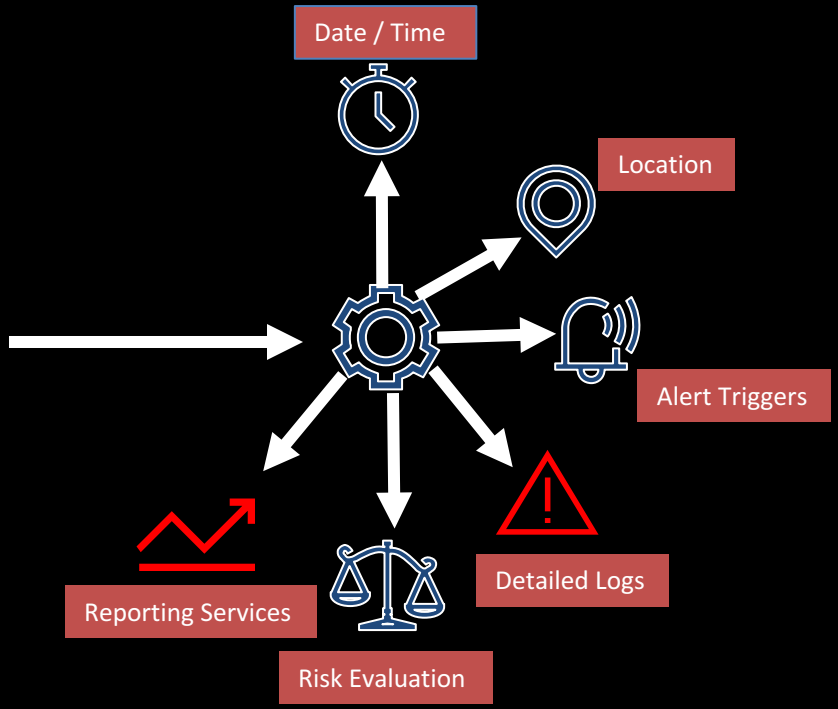
Azure Identity Protection

- Risk based Conditional Access automatically protects against suspicious logins and compromised credentials
- Detect and remediate configuration vulnerabilities to improve your security posture
- Gain insights from a consolidated view of machine learning based threat detection

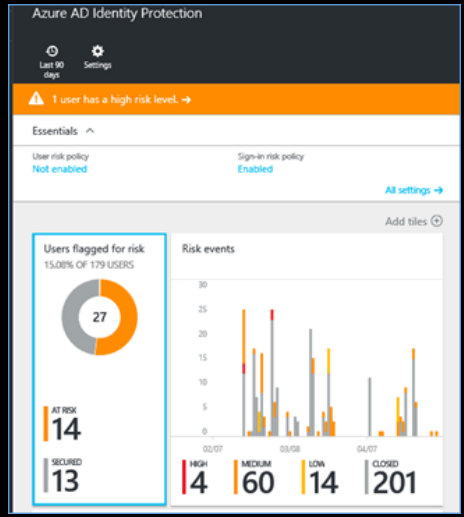


Azure AD Identity Protection

User Logs in



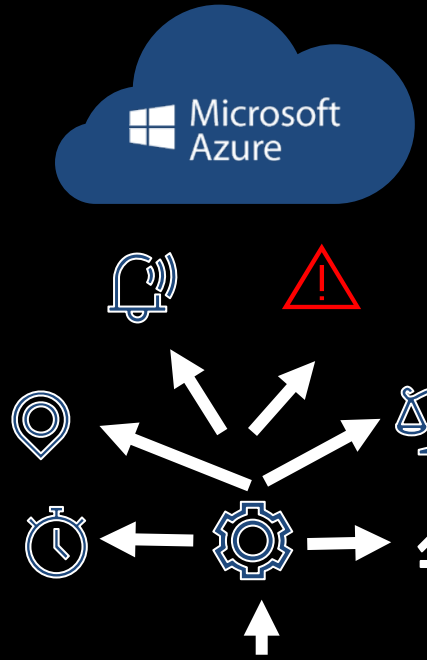
Azure Identity Protection



Detailed Heuristics

Azure AD Identity Protection!

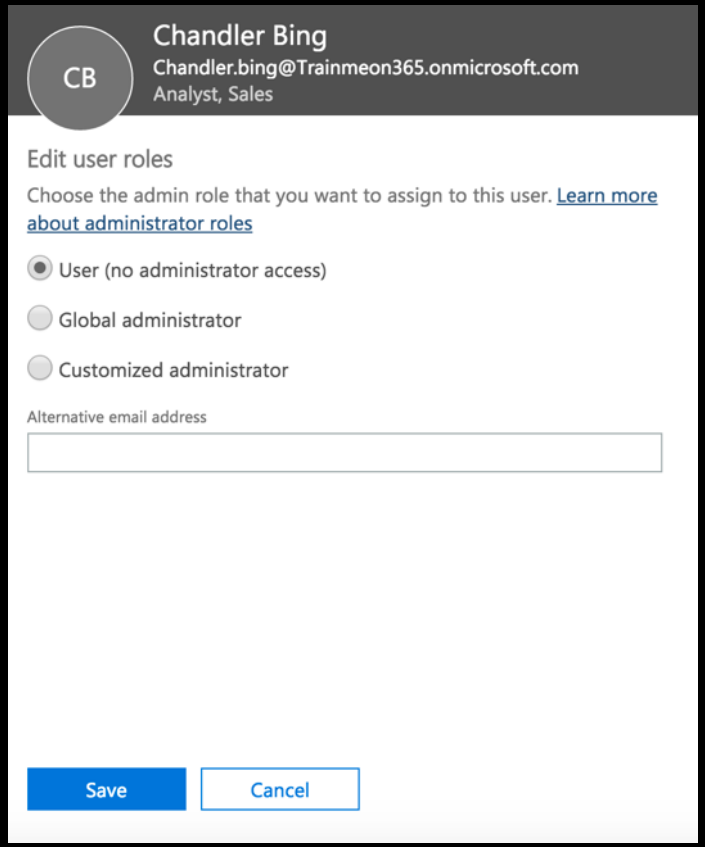
- Provides Detailed Reports on:
- Users with leaked credentials
- Irregular sign-in activity
- Sign-ins from possibly infected devices & unfamiliar locations
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from impossible travel
- & Much More …
- *Requires Azure AD Premium 2

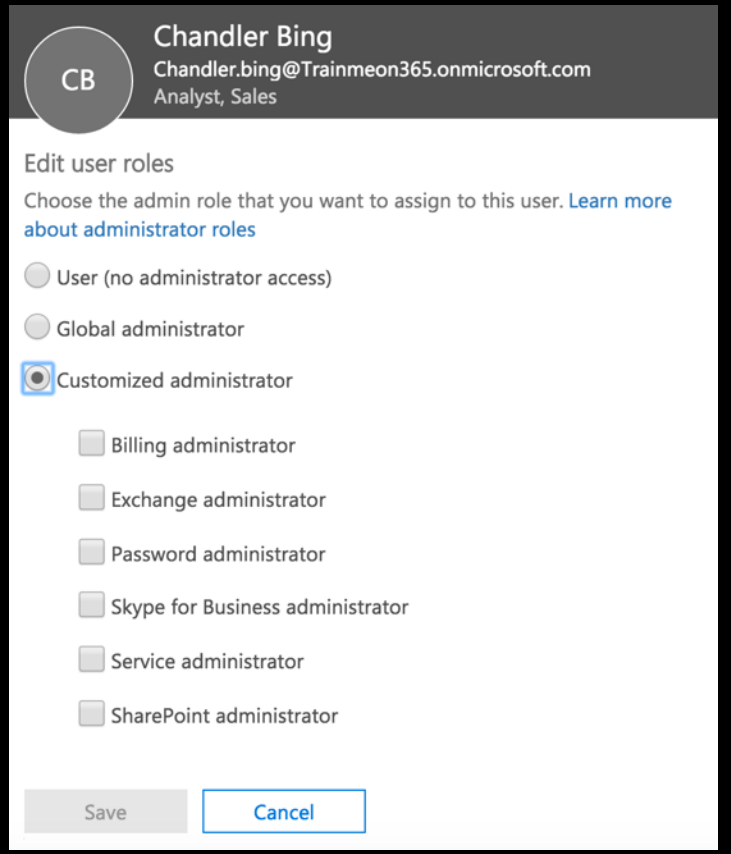


Demo: Azure AD Identity Protection

Lesson 4 Plug The Admin Holes

Beyond Role Based Admin Control?

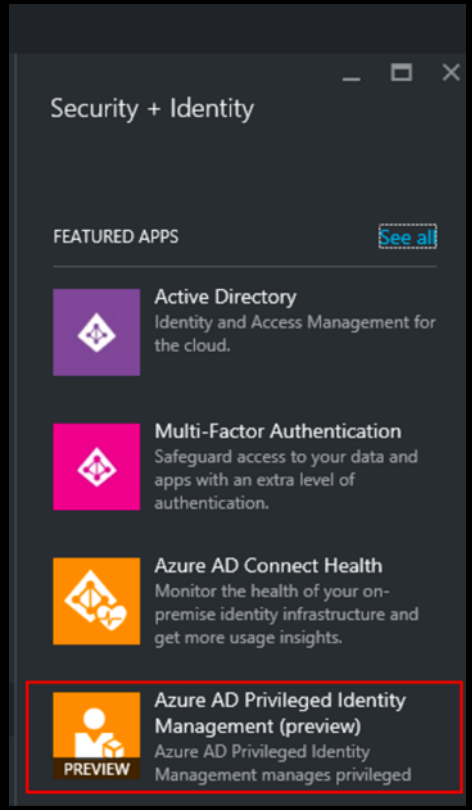




Azure AD Privileged Identity Management

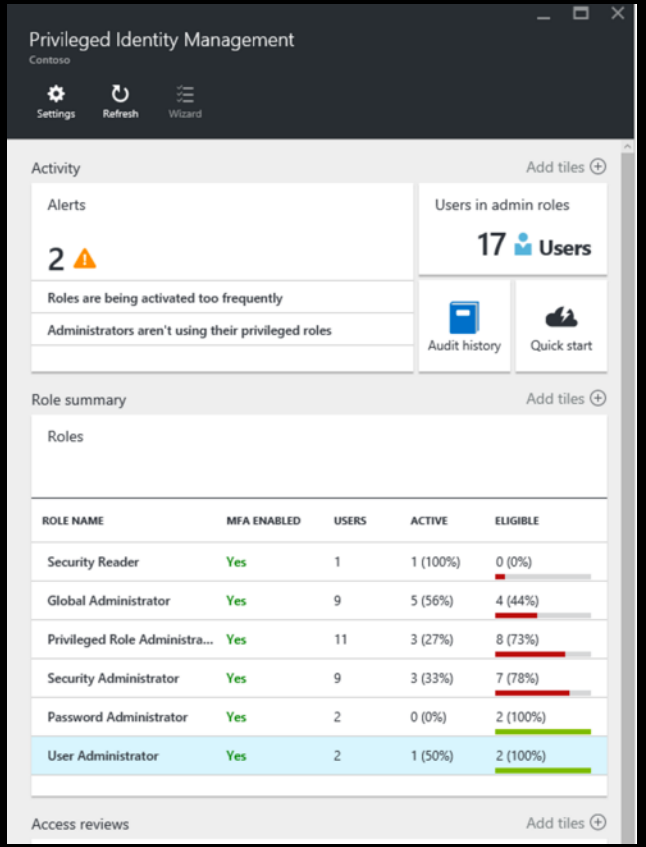
Azure AD Privileged Identity Management helps you

- See which users are Azure AD administrators
- Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune
- Get reports about administrator access history and changes in administrator assignments
- Get alerts about access to a privileged role

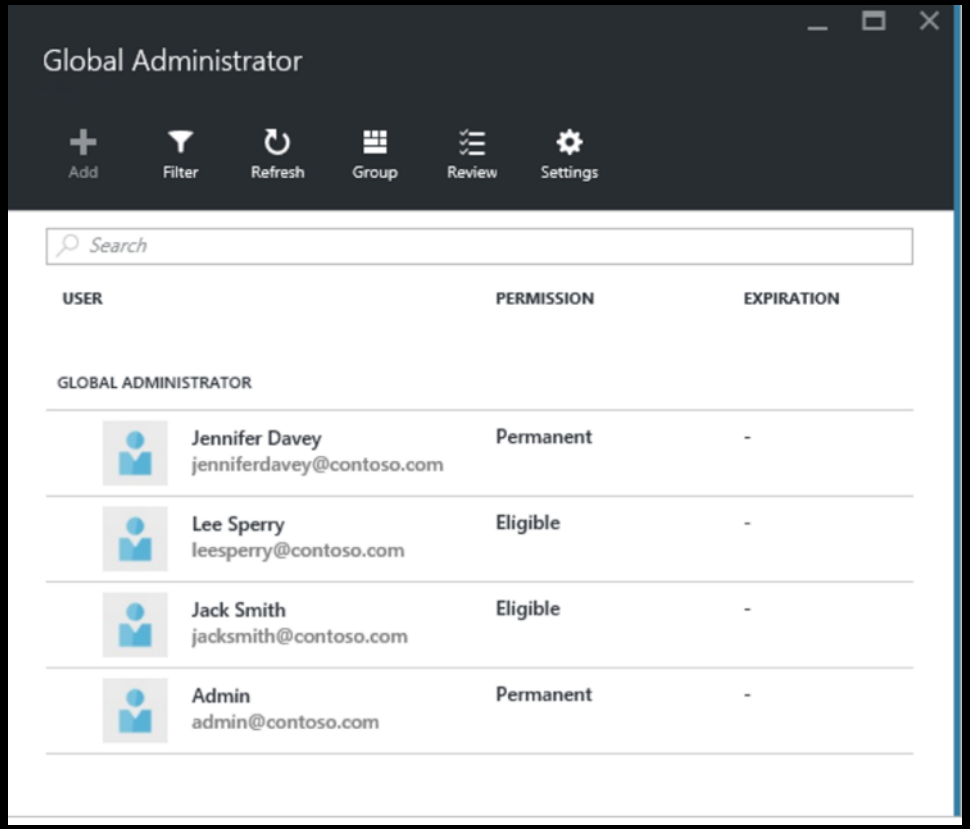


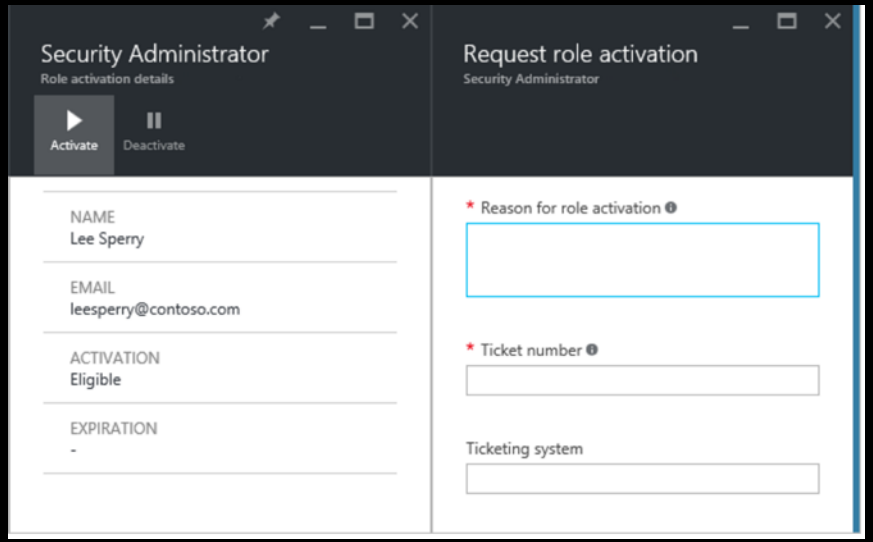
Azure AD Privileged Identity Management

- Alerts that point out opportunities to improve security
- The number of users who are assigned to each privileged role
- The number of eligible and permanent admins
- Ongoing access reviews



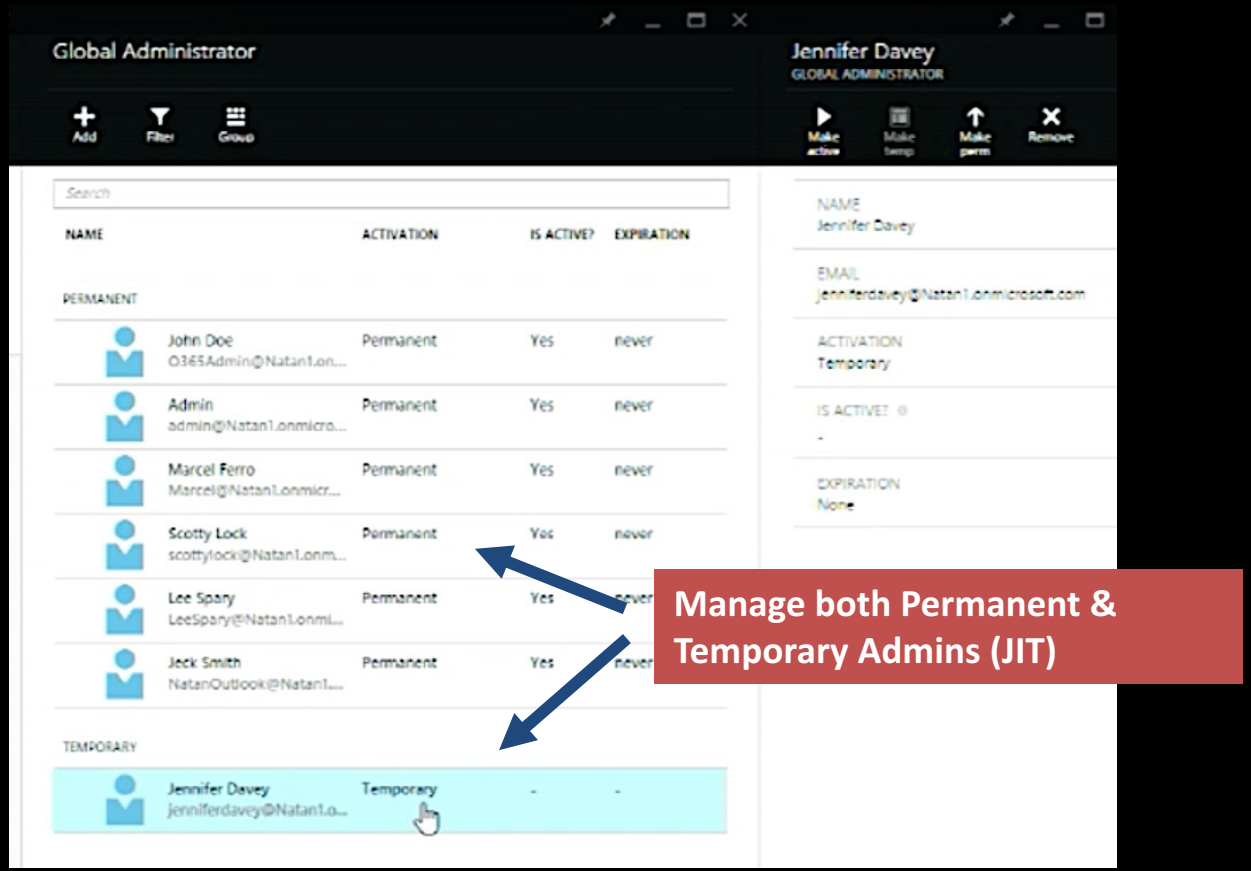
Azure AD Privileged Identity Management





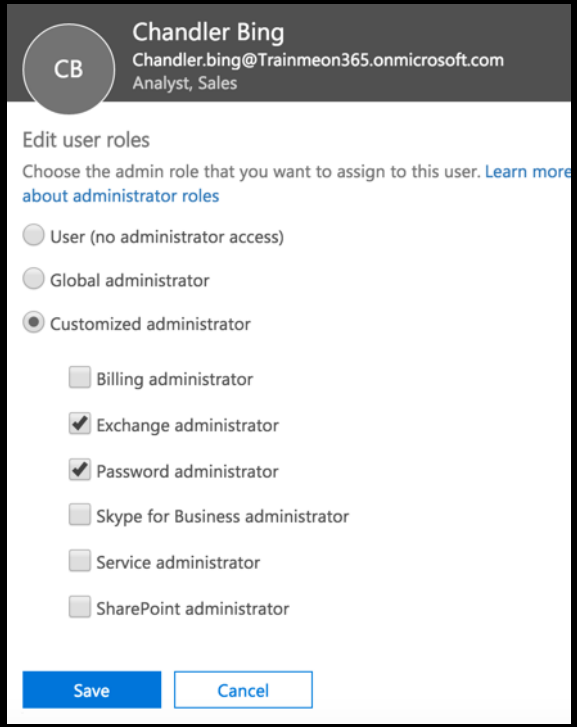
Demo: Azure Privileged Identity Management

Azure AD Privileged Identity Management



Top Tip: JIT & JEA AD Privileged Admins

- Global Admins can update which users are permanently assigned to roles in Azure AD.
- PowerShell cmdlets like Add-MsolRoleMember and Remove-MsolRoleMember
- The Azure classic portal as described in assigning administrator roles in Azure Active Directory
- Cannot be done in the Office 365 Portal yet!
- Global Admins can make temporary role assignments by making users **eligible** for a role
- An eligible admin can activate the role when they need it, and then their permissions expire once they're done.



Top Tip: Here's Lookin' at you Kid!

Start recording user and admin activities

When you turn this on, user and admin activity in your organization will be recorded to the Office 365 audit log and available to view in a report.

Turn on | Cancel

☆ Recommended for you ...

Search for activity

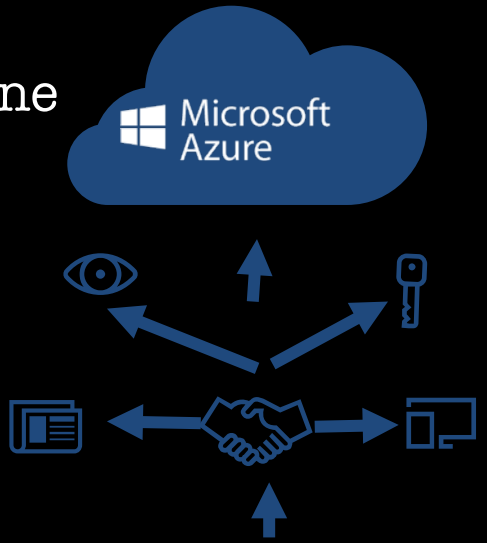
Want to know what your users and admins are doing? Start recording activities in Office 365.

Start recording now

Lesson 5 Azure Multi-Factor Authentication

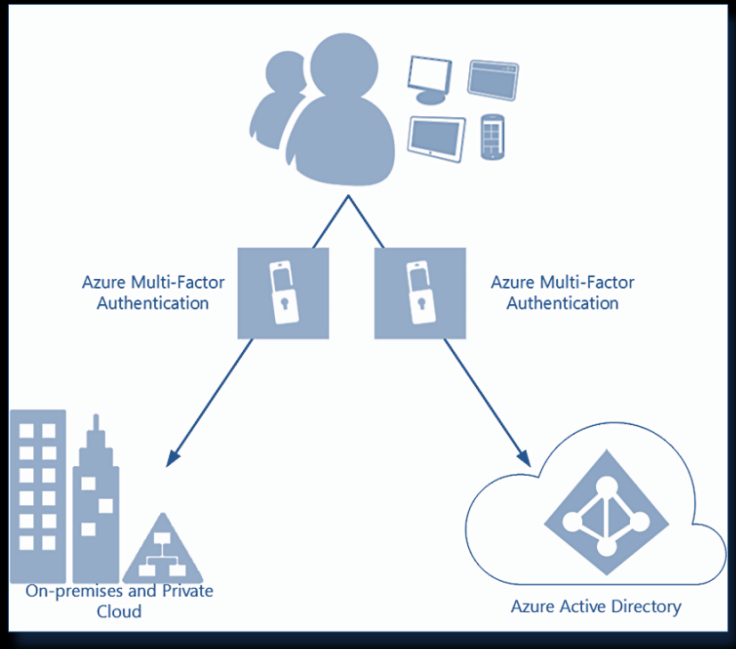
Azure Multi Factor Authentication!

- Method of authentication requiring more than one verification method
- Combines device as something you have or Somewhere you are
- Password Something you know
- Fully supports Biometrics (Something you are)
- Adds a critical second layer of security to user sign-ins and transactions
- Available for Azure, Office 365 & Hybrid Deployments

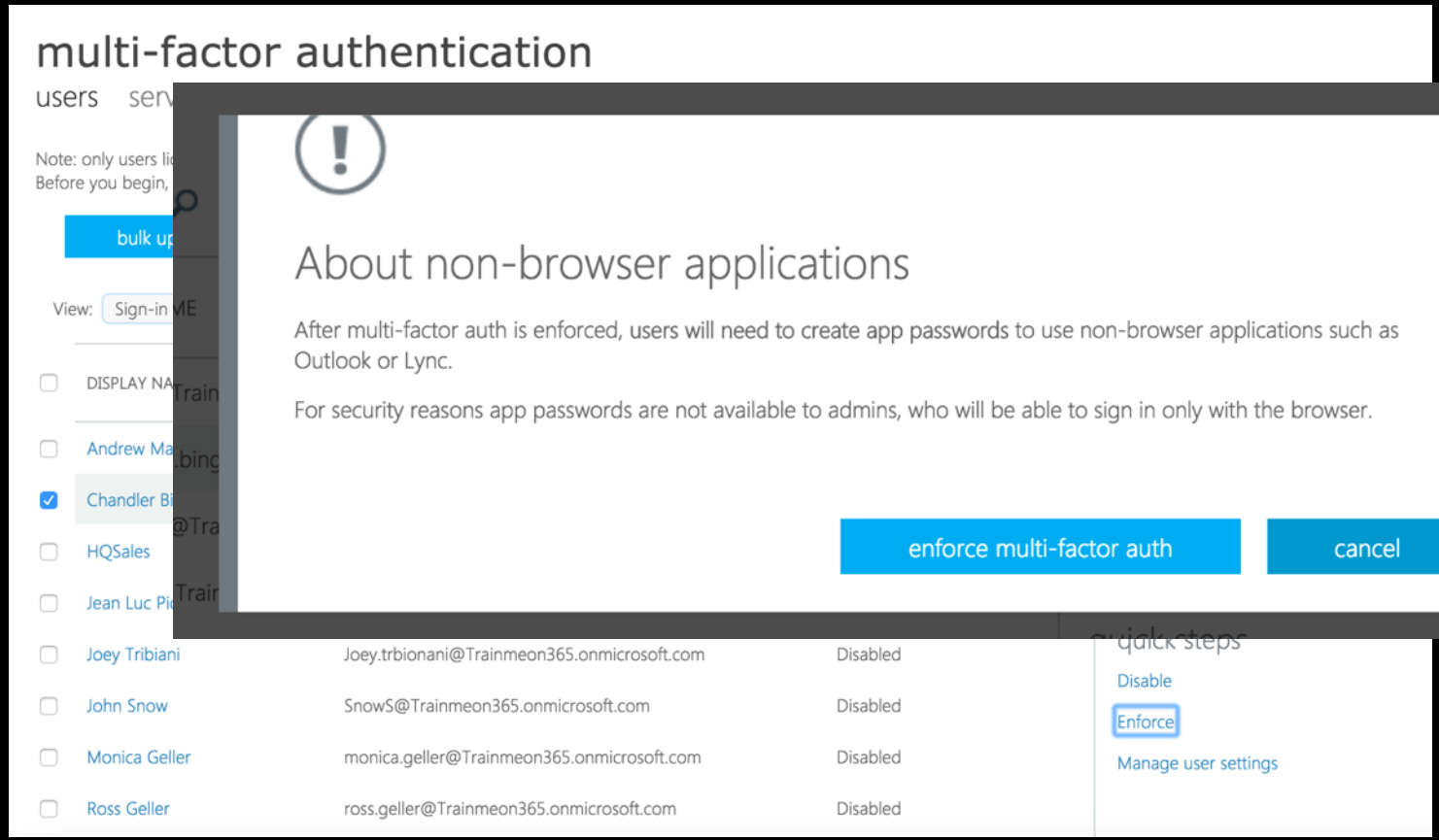


Azure Multi Factor Authentication!

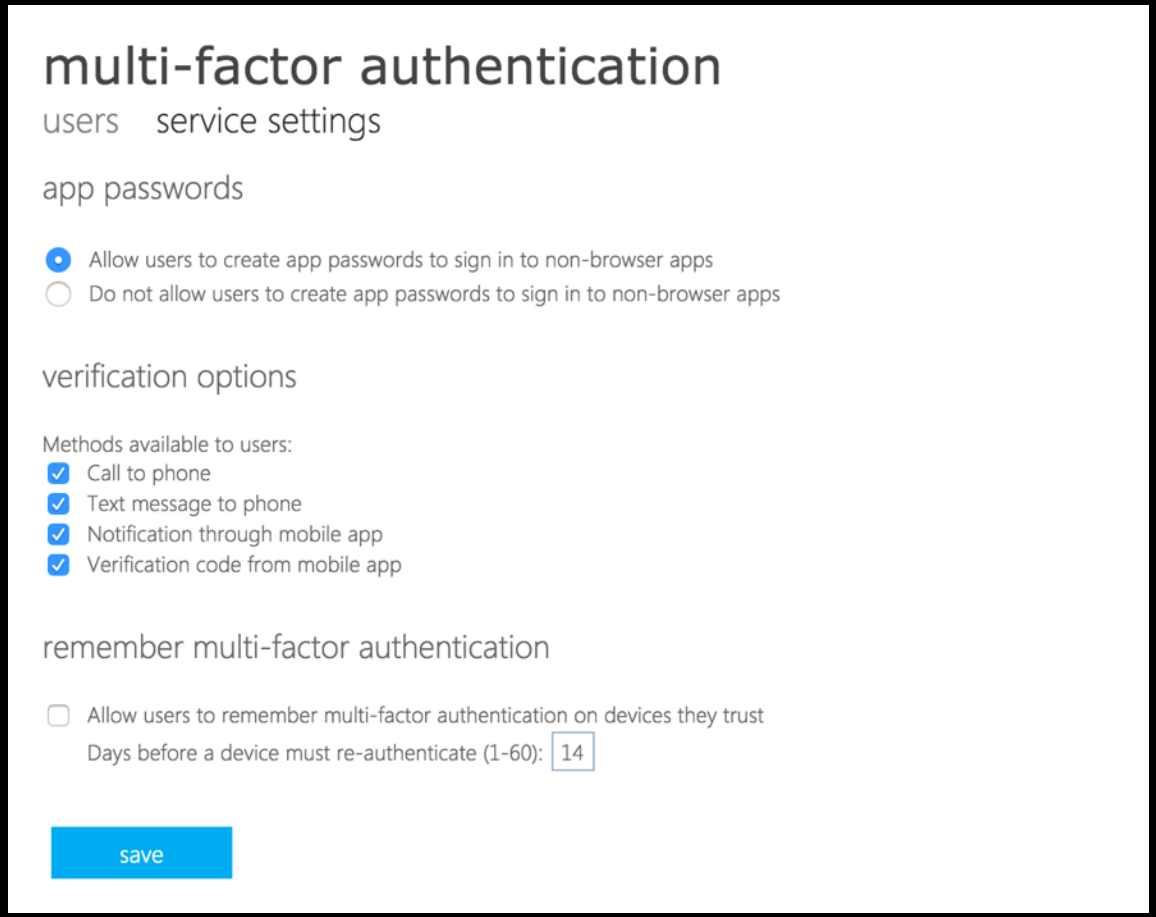
- Authentication Methods:
- Phone call
- Text message
- Mobile app notification
- Users can choose the method they prefer
- Mobile app verification code
- 3rd party OAUTH tokens



Azure Multi Factor Authentication!



Azure Multi Factor Authentication!



Multi Factor Auth PowerShell Step by Step

1: install the Microsoft Online Services Sign-In Assistant

Next Install the Azure Active Directory Module for Windows PowerShell

Get-ExecutionPolicy (If the output is anything other than "unrestricted", run the following command)

Set-ExecutionPolicy Unrestricted –Scope CurrentUser

Multi Factor Auth PowerShell Step by Step

2: Connect to MsolService via PowerShell

```
$UserCredential = Get-Credential
Import-Module MSOnline
Connect-MsolService –Credential $UserCredential
$auth = New-Object -TypeName
Microsoft.Online.Administration.StrongAuthenticatio
nRequirement
$auth.RelyingParty = "*”
```

3: Choose the MFA State $auth.State = "Enabled”

Multi Factor Auth PowerShell Step by Step

4: Choose the date – Any devices issued for a user before this date would require MFA setup

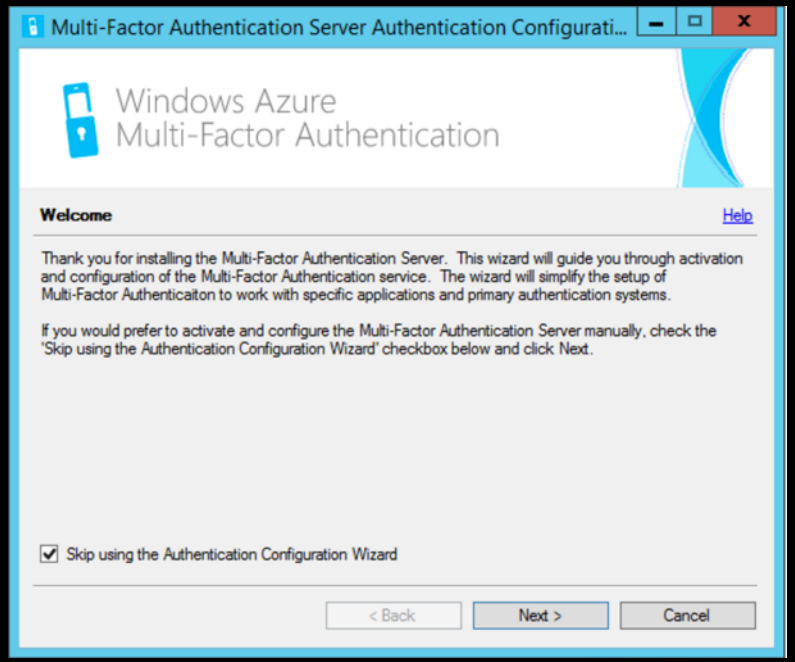
$auth.RememberDevicesNotIssuedBefore = (Get-Date)

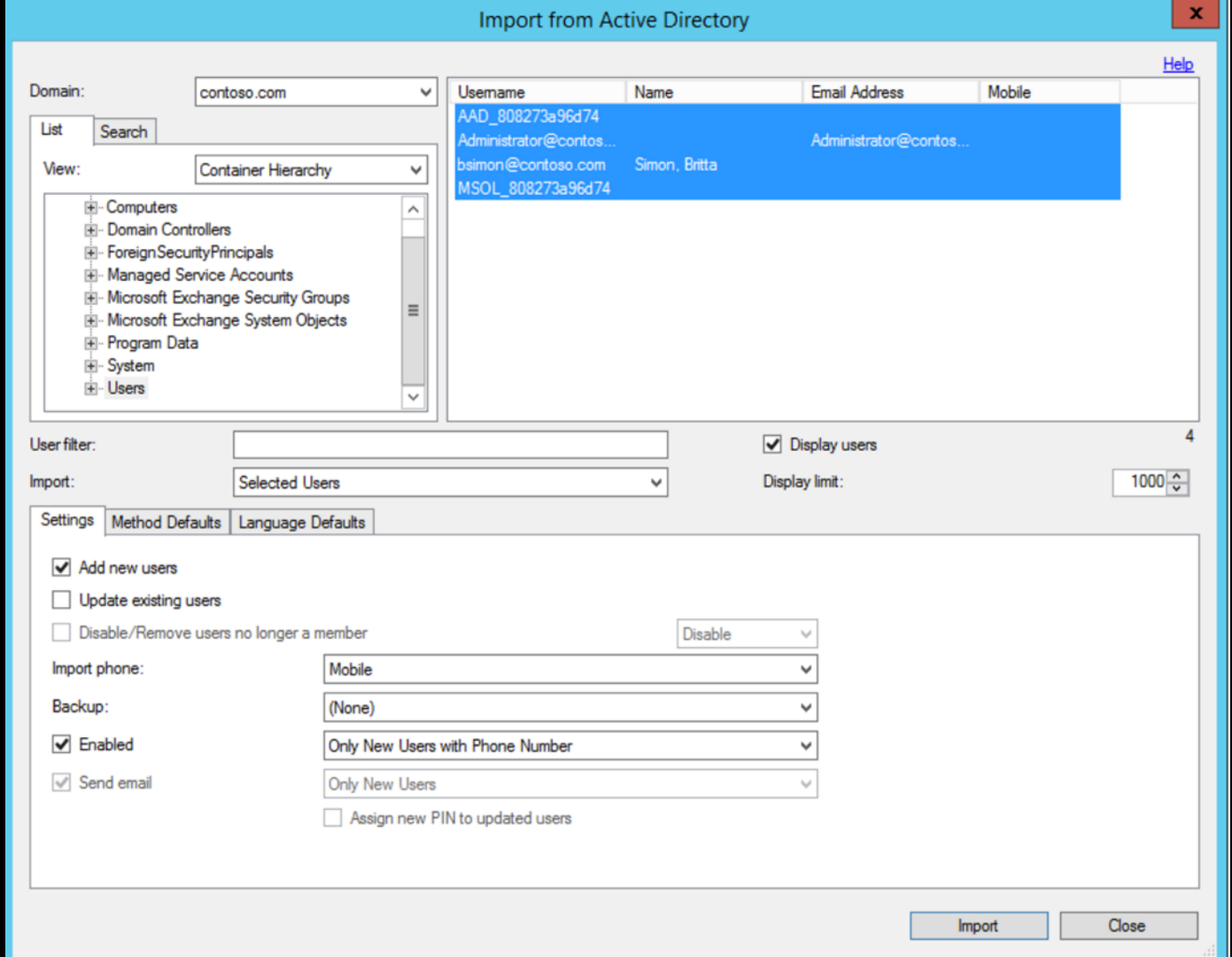
5: Enable MFA for all users: Get-MsolUser –All | Foreach{ Set-MsolUser -UserPrincipalName $_.UserPrincipalName -StrongAuthenticationRequirements $auth}

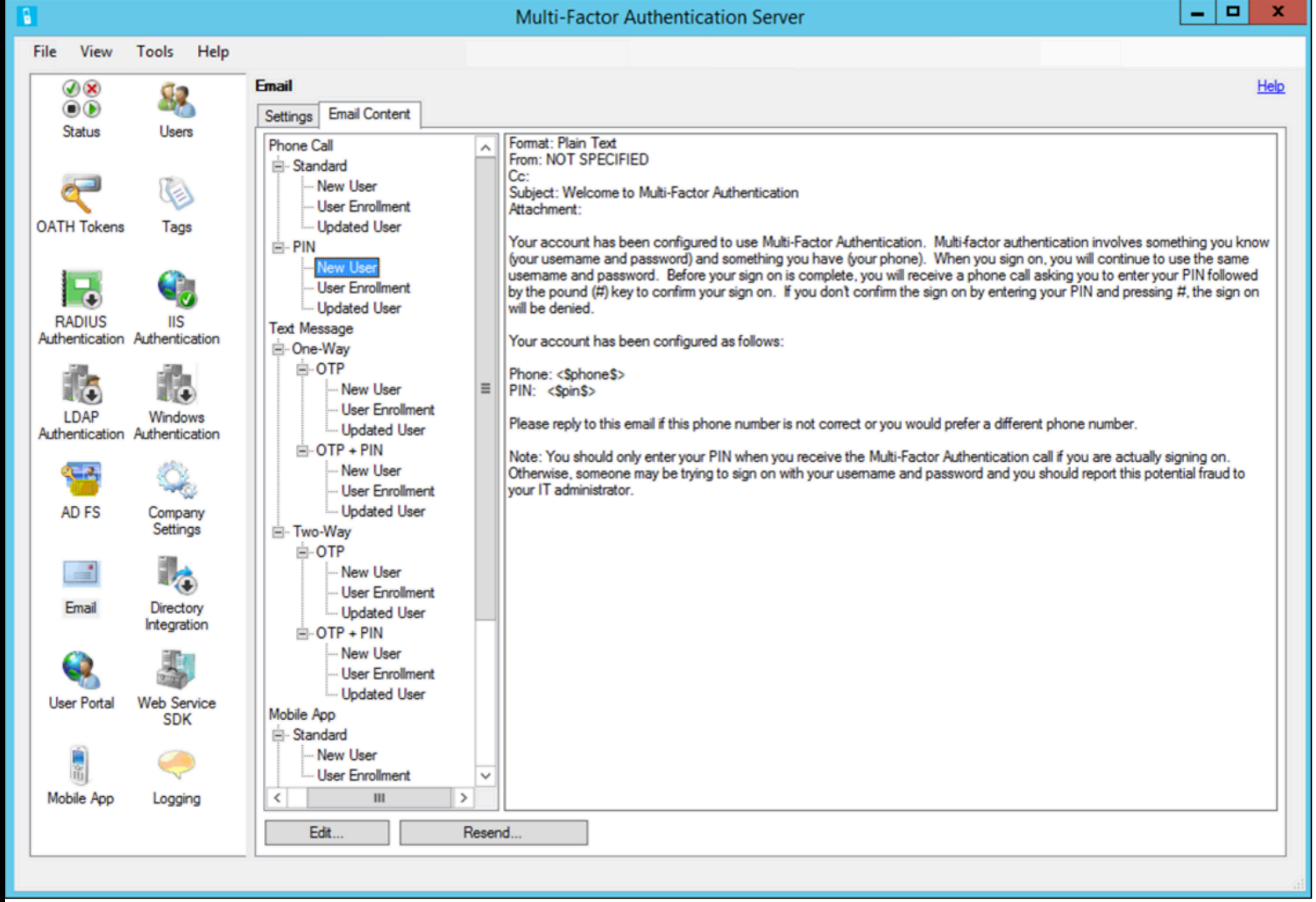
If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

Top Tip: Combine Multi Factor Auth with SSO

- On the Local ADFS Federation Server install WindowsAzureSDK-x64.exe
- On the Local ADFS Federation Server run the PowerShell Cmdlet run Register-ADFSAuthenticationProvider
- Run the Microsoft Azure Multi Factor Authentication Wizard – Server Authentication Wizard
- You're all set!

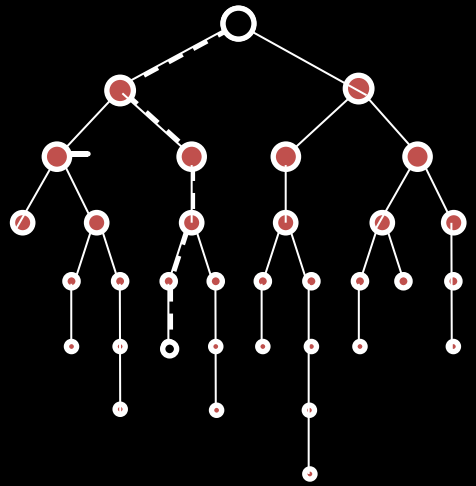



Import from Active Directory
Help
Domain:
contoso.com
List
Search
View:
Container Hierarchy
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Microsoft Exchange Security Groups
Microsoft Exchange System Objects
Program Data
System
Users
Username
Name
Email Address
Mobile
AAD_808273a96d74
Administrator@contos...
Administrator@contos...
bsimon@contoso.com
Simon, Britta
MSOL_808273a96d74
User filter:
Display users
4
Import:
Selected Users
Display limit:
1000
Settings
Method Defaults
Language Defaults
Add new users
Update existing users
Disable/Remove users no longer a member
Disable
Import phone:
Mobile
Backup:
(None)
Enabled
Only New Users with Phone Number
Send email
Only New Users
Assign new PIN to updated users
Import
Close


Multi-Factor Authentication Server
File
View
Tools
Help
Status
Users
OATH Tokens
Tags
RADIUS Authentication
IIS Authentication
LDAP Authentication
Windows Authentication
AD FS
Company Settings
Email
Directory Integration
User Portal
Web Service SDK
Mobile App
Logging
Email
Help
Settings
Email Content
Phone Call
Standard
New User
User Enrollment
Updated User
PIN
New User
User Enrollment
Updated User
Text Message
One-Way
OTP
New User
User Enrollment
Updated User
OTP + PIN
New User
User Enrollment
Updated User
Two-Way
OTP
New User
User Enrollment
Updated User
OTP + PIN
New User
User Enrollment
Updated User
Mobile App
Standard
New User
User Enrollment
Format: Plain Text
From: NOT SPECIFIED
Cc:
Subject: Welcome to Multi-Factor Authentication
Attachment:
Your account has been configured to use Multi-Factor Authentication. Multi-factor authentication involves something you know (your username and password) and something you have (your phone). When you sign on, you will continue to use the same username and password. Before your sign on is complete, you will receive a phone call asking you to enter your PIN followed by the pound (#) key to confirm your sign on. If you don't confirm the sign on by entering your PIN and pressing #, the sign on will be denied.
Your account has been configured as follows:
Phone: <$phone$>
PIN: <pin>
Please reply to this email if this phone number is not correct or you would prefer a different phone number.
Note: You should only enter your PIN when you receive the Multi-Factor Authentication call if you are actually signing on. Otherwise, someone may be trying to sign on with your username and password and you should report this potential fraud to your IT administrator.
Edit...
Resend...

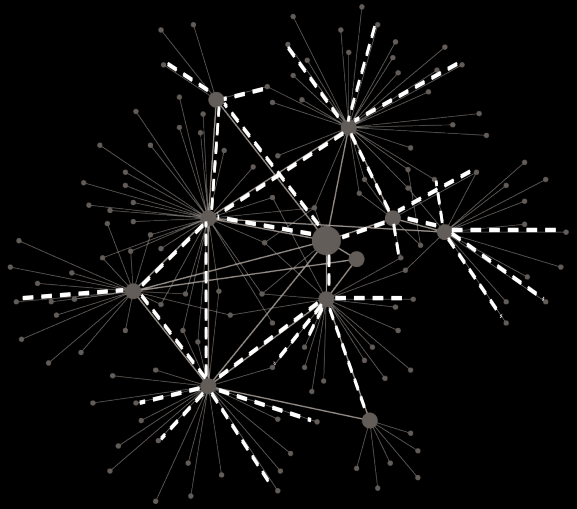
Lesson 6 Protecting your Info Azure Style!

The Changing Structure of Data!



TRADITIONAL HIERARCHIES

INFORMATION MOVES SLOWLY
COMMAND AND CONTROL

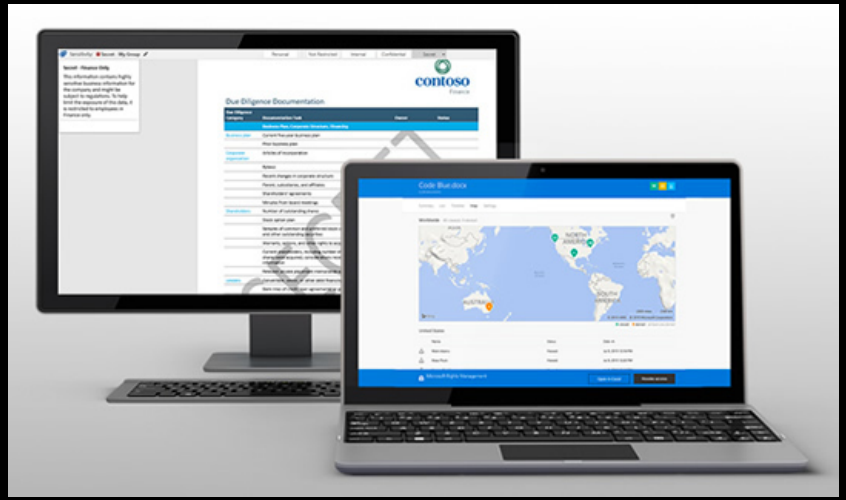


RESPONSIVE NETWORKS

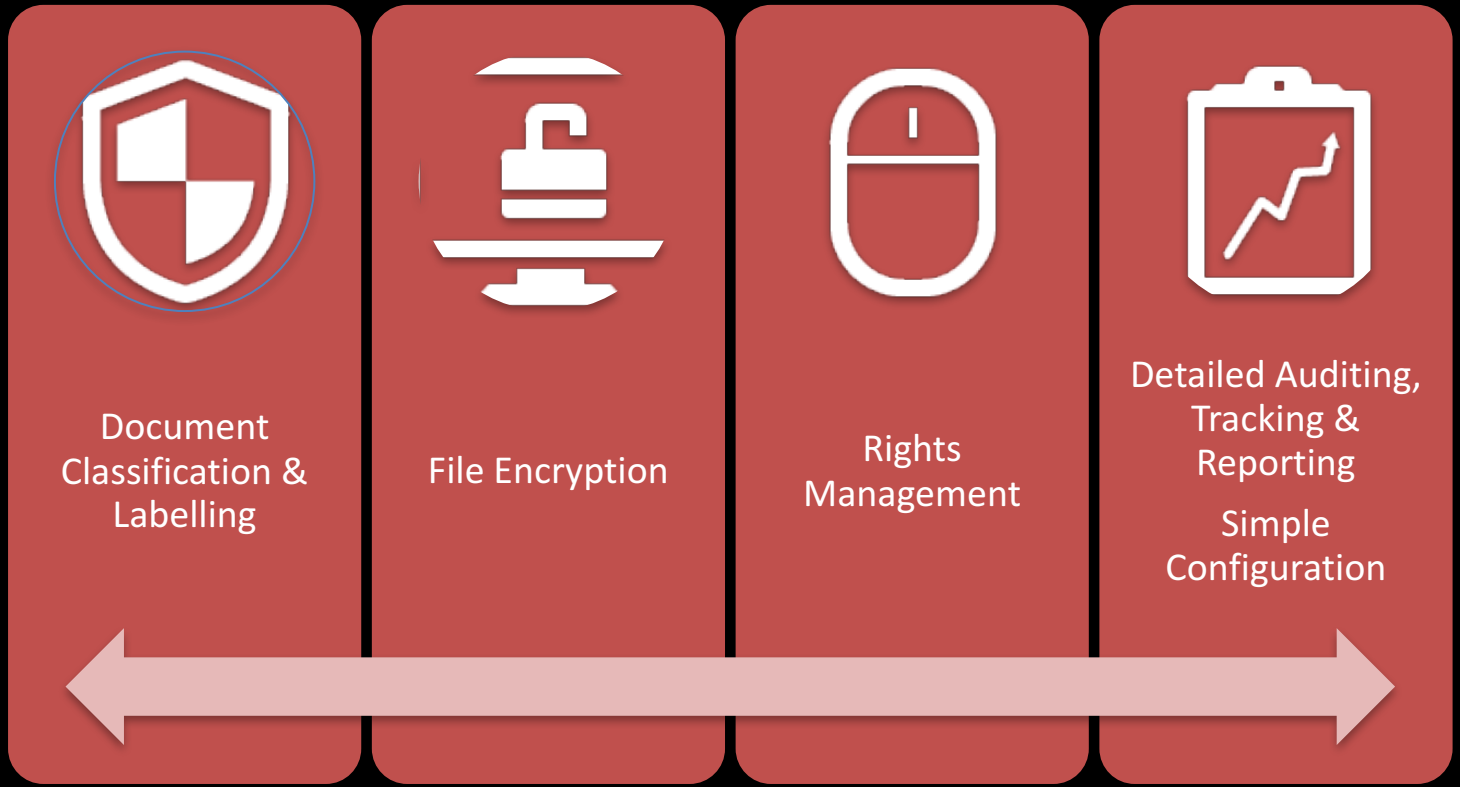
INFORMATION TRAVELS FAST
LEARN AND ADAPT

Azure Information Protection: Wild West Hero

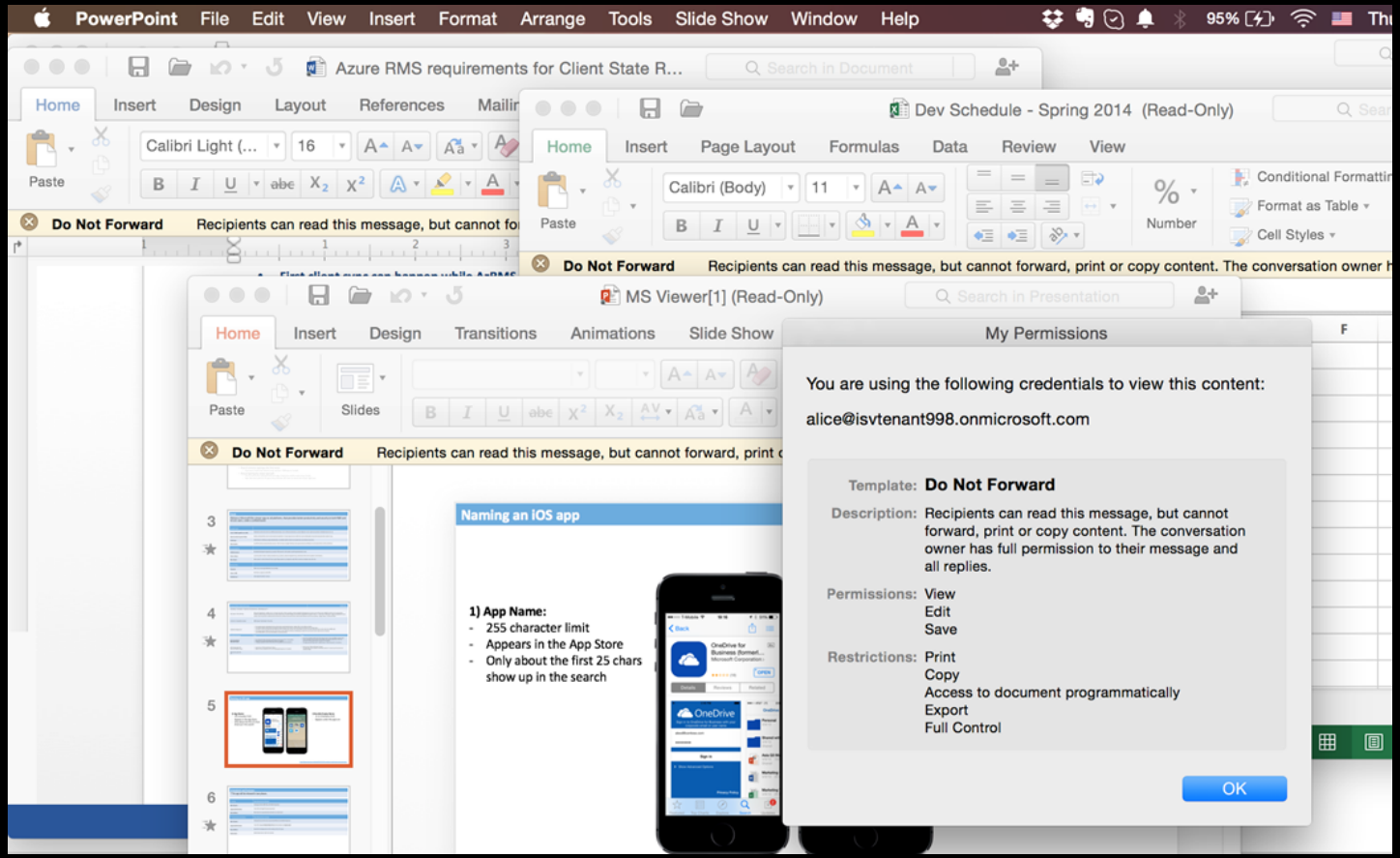
- Permissions Bleed
- Once data is outside organization, its beyond the realm of your control
- Anyone can plagiarise
- Content easily copied
- Potential Copyright Infringement Issues
- Plausible Deniability Reins
- Lack of Compliance



Azure Information Protection

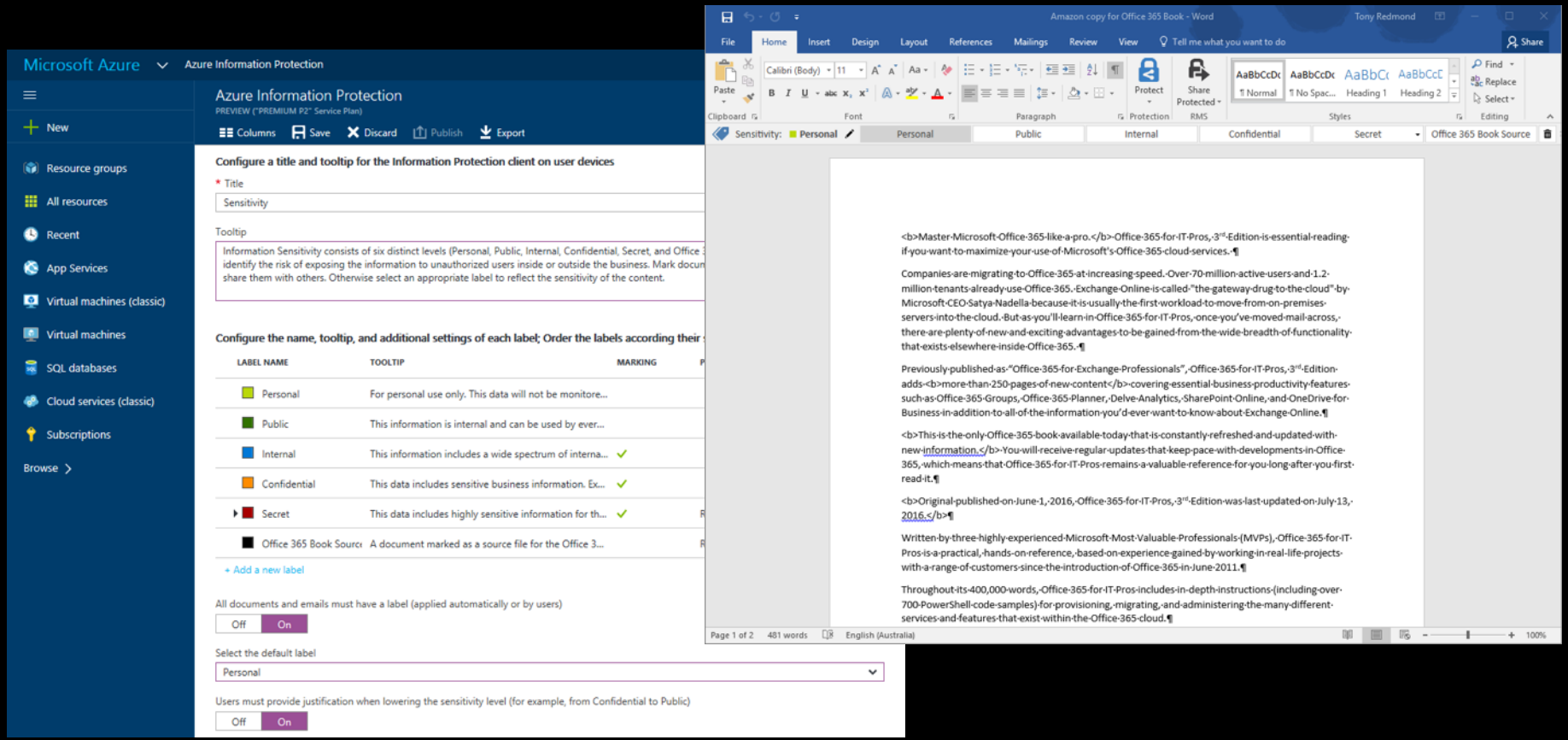


Azure AD Rights Management Services



Demo: Azure Information Protection

Azure Information Protection Office 2016 Add in



Lesson 7 Conditional Access

Conditional access

Conditions

User attributes

User identity

Group memberships

Devices

Is Domain Joined

Is Compliant

Platform type

Lost or Stolen

Application

Per application policy

Mobile apps or Cloud apps

Other

Location (IP Range)

Risk Profile

Requirements

Allow

Block

MFA

Enroll

Demo: Azure Conditional Access

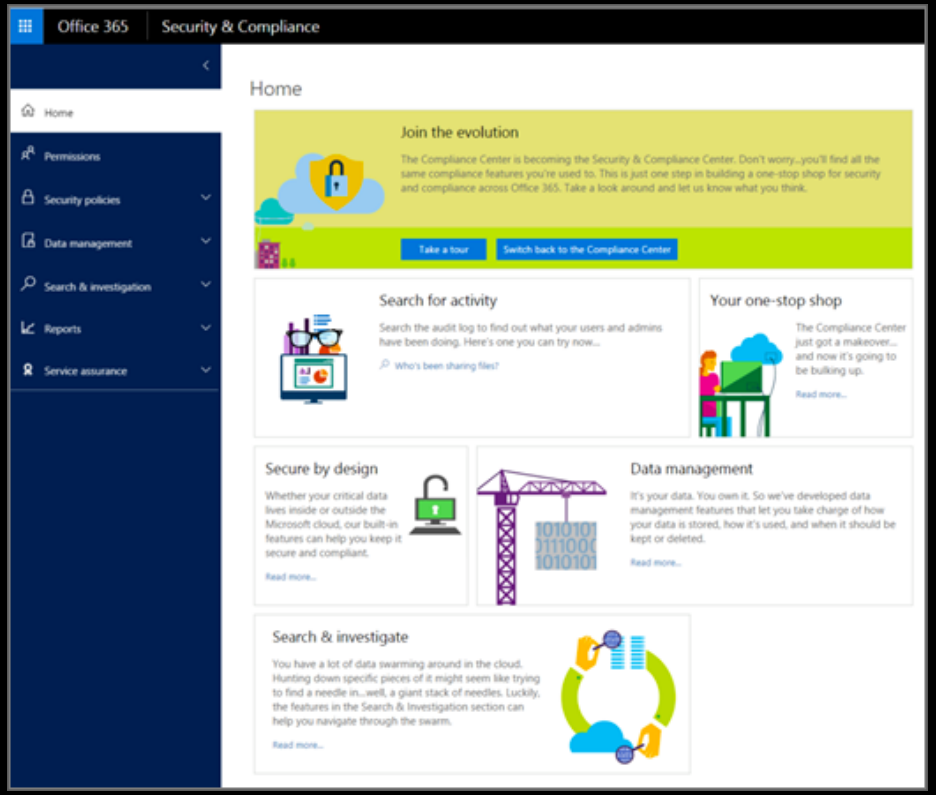
Lesson 8 Lessons in Compliance!

Microsoft Data Centres Policies & Procedures Ensure Compliance

- Highly Secured Physical Environments
- Multiple Redundancy Model
- Small number of Staff
- Separation of Duties & Roles
- Strict Security Policies & Procedures (Failure=Dismissal)
- Managed Data Destruction Policies
- PII & Non PII Stored Separately
- Free & Paid services Stored Separately
- Customer Breach Notification Policy
- Law enforcement Breach Notification Policy

Example: Office 365 Compliance Centre

- Single portal Solution
- Set up Alerts
- View Audit Logs
- Set Security Policies
- Import / Export / Archive Data
- Search & Investigate
- eDiscovery
- Service Assurance



Demo: Office 365 Compliance Centre

Lesson 8 Elementary my Dear Watson ...

Digital Forensics

"Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data."

But the World has Changed

- Need to update Security Policies & Procedures
- Develop & Maintain an Incident Response Plan
- Understand how will this effect your Disaster Recovery
- Need to Develop a Hybrid Backup Solution
- Ensure that any move to the cloud ticks all your organizations, countries & industries legal & compliance boxes

Surely Forensics Just became 50% Harder?

- Perceived Loss of data control
- No access to physical infrastructure
- Legal issues of multi-jurisdiction
- Multi-tenancy and multi-ownership
- Lack of tools for larger-scale distributed and virtualized systems
- No standard interfaces
- Little provider cooperation
- Difficulties in producing forensically sound and admissible evidence in court

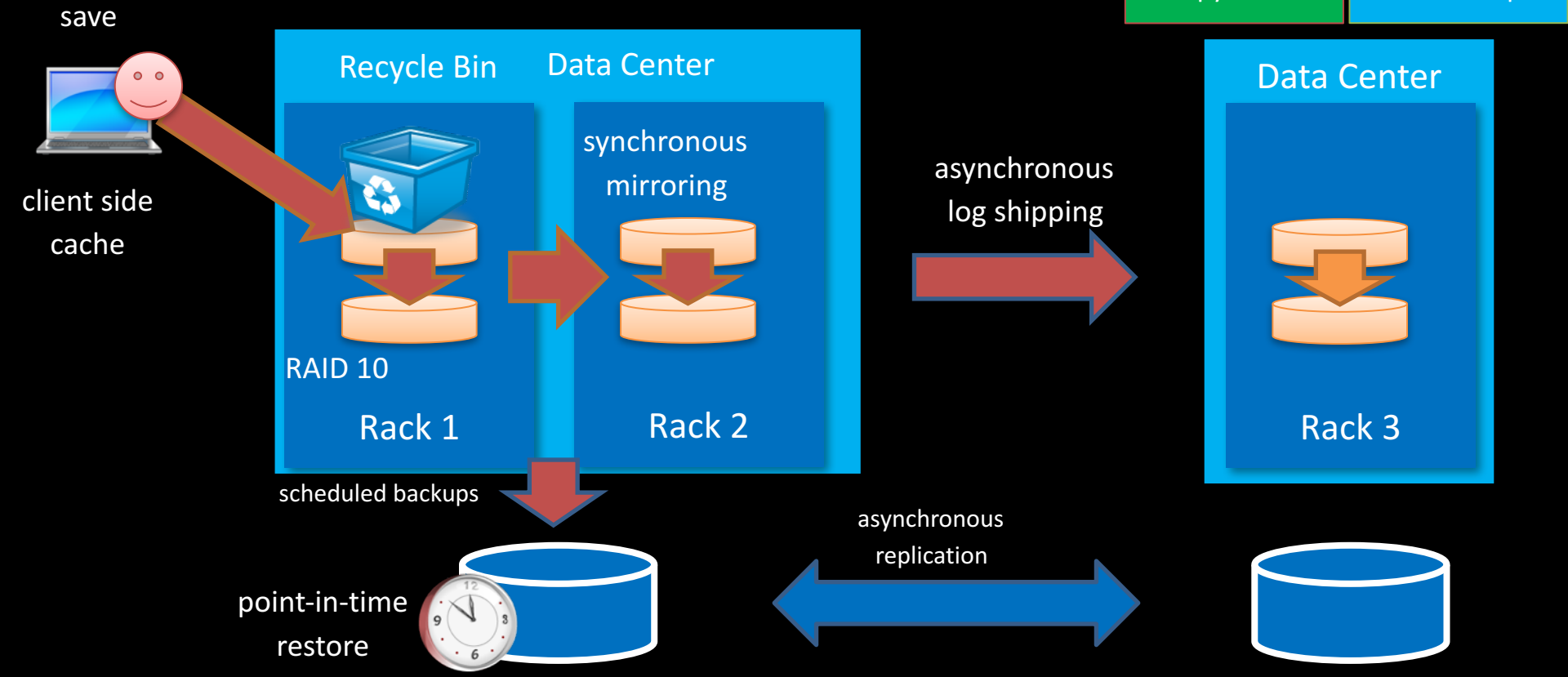
Actually it's now 50% Easier

- Improvement in Forensic Tools
- Users often Require Verified Accounts
- Improved Logs & Auditing Procedures
- Better eDiscovery & In Place Hold
- Shrink Wrapped Crime Scene (VMs)
- (CSA) Cloud Security Alliance – Strive to be Compliant
- Growth in Cross Platform Identity Standards – SAML 2.0 – Oauth 2.0
  - Microsoft Account – Google – Amazon – Facebook - LinkedIn
- Easier to Migrate in and Out of Cloud
- Improvement in International Legal Co-operation

It's not just where but How Data is Stored?

10+
Copy Count

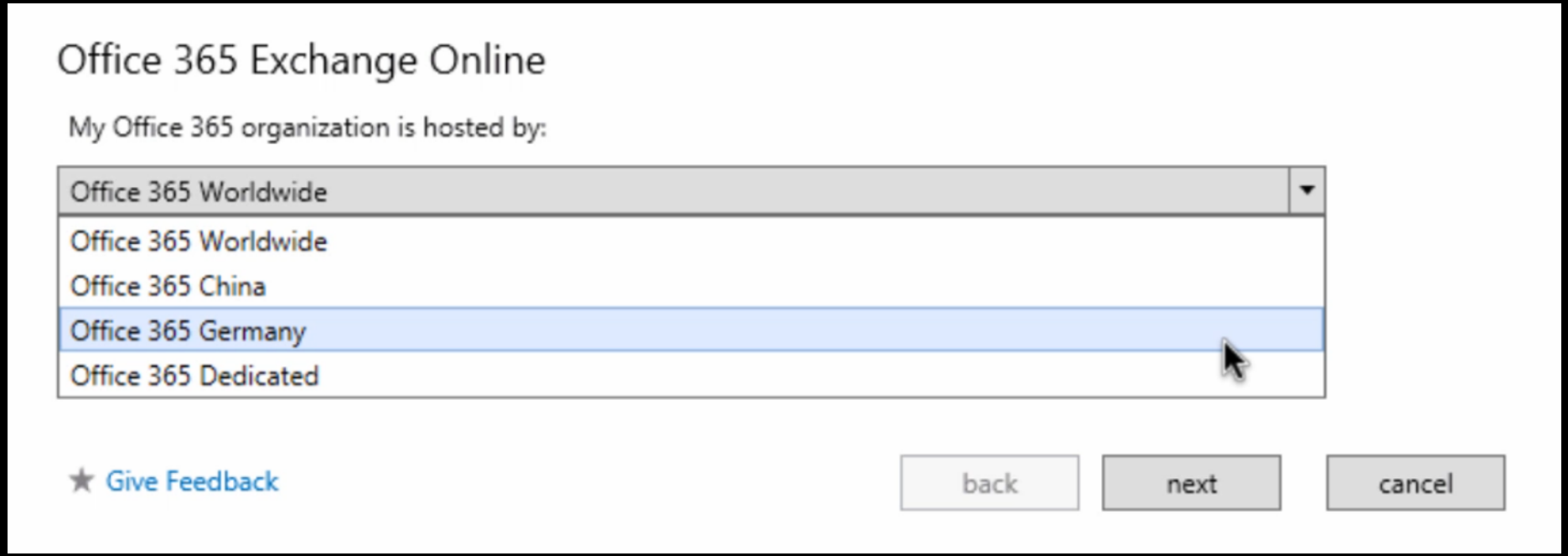
rack
Failure Scope



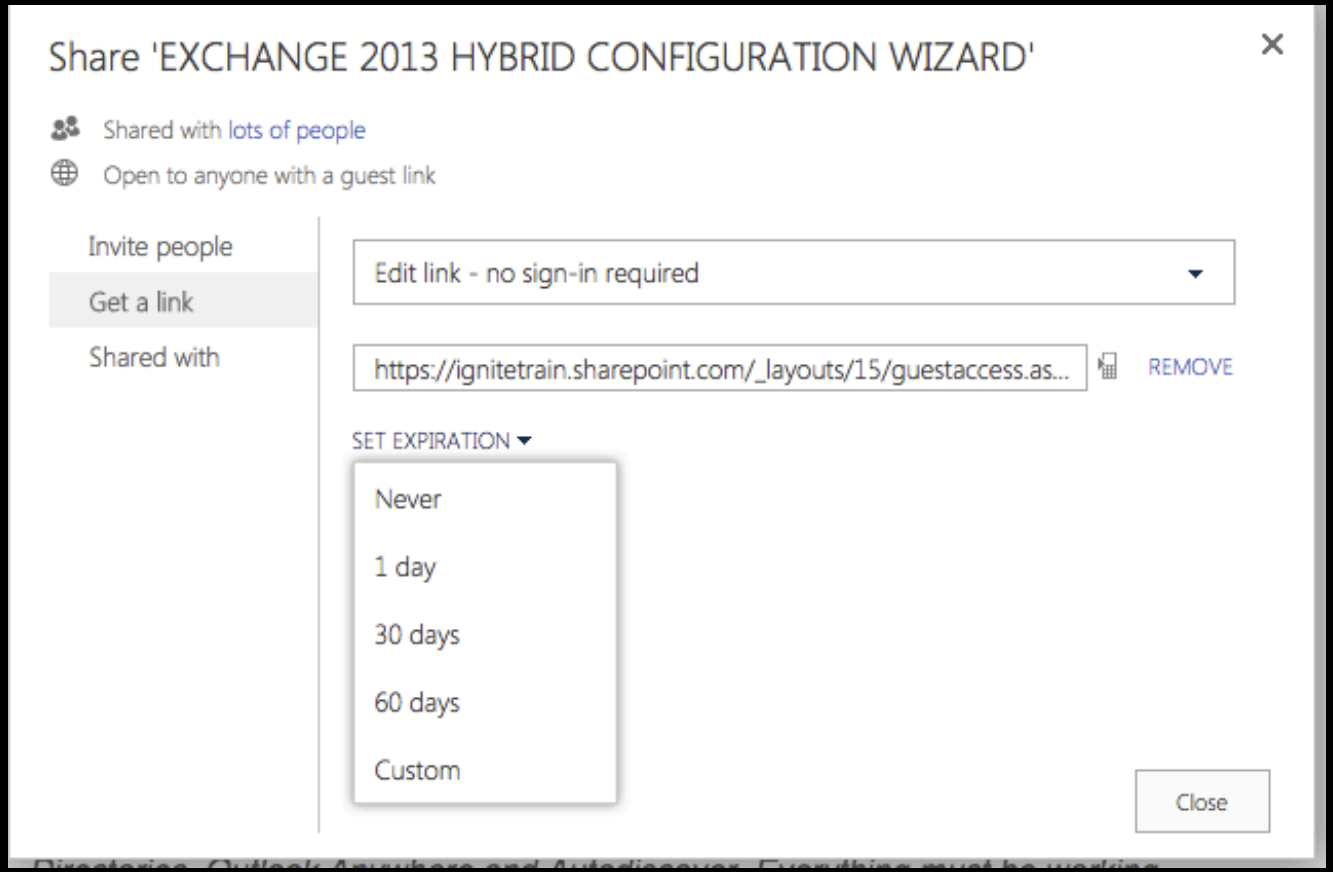
Demo: How Forensics is Adapting in the Cloud

Lesson 9 Nuggets of Gold ...

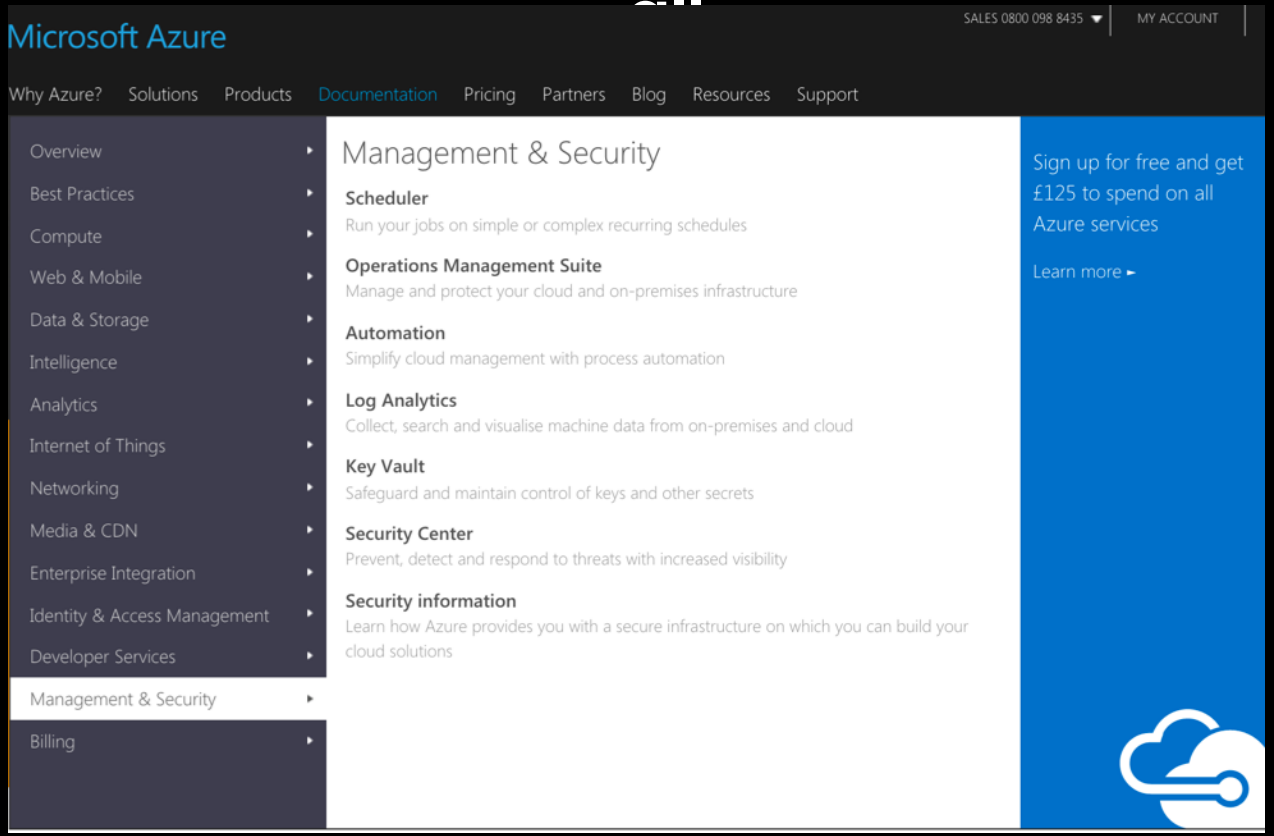
Where do you want (your data) to go today?



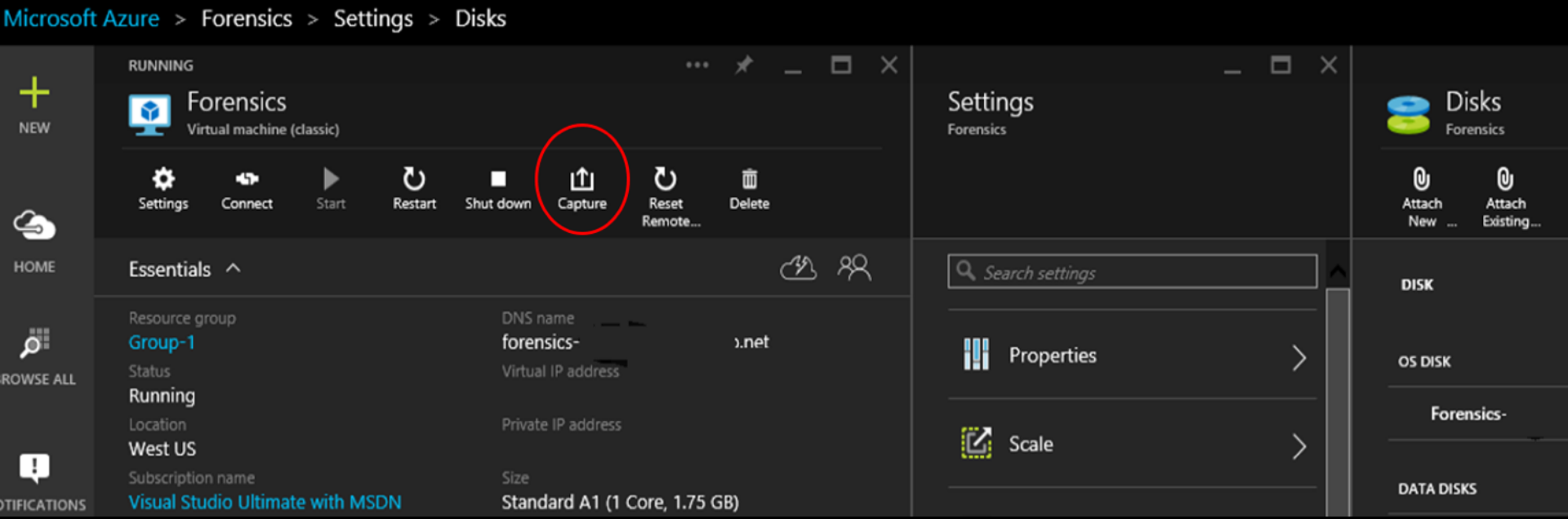
Top Tip: JIT & JEA Come to OneDrive for Business



Azure Documentation: One Repository to Rule them all

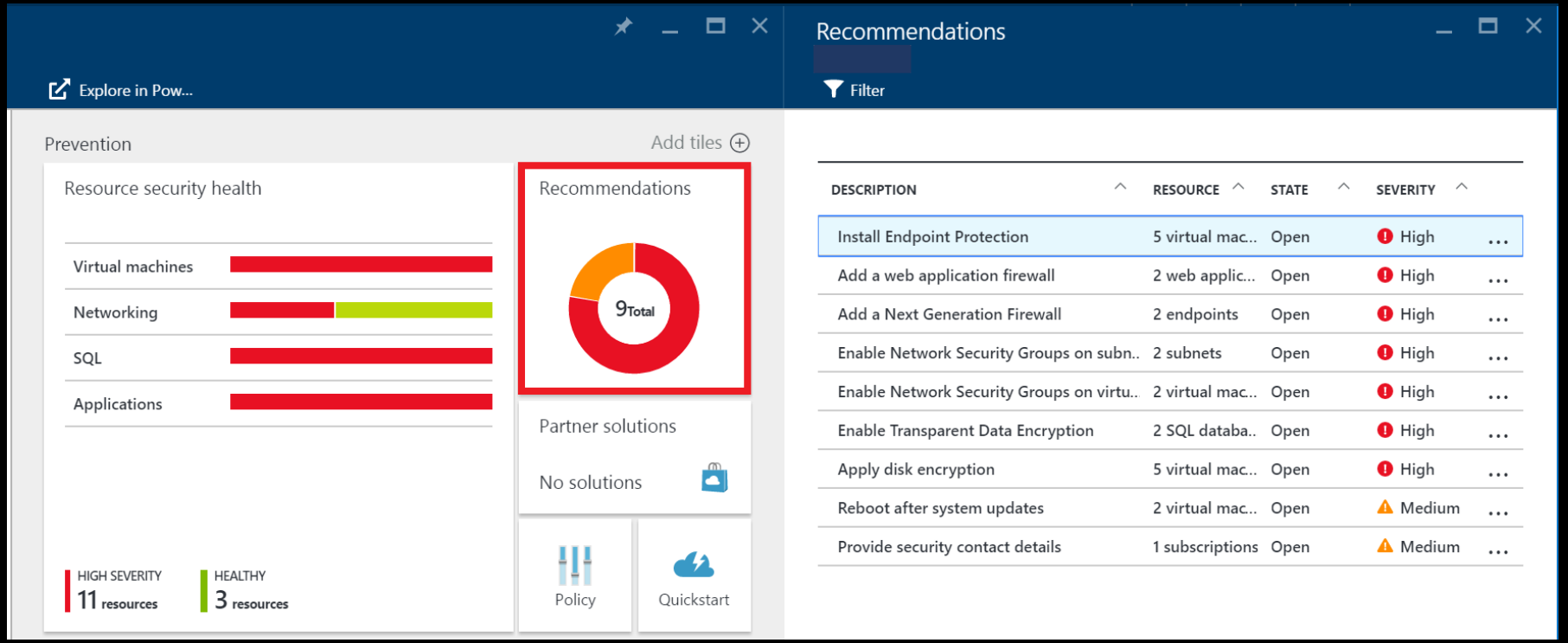


Incoming: Microsoft Azure Forensics as a Service (FaaS)



Lesson 10 All Hail the Azure Security Centre

Azure Security Centre



Review

Azure Information Protection

Azure Security Portal

BitLocker Disk Encryption

Azure Security Troubleshooter

Azure Security Documentation

Container Security

Multi Factor Authentication

Azure Forensics

Azure Security Health Monitoring

Azure AD Connect Health

Azure AD Privileged Identity Management

Hybrid Management

Microsoft Anti Malware For Cloud Services & Virtual Machines

Azure Key Vault

Azure AD Identity Protection

Azure Business Continuity

Follow me on Twitter
@AndyMalone

nordic infrastructure conference 2017

The premium event for IT-professionals

Feb. 1-3rd in Oslo Spektrum