Richard Young
Mark Montgomery

Principal Consultants – Enterprise Cloud and Security

Securing JDE from browser to binary

Agenda

- Why JDE in the Microsoft ecosystem?
- Zero-Trust overview and demo
- Infrastructure design considerations for JDE
- Preventing Lateral Movement in the event of a breach
- Blue / Green rolling upgrades – maintaining 24/7 uptime

ORACLE

aws

Azure

Why JDE in the Microsoft ecosystem?

You can run JDE in any vendors public cloud, however:

- You most likely already have Azure Active Directory (Azure AD) as part of your Microsoft 365 subscription
- It provides a phenomenal backplane for Authentication, Authorisation and Accounting (AAA) including MFA, Conditional Access and threat detection
- Azure AD can issue a JSON Web Token (JWT) which newer releases of JDE can use for authentication
- Mix in Microsoft's ability to harden and protect endpoints including servers and user workstations

And you have a winning combination!

Azure

The 3 guiding principles of Zero Trust

Explicit Verification

Always authenticate

Authorise based on identity, location, device health, service, data classification

Least Privilege

Limit access with Just-In-Time access

Use risk-based adaptive policies and data protection

Assume Breach

Minimise blast radius

Prevent lateral movement by segmenting network access

Use analytics to get visibility, drive threat detection and improve your defence

Zero Trust Maturity Model

Traditional

On-premises identities
Limited visibility
Flat network infrastructure

Advanced

Hybrid identity with some policies for data/apps

Devices are registered and compliant

Segmented networks with cloud threat protection

Optimal

Cloud identity with real-time analytics for data/apps

Data access decisions

Automated threat detection and response

Applying Zero Trust to JDE with Microsoft

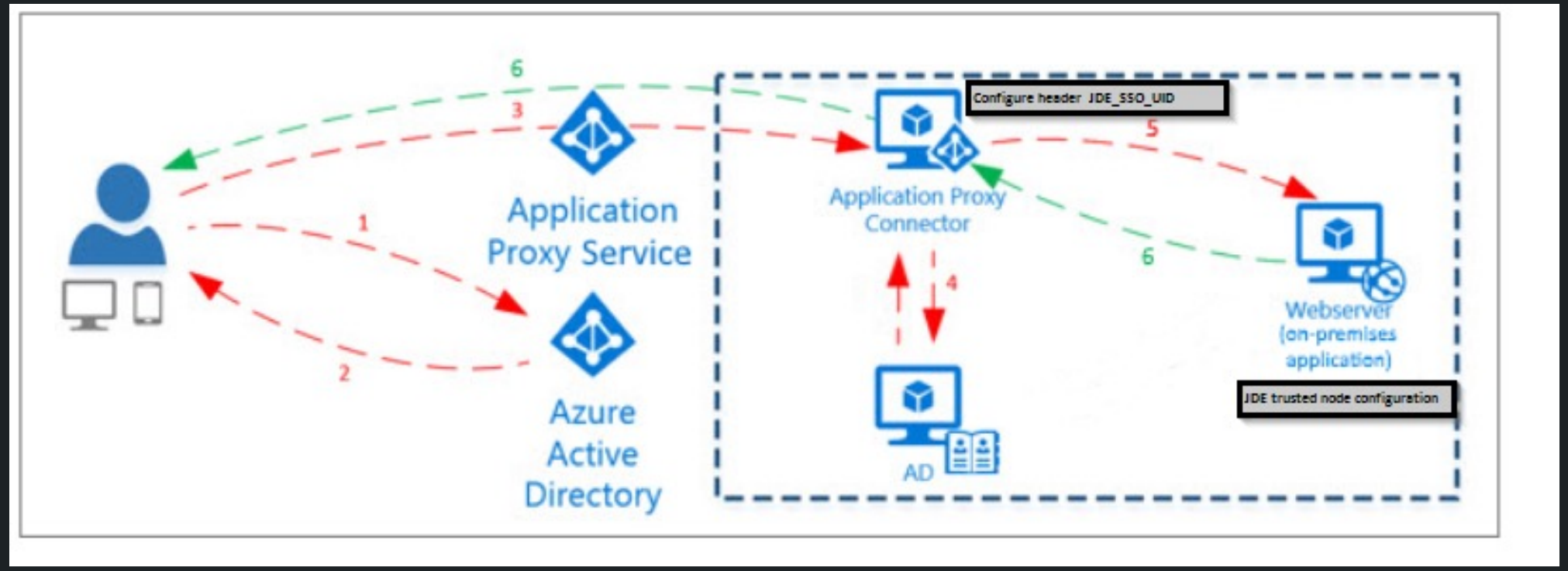
Explicit Verification – Identity and Devices:

- Enable/integrate JDE JAS login for SAML SSO with Azure AD as the iDP (Identity Provider)
- Register/join devices to Azure AD and Intune for MDM (Mobile Device Management), or use Hybrid Azure AD joined devices
- Use Azure AD Conditional Access Policies (adaptive MFA) to verify explicitly with strong authentication – using identity / device / location for signals

Assume Breach – Network segmentation:

- Integrate JDE with Azure AD Application Proxy to provide access from anywhere – no direct network access to JDE or VPN is required
- Azure AD logs provide visibility of access into the JDE application – can be extended to SIEM (Security Information and Event Management) for proactive MDR (Managed Detection & Response)

Azure AD Application Proxy with JDE



Zero Trust Demo

Securing access to JDE at Coopers Brewery with Microsoft Zero Trust

Windows 10 Client devices joined to Azure AD, managed by Intune

Passwordless Sign-in – Windows Hello for Business

Passwordless Sign-in – MS Authenticator Phone Sign-in

SSO to all SaaS applications integrated with Azure AD – inc. JDE

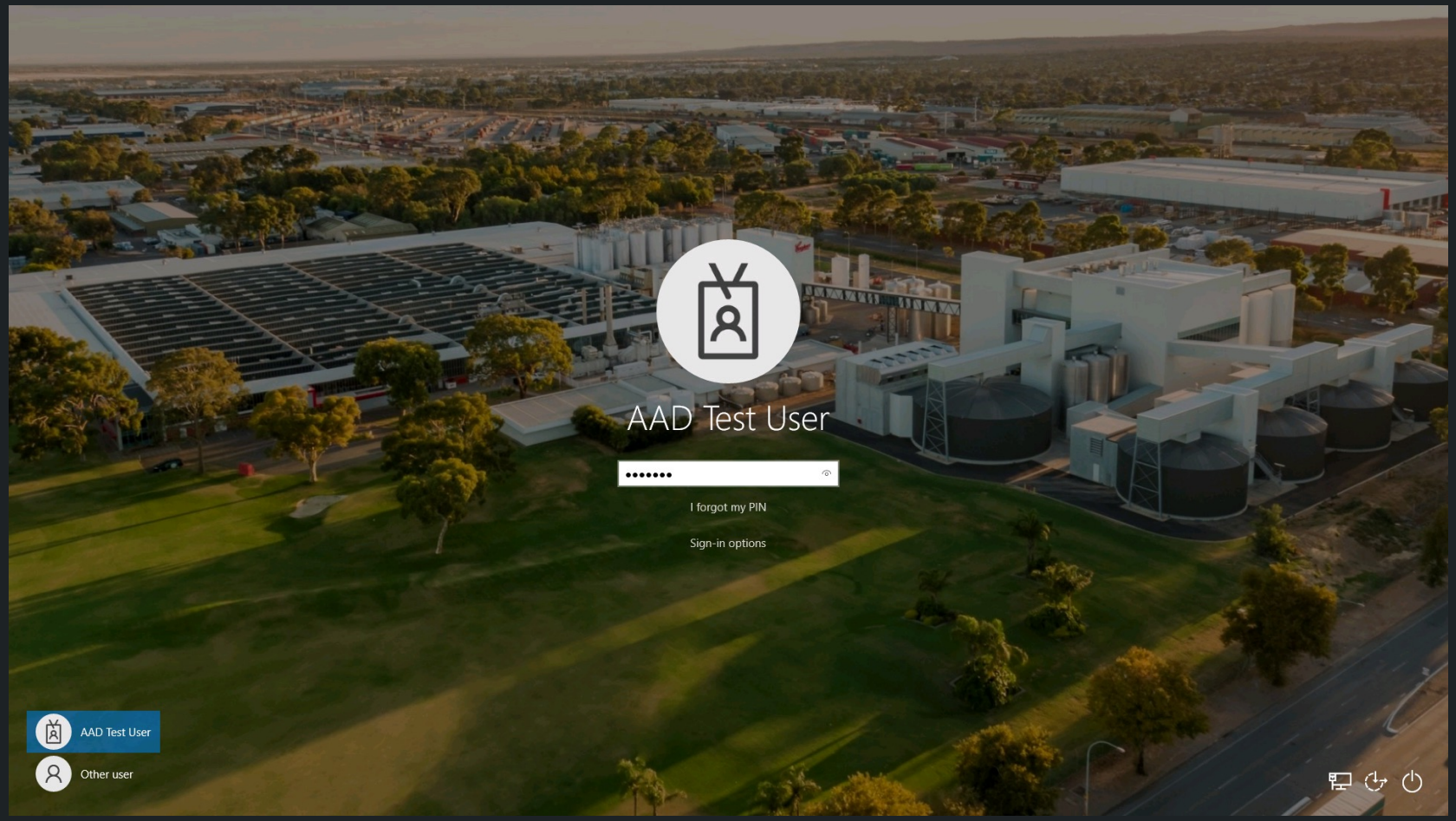
Azure AD Application Proxy – secure access from anywhere

Azure AD Conditional Access – require MFA / trusted device

Azure AD Conditional Access – Block JDE Prod from untrusted device

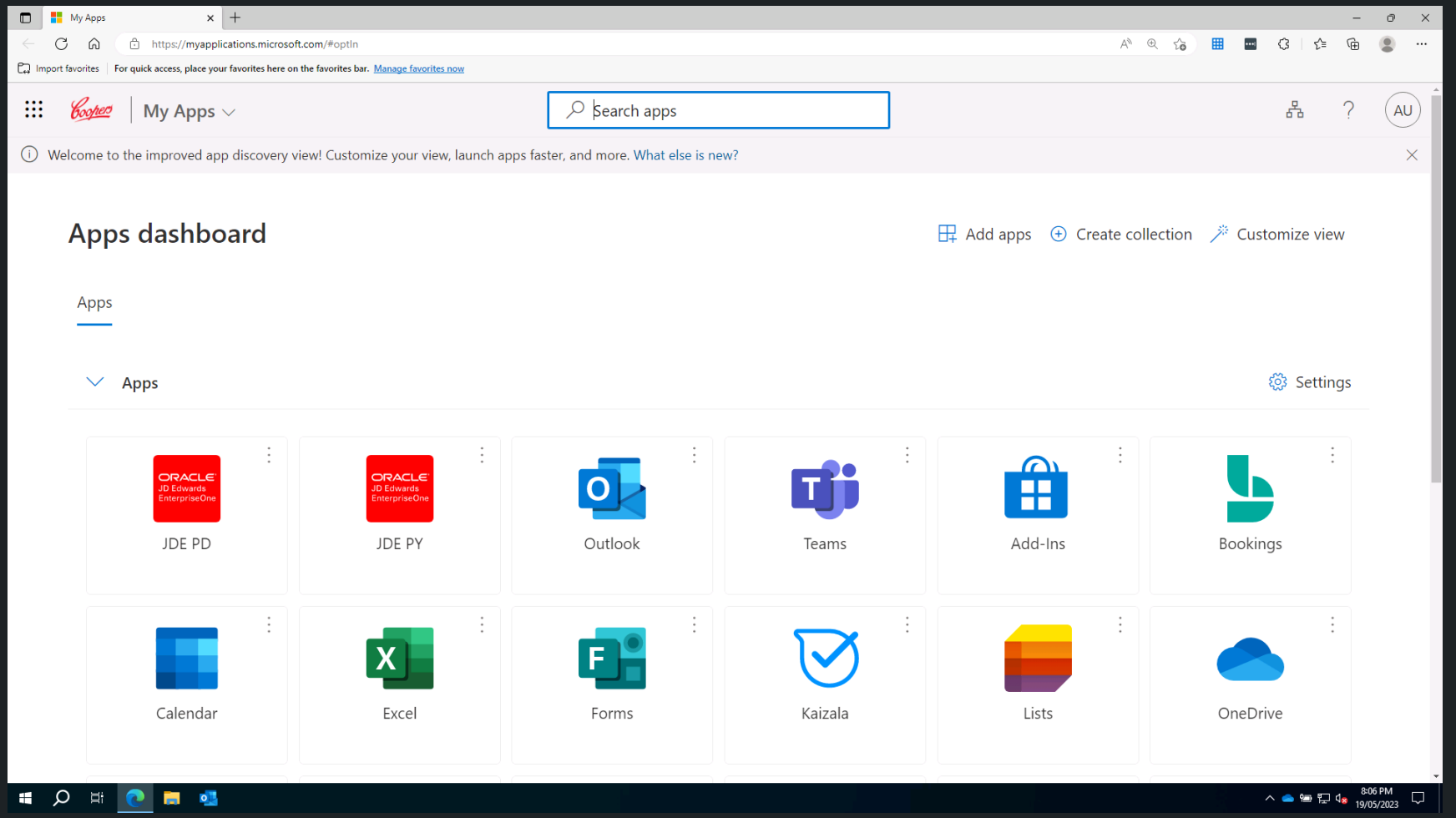
Windows Hello for Business

Passwordless Sign-in with PIN number



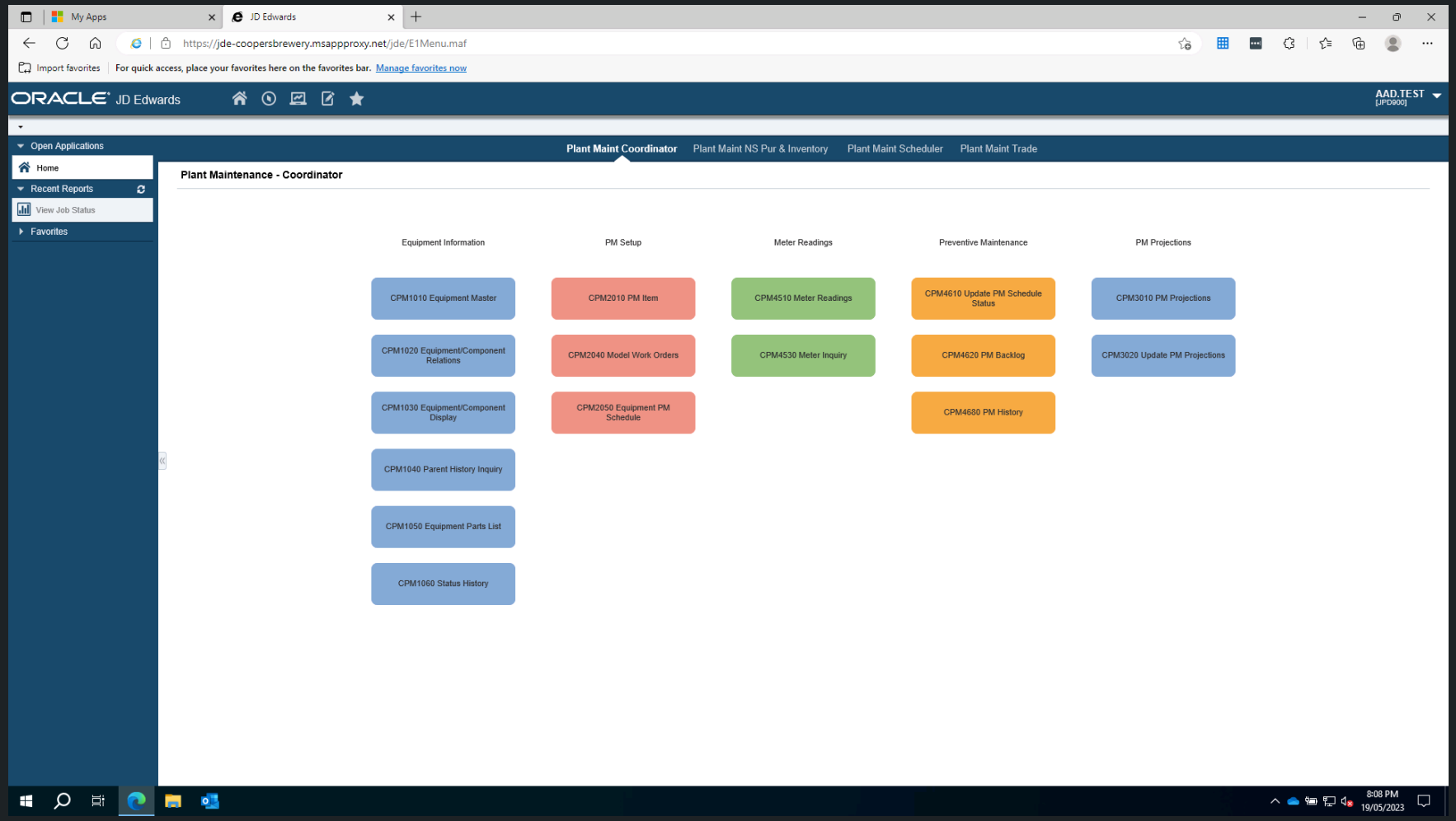
SSO to SaaS Applications

Microsoft MyApps Portal for access to SaaS applications – including JDE



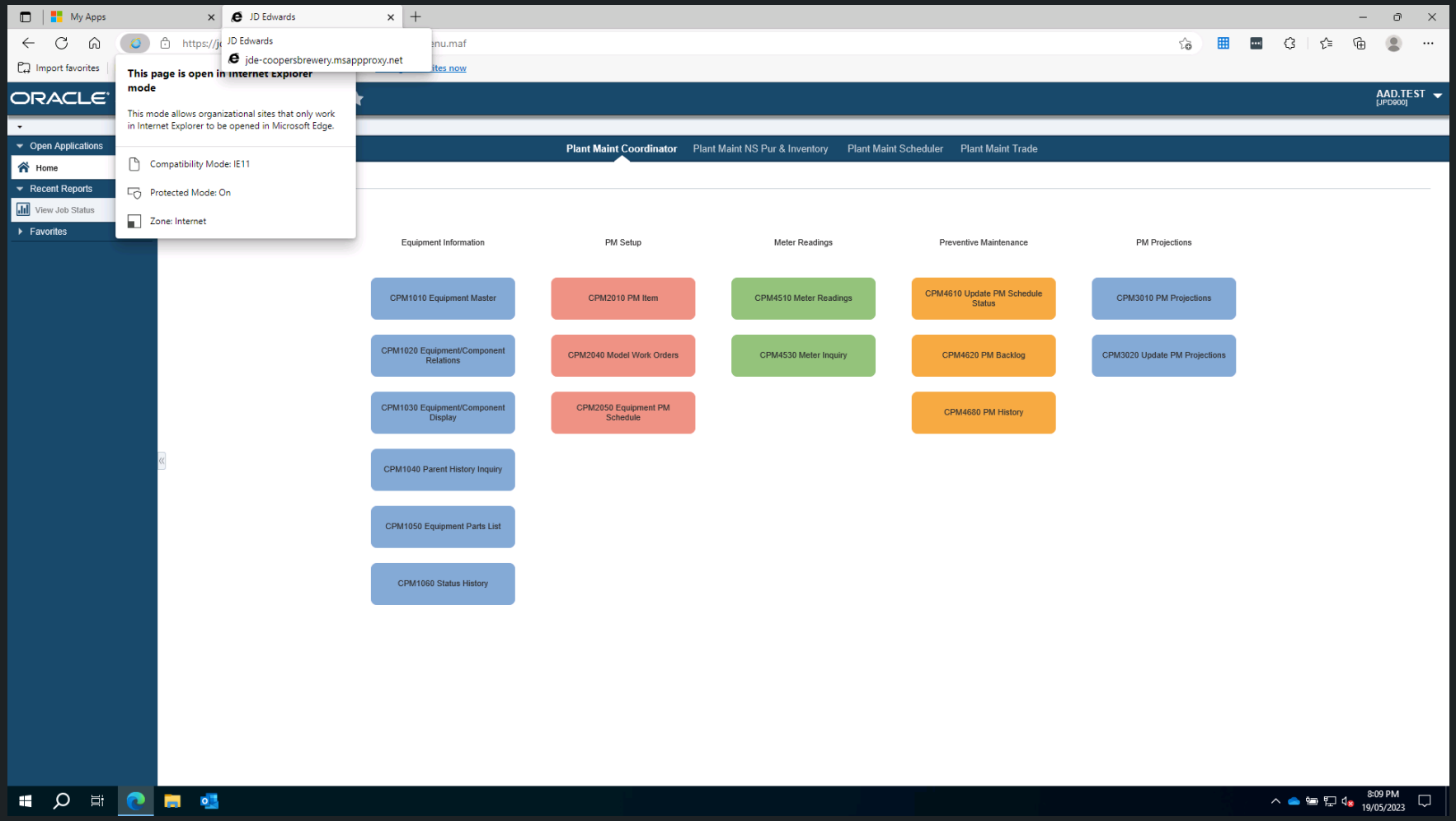
JDE access via Azure AD App Proxy

Access JDE environment securely from anywhere without VPN or direct network access



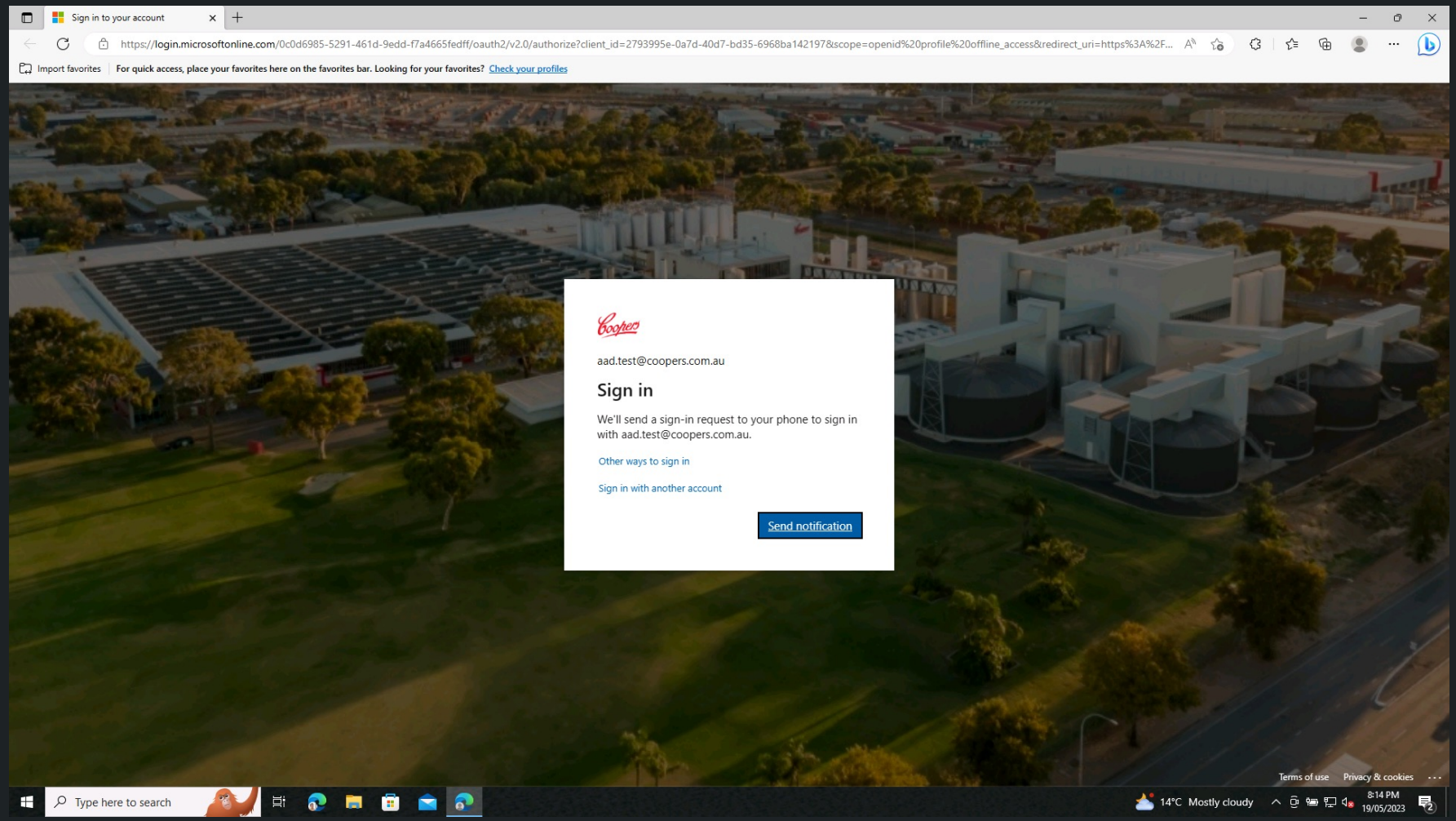
Compatibility mode for older versions of JDE

Microsoft Edge running in Internet Explorer 11 compatibility mode to support ActiveX plugins



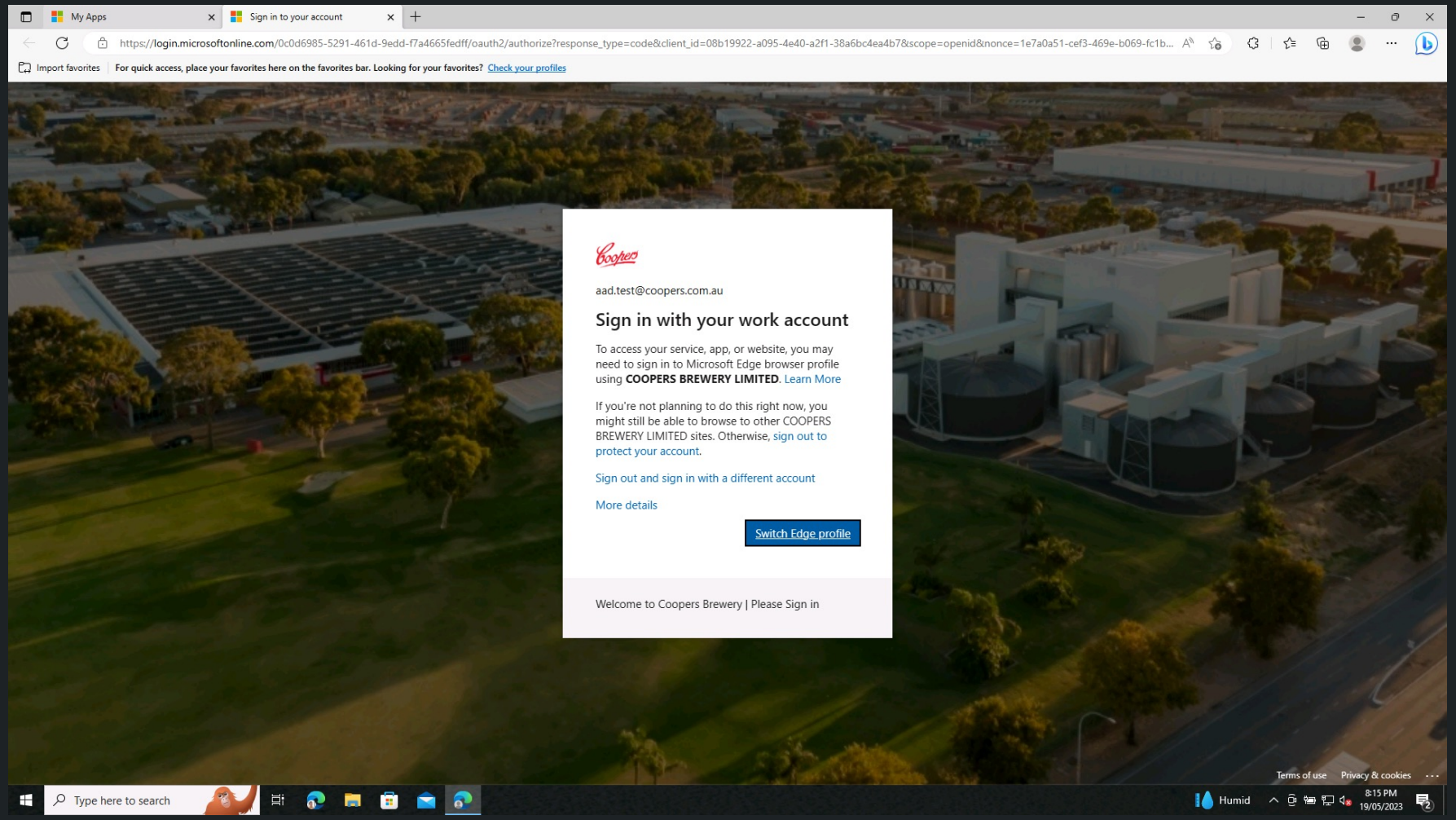
Access from an untrusted corporate device

No Single-Sign-On, but Passwordless Authentication via Microsoft Authenticator Phone Sign-In



Azure AD Conditional Access Policy enforcement

Access to JDE Production environment not possible from an unmanaged/untrusted device



Azure AD Conditional Access Logs

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only | ...

Date	[redacted]
Request ID	d30fb821-ae03-43bd-b2a4-d85d14dc6e00
Correlation ID	9993e7b4-5fbf-4ade-ad18-f4bf1c9e8121
Authentication requirement	Multifactor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	53000
Failure reason	Device is not in required device state: {state}. Conditional Access policy requires a compliant device, and the device is not compliant. The user must enroll their device with an approved MDM provider like Intune.
Additional Details	Your administrator might have configured a conditional access policy that allows access to your organization's resources only from compliant devices. To be compliant, your device must be either joined to your on-premises Active Directory or joined to your Azure Active Directory. More details available at https://docs.microsoft.com/azure/active-directory/active-directory-conditional-access-device-remediation
User	AAD Test User
Username	aad.test@coopers.com.au

Activity Details: Sign-ins

Basic info | Location | **Device info** | Authentication Details

Device ID	56be1dd1-c6c3-478c-b1cb-68ea60a6f101
Browser	IE 11.0
Operating System	Windows 10
Compliant	Yes
Managed	Yes
Join Type	Azure AD joined

Infrastructure design considerations for JDE

Normally a business separate Production and Non-Production into separate environments. However:

- JDE expects low latency
- Has its own internal segregation of environments i.e. PD, DV
- Has shared services – Easier to use a single Deployment Server….
- Non-Prod systems still need access to shared (system) tables in the Production database!

Other:

- JDE Sessions (stateful) – Don’t work with just any cloud-native load balancer!
- High availability
  - Database, load balancer, workload combo/POD (Web, AIS, Enterprise Server) boxes
  - Some processes in JDE need to run as single-threaded

Preventing Lateral Movement in the event of a breach (1 of 2)

Assume Breach:

- Assume that you've already been breached or that you will be soon.

Focuses on:

- Anomaly detection and signal correlation
- Pushing out the attacker as quickly as possible
- Making it as difficult as possible for an attacker to gain advantage once in your network!

Preventing Lateral Movement in the event of a breach (2 of 2)

What we do:

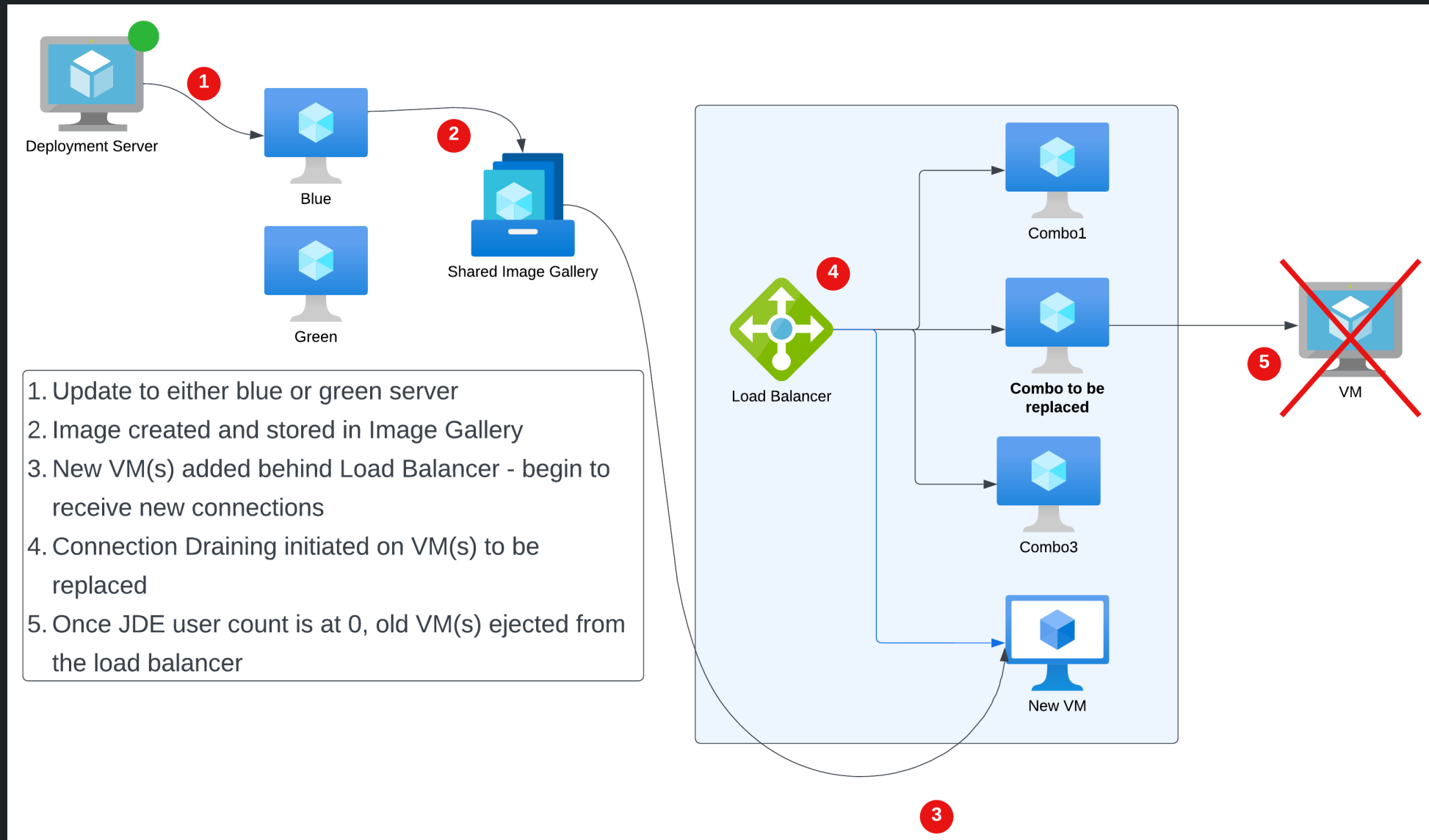
- Separate environments – production, non-production, sandboxes
- Segregate systems into separate networks/subnets – databases, applications, web, management
- Deny-All by default – ports/IP Addresses are whitelisted
- Block outbound Internet by default
- Defence in depth – Don’t assume that a firewall will save you!
- Logging – consistent flow of logs from NSGs, devices and Defender (endpoint protection) into SIEM

Blue / Green rolling upgrades – maintaining 24/7 uptime (1 of 2)

What is it? A way to:

- Validate JDE packages and OS software updates before rolling out to users
- Created versioned images - capable of initialising based on your needs such as for a specific timezone or JDE service i.e. AIS/BSSV
- Replace existing VMs behind a load balancer with newer versions without impacting users or creating downtime
- Scale up or down the number of VMs in a scale set based on:
  - Demand
  - Schedule i.e. overnight

Blue / Green rolling upgrades (2 of 2)



1. Update to either blue or green server
2. Image created and stored in Image Gallery
3. New VM(s) added behind Load Balancer - begin to receive new connections
4. Connection Draining initiated on VM(s) to be replaced
5. Once JDE user count is at 0, old VM(s) ejected from the load balancer

Thank You!