Configure Best Practices Security in Azure service_ocTony

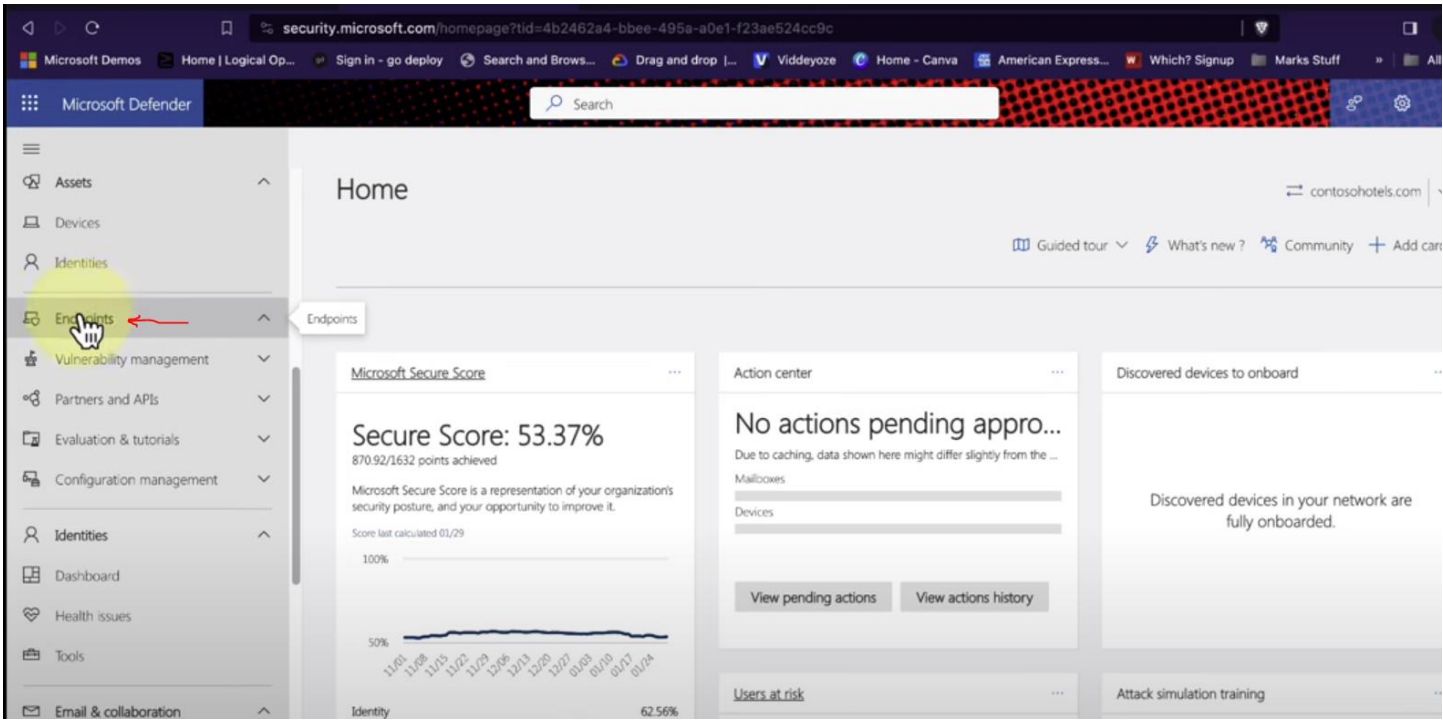
Setting up security in Azure involves multiple layers and best practices to ensure the protection of your resources and data. Below are the key steps to help you get started with securing your Azure environment:

1. **Azure Active Directory (Azure AD):**
   - **Set up Azure AD:** Azure AD is Microsoft's cloud-based identity and access management service. You can create and manage user identities, enforce authentication policies, and more.
   - **Configure users and groups:** Create users and groups in Azure AD and assign appropriate permissions to them based on the principle of least privilege.
   - **Enable Multi-Factor Authentication (MFA):** Add an extra layer of security by enabling MFA for user accounts accessing Azure resources.
2. **Network Security:**
   - **Virtual Networks (VNets):** Use VNets to isolate and segment your Azure resources. Implement network security groups (NSGs) to control inbound and outbound traffic to and from Azure resources.
   - **Firewalls:** Configure Azure Firewall or Network Security Groups (NSGs) with firewall rules to filter and allow/deny traffic based on IP addresses, protocols, and ports.
3. **Encryption:**
   - **Data Encryption:** Enable encryption at rest and in transit for your Azure resources. Use Azure Disk Encryption for virtual machines, Azure Storage Service Encryption for storage accounts, and enable HTTPS for web applications.
   - **Key Management:** Use Azure Key Vault to manage and safeguard cryptographic keys, secrets, and certificates.
4. **Identity and Access Management (IAM):**
   - **Role-Based Access Control (RBAC):** Implement RBAC to assign permissions to users, groups, and applications based on their roles. Use built-in roles or create custom roles as needed.
   - **Privileged Identity Management (PIM):** Use PIM to manage, control, and monitor access within your Azure AD directory. Assign just-in-time access and enforce approval workflows for elevated roles.
5. **Monitoring and Logging:**
   - **Azure Security Center:** Enable Azure Security Center to get security recommendations, threat detection, and continuous monitoring of your Azure resources.
   - **Azure Monitor:** Set up monitoring and logging for Azure resources using Azure Monitor. Configure alerts for suspicious activities, anomalies, and security incidents.
6. **Security Best Practices:**
   - **Regular Updates and Patching:** Keep your Azure resources, including virtual machines, databases, and applications, up to date with the latest security patches and updates.
   - **Backup and Disaster Recovery:** Implement regular backups and disaster recovery plans to protect against data loss and ensure business continuity in case of security incidents or failures.

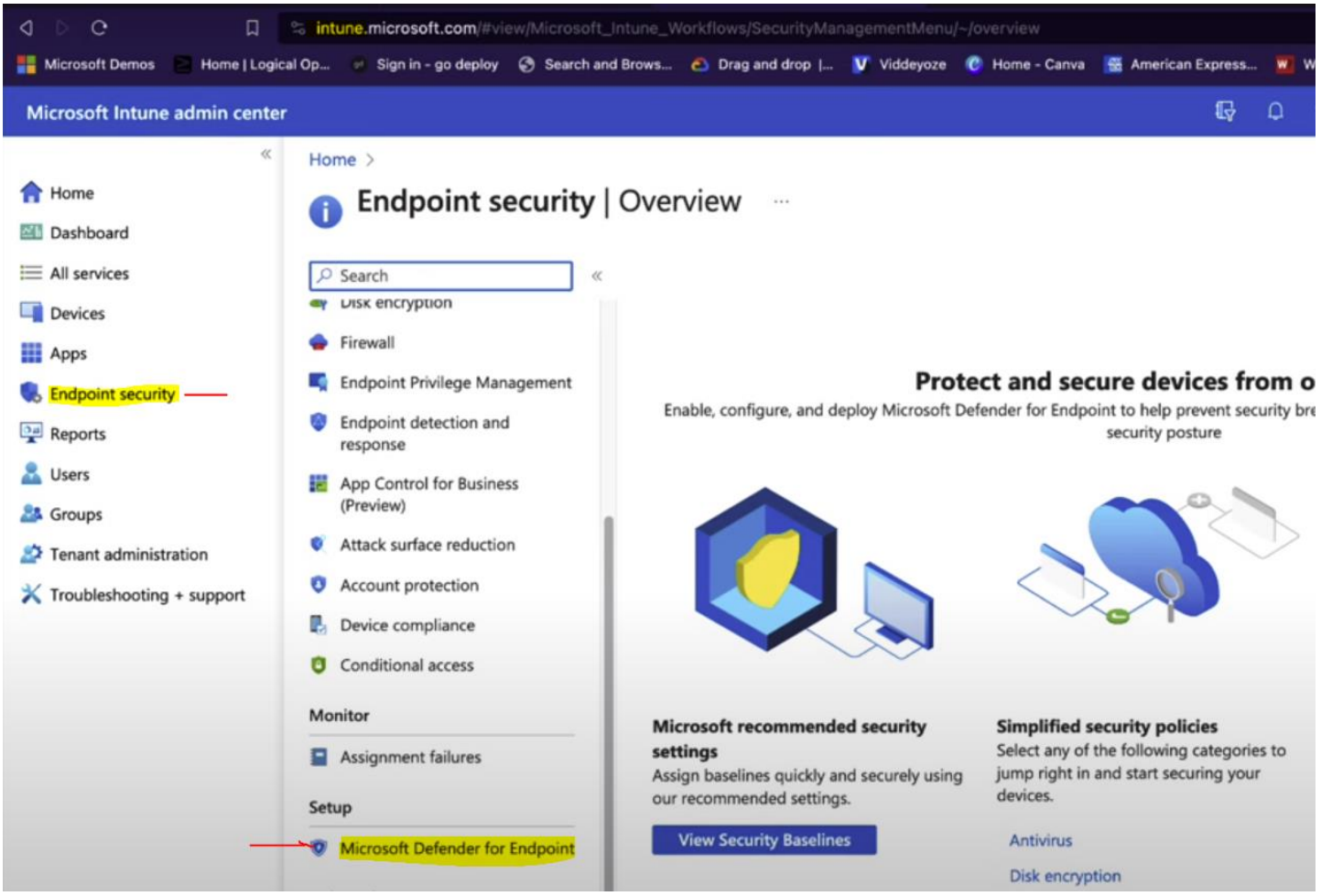
- **Security Policies and Compliance:** Define and enforce security policies, compliance standards (e.g., GDPR, HIPAA), and regulatory requirements for your Azure environment.

7. **Security Tools and Services:**
   - **Azure Security Center:** Utilize Azure Security Center's advanced threat protection, security policies, and integrated security tools for continuous security monitoring and management.
   - **Azure Sentinel:** Implement Azure Sentinel for cloud-native security information and event management (SIEM) to detect, investigate, and respond to security threats across your Azure environment.

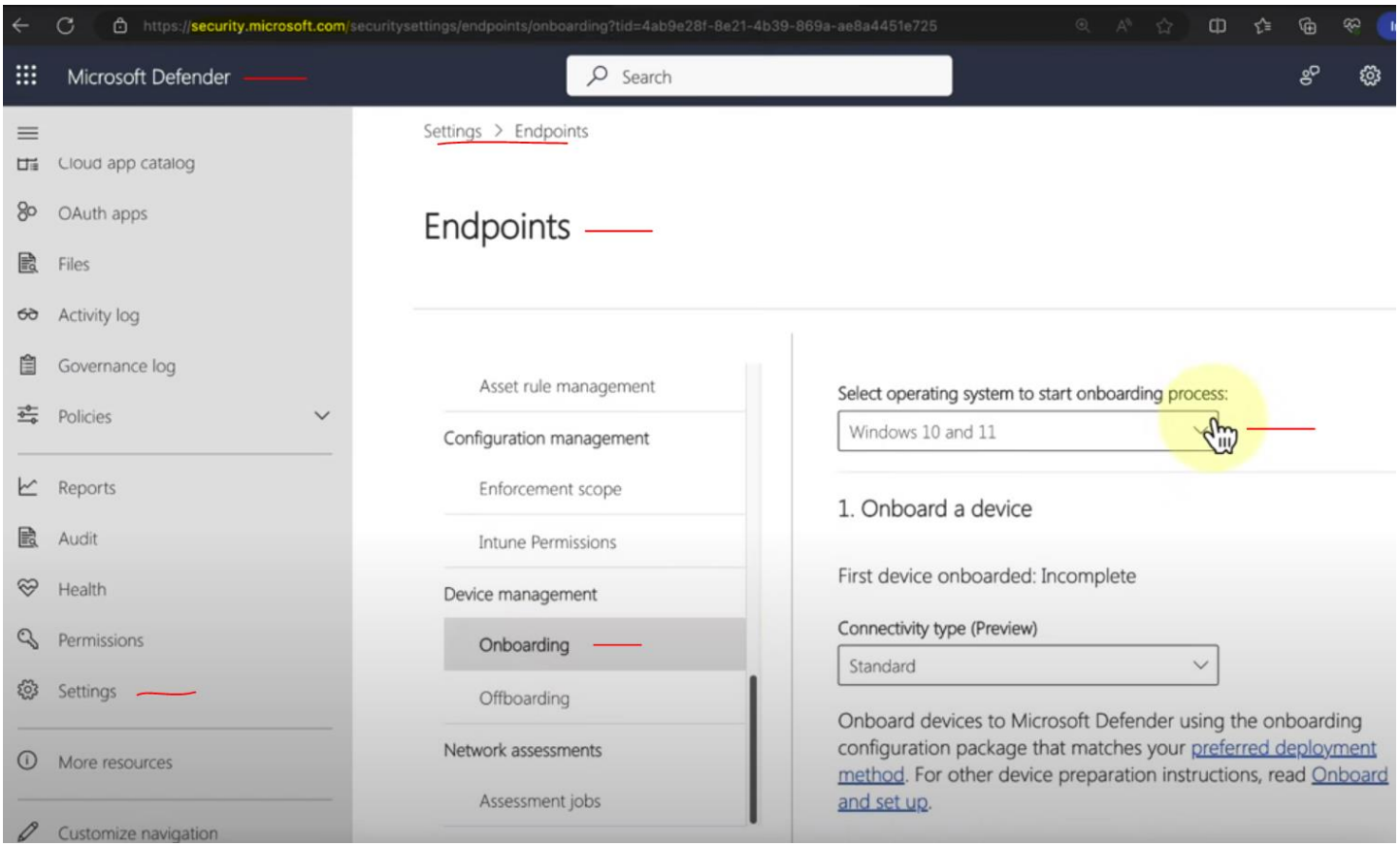
Setting of Security.Microsoft.com with license

1. 

2. **Intune.Microsoft.com set EndPoint Security has Defender for EndPoint**

3. 

4. **From Security.microsoft.com - Microsoft Defender go to settings – Select OS for Onboarding**

5. 
https://security.microsoft.com/securitysettings/endpoints/onboarding?tid=4ab9e28f-8e21-4b39-869a-ae8a4451e725
Microsoft Defender
Search
Cloud app catalog
OAuth apps
Files
Activity log
Governance log
Policies
Reports
Audit
Health
Permissions
Settings
More resources
Customize navigation
Settings > Endpoints
Endpoints
Asset rule management
Configuration management
Enforcement scope
Intune Permissions
Device management
Onboarding
Offboarding
Network assessments
Assessment jobs
Select operating system to start onboarding process:
Windows 10 and 11
1. Onboard a device
First device onboarded: Incomplete
Connectivity type (Preview)
Standard
Onboard devices to Microsoft Defender using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read Onboard and set up.
6.
7.