Daily Summary - Detailed Report

How to set the BIOS (Supervisor/Admin) password only

- Accessed BIOS setup during boot (usually by pressing F2, F10, or Del depending on device).
- Set a Supervisor/Admin password from the BIOS Security menu.
- Confirmed only the BIOS menu is locked, preventing unauthorized configuration changes.
- Normal boot continues without requiring a password for everyday use.
- This ensures extra security by protecting firmware settings while not impacting regular users.

Tested the Intune ID and verified all options today

- Logged in using Intune-provisioned credentials.
- Verified all available options in the Intune Admin Center including device compliance, app protection, and policy assignment.
- Disabled one user account and checked license behavior: system reported 9 active licenses and 1 inactive.
- Observed that the disabled user's device still had access to resources because the Entra ID account was still active and the device remained enrolled.
- This demonstrates that disabling a user in Intune does not immediately revoke device access unless combined with account deactivation in Entra ID.

How to add a calendar in pseudo mail (placeholder email)

- A pseudo/placeholder email cannot connect to a live calendar service.
- Simulated calendar functionality using shared .ics files that can be imported into Outlook or Google Calendar.
- Linked a shared calendar URL for test environments.
- Embedded static events as part of the placeholder environment to test calendar features without needing a live mailbox.

How to add a calendar in shared mail (Outlook / Intune context)

- Opened Outlook on the web and accessed the shared mailbox through profile selection.
- Navigated to the Calendar section within Outlook Web Access (OWA).
- Created a new calendar under the shared mailbox for team use.
- Alternatively, imported an external calendar by subscribing with a .ics link.
- Verified permissions for calendar sharing and delegated access so multiple users could view/edit.

Hosts file path in macOS and how to edit it

- Located the hosts file at: /etc/hosts.
- Used sudo nano /etc/hosts to edit the file with elevated privileges.
- Added entries mapping custom hostnames to IP addresses for testing environments.
- Saved changes and flushed DNS cache using: sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder.
- This ensures that macOS applies the new host mappings immediately without requiring a reboot.

Extracting access tokens is not possible from Microsoft login error page

- Reviewed the error page containing AADSTS900561 (endpoint accepts POST/OPTIONS but received GET).
- Confirmed that access tokens are never embedded in HTML responses from Microsoft login endpoints.
- Tokens must be obtained securely through OAuth 2.0 flows such as Authorization Code Flow, Device Code Flow, or Client Credentials Flow.
- Applications should be registered in Entra ID (Azure AD) and configured with appropriate client secrets or certificates.
- This ensures tokens are retrieved securely and used only by authorized apps.

Browser restrictions in Intune (default browser, AppLocker, WDAC)

- Created a configuration profile in Intune Admin Center for Windows 10/11.
- Set Edge as the default browser using the Settings Catalog.
- Explored AppLocker for restricting applications like Chrome or Firefox but found it not fully available in the UI.
- AppLocker policies may require OMA-URI XML import for granular control.
- Windows Defender Application Control (WDAC) was identified as the modern, recommended method for restricting apps.
- Assigned the profile to the intern’s device group and verified policy application.

Additional Observations & Learnings

- License management in Intune requires close coordination with Entra ID to ensure deactivated users lose access promptly.
- Shared mailboxes and calendars are useful for collaboration but require clear permission settings to avoid security gaps.
- Editing the hosts file remains a critical tool for developers to simulate environments and test DNS mappings.
- Security best practices suggest BIOS locking for device protection, Intune for software restrictions, and Entra ID policies for identity protection.
- Modern device management combines hardware (BIOS), OS-level (Intune policies), and cloud identity (Entra ID) for layered security.