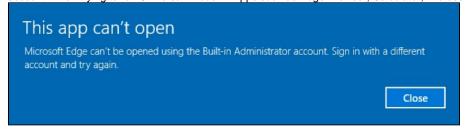
# **Enabling User Account Control**

## **Q: Enabling User Account Control**

Domain joined computers running Windows 8.1 and Windows 10 may receive the error "This app can't open for Built-in Administrator
account" when trying to run Universal "Modern" Apps such as Edge Browser, Calculator, Microsoft Store, Weather App, etc.:



#### Context

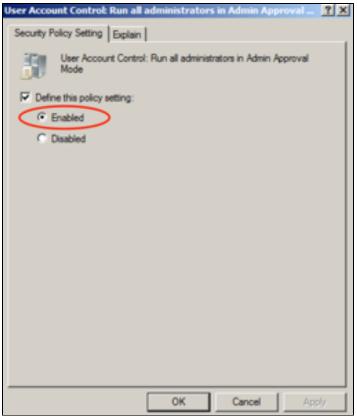
- This issue is occurring because these apps require User Account Control (UAC) to be enabled due to Application Sandboxing. By default
  UAC is disabled at the root level of the WIN domain due to current compatibility issues with MIT Kerberos for Windows.
- This fix is applied via a group policy object and must be performed by an IT technician with the appropriate permissions to the GPO.
- Important! If you are using SAP you will need to apply an environmental variable change first. Once this change is in place the UAC can
  be enabled in the case where MIT's Kerberos for Windows was only used for access to SAP.

#### Answer

- Access the related Organization Unit GPO through Group Policy Management Console. This is done through Citrix under the WIN Container Admin Tools. https://citrixapps.mit.edu/Citrix/XenApp/auth/login.aspx
- 1. Once you locate your related GPO right click and select edit
- 2. Navigate to Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options/

3. Set the parameter User Account Control: Run all administrators in Admin Approval Mode to Enabled.

Group Policy Management Editor \_ | \_ | × Action View Help GP.Endpoints/ Policy ^ Policy Setting Network security: Restrict NTLM: Add remote server exceptions for NTLM aut... Not Defined ☐ Policies Network security: Restrict NTLM: Add server exceptions in this domain Not Defined Citrix Policies Network security: Restrict NTLM: Audit Incoming NTLM Traffic Not Defined Software Settings Network security: Restrict NTLM: Audit NTLM authentication in this domain Not Defined ☐ I Windows Settings Network security: Restrict NTLM: Incoming NTLM traffic Not Defined Name Resolution Policy Network security: Restrict NTLM; NTLM authentication in this domain Not Defined Scripts (Startup/Shutdown) Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers Not Defined Security Settings Recovery console: Allow automatic administrative logon Not Defined Recovery console: Allow floppy copy and access to all drives and all folders Not Defined Shutdown: Allow system to be shut down without having to log on Not Defined Audit Policy
User Rights Assig
Security Options Shutdown: Clear virtual memory pagefile User Rights Assignment System cryptography: Force strong key protection for user keys stored on th... Not Defined System cryptography: Use FIPS compliant algorithms for encryption, hashing,... Not Defined Restricted Groups System objects: Require case insensitivity for non-Windows subsystems Not Defined System Services System objects: Strengthen default permissions of internal system objects (e.... Not Defined Registry **(** System settings: Optional subsystems Not Defined 7 File System System settings: Use Certificate Rules on Windows Executables for Software ... Not Defined Wired Network (IEEE 802.3) Policies User Account Control: Admin Approval Mode for the Built-in Administrator acc... Disabled Windows Firewall with Advanced Security User Account Control: Allow UIAccess applications to prompt for elevation wit... Disabled Network List Manager Policies User Account Control: Behavior of the elevation prompt for administrators in ... Prompt for consent for non-Windo. ₩ Wireless Network (IEEE 802.11) Policies User Account Control: Behavior of the elevation prompt for standard users Prompt for credentials on the secu. Public Key Policies User Account Control: Detect application installations and prompt for elevation Disabled Software Restriction Policies User Account Control: Only elevate executables that are signed and validated Network Access Protection User Account Control: Only elevate UIAccess applications that are installed in ... Application Control Policies User Account Control: Run all administrators in Admin Approval Mode 🖪 🌏 IP Security Policies on Active Directory (W User Account Control: Switch to the secure desktop when prompting for eleva... Advanced Audit Policy Configuration



- 4. **Please Note:** This change will enable UAC for all computers in the OU including Windows 7 computers. Users will experience additional approval prompts with UAC enabled.
- 5. A reboot will be required after the policy is applied (either with a gpupdate /force or wait 120 minutes).

### See Also

• WIN.MIT.EDU Landing Page