

UAC - položky klíče

Klíč: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Položky (pořadí viz Registry OS W10):

ConsentPromptBehaviorAdmin:

- 0 - operace, která vyžaduje zvýšená oprávnění bez souhlasu nebo pověření, bude „administrátorsky“ automaticky povolena
- 1 - výzva pro souhlas administrátora zadáním uživatelského jména a hesla (nebo jiného platného administrátorského termínu), je-li zvýšení oprávnění požadováno. Operace je prováděna na zabezpečené ploše
- 2 - výzva pro souhlas administrátora výběrem buď „Permit“ nebo „Deny“ pro operaci, která vyžaduje zvýšení oprávnění. V případě, že odpověď administrátora je „Permit“, bude operace pokračovat s nejvyššími možnými výsadami. „Výzva k souhlasu“ odstraňuje nepohodlí, které uživatele nutí zadat své jméno a heslo k provedení privilegovaného úkolu. Operace je prováděna na zabezpečené ploše
- 3 - výzva pro souhlas administrátora zadáním uživatelského jména a hesla (nebo jiného platného administrátorského termínu), je-li zvýšení oprávnění vyžadováno
- 4 - výzva pro souhlas administrátora výběrem buď „Permit“ nebo „Deny“ pro operaci, která vyžaduje zvýšení oprávnění. V případě, že odpověď administrátora je „Permit“, bude operace pokračovat s nejvyššími možnými výsadami. „Výzva k souhlasu“ odstraňuje nepohodlí, které uživatele nutí zadat své jméno a heslo k provedení privilegovaného úkolu
- 5 - volba je výchozí. Je to výzva pro souhlas administrátora výběrem buď „Permit“ nebo „Deny“ pro libovolný binární soubor, který není typu „Windows“. V případě, že odpověď správce je „Permit“, bude operace pokračovat s nejvyššími možnými výsadami. Operace je prováděna na zabezpečené ploše. Binární soubory typu „Windows“ budou moci provádět operace vyžadující zvýšení oprávnění bez souhlasu nebo pověření

ConsentPromptBehaviorUser:

- 0 - možnost, je-li nastavena, zajistí, že každá operace, která vyžaduje zvýšení oprávnění, bude pro standardního uživatele zamítnuta
- 1 - možnost, je-li nastavena, zajistí, že standardní uživatel, který potřebuje provést operaci vyžadující zvýšení úrovně oprávnění, bude vyzván k zadání administrátorského jména a hesla. Pokud uživatel platná oprávnění zadá správně, bude operace pokračovat s platným oprávněním
- 3 - možnost, je-li nastavena, zajistí, že standardní uživatel, který potřebuje provést operaci vyžadující zvýšení úrovně oprávnění, bude vyzván k zadání administrátorského jména a hesla na zabezpečené ploše. Pokud uživatel platná oprávnění zadá správně, bude operace pokračovat s platným oprávněním

dontdisplaylastusername:

- 0 - jméno posledního úspěšně přihlášeného uživatele se objeví v dialogovém okně přihlášení k systému Windows. Toto nastavení je navrženo proto, aby protokolování bylo rychlejší a jednodušší
- 1 - pole uživatelského jména v okně přihlášení k systému Windows bude prázdné. Nastavení je určeno pro zvýšení zabezpečení systému, který pak nezobrazuje platné uživatelské jméno

DSCAutomationHostEnabled (Desired State Configuration (získání stavu konfigurace) je možné např. použít pro zjištění existence klíčů v Registry. Popis zde je pouze přibližný, parametry vlastního prostředku jsou popsány na stránkách MS):

- 0 - zákaz hostování prostředku „DSC“
- 1 - povolení -,-

EnableCursorSuppression:

- 0 - kurzor potlačen
- 1 - kurzor povolen

EnableInstallerDetection:

- 0 - možnost, je-li nastavena, zakáže automatickou detekci instalačních balíčků, které vyžadují zvýšení práv k instalování
- 1 - možnost, je-li nastavena, provede heuristickou detekci aplikací, které vyžaduje zvýšení privilegií

EnableLUA:

- 0 - deaktivování této politiky zakáže „schvalování v režimu Administrator“
- 1 - tato politika povoluje uživatelskou možnost „schvalování v režimu Administrator“ a současně politiku User Account Control (UAC) povoluje všem ostatním

EnableSecureUIAPaths:

- 0 - zvýšení oprávnění aplikací UIA (User Interface Accessibility - uživatelský přístup k rozhraní), nainstalovaných v zabezpečených umístěních není povoleno. Zabezpečená umístění jsou omezená na „...\\Program Files (ččetně podsložek), „...\\Windows\\system32 a „...\\Program Files(86) (včetně podsložek pro 64-bit verze OS Windows)
- 1 - zvýšení „...“ je povoleno

EnableUIADesktopToggle:

- 0 - zobrazení výzvy aplikací UIA (User Interface Accessibility – uživatelský přístup k rozhraní) ke zvýšení oprávnění na nezabezpečené ploše není povoleno
- 1 - zobrazení „...“ je povoleno

Enable Virtualization:

- 0 - zákaz přesměrování dat pro interaktivní procesy
- 1 - politika umožňuje přesměrování odkazů souborů aplikací a zápisů do Registry, které by za normálních okolností byly pro uživatelské zápisy dat standardních uživatelů odmítnuty se musí přihlásit. Nastavení zmírňuje problémy s aplikacemi, které v minulosti byly provozovány jako administrátorské a zapisovaly data aplikací v režimu „run-time“ do míst zapisovatelných pouze v administrátorském režimu

FilterAdministratorToken:

- 0 - administrátorský účet je v režimu „plný token“ (úplná autorizace)
- 1 - „-“ schvalování, které je vyžadováno

legalnoticecaption a legalnoticetext:

text umístěný v položkách, se při startu OS použije k „legálnímu“ nebo „právnímu“ varování např. o tom, že jste/nejste majitelem OS - „...caption“ je použité v titulku okna a „...text“ v okně

PromptOnSecureDesktop:

- 0 - deaktivace této politiky zakáže výzvu na zabezpečené ploše. Všechna pověření nebo souhlasy s výzvou budou probíhat na ploše interaktivního uživatele
- 1 - tato politika nutí všechny UAC výzvy provádět na zabezpečené ploše uživatele

scforceoption:

- 0 - použití čipové karty k přihlášení není povolené
- 1 - „-“ je povolené

shutdownwithoutlogon:

- 0 - tlačítko Shutdown je zakázané. Objevuje se sice okně přihlášení, ale je zašedlé
- 1 - tlačítko Shutdown je povolené

undockwithoutlogon:

- 0 - uživatel, aby mohl z dokovací stanice odstranit počítač (odpojit ho), se musí přihlásit
- 1 - externí HW tlačítko pro vysunutí počítače (odpojení) z doku zafunguje bez přihlášení

ValidateAdminCodeSignatures:

- 0 - nevynucování kryptografických podpisů interaktivních aplikací, které vyžadují zvýšená práva
- 1 - prosazování kryptografických podpisů interaktivních aplikací, které vyžadují zvýšená práva

www.nemohouci.cz