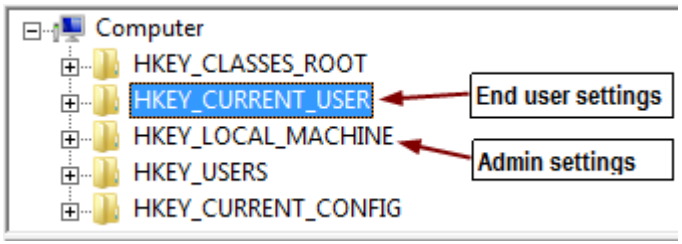
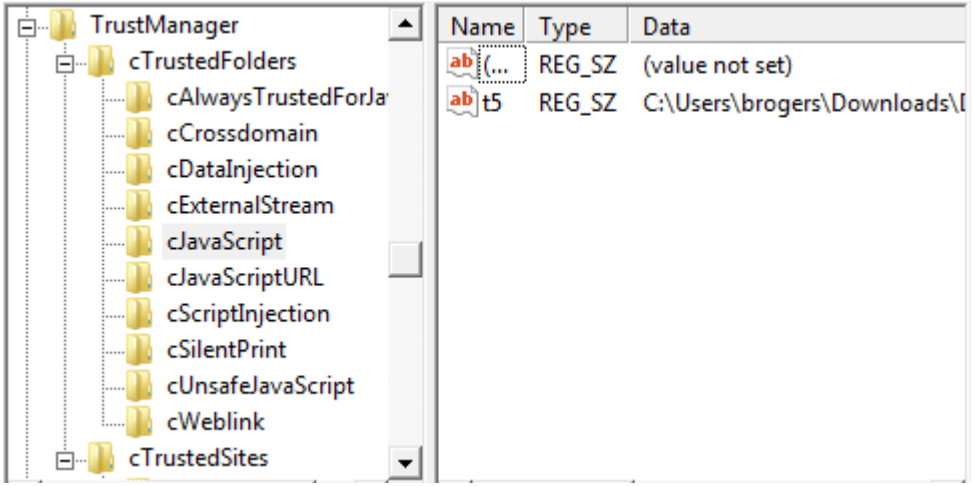
SECURITY QUICK KEY

General Rules:

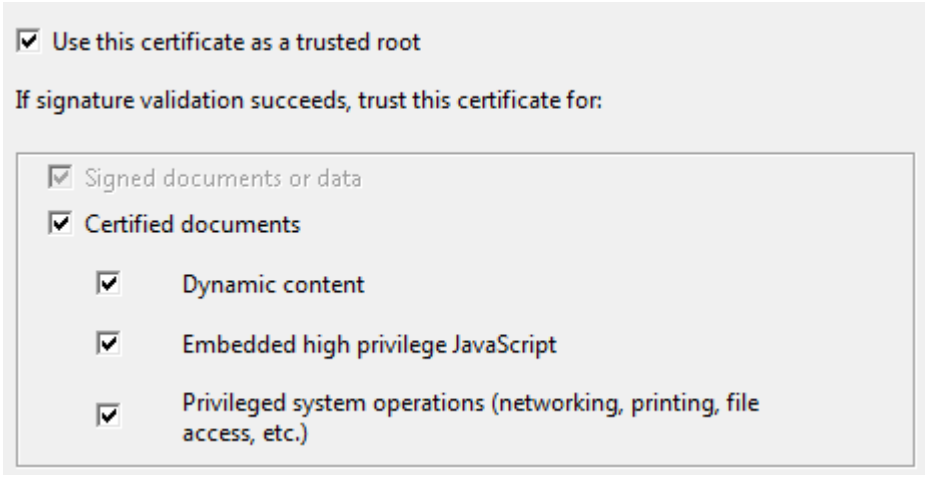


- Assign trust by:
  - Enabling features globally
  - Assigning trust via privileged locations, multimedia settings, and trust manager settings
  - Via the Edit Certificate Trust dialog for certified signature workflows
- Restrict content types and application behavior by:
  - Disabling features globally
  - Enabling sandboxing via Protected Mode (Reader) and Protected View (Acrobat 10.1+ and Reader 11+)
  - Enabling enhanced security and not trusting documents from unknown origins
  - Via the Edit Certificate Trust dialog for signature workflows
- Many HKCU settings have an HKLM mirror so that IT can disable, lock, and control permissions

Privileged locations stored in registry and plist



Edit Certificate Trust dialog trust settings



AVAILABLE PREFERENCES

Sandboxing	10.0: bProtectedMode	Sandboxes Reader processes	Sandboxing provides the strongest protection. Incompatible with some workflows/3rd party software. Use bUseWhitelistConfigFile to allow more actions 11.0 introduces PV support for Reader.
	10.0: tBrokerLogfilePath	Turns on Protected Mode logging	
	10.1: iProtectedView	Acrobat: Enables Protected View for untrusted files	
	10.1: bDisableTemporaryFileProtectedView	Acrobat: Disables Protected View for temporary internet files	
	10.1: bEnableAlwaysOutlookAttachmentProtectedView	Acrobat: Disables Protected View for Outlook attachments	
	10.1: tBrokerLogfilePath	Acrobat: Turns on Protected View logging	

JavaScript	9.0: bEnableGlobalSecurity	Controls JS object access across sessions	Interacts with privileged locations. Separate controls for JS, high privileged JS, blacklisted/whitelisted JS. Disable and lock JS, then set privileged locations
	9.0: bEnableJS	Turns JS on and off	
	9.0: bEnableMenuItems	Controls JS execution of menu items	
	9.0: tBlackList (HKLM only)	Block JS APIs	
	9.0: tWhiteList (HKLM only)	Controls JS-menu item interaction	
	10.1.2: bDisableJavaScript (HKLM only)	Disables and locks JS	
Privileged locations	9.0: cCrossdomain (YMB)	Allows cross domain access	All settings can be in HKCU and/or HKLM. Untrusted documents see Yellow Message Bar. Trust Win Trusted Sites since 9.3 and also Local Intranet since 9.5 and 10.1.2 via bTrustOSTrustedSites. These HKLM settings disable and lock trust: • bDisableOSTrustedSites • bDisableTrustedFolders • bDisableTrustedSites 11.0+: Certified documents can be trusted identically as all other privileged locations.
	9.0: cDataInjection (YMB)	Allows data injection	
	9.0: cExternalStream	Allows access to external streams (XObjects)	
	9.0: cJavaScript	Allows the execution of high privileged JavaScript	
	9.0: cScriptInjection (YMB)	Allows script injection	
	9.0: cSilentPrint	Allows silent printing to a file or a hardware printer	
	9.0: cWeblink	Allows URLs when the Trust Manager is set to block/ask	
	9.2: cAlwaysTrustedForJavaScript (YMB)	Enables JS when bEnableJS = 0	
	9.2: cUnsafeJavaScript (YMB)	Allows blacklisted JavaScript to execute	
	9.3.4: cJavaScriptURL (YMB)	Allows the execution of JavaScript invoked URLs	
	10.1.2 cFileAttachment (YMB)	Allows attachments to open non-PDF or FDF files	
	10.1.2 cTrustedSitesPrivate (HKLM only)	Specifies trusted hosts with less stringent wildcard restraints	
	10.1.2 cMultimedia (YMB)	Allows Legacy multimedia that uses 3rd party players	
	11.0 bTrustCertifiedDocuments	Elevates (trusts) certified documents as a privileged location	
	11.0 bEnableCertificateBasedTrust	Same as bTrustCertifiedDocuments, but licks the setting	
URLs	9.0 iUnknownURLPerms	Specifies whether to ask, allow, or block access to web sites	Controlled by Preferences > Trust Manager > Internet Access Can be overridden by privileged locations
	9.0 iURLPerms	Specifies whether to always ask, allow, or block all websites	
	9.0 tHostPerms	Lists the user-specified web sites and permissions	
ES	9.0 bEnhancedSecurityInBrowser	Controls enhanced security in the browser	ES blocks data and script injection, x domain access, silent printing and external stream access.
	9.0 bEnhancedSecurityStandalone	Controls enhanced security for the standalone application	
Network	9.0 cDefaultLaunchURLPerms	Protocol-specific ermissions	Adobe provides default permissions IT can add HKCU and HKLM permissions
	9.0 tFlashContentSchemeWhiteList	Protocols Flash can use to access external content	
	9.0 tSchemePerms	Protocols a PDF can use to access external content	
	9.0 tSponsoredContentSchemeWhiteList	A list of protocols sponsored content can use	
Attachments	9.0: c[someExtension]	A user list of file types	Most settings can be in HKCU and/or HKLM. With 10.1.2, attachments can be trusted via privileged locations.
	9.0: cAttachmentTypeToPermList	A list of extensions and their permissions	
	9.0: iFileAttachmentPerms	Prevents opening or launching file types other than PDF or FDF	
	9.0: iPerm	The attachment permissions for file types listed in sExtension	
	9.0: iUnlistedAttachmentTypePerm	The default permissions for untrusted file types	
	9.0: sExtension	The extensions whose permissions are specified by iPerm	
	9.0: tBuiltInPermList	A white/black list of file types that can be opened and saved	
Flash	9.5.1 (not in 10.x) bEnableFlash	Specifies whether to allow Flash to play in a PDF.	Flash player for rendering Flash in PDFs no longer bundled. IT can add HKCU and HKLM permissions
3D	9.5.1 (not in 10.x) bEnable3DContent	Specifies whether to allow 3D content in a PDF.	Also lockable via bEnable3D in HKLM