Windows Vista: the User Account Control Architecture

A Windows Vista Webinar by William R. Stanek

This is the third webinar in a three-part series of webinars on the Windows Vista support architecture from bestselling author and training instructor William Stanek.

William is a leading technology expert, award-winning author, and instructional trainer with over 20 years of experience in server technologies, encryption, Internet solutions, and advanced programming and development. He has written over 65 books and numerous whitepapers and training courses on a wide variety of topics. His most recent books include Microsoft Exchange Server 2007 Administrator's Pocket Consultant 2nd Edition, Microsoft Windows Server 2008 Administrator's Pocket Consultant, and Windows Server 2008 Inside Out. For more information on William's consulting and training courses, you can visit www.WilliamStanek.com.

The books featured here, Windows Vista Administrator's Pocket Consultant and Windows Server 2008 Administrator's Pocket Consultant, are William's highly acclaimed books on Windows Vista and Windows Server 2008 respectively. Most recent customer reviews have called them A Must Have manual, a great reference tool, technically accurate and best of the bunch, and the best manual for administrators.

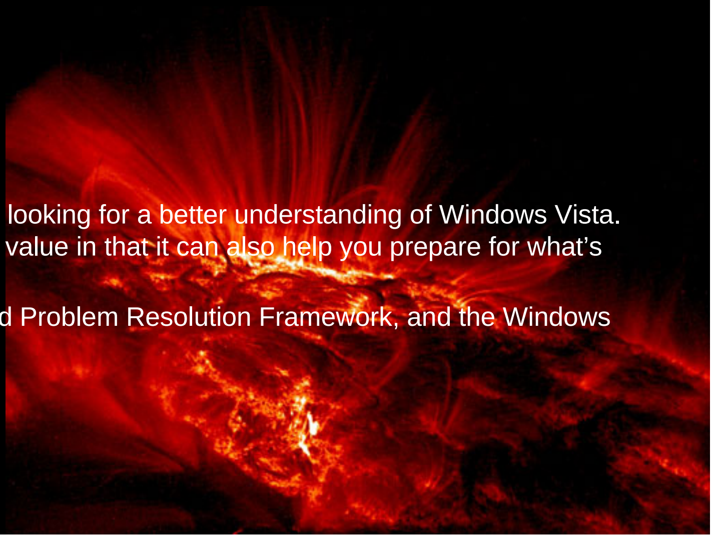
William's highly popular books and training courses for technical professionals cover Windows Vista, Windows Server 2008, Exchange Server 2007, SQL Server 2005, and Active Directory. In this presentation, William explores one of the least understood areas of the new support architecture in Windows Vista: the User Account Control architecture. The presentation examines:

- Elevation prompting, the secure desktop and Admin Approval mode
- File and Registry virtualization
- Application integrity and run levels
- Related administration tools
- Related Group Policy management settings

This presentation is suitable for IT managers, CIOs, executives, and administrators who are looking for a better understanding of Windows Vista. As many of these same features are in Windows Server 2008, this presentation has a twofold value in that it can also help you prepare for what's in Microsoft's next generation server operating system.

The other webinars in this series covering critical Windows Vista topics: the Diagnostics and Problem Resolution Framework, and the Windows Boot and Pre-Boot Architecture.

William Stanek's Training Seminars –
www.WilliamStanek.com

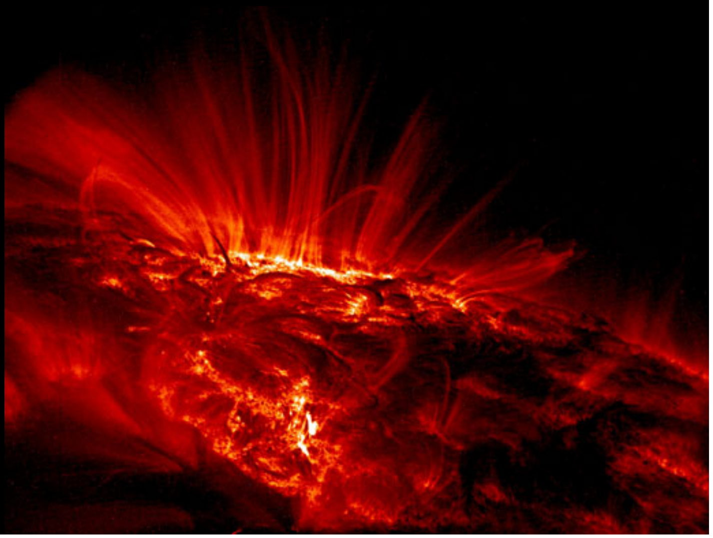


Windows Vista
Support Architecture:

User Account Control

What we’re going to discuss:

- Elevation prompting, the secure desktop and Admin Approval mode
- File and Registry virtualization
- Application integrity
- Access tokens and run levels
- Related administration tools
- Related Group Policy management settings



Session Objectives

You're in the right place if you are an IT pro who is looking for a better understanding of Windows Vista.

After completing this session, you'll have a better understanding of:

- User Account Control
- Elevation and the secure desktop
- File and Registry virtualization
- Application integrity
- Access tokens and run levels
- Configuration options

Bottom Line:

- Support framework almost identical in Windows Vista and Windows Server 2008
- IT pros must understand this support architecture to succeed.

Understanding User Account Control (UAC)

- How it Works
- Why its important

User Account Control Essentials

- Two general types of user accounts
  - Standard and administrator
  - No power user
- Standard users
  - Can perform general computing tasks
  - Can perform basic support tasks
- Administrators can perform
  - Have complete access to the computer
  - Can make changes that affect other users and security
- User Account Control (UAC)
  - Redefines how user accounts are used
  - Limits the scope of administrator-level access privileges
  - Requires all applications to run in a specific user mode
  - Prevents users from making inadvertent changes
  - Locks down the computer

Elevation, Prompts, and the Secure Desktop

- Windows Vista makes it easy to determine
  - Which tasks standard users can perform
  - Which tasks administrators can perform
- Permissions icon
  - Multicolored shield
  - Indicates administrator permissions are required
- User Account Control (UAC) prompt
  - Displays for tasks that requires administrator permissions by default
  - Works differently for standard user and administrator accounts

Elevation, Prompts, and the Secure Desktop

- Standard user account
  - Prompted to provide administrator credentials
  - Credentials prompt works differently in domains and workgroups
- Administrator account
  - Prompted for consent to continue
  - Consent prompt asks your approval to continue
- Elevation
  - Is the process of getting approval
  - Enhances security by reducing exposure
  - Provides notification prior to execution
  - Helps block malicious programs

Elevation, Prompts, and the Secure Desktop

- Secure desktop
  - Used by Windows Vista prior to displaying the elevation prompt
  - Prevents other processes or applications from providing required permissions or consent
  - Only the prompt runs on the secure desktop
- Elevation, prompts, and the secure desktop
  - Are aspects of UAC that affect you the most These features work together
  - Prevent inadvertent changes
  - Block unauthorized applications

Prompts for Administrators

- Admin Approval Mode
  - Controls prompting for administrators
  - Applies to all standard administrators
  - Doesn't apply to built-in local administrator
- Admin Approval Mode
  - Managed differently in domains and workgroups
  - In domain can be managed through Group Policy
  - In workgroups managed only through local security policy

Configuring UAC

- User settings
- Admin settings

UAC and Admin Approval Mode

- Configure through
  - Group Policy or local security settings
  - Under Local Policies\Security Options
- Related settings
  - User Account Control: Admin Approval Mode For The Built-in Administrator Account
  - User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode
  - User Account Control: Behavior Of The Elevation Prompt For Standard Users
  - User Account Control: Run All Administrators In Admin Approval Mode
  - User Account Control: Switch To The Secure Desktop When Prompting For Elevation

UAC and Your Applications

- Application integrity
- Access tokens
- Run levels

Maintaining Application Integrity

- Two run levels for applications
  - Standard
  - Administrator
- Run levels help maintain
  - Internal consistency
  - Application integrity
- Most applications and processes have a security token
  - A standard token means elevated privileges are not required
  - An administrator token means elevated privileges are required

Types of Applications

- Windows Vista–compliant applications
  - Any application written specifically for Windows Vista
  - Certified as compliant
  - Have the Windows Vista–Compliant logo
- Legacy applications
  - Any application written for an earlier version of Windows
  - Not certified as compliant
  - Do not have Windows Vista–Compliant logo
- Windows Vista–compliant applications
  - Use UAC to reduce the attack surface
  - Block unauthorized programs without consent
  - Restrict the default privileges granted
- Application Information service
  - Facilitates the running of interactive admin applications
  - Configured for manual start up by default

Application Access Tokens

- Security context
  - Derived from the current user’s access token
  - By default, UAC treats all as standard users
  - New access token is created when consent is given
  - Most applications run using standard user access token
- Administrator applications
  - Require elevated privileges
  - Can perform tasks that require administrator privileges
  - Can write to system locations of registry and file system
- Standard user applications
  - Do not require elevated privileges
  - Must request elevated privileges to perform administration tasks
  - Write data only to nonsystem locations of registry and file system

Application Run Levels

- Installing and running applications
  - Applications do not require power users group
  - Power users group only for legacy application compatibility
  - Windows Vista detects application installations and prompts users
  - Windows Vista–compliant applications use application manifests
- Application manifests
  - Contain run level designations
  - Define the application’s desired privileges
- Application run levels are
  - RunAsInvoker
  - RunAsHighest
  - RunAsAdmin

Application Integrity Levels

- Windows Vista labels application processes with integrity levels
  - Applications that modify system data are “high” integrity
  - Applications that could compromise operating system are "low" integrity
  - Lower integrity cannot modify data in higher integrity
- Windows Vista uses application categories that
  - Identify the publisher administrator applications
  - Mark the application based on the publisher
- Applications are marked as
  - Being Windows Vista applications
  - Publisher verified (signed) applications
  - Publisher not verified (unsigned) applications

Application Integrity Levels

- Elevation prompts
  - Help identify the potential security risk
  - Display unique messages by application category
- Color-coded Elevation prompts include:
  - Red, a strong warning, representing likely danger.
  - Yellow is a general warning, indicating potential danger
  - Blue/green is for administrative elevation
  - Gray is for general elevation

Configuring Application Security

- Configuring run levels
- Controlling installation
- Configuring run behavior

Configuring Run Levels

- Only applications running with admin access tokens run in elevated mode
- Standard applications can run in elevated mode
- Two ways to set the run level for applications
- You can:
  - Run an application once as an administrator
  - Always run an application as an administrator
- Prompting must be enabled to elevate
- Only nonsystem applications and processes can be marked to always run as an administrator

Controlling Application Installation and Run Behavior

- Configure through
  - Group Policy or local security settings
  - Under Local Policies\Security Options
- Related settings
  - User Account Control: Allow UIAccess Applications To Prompt For Elevation Without Using The Secure Desktop
  - User Account Control: Detect Application Installations And Prompt For Elevation
  - User Account Control: Only Elevate Executables That Are Signed And Validated
  - User Account Control: Only Elevate UIAccess Applications That Are Installed In Secure Locations
  - User Account Control: Virtualize File And Registry Write Failures To Per-User Locations

Windows Vista
Support Architecture:

User Account Control

What we've discussed:

- Elevation prompting, the secure desktop and Admin Approval mode
- File and Registry virtualization
- Application integrity
- Access tokens and run levels
- Related administration tools
- Related Group Policy management settings