User Account Control

Table of Contents

User Account Control ................................................................. 2
User Account Control (UAC) ...................................................... 3
Alerts ...................................................................................... 5
Configuring UAC ................................................................. 7
UAC Configuration Levels -1 ..................................................... 8
UAC Configuration Levels - 2 .................................................. 10
UAC Recommendations ......................................................... 11
Bypassing UAC ...................................................................... 13
Notices ................................................................................ 15
004 Let's start off with user account control.
User Account Control (UAC)

Introduced in Windows Vista and Server 2008 R2

Designed to prevent unauthorized changes

Requests permission or asks for an Administrator password before making changes that affect the computer’s operation or has an impact on other users

**005 When I think about user account control, it’s a-- I’d say it’s a fairly new element given to us from Windows. It showed up in Vista. And what it’s designed to do is prevent any unauthorized changes.

Early on in Vista maybe UAC was a little bit overzealous. And what I mean by overzealous was it seemed that every time we tried to do anything on a Vista machine, we had to get permission from UAC to do it. And so, that was one of the complaints that people had with Vista.
With Windows 7 they've given us that same type of functionality but from a user interface standpoint. It's not nearly as intrusive and obvious to our actions.

So, when we attempt to do something, if we do not have the proper privileges to do it, UAC might basically say you need to elevate your privileges. Do you have the ability to do it? Or they might say you have the privileges. Are you sure you want to do it in this privileged account?

And when does it decide to do this? Basically, UAC is going to kick in any time our behaviors are going to have any kind of impact on the system itself or on other users of that system. If I'm just going to create a file or a directory, UAC doesn't care. I don't impact the system. I don't impact anybody else. But if I'm going to maybe disable a service, UAC says wait a minute. If you disable that service, other people aren't going to be able to use it. And so, we've got to make sure we have that elevated privileges to do that.
**Alerts**

**UAC has four Alerts**

- Windows needs permissions
- A valid (digital signature) program needs permission
- An invalid (no digital signature) program needs permission
- You've been administratively blocked from running the program

**006 When we do something we shouldn't do, or when we do something that UAC is going to be triggered for, there are basically four different types of alerts UAC provides. One it says we need permissions. Windows needs elevated permissions to do this. Or two it might say this program has to have a proper signature. It needs to have a valid digital signature. Or it might say this particular program is trying to run. It does not have a valid digital signature, so you have to explicitly say yes I will allow it to run even though it does not have a valid signature. And then the last time that**
UAC will pop up if we try to do something we've been explicitly blocked from doing.

And I know it is difficult to read, especially in your handouts, but we just give you two examples of those alerts. I'll try to read them, one of them, just so you guys have an idea. This top alert says, "A Windows function or program that can affect other users of this computer needs your permission to start. Check the name of the action to insure it's a function or program you want to run." So, it can affect other people. Are you sure you want to do this?

The second one says a program that's not part of Windows-- so, we're talking about third-party things. It's not part of Windows needs your permission to start. It also goes on to tells that this particular one. It has a valid signature indicating its name and its publisher, which helps to insure the program is what it claims to be. But it then still says make sure that you are intending to run this particular program.

One of the nice things about UAC is the alerts actually have meaning. And the average everyday Joe, when they see those alerts, and they read those alerts, they can make heads or tails of them. Prior to UAC, when we had an issue, we might get an error code, error code twenty-two. What does that mean? So, UAC, the alerts-- I like them because the alerts are much more descriptive. They tell a story about what's going on.
Configuring UAC

**007 Now, we can adjust what level of-- what types of alerts UAC is going to give us. So, to open up the user account control, we go to the start menu. From there, we select control panel. And under the control panel, we have the search window. So, we type in that search window UAC. And it's going to populate and tell us here's the user account control settings window. Click on that.

So, obviously the highest setting is going to be the most interference, if you will, from user account control. And then the lowest setting is the one that says UAC, I don't want you to notify me at all.
Most of the time, most individuals will set it to one of the two intermediate locations.

And just as a side note, the default is this middle to high range for Windows 7. I don’t remember what it is for Windows 8 off the top of my head, but I think it’s probably going to be the same.

**UAC Configuration Levels -1**

<table>
<thead>
<tr>
<th>Setting</th>
<th>When Notified</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Notify</td>
<td>▪ Programs attempt to make changes or ▪ Attempts to change windows settings</td>
<td>Secure Desktop – Desktop is dimmed. User is prevented from doing anything else until the dialog box is addressed.</td>
<td>Most secure</td>
</tr>
<tr>
<td>Notify only when programs try to make changes</td>
<td>▪ Programs try to make changes ▪ Programs outside of windows attempt to change Windows settings ▪ NOT notified if Windows attempts to change settings</td>
<td>Secure Desktop – Desktop is dimmed. User is prevented from doing anything else until the dialog box is addressed.</td>
<td>Usually safe. However, malicious programs may be able to pass commands or data to Windows programs.</td>
</tr>
</tbody>
</table>

**008 So, what do each of those settings mean?** If we say always notify, as its name implies, it’s going to tell us everything. So, any time a program attempts to make a change, or we try to adjust Windows settings,
it’s going to notify us. This is considered to be the most secure.

Notice the description. It says it gives us that secure desktop. Remember what a secure desktop is? It’s where we get that window that everything else is grayed out, if you will. I don’t have any access. And I must address the UAC message. I have to either say yes I’ll do this, or no I’m not going to do this, or provide whatever credentials are requested, or cancel, cancel the action. I can’t do anything when I’m in this most secure state.

The next level down is notify only when programs try to make changes. So, they give you an example. What types of changes? If a program that’s not a Windows based program, for example, tries to modify Windows settings. So, you might try to install antivirus programming. It might try to modify something in your registry. And we would get a message.

And notice, again, that this is the secure desktop. I said this is the default. And it’s the recommended minimum level if you want to try to prevent malicious applications from making changes to your system.
# UAC Configuration Levels - 2

## UAC Configuration Levels - 2

<table>
<thead>
<tr>
<th>Setting</th>
<th>When Notified</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify only when programs try to make changes</td>
<td>Same as above except the Secure Desktop is not used</td>
<td>Does not use the Secure Desktop. Programs may be able to interfere with the dialog box.</td>
<td>- Programs may be able to interfere with the dialog box.</td>
</tr>
<tr>
<td>(do not dim desktop)</td>
<td></td>
<td></td>
<td>- Dangerous if malicious programs already exist on the computer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Never notify</td>
<td>▪ If logged on as Administrator, no notification happens</td>
<td>UAC is turned off.</td>
<td>Least Secure – Programs have the same access as the logged on user</td>
</tr>
<tr>
<td></td>
<td>▪ If logged on as a standard user, changes requiring administrator privileges are automatically denied</td>
<td>When logged on as Administrator, all tasks are completed with Administrator privileges.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Requires computer restart because UAC is being disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**009** The two lower levels, steer away from them, if at all possible. The second from the bottom, notify only when programs try to make changes. And when we do this, now my alert does not dim my desktop. The secure desktop is not being used. So, even with that alert up, I can still do other things. So, I don’t have to address the UAC message right away.

And in the bottom one, never notify, basically, UAC is turned off. There is a note when you’re logged on as administrator. All tasks are completed with administrator privileges. So, do we really want to turn UAC off if all
tasks are going to be done with administrator privileges? I don't know. It's considered to be the least secure. So, you have your choices for what you going to do.

UAC Recommendations

UAC Recommendations

Do NOT disable UAC.

UAC slider setting should be derived from Group Policy.

Use standard user accounts (with few exceptions).

Every user should have their own separate standard user account.

Configure UAC Group Policy appropriately for your environment.


**010 Don't disable it completely.**
Don't turn it off completely. If you do turn it off completely, maybe consider turning off only for a short period of time. You have a specific task that you want to try to accomplish. UAC seems like it might be interfering with what you're trying to accomplish. Turn it off. Do the task. Turn it back on again. That would probably be the best recommendation.
I would also suggest that if you're going to do that, maybe if it's really a task that UAC is interfere with, maybe I'm going to try this in a lab environment first, rather than in a production environment. Try it in the lab and see what happens, see what adverse effects we have.

I also say where's that setting going to be? It should not be an arbitrary setting. Your organizational policy should define where we want that setting to be. And we can use group policy to push that out to all the systems within our organization so that we have a consistent baseline for the settings for all machines. I don't have to do it manually.

Standard accounts are used. That's a basic recommendation for all Windows systems. Use your average, everyday, Joe user account. Don't use elevated privileges unless you absolutely have to.
Bypassing UAC

Easiest way for UAC to be bypassed is when users disable UAC.

- Social engineering

UAC Trust Shortcut

- Turn off UAC for a specific application
- www.itknowledge24.com

Exploits also can bypass it

- MS11-011 - WinAPI


**011 So, a couple of basic recommendations. Now bypassing UAC, I just told you that we can turn UAC off. That's one of the classic ways that bad guys get malware on your system. They might send an email. They might pick up a telephone. They might even have something posted on their website.

Have you ever tried to download and install an application? And when you download and install the application, on the website it gives you the instructions. I love it when it says you will get this alert. Just say okay. Most people just, "Oh, if the instructions
tell me to do it, I should follow the
instructions. I can blindly go there
because somebody told me it's okay."

Well, that's effectively what they're
saying happens here. There might be
the-- hey, this is Bob from the help
desk. We're trying to accomplish such
and such a task on your computer
system. We would like you to disable
user account control. And they might
even give you some legitimate
reason, blow a little bit of smoke
about why it's not a big deal to
disable this. So, they get the Joe user
to disable user account control while
they install their malicious
application.

They talk about the trusted short cut.
Again, the applications, you might
want to install an application. And
when you click on that application to
do the install, that installer might go
in and let's temporarily disable UAC
while we do the install.

So, they talk about one particular
exploit. It's listed up there. We didn't
show you exactly, but an exploit that
takes advantage of bypassing UAC,
user account control.
Notices

© 2014 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.