

Enforcing No Internet or E-mail from Privileged Accounts

Browsing the Internet or reading e-mail with admin, root, or other elevated privileges is a **very serious security risk!** Malicious websites, e-mails, and e-mail attachments can quickly make use of the elevated privileges to install malware throughout the network.

Limit Use of Administrator Account

Often the computer systems on a network are configured with only administrator accounts, and these high-privileged accounts are used for everything. This is usually done for practical reasons, but it is a definite security risk.

A non-privileged “user” account should be created and used for most of the activities conducted on a computer, including web browsing and e-mail access. The high-privileged administrator account should only be used when absolutely needed, such as to install software or reconfigure the system.

Many users may never need to use these elevated privileges. These users should not be given the password to the administrator account so that they do all their work in their non-privileged accounts. Those users that do need elevated privileges should have access to both accounts, but should do most of their work (including browsing and reading e-mail) in their non-privileged accounts and only log onto their high-privileged accounts when needed. This is a significantly more secure approach, and can prevent user mistakes and help to secure other applications as well.

- A user may not need to directly log onto his high-privileged account to do occasional high-privilege actions. High-privilege actions can be executed from a non-privileged account by using runas (Windows command line) or sudo (Unix/Linux).
 - In Windows XP, applications can be run as administrator by right-clicking, selecting “Run as ...”, and then providing the administrator name and password. In Windows Vista and Windows 7, applications can be run as administrator by right clicking, selecting “Run as administrator”, and then providing the administrator password. (In either case, holding down the SHIFT key may be required for the menu option to appear.)
 - **Note that there is a potential danger here.** If the non-privileged account is infected with a software key logger, then the key logger will capture the administrator password

when it is typed in. The only way to mitigate this threat on Windows XP is for the user to actually log off and then log back on as administrator. However on Windows Vista and Windows 7, this threat can be mitigated by requiring CTRL-ALT-DEL prior to entering the password. CTRL-ALT-DEL invokes the Secure Desktop which works with User Account Control (UAC) to provide a safer environment in which to enter the password, thus making it far more difficult for user-level key loggers to intercept credentials. Requiring CTRL-ALT-DEL can be set through Group Policy by enabling:

```
Computer Configuration / Administrative
Templates / Windows Components /
Credential User Interface / Require
Trusted Path for Credentials Entry
```

Note that despite this potential danger and even without using these mitigations, limiting the use of high-privileged accounts is still significantly more secure than running as administrator all the time.

Enforce Limited Use of Administrator Account

Unfortunately, if a user has a high-privileged account available to him, it becomes difficult to enforce that the user does all of his Internet and e-mail access from his non-privileged account. Some enforcement options:

- **Restrict Applications:** On Windows, Software Restriction Policies (or AppLocker on Windows 7) can be used to prevent high-privileged users from launching web browsers and e-mail readers. Since getting around this setting requires a user to actively disable or circumvent the policy, it provides justification for administrative action against any user who is found to be violating the policy.
- **Prevent Admin Log On:** Prevent a user from directly logging onto his high-privileged account by a logon script on the high-privileged account that immediately calls logoff. In this case, the user can only log onto his non-privileged account and he must run any high-privilege things by using “Run as” or sudo, as described above. (But note the potential danger described there.)
 - Note that if there are tasks that the user must do or applications that the user must run that do not work via “Run as” or sudo, then this method cannot be used.



The Information Assurance Mission at NSA

- All sudo accesses are logged. This allows checking for any misuse of the command.
- On Windows, there is a Group Policy setting to “Deny logon locally” for selected accounts. This policy setting cannot be used to deny local logon to administrators because “Run as” is treated as a local logon

• **Prevent Browser Internet Access:** In the high-privileged account, set the browser proxy to 127.0.0.1 (localhost). This will prevent the browser from accessing the Internet with elevated privileges. Note that this only applies to the browser and is really only a reminder, because the browser proxy can easily be changed by the high-privileged user.

- For Internet Explorer on Windows, this can be set through Group Policy. As a bonus, if this policy is set on the domain, then Internet Explorer’s proxy cannot be changed locally even by a high-privileged user (the field will be grayed out).

User Configuration / Policies /
Windows Settings / Internet Explorer
Maintenance / Connection / Proxy
Settings

- **Prevent Internet Access:** In Windows Active Directory, all high-privileged users can be put into a separate Organizational Unit (OU) and the Active Directory-aware web proxy can be set to not allow that OU access to the Internet.
- **Disable E-mail:** Do not enable e-mail for the high-privileged accounts. As long as an administrator has multiple accounts, there is no need for any but the non-privileged account to have a mailbox.
- Additionally, a script can be set up to periodically gather a list of running processes to determine whether any browsers or e-mail readers are running with high privileges.

Run More Safely in Administrator Account

There are serious risks associated with allowing a user to run as a high-privileged administrator all the time. That said, if a user truly needs this level of privilege and the organization is willing to accept the risks, the user’s browser and e-mail reader should be set up to run more safely within the administrator account. This can be done by running them in a sandbox or

virtual machine (VM). Sandboxing and running in a VM can keep malware contained and protect the host computer.

On Windows, consider options to run applications without elevated privileges even in the administrator account:

- Beginning with Windows Vista, Internet Explorer 7 and later versions run in a restricted privilege mode known as Protected Mode. Protected Mode is turned on by default in the Internet, Intranet, and Restricted sites zones. “Protected Mode: On” will appear on the IE status bar to show that it is turned on.
- On Windows XP, Software Restriction Policies can be used to force applications to run as “Basic User”; see <http://www.windowsitpro.com/article/internet/secure-your-desktops-using-srps-hidden-security-levels>.
- Alternatively on Windows XP, the free DropMyRights program from Microsoft can be used; see <http://msdn.microsoft.com/en-us/library/ms972827.aspx>.

Also consider using web browsers and document readers with sandboxing capabilities. Several currently available third-party browsers now provide sandboxing capability. Several commercial and open source PDF readers also provide sandboxing capability as well as block execution of embedded URLs by default, so PDF documents received as e-mail attachments can be read more safely.

Separate Networks

In the extreme case where the security risk from malicious content on the Internet and in e-mail cannot be tolerated, establish completely separate networks: Internet-connected vs. internal. Users that need elevated privileges for their daily activities (such as the internal application developers) will use internal network machines for those activities. All browsing and external e-mail is done from separate machines on the Internet-connected network. Users on these Internet-connected machines should still use non-privileged accounts, as described previously.

This setup can dramatically reduce the risk to the internal network. However, it may be costly in terms of infrastructure, and it will make useful file transfers from the Internet to the internal network very difficult (for example, the developers looking for sample code on the Internet).



The Information Assurance Mission at NSA

The Mitigations Group

“One Voice”

www.nsa.gov/mitigations

OneVoice@radium.nesc.mil

Creative Imaging 49635JRS

AUGUST 2011