



SECURE MANAGEMENT SYSTEMS

SUPPORTING WINDOWS UAC IN THE ENTERPRISE

Gartner highlight, in their “Five High Impact IT Security Risks”, the power of having locked down PC’s as part of an enterprises security regime. They strongly advise the need to enforce Least Privilege for access rights. This approach assumes even more importance for Enterprises when planning migration of their IT infrastructure to Windows 7. Secure Management Systems (SMS) proven products provide a cost effective approach to managing Microsoft’s User Access Control (UAC) within large enterprises, providing a secure method of protecting Least Privilege policies without the need for high levels of desk side support and avoiding the operational flexibility limitations often experienced in operating in a least privilege environment.

Few enterprises today manage Least Privileges solutions effectively, incurring extra costs, reduced security, reduced effectiveness of operational support and in migration to Windows7, higher management costs. Typically Large Enterprise would incur additional help desk costs in excess of £250K a year (based on an enterprise with 10,000 desktops) to support an effective least privilege management model. This cost could be much reduced using the SMS Elevation Management System (EMS). An additional benefit of the SMS software is the facility it brings in enabling legacy applications in a Windows XP environment to function in the Windows 7 without the need for virtualisation. A large Enterprise could typically save many hundreds of thousands of pounds by using our software to avoid the need to procure legacy application upgrades or additional infrastructure when migrating to a Windows 7 environment. In summary for enterprises contemplating migration to a Windows 7 environment, SMS provides a unique approach to managing Least Privilege environments within Microsoft UAC as well as facilitating the continued effective operation of legacy applications.

Why is Least Privilege operation important? Analysis of security bulletins from Microsoft indicates that 92% of the critical vulnerabilities could have been mitigated by the principle of the least privilege embodied in UAC, i.e. the removal of administrator rights of desktop users. Some key points from Microsoft bulletins:

- 92% of Critical Microsoft vulnerabilities are mitigated by configuring users to operate without administrator rights
- Of the total published Microsoft vulnerabilities, 69% are mitigated by removing administrator rights
- By removing administrator rights, companies will be better protected against exploitation of 94% of Microsoft Office, 89% of Internet Explorer, and 53% of Microsoft Windows vulnerabilities
- 87% of vulnerabilities categorized as Remote Code Execution vulnerabilities are mitigated by removing administrator rights

Windows 7 provides more ways than ever to ensure a safe secure computing environment. With the introduction of User Account Control (UAC) Microsoft provides more control for network administrators to ease users into running with standard user accounts. When UAC is enabled it prevents users from making system level changes without an administrator’s approval. This better secures desktops from drive-by malware attacks taking advantage of users Administrative rights, but also simplifies the process for administrators to authorize behaviours that they know to be safe. However if enterprises are to make use of UAC effectively they need assistance. A Large International accountancy firm with some 10,000 desktops, has integrated our Elevation Management Software into their IT management. They achieved the following benefits:

- Reduced direct costs of managing large numbers of computers and the threat and consequent costs of security failures (saved 4 help desk positions)
- Retained the immense security benefits provided by Windows UAC, while still being able to provide timely support in a secure manner.
- Ensured that remote and travelling users are still secured with UAC but allowing them to receive the same high level of support as static users.



- Reduced desk side visits by support personnel by allowing users to be given the required access. This can be further enhanced by allowing users to self-serve qualified applications.
- Greatly reduced the development time of Enterprise implementations of Windows 7.
- Reduced migration and computing costs of migrating legacy applications. Windows 7 UAC prevents many of the legacy systems from running under UAC. Applications that have been written to access certain folders on the local hard drive or registry settings under Windows XP will fail to run when UAC is enabled. With our EMS this problem can be overcome, saving substantially on legacy applications costs.
- Provided a clear audit trail of all activities surrounding applications in use by users.

The SMS Product Set

The SMS solution has already been adopted by an international accountancy firm with 10,000 users in the UK. It allows a central resource to provide access to an application in elevated form when needed without providing any administrator rights to the user or UAC prompts.

To provide access a central system is used to grant a licence key that allows access under the following conditions:

1. A single user or group of users
2. On one computer or a group of computers
3. For a specific period of time

Flexible usage

Licences are generated by a helpdesk operator or a self-service system from a central intranet system depending on client requirements.

Access to elevated processes on a client can be started by entering the licence key into a small application or clicking on a special shortcut.

Client organisations have the ability to manage the applications elevated by the system. In addition to standard Windows processes, they can add their own line of business applications.

Security

All functions within the entire system have been designed with full security as a requirement. All data communicated through the system is fully encrypted and all processes are tightly controlled by Windows security.

Auditing

Every action performed by the system is audited and communicated back to a central server for checking. This data is then made available through the central administration system for reporting purposes.

Sometimes Connected

The entire system has been designed to work in a 'sometimes connected' environment where travelling laptop users are fully supported when working in the field. The users are still able to use the elevation processes they are authorised to perform.

New access can still be granted when disconnected and all usage data is stored in a local, fully encrypted, cache. The cached data is automatically uploaded once the computer is reconnected to the organisation's network.



Security Scenarios

Scenario 1 - Malware Protection

By implementing the “least privilege” security model, a company can prevent their end users from inadvertently introducing a wide range of Malware into the company’s systems. With Windows UAC switched on to an effective level, users without administrator privileges on their machine simply cannot run the Malware payload with the rights to make damaging changes to the machine.

A simple example would be an executable file distributed as an attachment via some form of email and the user opens the attachment unknowing of the potential dangers contained. With the “least privilege” protection of Windows UAC, the operating system would detect a change to the operating system and challenge the end user for an Administrator user account and password. The user would not be able to supply this and so the Malware will be stopped in its tracks.

Scenario 2 - Mobile workers

The IT Manager of a large firm of auditors was under pressure to migrate to Windows 7 so staff could realise the benefits of the new system. Approximately 100 members of staff carry out on-site audits for customers and were used to linking in to their client company’s IT system, check and upload data using their laptops. Windows 7 was installed shortly before a large contract with a long-standing, key customer was about to begin. The project had a tight deadline. The mobile team quickly realised that they couldn’t connect to the network as before. Unfortunately, key senior members of the IT team were off sick and it took six hours for the IT team to work out what had happened. Meanwhile time that could have been charged to the client was being lost and the IT helpdesk was being bombarded with calls from frustrated members of staff.

The only solution to the problem was to give administrator passwords to the mobile team. This presented major security problems to the company and the client and allowed staff to download data to USB drives and install unauthorised software. Questions were raised about the delay to the project which meant the deadline was missed. When the reasons for the delay were explained, the IT Director had to report formally to the board and was fired for seriously compromising the security of the company and the customer.

Scenario 3 - Fraud

A large telecoms company with a call centre in India installed Windows 7 to enhance its data security. The IT team was not aware that the work of its mobile users would be affected. It was essential that the mobile team was able to continue to visit clients otherwise the company faced huge losses in revenue. Knowing that staff in the call centre were poorly paid, a criminal gang had approached one worker and offered payment for the customers banking details and other data.

When the IT team gave administrator rights to all members of the call centre team, the corrupt member of staff simply plugged into the USB drive and was able to copy data belonging to 5,000 customers.

If you would like to discuss EMS further please contact:

Secure Management Systems Ltd
Email: info@securemanagementsystems.com

Secure Management Systems Ltd.
Enterprise Centre
Spelthorne Civic Offices
Knowle Green
Staines TW18 1XB Telephone: 05601 290242

www.securemanagementsystems.com