adaptiva

SCCM Security Best Practices

Table of Contents

Introduction

In 2015, an IBM-sponsored survey pegged the average cost of a data breach at $4 million.

A single security breach can turn a company's fortunes overnight. In 2015, an IBM-sponsored survey pegged the average cost of a data breach at $4 million. Every year, more major attacks are reported than the year before. IT security isn't just a problem—it's a global crisis. Microsoft System Center Configuration Manager (SCCM) administrators are at the heart of the solution.

SCCM keeps anti-virus, malware, and other security software up to date and configured correctly. SCCM delivers and applies security patches and fixes to operating systems and applications in a timely manner. It makes sure that only authorized staff get sensitive applications, and only authorized computers are on the network. SCCM is a first responder in the unfortunate event of a security breach, reporting on the problem and delivering remediation to thousands of endpoints.

The 20 best practices in this document are a good starting point for administrators to see if they are covering some key SCCM security essentials. They are numbered for ease of reference only—the most important security best practices for your environment may be less critical in another organization. Also, it is important to take a good look at the entire SCCM landscape and create a security strategy that fits your organization. SCCM does a lot more than manage endpoints, it keeps your company safe.

1. Restrict and Review SCCM Administrative Users

Review administrative user assignments regularly.

If somebody with malicious intent has access to even a fraction of the power a full SCCM administer possesses, they can wreak havoc on thousands of endpoint systems and Active Directory (AD) itself. For example, they could install malware, change security settings, or wipe hard disks. They could configure rapid polling cycles and huge amounts of inventory to create denial of service attacks. They could overwrite a particular site's AD data with another's. The list is almost endless.

For this reason, it is critical to: (1) restrict administrative users to the least privileges possible using role-based security and least privilege management (LPM), (2) carefully vet all new administrators with a background check, (3) review administrative user assignments regularly, and (4) audit administrator activity by reviewing audit logs periodically.

It is important to treat the possibility of internal breaches as a serious, ongoing threat. It may not be convenient, but it is critical.

2. Restrict Local Administration and Storage Access

If you fail to lock down administrative access to the local file system on endpoints, or do not properly maintain LPM on the ACL/NTFS permissions, you expose your organization to a variety of vulnerabilities. For example, an SCCM package containing a VB script that is stored locally in the SCCM cache can be modified with malicious script content, and re-run on the client. The script would run under the context of the SCCM client and have full system permissions.

By default, the SCCM cache gives full privileges only to the local admin, and it is restricted by User Account Control (UAC) as well. Ensure no broader file system permissions are granted. Ensure that no users are given local the administrative permissions required for access unless they are trusted, vetted, and audited.

3. Do not Install SCCM on a Domain Controller

When you install SCCM on a Domain Controller (DC), you expose all SCCM accounts and permission assignments in AD, increasing the attack surface on your DC. This happens because a DC does not have a local Security Accounts Management (SAM) database, and instead stores local permissions globally in AD.

By installing SCCM on member server, you are able store local SCCM permissions locally, only on the server where they apply. Note that if you install SCCM on a member server and then promote that server to a DC, all local security will be stored globally in AD. So, a corollary best practice is: Do not Promote the Server Running SCCM to a DC.

4. Secure the SCCM SQL Server

SQL Server should be treated as a very high risk access point.

If an attacker gains access to SCCM's back-end SQL Server database, they can launch a global attack on all SCCM-managed endpoints. SQL Server should be treated as very high risk access point, and every effort taken to ensure its security. An entire list of best practices for SQL Server security exceeds the scope of this document and may depend on your environment, so you should work with your DBA. However, two critical SQL Server security best practices are worth noting here: (1) always use Windows Authentication (never Mixed Mode), (2) secure the "sa" account by disabling it, deleting it, or protecting it with a complex password—the default password is the first thing hackers try.

5. Update Secondary Sites Running SQL Express

Running an out of date version of SQL Express can expose your organization to security vulnerabilities as serious as remote code execution. Normally, it goes without saying that all software should be kept up to date, but SCCM administrators must pay special attention to SQL Express because it is easy to overlook and even the initial install could be vulnerable.

SCCM administrators must pay special attention to SQL Express.

When SCCM creates a secondary site, it copies the SQL Express install files from the primary site. Instead of getting the current version of SQL Express, new secondary sites get the version that was current when the primary site was installed, which could be quite out of date. To resolve this, you can update SQL Express after it is installed. Also, you can install the latest version on the secondary site server prior to installing the secondary site, and choose the option to use an existing SQL Server instance.

6. Never Alter Default SCCM Security Groups

If you alter the default security groups in SCCM, you could give attackers visibility into and access to SCCM servers. SCCM automatically creates and manages security groups used for communications between site systems. These are:

- SMS_SiteSystemToSiteServerConnection_MP_<SiteCode>
- SMS_SiteSystemToSiteServerConnection_SMSProv_<SiteCode>
- SSMS_SiteSystemToSiteServerConnection_Stat_<SiteCode>

SCCM uses these groups to ensure business continuity as securely as possible by granting the least privileges required. SCCM expects the group definitions, their uses, and their permissions to be predictable so it can perform automated management such as performing clean-up by removing computer accounts when a site system role is removed. If you change the groups in any way, you could compromise security as well as basic functionality.

7. Configure Static IP Addresses for Site Systems

Microsoft takes a clear stance on the issue for SCCM site servers: use static IP.

In the face of name resolution attacks, servers with static IP addresses are much easier to protect than those with dynamic IP addresses. Also, an attacker who has breached an organization's network perimeter security could plant an unauthorized DHCP server, and route a victim server's traffic wherever it likes. Further, static IP addresses make it easier to configure IPsec and implement third-level firewall rules.

While there is some debate in the global IT community on the question of dynamic vs. static IP addresses for servers, everybody agrees it's a small part of a vastly larger set of security challenges to address. Microsoft takes a clear stance on the issue for SCCM site servers though: use static IP.

There are some additional benefits not related to security. For example, using static IP addresses for servers improves general reliability in the event of a non-malicious DNS failure or problem, since servers with static IP addresses don't depend as immediately on name resolution.

8. Protect the Admin$ Share

If you disable or remove the Admin$ share, the site server will fail. SCCM uses the Admin$ share to connect to and perform service operations on site systems. This is not strictly a security best practice in and of itself, but is worth calling out because some organizations will remove administrative shares such as Admin$ as part of their security policy—even though Microsoft does not recommend it.

Use file system and sharing security best practices such as most restrictive permissions everywhere possible, but leave the Admin$ share in place on SCCM servers.

9. Require Approval for Computers from Untrusted Domains

Never choose the "automatic for all computers" security setting.

If you allow automatic approval of computers from untrusted domains, then attackers can exploit this vulnerability to gain network authority, and use it as a starting point to gain access to critical resources or permissions.

There are three settings for approval: manual, automatic for computers in trusted domains, or automatic for all computers. Never choose the "automatic for all computers" security setting. Choosing manual approval is the most secure, but can create administration overhead and delays in large environments. Automatic for computers in trusted domains is considered secure, as the computer has already undergone the vetting process of a domain join.

10. Remove Security Certificates from OSD Images

If an OS image containing certificates, such as PKI certificates and self-signed certificates, is used to build multiple machines, then those clients would all have the same certificates and might impersonate each other. In that case, you would be unable to verify the data for each client, creating a number of potential security concerns.

The solution is simple, but important: remove security certificates from the reference computer before creating an image for OSD.

11. Use HTTPS for all Supported SCCM Communications

If you fail to encrypt content when transferring it over the intranet, cyber attackers could gather information about your organization's systems, site hierarchy, configurations, applications, etc., that they could use to look for possible vulnerabilities. They could access or even tamper with unencrypted content while it is being delivered. For this reason, HTTPS is recommended for all applicable SCCM traffic.

Some SCCM site systems cannot be configured to use HTTPS for intrasite communication, such as the communication channel between the site server and the package source server. In these cases, it is a best practice to secure the communication in some other way, such as IPSec.

12. Protect .PFX Certificate Files used by SCCM Servers

If you expose a .pfx certificate file, an attacker could use it to get access to the private key, which can open your organization up to a variety of possible exploits. Cyber attackers have a number of tools at their disposal to attempt to extract private keys from .pfx files.

If you expose a .pfx certificate file, an attacker could use it to get access to the private key.

You can protect a .pfx certificate file in a number of ways, including:

- If it is copied to a server, remove it from the server after it is applied.
- If you store the file on the network, secure it carefully and use only secure network channels when importing it into SCCM.
- Use a strong password. This may seem obvious, but is very commonly overlooked.

13. Avoid Deploying the Task Sequence to Unknown Computers

Improperly using the All Unknown Computers collection can allow an attacker with physical access to your premises to create a domain-joined computer. The system could contain a VPN client or expose other ways for them to access the company network and resources. Restrict physical access to the network, and monitor clients to detect unauthorized computers.

Do not deploy to the All Unknown Computers collection

When you take a new machine out of the box, it's a new computer to SCCM. Within SCCM, there are two resources called Unknown Computer x64 and Unknown Computer x86 in an All Unknown Computers collection representing unknown computers. This creates a security risk because any person with physical access to the network can connect a machine, PXE boot, and create a system with a standard company build.

There are several ways to mitigate this risk, and a few key ones are listed below:

- Do not deploy to the All Unknown Computers collection. Instead, whitelist computers for OSD (details provided under "Use PXE Passwords or MAC/ SMBIOS Authorization for OSD").
- If unknown computer support absolutely must be granted, ensure that physical access controls are in place to prevent unauthorized machines from getting on the network and imaging. Also, monitor for unauthorized clients.
- If you are using unknown computers, require PXE password protection.

14. Use System-specific Authorization for OSD

Whitelist computers for OSD.

Allowing any computer on the physical network to get a new OS build without some form of authentication/validation is a security vulnerability. This could allow a system to get built or rebuilt as a brand new company system joined to the domain as well as the SCCM hierarchy.

These risks can be eliminated in different ways, depending on your environment. If you are using zero-touch deployment methodologies, then you can allow deployment only to systems specifically authorized for OSD. The authorization can be done by creating a collection for OSD based on MAC or SMBIOS GUID, importing computers when they are eligible for OSD, and removing them when they have been re-imaged.

Alternatively, you can configure PXE points to require a password for PXE booting. PXE passwords have an added benefit: a well-meaning user cannot accidentally PXE boot and wipe their hard disk. However, PXE password protection has a major drawback because it requires on-site staff to enter the password. For that reason, PXE passwords are not used in zero-touch, high-volume OSD strategies that eliminate the need for at desk visits.

15. Keep Task Sequences Clear of Sensitive Data

If you store sensitive data such as passwords in a Task Sequence, they can be output as clear text at runtime, potentially giving attackers direct access to critical systems. In the task sequence, everything is stored as text. Even passwords that you create as part of the built-in native image can be output at runtime. The OSD process generally will not output values associated with the word *password*, but even that minor check can be easily bypassed. Avoid adding sensitive data such as passwords as plain text in scripts, task sequence variables, or forms.

16. Restrict Physical Access to OSD Media

If an attacker has access to OSD media, they can tamper with it. For example, they can use the DISM tool to open the WIM file and edit it. They could replace content, or add new content, such as Trojan horses.

To mitigate this risk, ensure all physical media used for OS provisioning is stored in a secure location to avoid tampering. Likewise, carefully protect all disk-stored images as well.

Ensure all physical media used for OS provisioning is stored in a secure location.

17. Keep Captured WIM Current with the Latest Security Updates

If you build a computer and security is severely out of date, you leave it vulnerable because an exploit may be run on it before the security updates can be applied. For this reason, it is important to keep the captured WIM updated with all latest security fixes. Maintain the image and/or task sequence with the latest security updates by using offline servicing and/or the Install Software Updates Task Sequence step.

18. Extend the Active Directory Schema

Companies that fail to extend the AD schema in SCCM may expose vulnerabilities by using less secure workarounds for essential systems management functions. For example, a client that is not using AD to find the closest site server could be misdirected to a fake server if an effective alternative security measure is not put in place. If your organization wants to use Network Access Protection, then extending the AD schema is mandatory in order for the System Health Validator point to be able evaluate client statements of health.

Companies that fail to extend the AD schema in SCCM may expose vulnerabilities.

Microsoft began allowing administrators to extend the AD schema for configuration manager data with SCCM 2007. The extensions allow clients and site servers to retrieve many types of important information securely from a known, trusted source. Without the extensions, workarounds such as logon scripts and GPO may be needed. Not only can they be less secure in some cases, they will take up an administrator's valuable free time to build, test, and deploy.

19. Always Log Off Before Killing Remote Sessions

The dangers of leaving a distant computer logged in are grave, potentially giving anybody who happens by the computer complete administrative access to a domain. For this reason, it is important to log out of the system prior to disconnecting the remote control session.

20. Make Time for Security

Establish security metrics on which SCCM administrators' performance is graded.

A common quote from SCCM system administrators on security is, "Oh, yeah, I should do that, but I don't have the time." Security is a trade-off. It can take a lot of time. In return for the time you invest, your company gets a lower risk of catastrophic financial loss due to a breach. However, as many IT professionals can attest, companies rarely reward people just because nothing goes wrong.

To make time for security, companies and managers can:

- Establish security metrics on which SCCM administrators' performance is graded, so that security is given priority and time is allocated along with other tasks.
- Conduct periodic security reviews with the SCCM team so that everybody knows it's important and keeps track of what is being done.

To make time for security, SCCM IT professionals can:

- Clarify any trade-offs that are being made to security when you are asked to do something "superfast." For example, suppose you are asked to complete a three-day project in one day and you would have to shortcut security to do it. Clarify that trade-off to the person who needs the work done so fast and to your manager so that your company can make an informed decision.
- Consider security a career-building skill. Learn everything about it that you can, and put as much into practice as is practical. Security is not going to go away as an issue any time soon. The more you know about it, the higher your value in the marketplace.

Adaptiva OneSite Anywhere, a smart scaling content distribution and management product, can help support your enterprise security needs.

- **Eliminates** hundreds of servers (DPs, PXE points, SMPs), greatly reducing attack surface and potential vulnerabilities.
- **Accelerates** content distribution, providing faster deployments with higher success rates for security fixes, critical updates, and even Windows 10 migrations.
- **Reduces** SCCM administration and management though automation, slashing opportunities for security violations, omissions, and configuration errors.
- **Protects** the network from SCCM traffic—no need to throttle or wait—instantly send massive updates in the middle of a weekday to hundreds of thousands of systems.
- **Ensures** security with FIPS 140-2 compliant encryption, tamperproofing that exceeds NSA Suite B recommendations, and on-disk encryption for SCCM content.

For more information, visit www.adaptiva.com/products/onesite-anywhere.

About Adaptiva

Adaptiva is a leading, global provider of IT systems management solutions for Microsoft System Center Configuration Manager. Founded in 2004 by the lead architect of Microsoft SMS 2003, Adaptiva pioneered the world's first smart scaling peer-to-peer technology for systems management. This technology empowers IT professionals to use automated intelligence, not costly infrastructure, to scale to meet the software and security needs of their business. Adaptiva's suite of smart scaling systems management products include OneSite Anywhere™ for content distribution and management, Client Health™ for endpoint security, troubleshooting, and remediation, and Green Planet™ for energy efficient power management and patching. Adaptiva's software is used by Fortune 500 companies and deployed on millions of devices in over 100 countries. Learn more at www.adaptiva.com.

Contact
info@adaptiva.com
+1 (425) 823-4500

Facebook
Twitter
LinkedIn