Checklist for Security Best Practices

07/12/2011 7 minutes to read

In this article

Recommended Security Configuration

Best Practices for Security Fundamentals

Best Practices for Hierarchy Security

Best Practices for Service Continuity

Best Practices for Securing Communications

Best Practices for Securing Site Systems

Best Practices for Securing Clients

Best Practices for Securing Internet-Based Clients

Best Practices for Securing Name Resolution

Best Practices for Certificate Management

Best Practices for Maintaining Configuration Manager Security

See Also

Applies To: System Center Configuration Manager 2007, System Center Configuration Manager 2007 R2, System Center Configuration Manager 2007 R3, System Center Configuration Manager 2007 SP1, System Center Configuration Manager 2007 SP2

Use this checklist to verify that your Microsoft System Center Configuration Manager 2007 environment conforms to the recommended security best practices. This topic supports and summarizes content in the Security and Privacy for Configuration Manager 2007 section of the Configuration Manager Documentation Library. Before implementing these best practices in your environment, test them thoroughly.

If you are experienced with Configuration Manager 2007 concepts and security procedures, you might be able to work directly from this checklist and use this guide as reference information.

Recommended Security Configuration

Configuration Manager Security and Privacy Planning

□	Use native mode throughout the hierarchy
□	Extend the Active Directory schema for Configuration Manager 2007 and enable Active Directory publishing
□	Do not use workgroup clients or clients in other forests because they cannot query Active Directory
□	Use IPsec to secure communications between site systems.

Best Practices for Security Fundamentals

Best Practices for Security Fundamentals

□	Physically secure your computers
□	Apply the most recent security updates to all computers
□	Protect against unauthorized administrators
□	Enforce role separation to limit administrative exposure
□	Design for defense in depth
□	Create and maintain secure baselines for all systems
□	Use strong passwords or pass phrases
□	Control access to exported files
□	Secure package source files

Best Practices for Hierarchy Security

Best Practices for Hierarchy Security

□	Isolate sites in high security environments
□	Use the fewest sites possible
□	Avoid having sites span forests
□	Require secure key exchange between all sites in the hierarchy
□	In mixed mode, upgrade all clients to Configuration Manager 2007 and configure the site to contain only ConfigMgr 2007 clients
□	Upgrade all sites to Configuration Manager 2007

Best Practices for Service Continuity

Best Practices for Service Continuity

□ Design a fault tolerant site

□ Create a backup and recovery plan

□ Secure your backup media

□ Use role separation to increase recoverability

Best Practices for Securing Communications

Best Practices for Securing Communications

□ Use native mode

□ Require Secure Key Exchange

□ Consider using nondefault port numbers for client communication

□ If clients cannot query Active Directory, manage the trusted root key provisioning process

□ Use IPsec to secure communications between site systems

□ Configure your firewalls to permit required Configuration Manager traffic

□ Secure the communication channel between the site server and package source server

□ Secure the communication channel between the Setup media and the site server

Best Practices for Securing Site Systems

Best Practices for Securing Site Systems

□ Use role separation on site systems

□ Reduce the attack profile

□ Run the Security Configuration Wizard on all site systems, using the Configuration Manager 2007 template

□ Use NTFS for all site systems

□ Do not remove the admin$ share on site systems

□ Closely monitor Internet-based site settings on site systems

□ Configure static IP addresses for site systems

□ Use FQDN server names

□ Do not install other services that use the local system account

Best Practices for Site Server

□ Install Configuration Manager 2007 on a member server instead of a domain controller

□ Install secondary sites at the secondary site server instead of using push installation

Best Practices for SQL Server

□ Use a dedicated SQL Server for each site

□ Do not use the Configuration Manager site database server to run other SQL Server applications

□ Configure SQL Server to use Windows authentication

□ Install Configuration Manager and SQL Server on the same computer

□ Follow security best practices for SQL Server, noting the following issues:

- The site server computer account must be a member of the Administrators group on the computer running SQL Server
- If you install SQL Server using a domain user account, you must ensure that a Service Principal Name (SPN) is populated to Active Directory Domain Services

Best Practices for Site Systems Requiring IIS

□ Disable IIS functions that you do not require

□ Do not put the site server on a computer with IIS

□ Use dedicated IIS servers for Configuration Manager

Best Practices for Management Points

- □ In a single site hierarchy that requires trusted root key authentication, always use a separate management point
- □ If this site system role is configured in a perimeter network, configure the site server to retrieve the data from the site system
- □ Use the fewest management points possible

Best Practices for Fallback Status Point

- □ Do not co-locate any other site system roles with the fallback status point
- □ Do not install the fallback status point on a domain controller
- □ In native mode, deploy the fallback status point prior to deploying clients
- □ Avoid using the fallback status point in the perimeter network

Best Practices for Server Locator Point

- □ Do not put a server locator point in the perimeter network

Best Practices for Securing Clients

The following section applies only to client computers. For information about mobile device clients, see Mobile Device Clients Security Best Practices and Privacy Information. For details about this checklist, see Best Practices for Securing Clients.

Best Practices for Mixed Mode

- □ Automatically approve clients from trusted domains
- □ Do not rely on blocking to prevent clients from accessing the site
- □ Upgrade all clients to Configuration Manager 2007 and select **This site contains only ConfigMgr 2007 clients**

Best Practices for Native Mode

□ Use native mode whenever possible

□ Configure all distribution points to use BITS

□ Do not enable "HTTP communication for roaming and site assignment"

□ Follow the recommended best practices for certificate management

Best Practices for All Client Computers

□ Choose a client installation method that fits your risk profile

□ Remove certificates prior to imaging clients

□ Configure client computers to use Active Directory Only mode

□ Ensure maintenance windows are large enough to deploy critical software updates

Best Practices for Securing Internet-Based Clients

Best Practices for Securing Internet-Based Clients

□ Use SSL bridging to SSL, using termination with authentication

□ Use Active Directory to deploy the site server signing certificate

□ Do not create distribution point shares or branch distribution points on Internet-based clients

□ Do not use site systems that bridge the perimeter network and intranet

Best Practices for Securing Name Resolution

Best Practices for Securing Name Resolution

□ Do not rely on WINS for name resolution

□ Specify FQDNs for all site systems and senders

Best Practices for Certificate Management

Best Practices for Certificate Management

□	Carefully plan for and secure your PKI
□	Follow industry and organizational best practices for certificate management
□	Enable CRL checking on native mode clients
□	Protect the integrity of your client authentication certificates
□	Use a certificate trust list to define the trusted root certification authorities
□	Use Active Directory to deploy the site server signing certificate
□	Guard the security of the site server signing certificate
□	Use a new key pair when renewing the site server signing certificate
□	Verify that all certificates are stored in secure certificate stores

Best Practices for Maintaining Configuration Manager Security

Best Practices for Maintaining Configuration Manager Security

□	Create security policies and adhere to them
□	Use a test lab to test future change configurations for security concerns
□	Secure your test lab
□	Test your backup and recovery procedures
□	Secure your backup media
□	Review your Configuration Manager settings
□	Review audit logs
□	Periodically test Configuration Manager security
□	Develop an incident response plan

□ Secure your internal Configuration Manager documentation

□ Train your organization to follow security best practices

□ Monitor Configuration Manager operations:

- Security rights created, modified, or deleted
- Advertisements created, modified, or deleted
- Packages created, modified, or deleted
- Programs created, modified, or deleted
- Clients that (failed to run) (failed to start) a specific advertised program
- Server component configuration changes
- Client component configuration changes
- Remote tools activity (all)
- Site addresses created, modified or deleted
- Site boundaries created, modified or deleted
- SQL commands created, modified or deleted
- SQL tasks created, modified, or deleted
- All audit status messages (for a specific user) (from a specific site)

See Also

Other Resources

How to Manage the Trusted Root Key in Configuration Manager
Security Best Practices for Configuration Manager
Security Checklists for Configuration Manager
Tasks for Configuration Manager Security

For additional information, see Configuration Manager 2007 Information and Support.
To contact the documentation team, email SMSdocs@microsoft.com.