ISA Server 2004 – Best Practice Analyzer

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how to install and use the ISA Best Practice Analyzer (ISABPA). You can use ISABPA to analyze your ISA Server 2004 environment for security holes, performance problems and configuration mismatches.

Let's begin

The ISA Server Best Practices Analyzer is a diagnostic tool like the well known EXBPA (Exchange Best Practice Analyzer Tool) that automatically performs specific tests on configuration data collected on the local ISA Server 2004 computer from the ISA Server hierarchy of administration COM objects, Windows Management Instrumentation (WMI) classes, the system registry, files on disk, and the Domain Name System (DNS) settings. You can use ISABPA for both ISA Server 2004 Standard and ISA Server 2004 Enterprise.

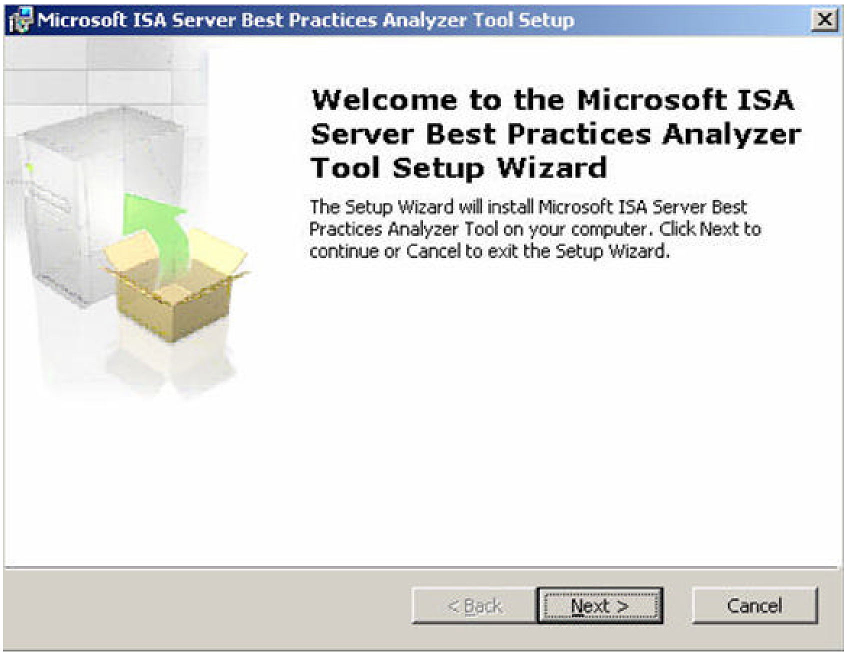
The resulting report details critical configuration issues, potential problems, and information about the ISA Server 2004.

First we need to download the ISA Server 2004 Best Practice Analyzer (ISABPA). After downloading you can install the ISABPA tool following the instructions of the wizard.

Please note: ISABPA requires and installed .NET Framework 1.1.

Installation

Follow the installation instructions of the Microsoft ISA Server Best Practice Analyzer Tool Setup.



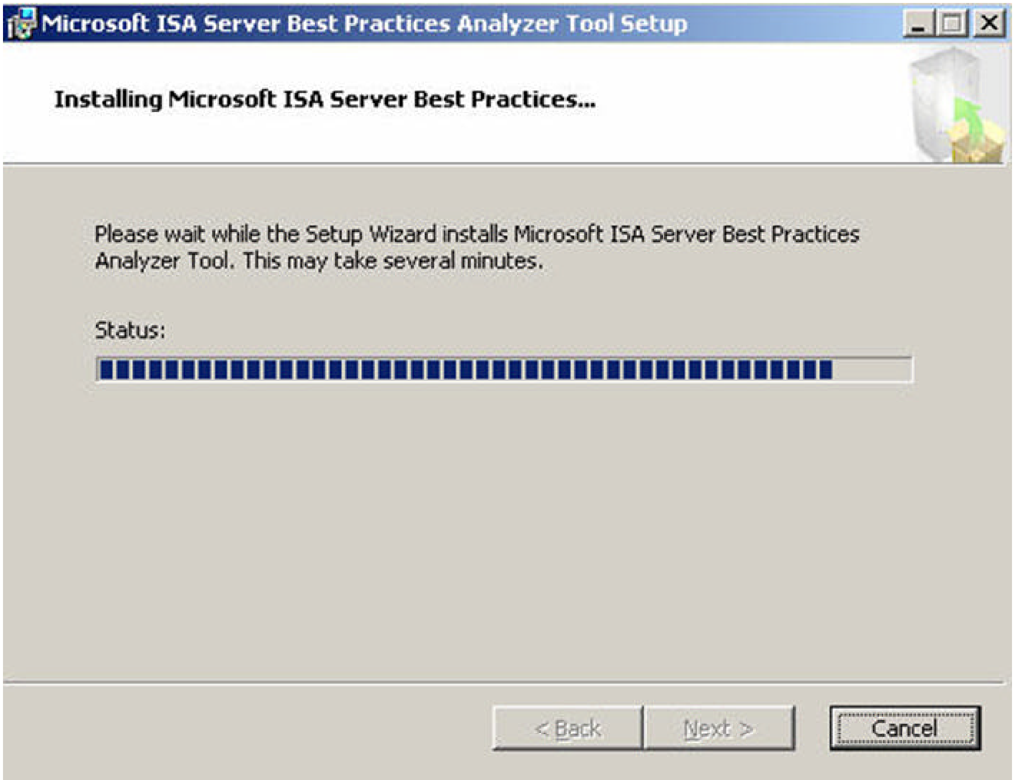
Microsoft ISA Server Best Practices Analyzer Tool Setup

Welcome to the Microsoft ISA Server Best Practices Analyzer Tool Setup Wizard

The Setup Wizard will install Microsoft ISA Server Best Practices Analyzer Tool on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 1: Installation of ISABPA

The installation process takes only some minutes.



Microsoft ISA Server Best Practices Analyzer Tool Setup

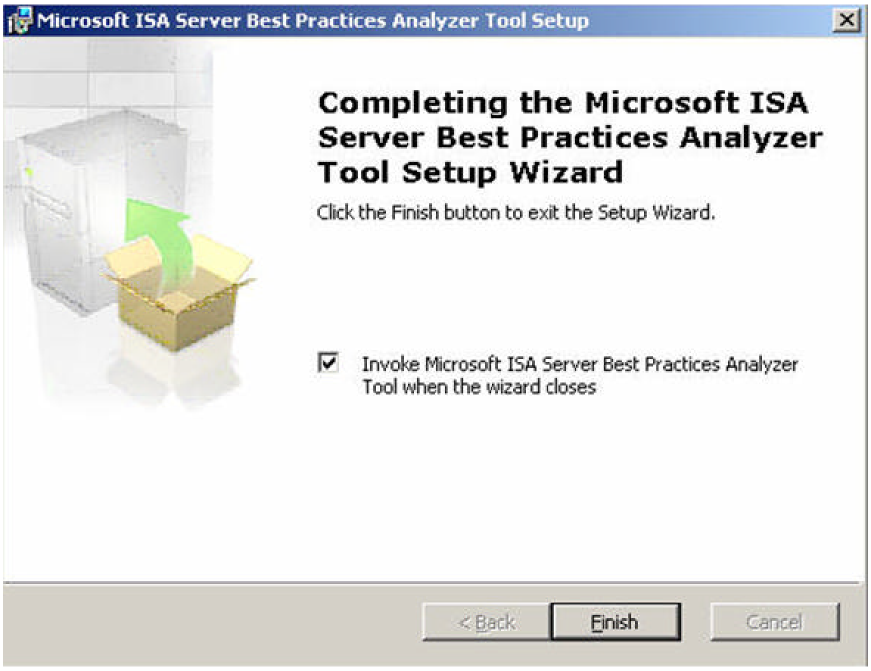
Installing Microsoft ISA Server Best Practices...

Please wait while the Setup Wizard installs Microsoft ISA Server Best Practices Analyzer Tool. This may take several minutes.

Status:

Figure 2: Installation process

After installation ISABPA starts automatically unless you clear the checkbox.



Completing the Microsoft ISA Server Best Practices Analyzer Tool Setup Wizard

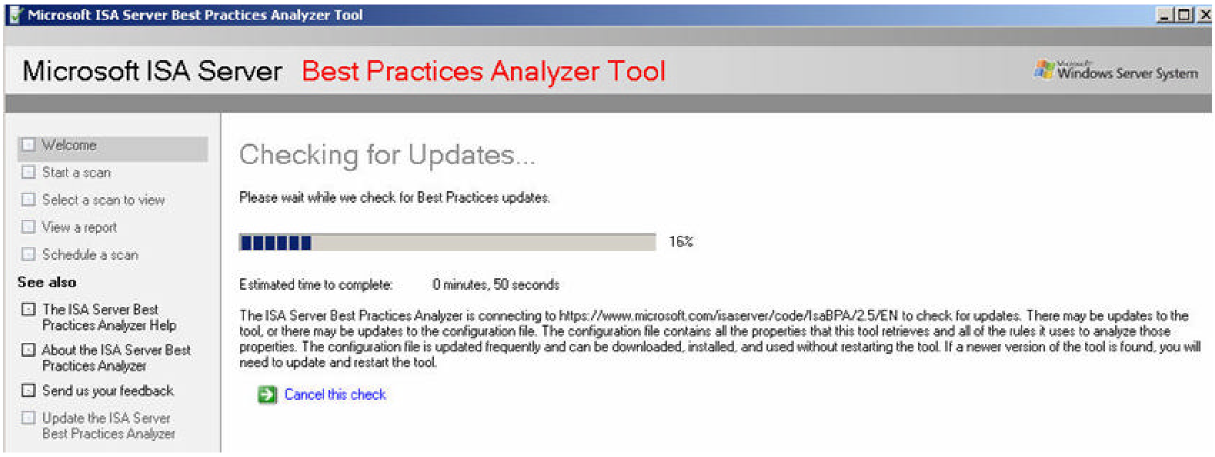
Click the Finish button to exit the Setup Wizard.

☑ Invoke Microsoft ISA Server Best Practices Analyzer Tool when the wizard closes

Figure 3: Launch ISABPA after installation

Updating ISABPA

After installing ISABPA you can start a new Best Practice scan. If you don't have used the ISA Best Practice Analyzer over a long period, it is recommended to look for an update of ISABPAs configuration. To update ISABPA click *Update the ISA Server Best Practice Analyzer* under *See also*.


Microsoft ISA Server Best Practices Analyzer Tool
Microsoft ISA Server Best Practices Analyzer Tool
Windows Server System
□ Welcome
□ Start a scan
□ Select a scan to view
□ View a report
□ Schedule a scan
See also
□ The ISA Server Best Practices Analyzer Help
□ About the ISA Server Best Practices Analyzer
□ Send us your feedback
□ Update the ISA Server Best Practices Analyzer

Checking for Updates...

Please wait while we check for Best Practices updates.

16%

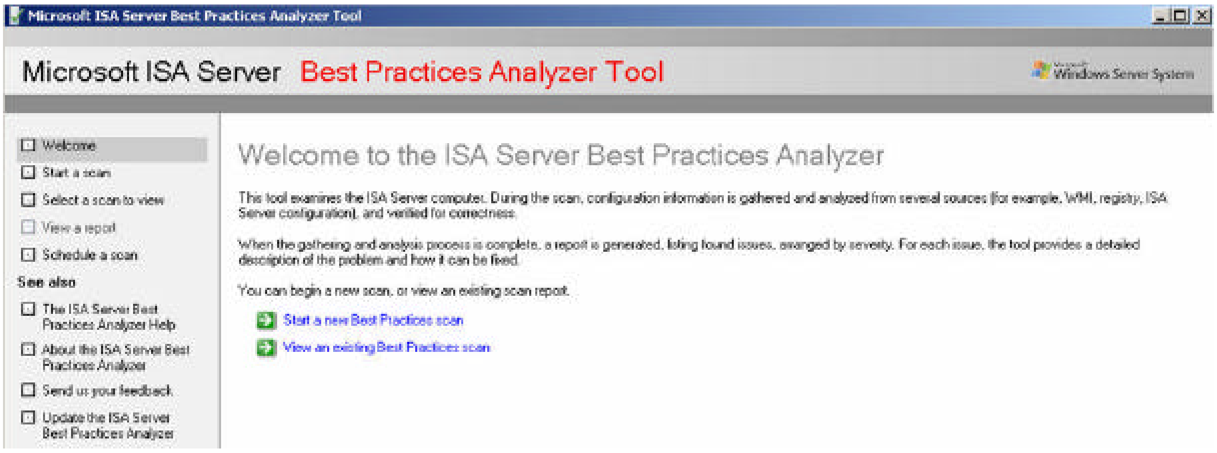
Estimated time to complete: 0 minutes, 50 seconds

The ISA Server Best Practices Analyzer is connecting to https://www.microsoft.com/isaserver/code/IsaBPA/2.5/EN to check for updates. There may be updates to the tool, or there may be updates to the configuration file. The configuration file contains all the properties that this tool retrieves and all of the rules it uses to analyze those properties. The configuration file is updated frequently and can be downloaded, installed, and used without restarting the tool. If a newer version of the tool is found, you will need to update and restart the tool.

Figure 4: Update ISABPA

ISABPA looks for online updates on the Microsoft website. If the update process founds new updates, ISABPA will be updated and the tool will be restarted.

After updating ISABPA you can start a new Best Practice scan by clicking the *Start a new Best Practices scan* button.


Microsoft ISA Server Best Practices Analyzer Tool
Microsoft ISA Server Best Practices Analyzer Tool
Windows Server System
□ Welcome
□ Start a scan
□ Select a scan to view
□ View a report
□ Schedule a scan
See also
□ The ISA Server Best Practices Analyzer Help
□ About the ISA Server Best Practices Analyzer
□ Send us your feedback
□ Update the ISA Server Best Practices Analyzer

Welcome to the ISA Server Best Practices Analyzer

This tool examines the ISA Server computer. During the scan, configuration information is gathered and analyzed from several sources (for example, WMI, registry, ISA Server configuration), and verified for correctness.

When the gathering and analysis process is complete, a report is generated, listing found issues, arranged by severity. For each issue, the tool provides a detailed description of the problem and how it can be fixed.

You can begin a new scan, or view an existing scan report.

Start a new Best Practices scan
View an existing Best Practices scan

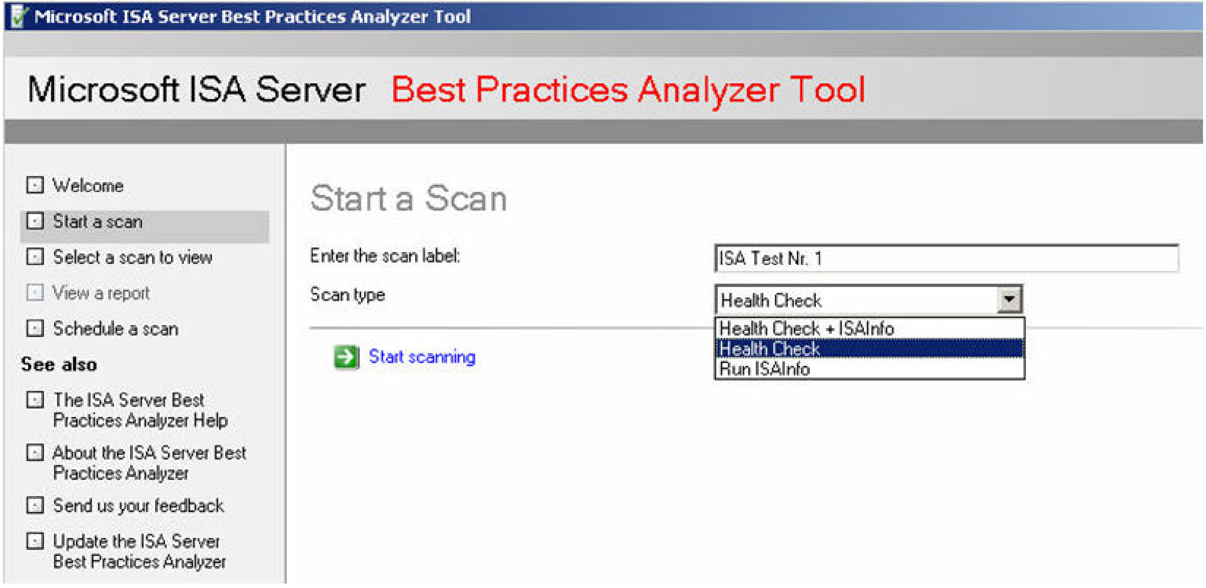
Figure 5: Start a new Best Practice scan

You can choose between three scantypes:

- Health Check + ISAInfo
- Health Check
- Run ISAInfo

The ISABPA health check executes an ISA Server 2004 diagnose based on the configuration file downloaded from the Microsoft website.

Isainfo ist the well known tool to collect information about the ISA Server configuration and to display the configuration settings. You can download ISAInfo as a separate installation from here. ISAInfo is included in the ISA Server Best Practice Analyzer tool.


Microsoft ISA Server Best Practices Analyzer Tool
Microsoft ISA Server Best Practices Analyzer Tool
□ Welcome
□ Start a scan
□ Select a scan to view
□ View a report
□ Schedule a scan
See also
□ The ISA Server Best Practices Analyzer Help
□ About the ISA Server Best Practices Analyzer
□ Send us your feedback
□ Update the ISA Server Best Practices Analyzer

Start a Scan

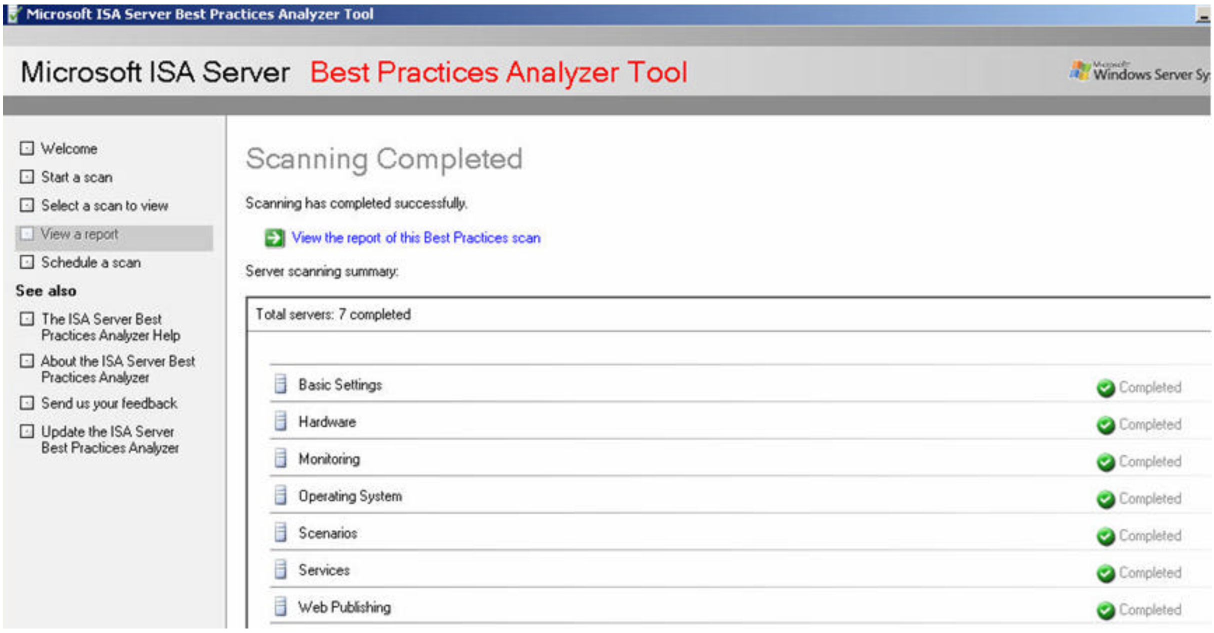
Enter the scan label: ISA Test Nr. 1

Scan type Health Check

Health Check + ISAInfo
Health Check
Run ISAInfo
Start scanning

Figure 6: Start a scan

An ISABPA scan requires only some minutes to execute. After collecting data, you can view the report of this Best Practices Scan.
Click *View the report of this Best Practice scan*.


Microsoft ISA Server Best Practices Analyzer Tool
Microsoft ISA Server Best Practices Analyzer Tool
Windows Server Sy
Welcome
Start a scan
Select a scan to view
View a report
Schedule a scan
See also
The ISA Server Best Practices Analyzer Help
About the ISA Server Best Practices Analyzer
Send us your feedback
Update the ISA Server Best Practices Analyzer
View the report of this Best Practices scan

Scanning Completed

Scanning has completed successfully.

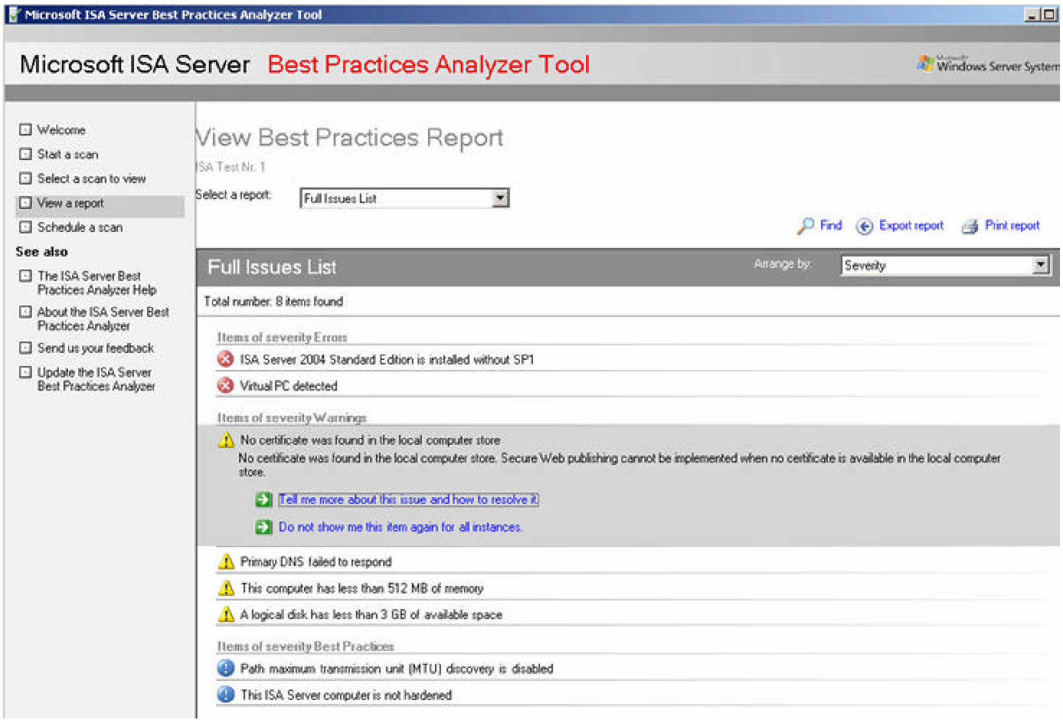
Server scanning summary:

Total servers: 7 completed

Basic Settings	✓ Completed
Hardware	✓ Completed
Monitoring	✓ Completed
Operating System	✓ Completed
Scenarios	✓ Completed
Services	✓ Completed
Web Publishing	✓ Completed

Figure 7: View a best practice scan

For this example I have used an ISA Server 2004 without SP1 running on Microsoft Virtual Server 2005 R2. ISABPA reports that ISA Server 2004 is running on Microsoft Virtual OC which is not correct.


Microsoft ISA Server Best Practices Analyzer Tool
Microsoft ISA Server Best Practices Analyzer Tool
Windows Server System
Welcome
Start a scan
Select a scan to view
View a report
Schedule a scan
See also
The ISA Server Best Practices Analyzer Help
About the ISA Server Best Practices Analyzer
Send us your feedback
Update the ISA Server Best Practices Analyzer
Find
Export report
Print report
Tell me more about this issue and how to resolve it
Do not show me this item again for all instances.

View Best Practices Report

ISA Test Nr. 1

Select a report: Full Issues List

Full Issues List

Arrange by: Severity

Total number: 8 items found

Items of severity Errors

- ISA Server 2004 Standard Edition is installed without SP1
- Virtual PC detected

Items of severity Warnings

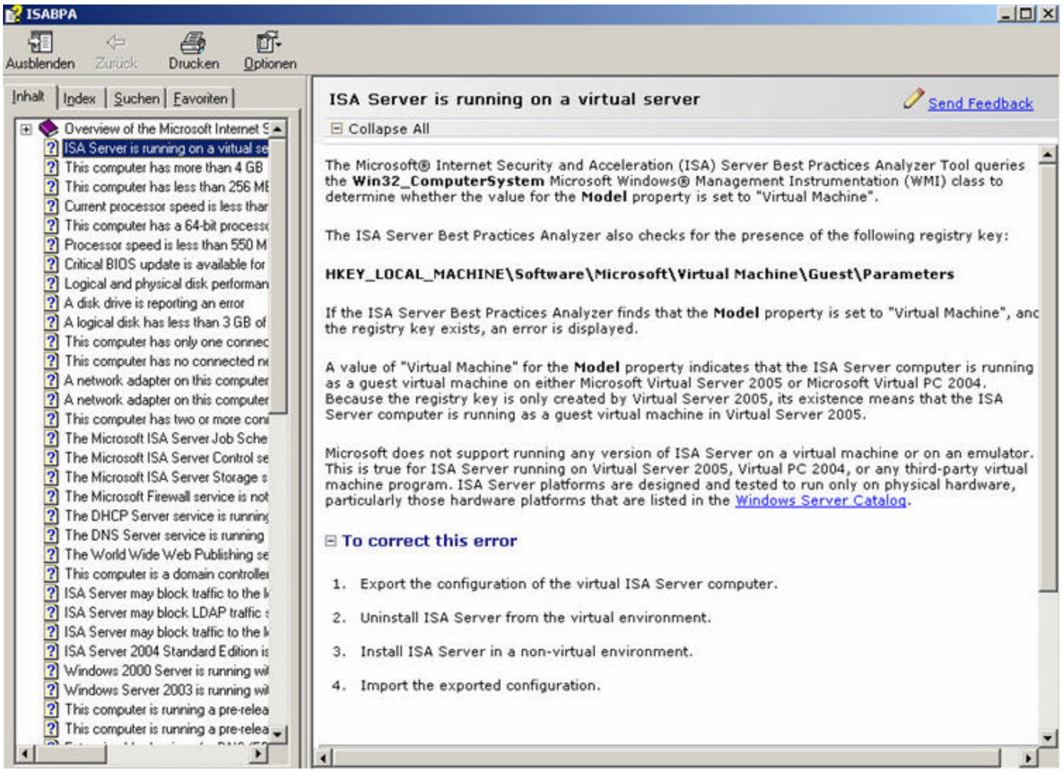
- No certificate was found in the local computer store
  No certificate was found in the local computer store. Secure Web publishing cannot be implemented when no certificate is available in the local computer store.
- Primary DNS failed to respond
- This computer has less than 512 MB of memory
- A logical disk has less than 3 GB of available space

Items of severity Best Practices

- Path maximum transmission unit (MTU) discovery is disabled
- This ISA Server computer is not hardened

Figure 8: Analyze collected information

If you are using ISABPA the first time or if you are an ISA beginner, you should spend some time to read the ISABPA help file which contains several information about ISA Server, the analyzing process of ISABPA and best Practice recommendations.


ISABPA
Ausblenden
Zurück
Drucken
Optionen
Inhalt
Index
Suchen
Favoriten
Overview of the Microsoft Internet S
ISA Server is running on a virtual se
This computer has more than 4 GB
This computer has less than 256 MB
Current processor speed is less than
This computer has a 64-bit process
Processor speed is less than 550 M
Critical BIOS update is available for
Logical and physical disk performan
A disk drive is reporting an error
A logical disk has less than 3 GB of
This computer has only one connec
This computer has no connected ne
A network adapter on this computer
A network adapter on this computer
This computer has two or more conn
The Microsoft ISA Server Job Sche
The Microsoft ISA Server Control se
The Microsoft ISA Server Storage s
The Microsoft Firewall service is not
The DHCP Server service is running
The DNS Server service is running
The World Wide Web Publishing se
This computer is a domain controller
ISA Server may block traffic to the l
ISA Server may block LDAP traffic s
ISA Server may block traffic to the l
ISA Server 2004 Standard Edition is
Windows 2000 Server is running wi
Windows Server 2003 is running wi
This computer is running a pre-relea
This computer is running a pre-relea
Send Feedback
Collapse All

ISA Server is running on a virtual server

The Microsoft® Internet Security and Acceleration (ISA) Server Best Practices Analyzer Tool queries the **Win32_ComputerSystem** Microsoft Windows® Management Instrumentation (WMI) class to determine whether the value for the **Model** property is set to "Virtual Machine".

The ISA Server Best Practices Analyzer also checks for the presence of the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Virtual Machine\Guest\Parameters

If the ISA Server Best Practices Analyzer finds that the **Model** property is set to "Virtual Machine", anc the registry key exists, an error is displayed.

A value of "Virtual Machine" for the **Model** property indicates that the ISA Server computer is running as a guest virtual machine on either Microsoft Virtual Server 2005 or Microsoft Virtual PC 2004. Because the registry key is only created by Virtual Server 2005, its existence means that the ISA Server computer is running as a guest virtual machine in Virtual Server 2005.

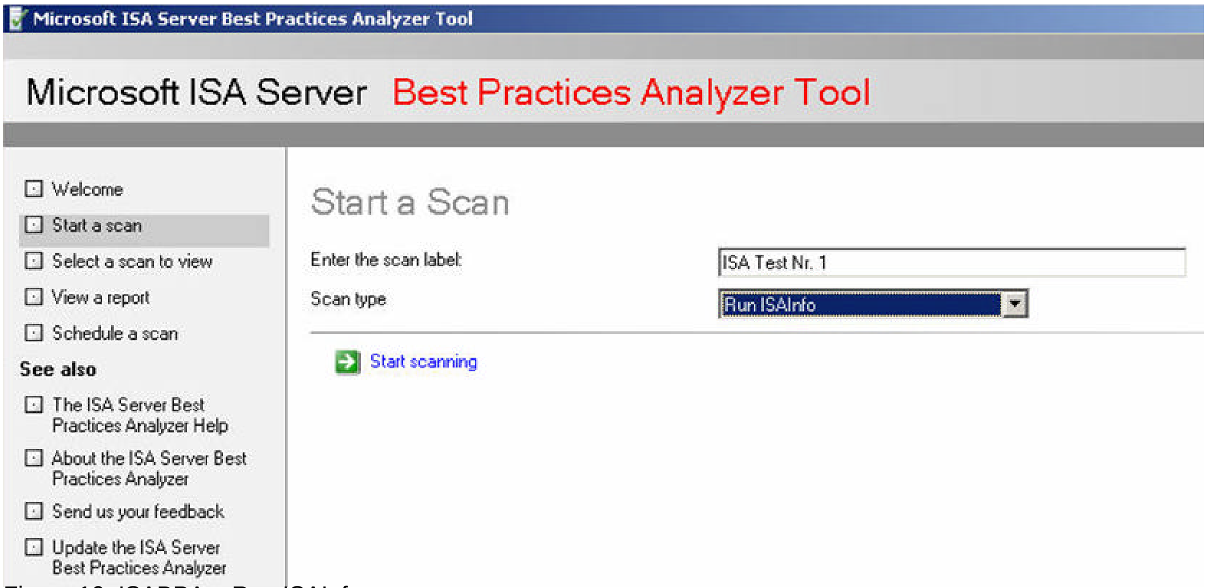
Microsoft does not support running any version of ISA Server on a virtual machine or on an emulator. This is true for ISA Server running on Virtual Server 2005, Virtual PC 2004, or any third-party virtual machine program. ISA Server platforms are designed and tested to run only on physical hardware, particularly those hardware platforms that are listed in the Windows Server Catalog.

To correct this error

1. Export the configuration of the virtual ISA Server computer.
2. Uninstall ISA Server from the virtual environment.
3. Install ISA Server in a non-virtual environment.
4. Import the exported configuration.

Figure 9: ISABPA help file

After executing ISABPAs Health Check you can execute ISAINFO within ISABPA – theoretically. I had tried opening ISAINFO with ISABPA Version 2.5.3439.50 and the configuration file 4.0.3440.277 but I did not succeed. ISAInfo will NOT display informations created by ISABPA. I have tried the ISAINFO option from ISABPA with different ISA Server 2004 Enterprise servers and ISA Server 2004 Standard servers in german and English language but no success.


Microsoft ISA Server Best Practices Analyzer Tool
Microsoft ISA Server Best Practices Analyzer Tool
Welcome
Start a scan
Select a scan to view
View a report
Schedule a scan
See also
The ISA Server Best Practices Analyzer Help
About the ISA Server Best Practices Analyzer
Send us your feedback
Update the ISA Server Best Practices Analyzer
Start scanning

Start a Scan

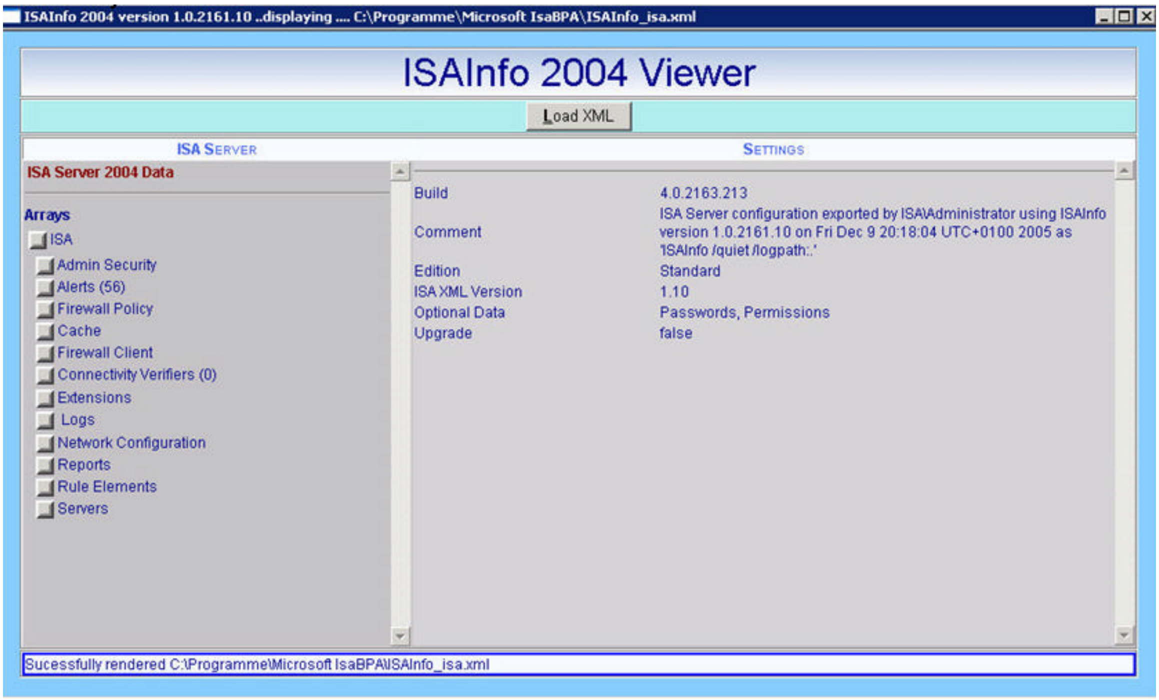
Enter the scan label: ISA Test Nr. 1

Scan type: Run ISAInfo

Figure 10: ISABPA – Run ISAInfo

ISABPA executes the ISAINFO tool correctly. ISAINFO creates an ISAINFO XML-file but this information's will not be displayed in ISABPA. I assume that this is a bug in ISABPA.

To overcome this limitation you can start ISAINFO manually and open the XML file created by ISABPA. You can find the ISAINFO XML file in the ISABPA installation directory.



ISAInfo 2004 version 1.0.2161.10 ..displaying .... C:\Programme\Microsoft IsaBPA\ISAInfo_isa.xml

ISAInfo 2004 Viewer

Load XML

ISA SERVER

ISA Server 2004 Data

Arrays
- ISA
  - Admin Security
  - Alerts (56)
  - Firewall Policy
  - Cache
  - Firewall Client
  - Connectivity Verifiers (0)
  - Extensions
  - Logs
  - Network Configuration
  - Reports
  - Rule Elements
  - Servers

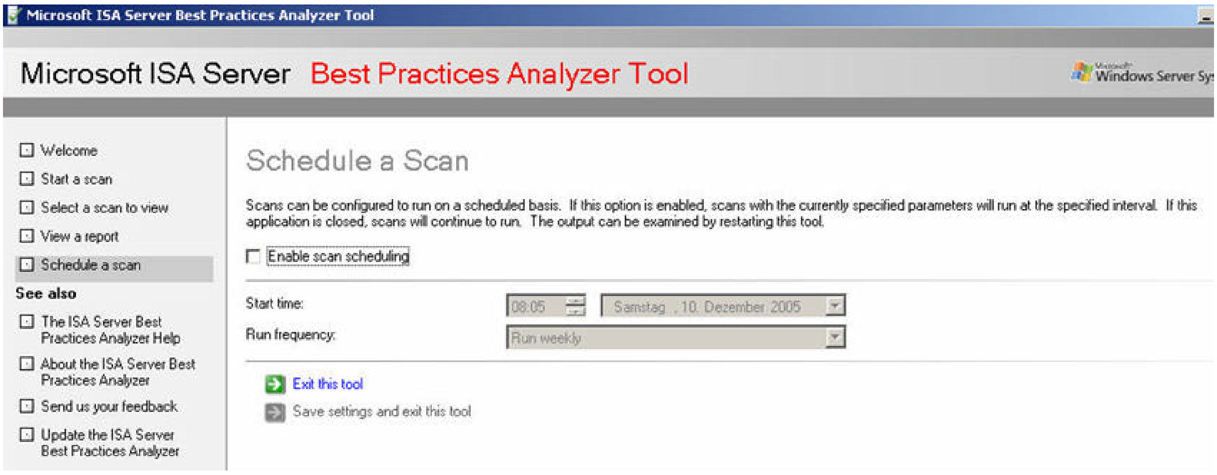
SETTINGS

Build	4.0.2163.213
Comment	ISA Server configuration exported by ISA\Administrator using ISAInfo version 1.0.2161.10 on Fri Dec 9 20:18:04 UTC+0100 2005 as 'ISAInfo /quiet /logpath:.'
Edition	Standard
ISA XML Version	1.10
Optional Data	Passwords, Permissions
Upgrade	false

Sucessfully rendered C:\Programme\Microsoft IsaBPA\ISAInfo_isa.xml

Figure 11: Manually executing ISAINFO

It is possible to automate the execution of ISABPA scans. To enable scheduled scanning click *Schedule a scan* and enable scan scheduling and the start time and run frequency.



Microsoft ISA Server Best Practices Analyzer Tool

Microsoft ISA Server Best Practices Analyzer Tool

Windows Server Sy
Welcome
Start a scan
Select a scan to view
View a report
Schedule a scan
See also
The ISA Server Best Practices Analyzer Help
About the ISA Server Best Practices Analyzer
Send us your feedback
Update the ISA Server Best Practices Analyzer

Schedule a Scan

Scans can be configured to run on a scheduled basis. If this option is enabled, scans with the currently specified parameters will run at the specified interval. If this application is closed, scans will continue to run. The output can be examined by restarting this tool.

☐ Enable scan scheduling

Start time: 08:05 Samstag , 10. Dezember 2005

Run frequency: Run weekly

Figure 12: Scheduling ISABPA scans.

Bugs

- ISABPA reports ISA installed on Virtual Server 2005 R2 as Virtual PC.
- It is not possible to automatically create an ISAInfo Report. ISAInfo will be installed with ISABPA but you must manually execute ISAInfo with the XML file created by ISABPA.
- One guy in the German ISA Server newsgroup posted that ISABPA doesn't listed any installed certificate although it was installed.
- The Link to the ISA Server 2004 Security Hardening Guide is wrong. The correct link is:

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx

I spoke with a member of the ISA Server Product team and they said me that the first bug (wrong report of Virtual PC) and the wrong link will be corrected in a next ISABPA update/version.
ISABPA listed missing certificates only when there is no corresponding private key for this certificate.
For running ISAINFO on ISABPA you have to install the ISAINFO XML Parser which is not included in ISABPA.

Conclusion

In this article I have shown you how to use the ISABPA – ISA Server 2004 Best Practice Analyzer to analyze your existing ISA Server environment to find security holes, performance bottlenecks and configuration mismatches.

Related Links

ISABPA Download
http://www.microsoft.com/downloads/details.aspx?FamilyID=D22EC2B9-4CD3-4BB6-91EC-0829E5F84063&displaylang=en