

Secedit command in Windows

The secdit command helps configure and analyze system security by comparing your current configuration with the specified security patterns.

The **secdit** command helps configure and analyze system security by comparing your current configuration with the specified security patterns.

Syntax secdit command

```
secdit
[/ analyze / db / cfg [/ overwrite] / log [/ quiet]]
[/ configure / db [/ cfg] [/ overwrite] [/ areas [securitypolicy | group_mgmt
[/ export / db [/ mergedpolicy] / cfg [/ areas [securitypolicy | group_mgmt |
[/ generaterollback / db / cfg / rbk [/ log] [/ quiet]]
[/ import / db / cfg [/ overwrite] [/ areas [securitypolicy | group_mgmt | u
[/ h?p l?]
```

The secdit command parameter

Parameter (subcommand)

Describe

Secedit: analyze

Allows you to analyze the current system settings based on the basic settings stored in the database. The analytical results will be stored in a separate area of the database and can be viewed in the attachment of the Security Configuration and Analysis section.

Secedit: configure

Allows you to configure the system with security settings stored in the database.

Secedit: export

Allows you to export security settings stored in the database.

Secedit: generaterollback

Allows you to create rollback patterns for configuration templates.

Secedit: import

Allows you to enter security templates into the database so that the settings specified in the form can be applied to the system or analyzed by the system.

Secedit: validate

Allows you to validate the syntax of the security template.

Note the secedit command

For the filenames parameter, the current directory will be used by default if no path is specified. When a security pattern is created using the Security Template attachment and the attachment of Security Configuration and Analysis is run, the following files will be created:

File

Describe

Scesrv.log

Location: % Windir% securitylog

Created by: Operating system

File type: Text

Refresh rate: Perform overwriting when the sub-command **secedit / analyze, / configure, / export** or **/ import** is started.

Content: Contains analytical results grouped by type of policy.

User-selected name.sdb

Location: % windir% * user accountDocumentsSecurityDatabase

Created by: When running the attachment of Security Configuration and Analysis

File type: Exclusive

Refresh rate: Perform an update whenever a new security template is created.

Content: Includes local security policies and user-created security templates.

User-selected name.log

Location: Can be specified by the user but by default it will be % windir% * user accountDocumentsSecurityLogs

Created by: When running child **/ analyze** commands and **/ configure** (or using the attachment of Security Configuration and Analysis)

File type: Basic

Refresh rate: Override when sub-commands the child / analyze and / configure commands (or use the attachment of the Security Configuration and Analysis) are initialized.

Content included:

1. Log file name
2. Date and time
3. Results of analysis or investigation.

User-selected name.inf

Location: % windir% * user accountDocumentsSecurityTemplates

Created by: When running an attachment of Security Template

File type: Text

Refresh rate: Each time the security template is updated

Content: Contains setting information for the template for each policy selected by the attachment.

Note: Microsoft Management Console (MMC) and the Security Configuration and Analysis attachments are not available on Server Core.

See more:

1. Summary of 20 common Run commands on Windows operating system
2. Summary of shortcuts to know in Windows 10
3. Basic Linux commands everyone needs to know
4. Table summarizes the basic PowerShell commands

You finished reading the article "**Secedit command in Windows**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.