Knowledge Base

HOW TO: Analyze System Security in Windows 2000

PSS ID Number: 313203

Article Last Modified on 11/5/2003

The information in this article applies to:

- Microsoft Windows 2000 Server

This article was previously published under Q313203

IN THIS TASK

SUMMARY

This step-by-step article describes how you can use the Security Configuration and Analysis snap-in to analyze and configure security on a Windows 2000-based computer. This snap-in includes the following components:

- The Security Templates MMC snap-in
- The Security Configuration and Analysis MMC snap-in
- The Secedit.exe command-line tool

You can use the Security Configuration and Analysis MMC snap-in to quickly and easily compare the current security configuration with a security configuration that is stored in a database. You can create a database that contains a preferred level of security, and then run an analysis that compares the current configuration with the settings in the database.

The following two steps are required to analyze a computer's security configuration:

1. Create the security database by using a security template.
2. Run the computer security analysis against the database settings.

back to the top

Creating the Security Database

1. Click **Start**, click **Run**, type `mmc`, and then click **OK**.
2. In the **Console1** console, click **Add/Remove snap-in** on the **Console** menu.
3. In the **Add/Remove Snap-in** dialog box, click **Add**.
4. In the **Add Standalone Snap-in** dialog box, click the **Security Configuration and Analysis** entry, click **Add**, and then click **Close**.
5. In the **Add/Remove Snap-in** dialog box, click **OK**.
6. In the left pane of the console, click the **Security Configuration and Analysis** node. Read the instructions in the right pane of the console.
7. Right-click the **Security Configuration and Analysis** node, and then click **Open Database**.
8. In the **Open Database** dialog box, type `compare_basicwk` in the **File name** box, and then click **Open**.
9. In the **Import Template** dialog box, click the Basicwk.inf template, and then click **Open** to import the entries that are contained in the Basicwk.inf security template into the database. You do not need to click the **Clear this database before importing** option because there are no entries in the database at this time. If the database had been using previously, you can click this option to clear previous entries from the database. Click **Open**.

back to the top

Analyzing System Security

No changes are made to the system when you analyze system security. The results of the security analysis show where there are discrepancies between the settings in the template and the actual system settings.

Use the following steps to compare system security with the settings in the security database:

1. Right-click the **Security Configuration and Analysis** node in the left pane, and then click **Analyze Computer Now**.
2. In the **Perform Analysis** dialog box, note the location of the Error log file path. Note that you can change the path if you want. Click **OK**.
3. The **Analyzing System Security** dialog box shows the configuration analysis steps as they proceed.
4. When the security analysis is complete, expand all nodes in the left pane of the console except for the nodes under **Registry and File System** (these trees are very deep so you might want to look at these last).
5. Look at the entries in the right pane as you click on each of the nodes. Entries with a green check mark indicate that the local system settings are the same as those that are contained in the database. Entries with a red "x" indicate a conflict between the entries in the database and the current system settings. You can see which settings are in the database or the computer configuration by looking at the **Database Setting** and **Computer Setting** columns.
6. If a setting is not contained in the database, a green check mark or a red "x" does not exist. In this case, you can add the setting to the database. Right-click on a setting that is not defined in the database, and then click **Security**.
7. To enter the setting into the database, click to select the **Define this policy in the database** check box, and then define the policy. Click **OK** to enter the policy into the database.
8. After the security analysis, you can apply the database settings to the computer configuration. To save the changes you made to the database, right-click the **Security Configuration and Analysis** node in the left pane, and then click **Save**.

back to the top

Keywords: kbenv kbhowto kbHOWTOmaster KB313203
Technology: kbwin2000Search kbwin2000Serv kbwin2000ServSearch

---