

Authentication Packages - Win32 apps

By GrantMeStrength

Archived: 2026-04-05 20:41:35 UTC

[Authentication packages](#) are contained in dynamic-link libraries. The [Local Security Authority](#) (LSA) loads authentication packages by using configuration information stored in the registry. Loading multiple authentication packages permits the LSA to support multiple logon processes and multiple [security protocols](#).

Logon processes use authentication packages to analyze logon data. New logon processes are added to a system by adding a [GINA](#) to collect the required logon data and, if needed, by adding a new authentication package to analyze the data.

Security protocols are implemented by authentication packages. An authentication package analyzes logon data by following the rules and procedures set forth in a security protocol.

Authentication packages are responsible for the following tasks:

- Analyzing logon data to determine whether a [security principal](#) is allowed to log on to a system.
- Establishing a new [logon session](#) and creating a unique [logon identifier](#) for the successfully authenticated principal.
- Passing security information to the LSA for the principal's security token.

When a user attempts an interactive logon, the LSA calls an authentication package to determine whether to permit the user to log on. MSV1_0, for example, is an authentication package installed with the Microsoft Windows operating system. The MSV1_0 package accepts a user name and a [hashed](#) password. It looks up the user name and hashed password combination in the Security Accounts Manager (SAM) database. If the logon data matches the stored [credentials](#), the authentication package permits the logon to succeed.

After successfully authenticating a [security principal's](#) credentials, an authentication package is responsible for creating a new LSA logon session for the principal and allocating the [logon identifier](#) that uniquely identifies the logon session. The authentication package may associate credential information with the logon session for subsequent authentication requests. For example, the MSV1_0 authentication package (provided by Microsoft) associates the user account name and a hash of the user's password with each logon session.

The authentication package also provides a set of [security identifiers](#) (SIDs) and other information appropriate for inclusion in the security token created by the LSA. This token will represent the principal's security [context](#) for access to Windows operations.

After a logon session is created and associated with a principal, subsequent authentication requests made on behalf of the principal are handled differently than the initial logon. The authentication package does not create a new logon session nor return information for creating a token. The authentication package can, however, associate [supplemental credentials](#) obtained during a subsequent authentication with the principal's existing logon session.

Supplemental credentials are obtained when access to a requested resource requires information beyond the credentials established by the initial logon. For example, when a logged-on user requests a Novell network logon, a Novell-specific authentication package can be called and Novell-specific credentials can be authenticated and associated with the logon session. These credentials can be referenced by a Novell redirector (by way of the Novell authentication package) when the user accesses the Novell network.

The following topics discuss the various types of [Authentication packages](#):

- [Windows Authentication Packages](#)
- [Security Support Provider/Authentication Packages](#)
- [Authentication Packages Provided by Microsoft](#)
- [Subauthentication Packages](#)

Source: <https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx>