Permissions Security Checks

Permission Security Checks control the permissions for objects and roles.

The Permissions Security Checks available on the Configure the Policy section are the following:

Name	Description
Agent Job Execution	Determine whether only administrators can execute SQL Agent CmdExec Jobs
ALTER TRACE Permission Granted To Unauthorized Users	Determine whether unauthorized users have been granted the ALTER TRACE permission on SQL Server 2005 or later
CONTROL SERVER Permission Granted To Unauthorized Users	Determine whether unauthorized users have been granted the CONTROL SERVER permission on SQL Server 2005 or later
Database File Owners Not Acceptable	Determine whether SQL Server database files have unapproved owners
Database File Permissions Not Acceptable	Determine whether users have unapproved access to SQL Server database files
Database Files Missing Required Administrative Permissions	Determine whether the required administrative accounts have access to all database files
Direct Access Permissions	Check for logins that have had server level permissions granted directly to them.
Everyone Database File Access	Determine whether the Everyone group has access to SQL Server database files
Everyone System Table Access	Determine whether the Everyone group has read access to system tables on the SQL Server
Executable File Owners Not Acceptable	Determine whether SQL Server executable files have unapproved owners
Executable File Permissions Not Acceptable	Determine whether users have unapproved access to SQL Server executable files
Executable Files Missing Required Administrative Permissions	Determine whether the required administrative accounts have access to all executable files (any .exe or .dll file)
Integration Services Roles Have Dangerous Security Principals	Determine whether dangerous security principals belong to any SQL Server Information Services (SSIS) database roles.
Integration Services Roles Permissions Not Acceptable	Determine whether unapproved roles have been granted permissions on an Integration Services stored procedure.
Integration Services Users Permissions Not Acceptable	Determine whether unapproved users have been granted permissions on an Integration Services stored procedure.
Limit Propagation of access rights	Check for users that have GRANT_WITH_GRANT_OPTION, as they can grant those rights to other users.
Public Database Role Has Permissions	Determine whether the public database role has any permissions
Public Role Has Permissions on User Database Objects	Determine whether the public database role has been granted permissions on user database objects.
Public Server Role Has Permissions	Determine whether the public server role has been granted permissions
Registry Key Owners Not Acceptable	Determine whether registry keys that can affect SQL Server security have unapproved owners
Registry Key Permissions Not Acceptable	Determine whether users have unapproved access to registry keys
Registry Keys Missing Required Administrative Permissions	Determine whether the required administrative accounts have access to all SQL Server registry keys
Sysadmins Own Databases	Determine whether any databases are owned by a system administrator