Access Security Checks

The Access Security Checks audit access and configuration for data access and objects. These security checks take a look at data encryption, remote access, and other object configurations that allows access to the data or object.

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

Name	Description
Always Encrypted	Determine whether always encryption is configured for specified columns on SQL Server 2016 or later.
Appropriate cryptographic modules have been used to encrypt data.	Check all databases for appropriate encryption algorithms.
Assembly host policy	Determine whether there are user defined assemblies with host policy other than SAFE.
Backup Encryption (Native)	Determine whether native backup encryption was configured on SQL Server 2014 or later.
Backup Encryption (Non-Native)	Determine whether non-native backups were configured on SQL Server 2008 or later.
Certificate private keys were never exported	Determine whether certificate private keys were not exported.
Contained database authentication type	Determine whether authentication type set to Mixed mode with contained databases exists on instance.
DAC Remote Access	Determine whether the Dedicated Administrator Connection is available remotely.
Dangerous Extended Stored Procedures (XSPs)	Determine whether permissions have been granted on dangerous Extended Stored Procedures (XSPs).
Database Master Key encrypted by Service Master Key	Check for databases where the Database Master Key is encrypted by Service Master Key. The Service Master Key is the root of SQL Server's Encryption Hierarchy. As such, there can only be one service master key per SQL Server instance. The service master key is used to protect (encrypt) other keys, mainly the database master keys. It cannot be used directly to encrypt data.
Database Master Keys Encrypted by Password	Returns Database Master Keys passwords that are stored in credentials within the database. This is simply a count of Database Master Keys, use the family_guid value for each credential to check against the backup file to identify the database the credential is associated with.
Database roles and members	Shows information about database roles and their members.
Dynamic Data Masking	Determine whether dynamic data masking is configured for specified columns on SQL Server 2016 or later.
Encryption Methods	Determine whether there are encryption keys with algorithms other than supported.
Files On Drives Not Using NTFS	Determine whether all SQL Server files are stored on drives that use NTFS.
Fixed Roles Assigned To public Or guest	Determine whether public or guest are members of any fixed database roles.
Guest User Enabled	Determine whether Guest user access is available on the SQL Server.
Linked server is running as a member of sysadmin group	Determine whether linked servers are running as a member of sysadmin group.

NTFS Folder Level Encryption	Determine whether NTFS folder level encryption is configured for Windows folders.
Operating System Version	Determine whether the Operating System version is at an acceptable level.
Public role permissions	Determine whether the public roles have permissions to user defined objects.
Remote Access	Determine whether Remote Access is enabled on the SQL Server.
Required Administrative Accounts Do Not Exist	Determine whether the required administrative accounts exist on the SQL Server.
Row-Level Security	Determine whether row-level security is configured for specified tables on SQL Server 2016 or later.
Server roles and members	Shows information about server roles and their members.
Signed Objects	Determine whether a digital signature has been added to sepcified stored procedure, function, assembly or trigger on SQL Server 2008 or later.
SQL Job permissions	Determine whether SQL Server Agent account or job proxies are members of local Administrators group.
SQL Jobs and Agent	Determine whether job steps are running on behalf of proxy account.
SQL Server Browser Running	Determine whether the SQL Server Browser is running on the SQL Server.
SQL Server database level encryption	Determine the encryption status of all databases in the instance.
Startup Stored Procedures	Determine whether there are unapproved stored procedures set to run at startup on the SQL Server.
Startup Stored Procedures Enabled	Determine whether the "Scan for startup stored procedures" configuration option has been enabled on the SQL Server.
Startup Stored Procedures permissions	Determine whether startup stored procedures can be run or are owned by accounts without sysadmin permissions.
Stored Procedures Encrypted	Determine whether user stored procedures are encrypted on the SQL Server.
Symmetric key	Determine whether master, msdb, model or tempdb have user-created symmetric keys.
Symmetric Keys Not Encrypted with a Certificate	Lists all symmetric keys in a database that are not the database master key and are encrypted by either password or another symmetric key.
Sysadmins Own Trustworthy Databases	Determine whether any trustworthy databases are owned by system administrators on SQL Server 2005 or later.
Transparent Data Encryption	Determine whether transparent data encryption is configured for any databases on SQL Server 2008 or later.
Unacceptable Database Ownership	Determine whether if a database is found with an unacceptable owner.
User Defined Extended Stored Procedures (XSPs)	Determine whether unapproved user-defined Extended Stored Procedures (XSPs) exist.