

Konfigurationsspeicher und -tools

In den nachstehenden Tabellen finden Sie eine Zusammenfassung der Dienste und Dienstkombinationen für Authentifizierung, Autorisierung und sichere Kommunikation, die für .NET-Webanwendungen zur Verfügung stehen. Die Tabellen enthalten die verschiedenen Sicherheitsdienste für die jeweiligen Kerntechnologien, auf deren Basis .NET-Webanwendungen entwickelt werden. Darüber hinaus wird für jede Technologie angegeben, wo die zugehörigen Sicherheitskonfigurationseinstellungen verwaltet werden und welche Tools zum Bearbeiten der Einstellungen verwendet werden können.

Hinweis: Die Einstellungen in der Metabasis der Internet-Informationdienste (IIS) werden unter Verwendung des IIS-MMC-Snap-Ins oder programmgesteuert per Skript konfiguriert. Die Einstellungen in den Dateien **Machine.config** oder **Web.config** können mit einem beliebigen Texteditor (wie z. B. Notepad) oder XML-Editor (wie dem XML-Editor von Microsoft Visual Studio® .NET) bearbeitet werden.

Tabelle 1: IIS-Sicherheitskonfiguration

Authentifizierung	Konfiguration	Tools
Anonyme Authentifizierung	IIS-Metabasis	IIS-MMC-Snap-In
Standardauthentifizierung		
Digestauthentifizierung		Skript
Integrierte Windows-Authentifizierung		
Clientzertifikate		Zum Erstellen von Testzertifikaten kann Makecert.exe verwendet werden.
Autorisierung	Konfiguration	Tools
NTFS-Berechtigungen (Windows-Zugriffssteuerungslisten)	Windows- (NTFS-) Dateisystem	Windows-Explorer Cacls.exe Sicherheitsvorlagen Secedit.exe
	IIS-Metabasis	Gruppenrichtlinie
IP- und DNS-Einschränkungen		

Sichere Kommunikation	Konfiguration	Tools
SSL	Windows- (NTFS-) Dateisystem	IIS-MMC-Snap-In Skript
IPSec	Lokale Richtlinie des Computers (Registrierung) oder Verzeichnisdienst Microsoft Active Directory®	MMC-Snap-In Lokale Sicherheitsrichtlinie MMC-Snap-In Domänen-sicherheitsrichtlinie Ipsecpol.exe
Weitere Gatekeeper	Konfiguration	Tools
IP-Adress- und Domänen-nameneinschränkungen	IIS-Metabasis	IIS-MMC-Snap-In Skript

Tabelle 2: ASP.NET-Sicherheitskonfiguration

Authentifizierung	Konfiguration	Tools
Windows-Authentifizierung	< authentication >-Element von Machine.config oder Web.config .	Notepad.exe
Formularauthentifizierung		Visual Studio .NET
Passport-Authentifizierung		Beliebiger XML-Editor
Keine (Benutzerdefiniert)		
Autorisierung	Konfiguration	Tools
URL-Autorisierung	< authorization >-Element von Machine.config oder Web.config .	Notepad.exe Visual Studio .NET Beliebiger XML-Editor
Dateiautorisierung	Windows- (NTFS-) Dateisystem Active Directory – oder – SAM-Datenbank – oder – benutzerdefinierter Datenspeicher (z. B. SQL Server)	Windows-Explorer Cacls.exe Sicherheitsvorlagen Secedit.exe Gruppenrichtlinie Verwenden Sie für Windows-Gruppen das MMC-Snap-In Active Directory-Benutzer und -Computer oder (für lokale Einstellungen) das Verwaltungstool
.NET-Rollen		ADSI-Skript Net.exe Für benutzerdefinierte Gruppen – abhängig vom benutzerdefinierten Datenspeicher

Tabelle 3: Enterprise Services-Sicherheitskonfiguration*

Authentifizierung	Konfiguration	Tools
DCOM/RPC-Authentifizierung	COM+-Katalog Hinweis: Computerweite Einstellungen für Serviced Component- (und reguläre DCOM-) Proxys werden in Machine.config verwaltet.	MMC-Snap-In Komponentendienste Skript (Katalogautomatisierungsobjekte)
Autorisierung	Konfiguration	Tools
Enterprise Services (COM+)-Rollen	COM+-Katalog	MMC-Snap-In Komponentendienste Skript (Katalogautomatisierungsobjekte)
Windows-Zugriffssteuerungslisten (wenn die Serviced Component in Verbindung mit Identitätswechsel verwendet wird)	Windows- (NTFS-) Dateisystem	Windows-Explorer Cacls.exe Sicherheitsvorlagen Secedit.exe Gruppenrichtlinie
Sichere Kommunikation	Konfiguration	Tools
RPC-Verschlüsselung (Paketsicherheit)	COM+-Katalog Hinweis: Computerweite Einstellungen für Serviced Component- (und reguläre DCOM-) Proxys werden in Machine.config verwaltet.	Komponentendienste Skript (Katalogautomatisierungsobjekte)
IPSec	Lokale Richtlinie des Computers (Registrierung) oder Active Directory	MMC-Snap-In Lokale Sicherheitsrichtlinie Ipsecpol.exe

* Die Sicherheitsdienste für Enterprise Services-Komponenten gelten sowohl für Komponenten, für die der Server als Host fungiert, als auch für Bibliotheksanwendungen. Bei Bibliotheksanwendungen müssen jedoch diverse Einschränkungen berücksichtigt werden, da viele der Sicherheitsstandards vom Hostprozess vererbt werden und daher nicht direkt konfigurierbar sind. Die prozessweite Authentifizierung kann von Bibliotheksanwendungen zudem explizit ausgeschaltet werden. Weitere Informationen finden Sie in Kapitel 9, "Enterprise Services-Sicherheit".

Tabelle 4: Sicherheitskonfiguration für Webdienste (implementiert unter Verwendung von ASP.NET)

Authentifizierung	Konfiguration	Tools
Windows-Authentifizierung	< authentication >-Element von Machine.config oder Web.config .	Notepad Visual Studio .NET Beliebiger XML-Editor
Benutzerdefiniert	Benutzerdefinierter Datenspeicher (z. B. SQL Server oder Active Directory)	Abhängig vom benutzerdefinierten Datenspeicher
Autorisierung	Konfiguration	Tools
URL-Autorisierung	Web.config	Notepad Visual Studio .NET Beliebiger XML-Editor
Dateiautorisierung	Windows- (NTFS-) Dateisystem	Windows-Explorer Cacls.exe Sicherheitsvorlagen Secedit.exe Gruppenrichtlinie
.NET-Rollen	Active Directory – oder – SAM-Datenbank – oder – benutzerdefinierter Datenspeicher (z. B. SQL Server)	Verwenden Sie für Windows-Gruppen das MMC-Snap-In Active Directory-Benutzer und -Computer oder (für lokale Einstellungen) das Verwaltungstool ADSI-Skript Net.exe <hr/> Für benutzerdefinierte Gruppen – abhängig vom benutzerdefinierten Datenspeicher
Sichere Kommunikation	Konfiguration	Tools
SSL	IIS-Metabasis	IIS-MMC-Snap-In Skript
IPSec	Lokale Richtlinie des Computers (Registrierung) oder Active Directory	MMC-Snap-In Lokale Sicherheitsrichtlinie Ipsecpol.exe

Tabelle 5: .NET Remoting-Sicherheitskonfiguration** (wenn ASP.NET unter Verwendung des HTTP-Kanals als Host fungiert)

Authentifizierung	Konfiguration	Tools
Windows-Authentifizierung	IIS-Metabasis	IIS-MMC-Snap-In
Benutzerdefiniert	Benutzerdefinierter Datenspeicher (z. B. SQL Server)	Skript Abhängig vom benutzerdefinierten Datenspeicher
Autorisierung	Konfiguration	Tools
URL-Autorisierung	Web.config	Notepad Visual Studio .NET Beliebiger XML-Editor
Dateiautorisierung	Windows- (NTFS-) Dateisystem	Windows-Explorer Cacls.exe Sicherheitsvorlagen Secedit.exe Gruppenrichtlinie
.NET-Rollen	Active Directory – oder – SAM-Datenbank – oder – benutzerdefinierter Datenspeicher (z. B. SQL Server)	Verwenden Sie für Windows-Gruppen das MMC-Snap-In Active Directory-Benutzer und -Computer oder (für lokale Einstellungen) das Verwaltungstool ADSI-Skript Net.exe Für benutzerdefinierte Gruppen – abhängig vom benutzerdefinierten Datenspeicher
Sichere Kommunikation	Konfiguration	Tools
SSL	IIS-Metabasis	IIS-MMC-Snap-In
IPSec	Lokale Richtlinie des Computers (Registrierung) oder Active Directory	Skript MMC-Snap-In Lokale Sicherheitsrichtlinie Ipsecpol.exe

** Die für .NET Remoting aufgeführten Sicherheitsdienste setzen voraus, dass ASP.NET als Host für die .NET-Remotekomponente fungiert und der HTTP-Kanal verwendet wird. Für .NET-Remotekomponenten, für die IIS nicht als Host fungiert (sondern beispielsweise ein benutzerdefinierter Win32-Prozess oder ein Win32-Dienst) und die den TCP-Kanal verwenden, stehen keine standardmäßigen Sicherheitsdienste zur Verfügung. Weitere Informationen finden Sie in Kapitel 11, ".NET Remoting-Sicherheit".

Tabelle 6: SQL Server-Sicherheitskonfiguration

Authentifizierung	Konfiguration	Tools
Integrierte Windows-Authentifizierung	SQL Server	SQL Server Enterprise Manager SQL Server Enterprise Manager
SQL Server-Standard-authentifizierung	SQL Server	
Autorisierung	Konfiguration	Tools
Objektberechtigungen Datenbankrollen Serverrollen Benutzerdefinierte Datenbankrollen Anwendungsrollen	SQL Server	SQL Server Enterprise Manager Osql.exe (Datenbankskript)
Sichere Kommunikation	Konfiguration	Tools
SSL	Zertifikatspeicher des Servercomputers Registrierungseinstellungen von Client und Server Verbindungszeichenfolge	MMC-Snap-In Zertifikate SQL Server-Netzwerkkonfiguration SQL Server-Clientkonfiguration
IPSec	Lokale Richtlinie des Computers (Registrierung) oder Active Directory	MMC-Snap-In Lokale Sicherheitsrichtlinie Ipsecpol.exe