Credentials Protection and Management

learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn408190(v=ws.11)

- Article
- 08/31/2016

In this article

1. Restricted Admin mode for Remote Desktop Connection
2. LSA protection
3. Protected Users security group
4. Authentication Policy and Authentication Policy Silos
5. See also

Applies To: Windows Server 2012 R2

This topic for the IT professional discusses features and methods introduced in Windows Server 2012 R2 and Windows 8.1 for credential protection and domain authentication controls to reduce credential theft.

Restricted Admin mode for Remote Desktop Connection

Restricted Admin mode provides a method of interactively logging on to a remote host server without transmitting your credentials to the server. This prevents your credentials from being harvested during the initial connection process if the server has been compromised.

Using this mode with administrator credentials, the remote desktop client attempts to interactively logon to a host that also supports this mode without sending credentials. When the host verifies that the user account connecting to it has administrator rights and supports Restricted Admin mode, the connection succeeds. Otherwise, the connection attempt fails. Restricted Admin mode does not at any point send plain text or other re-usable forms of credentials to remote computers.

For more information, see What's New in Remote Desktop Services in Windows Server.

LSA protection

The Local Security Authority (LSA), which resides within the Local Security Authority Security Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies. The Windows 8.1 operating system provides additional protection for the LSA to prevent code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages. This protected process setting for LSA can be configured in Windows 8.1 but is on by default in Windows RT 8.1 and cannot be changed.

For information about configuring LSA protection, see Configuring Additional LSA Protection.

Protected Users security group

This new domain global group triggers new non-configurable protection on devices and host computers running Windows Server 2012 R2 and Windows 8.1. The Protected Users group enables additional protections for domain controllers and domains in Windows Server 2012 R2 domains. This greatly reduces the types of credentials available when users are signed in to computers on the network from a non-compromised computer.

Members of the Protected Users group are limited further by the following methods of authentication:

- A member of the Protected Users group can only sign on using the Kerberos protocol. The account cannot authenticate using NTLM, Digest Authentication, or CredSSP. On a device running Windows 8.1, passwords are not cached, so the device that uses any one of these Security Support Providers (SSPs) will fail to authenticate to a domain when the account is a member of the Protected User group.
- The Kerberos protocol will not use the weaker DES or RC4 encryption types in the preauthentication process. This means that the domain must be configured to support at least the AES cypher suite.
- The user's account cannot be delegated with Kerberos constrained or unconstrained delegation. This means that former connections to other systems may fail if the user is a member of the Protected Users group.
- The default Kerberos Ticket Granting Tickets (TGTs) lifetime setting of four hours is configurable using Authentication Policies and Silos accessed through the Active Directory Administrative Center (ADAC). This means that when four hours has passed, the user must authenticate again.

Warning

Accounts for services and computers should not be members of the Protected Users group. This group provides no local protection because the password or certificate is always available on the host. Authentication will fail with the error "the user name or password is incorrect" for any service or computer that is added to the Protected Users group.

For more information about this group, see Protected Users Security Group.

Authentication Policy and Authentication Policy Silos

Forest-based Active Directory policies are introduced, and they can be applied to accounts in a domain with a Windows Server 2012 R2 domain functional level. These authentication policies can control which hosts a user can use to sign in. They work in conjunction with the Protect Users security group, and admins can apply access control conditions for authentication to the accounts. These authentication policies isolate related accounts to constrain the scope of a network.

The new Active Directory object class, Authentication Policy, allows you to apply authentication configuration to account classes in domains with a Windows Server 2012 R2 domain functional level. Authentication policies are enforced during the Kerberos AS or the TGS exchange. Active Directory account classes are:

- User
- Computer
- Managed Service Account
- Group Managed Service Account

For more information, see Authentication Policies and Authentication Policy Silos.

For more information how to configure protected accounts, see How to Configure Protected Accounts.

See also

For more information about the LSA and the LSASS, see the Windows Logon and Authentication Technical Overview.

For more information about how Windows manages credentials, see Cached and Stored Credentials Technical Overview.