



TECHNICAL BULLETIN 1009

Product: DigitalPersona Pro for Active Directory

Product Version: 3.x and 4.x

DigitalPersona Pro DCOM Configuration

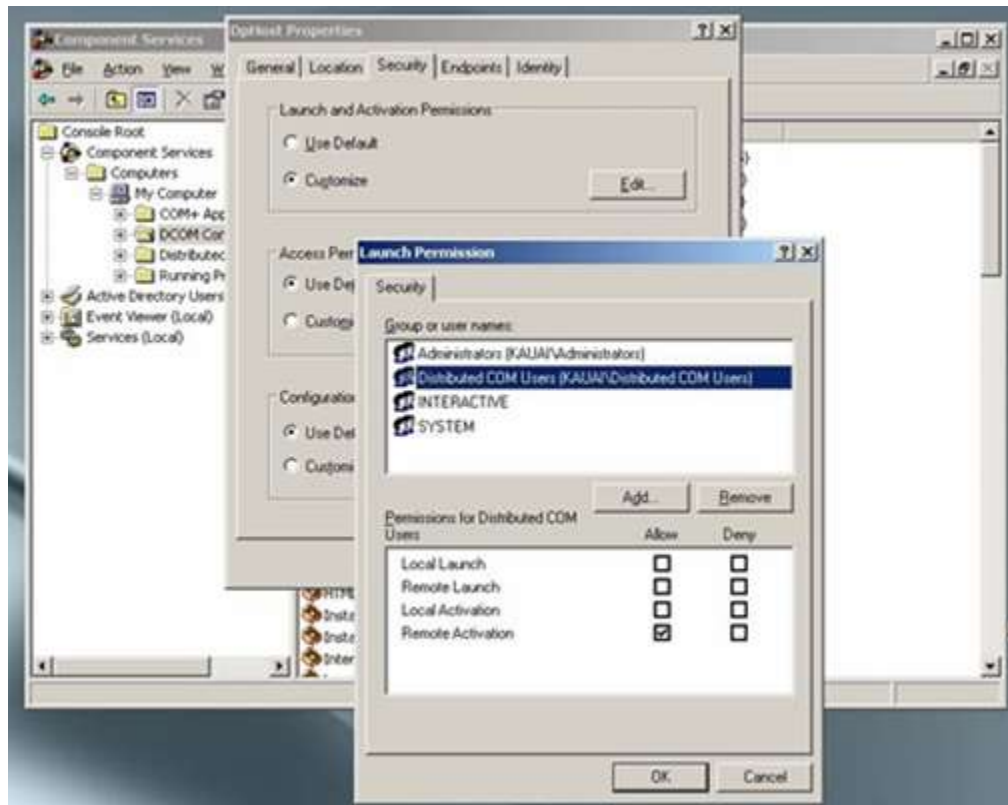
DigitalPersona Pro DCOM Configuration

Applicable to DigitalPersona installations of Pro Server v3.x or v4.x and Pro Workstation v3.x

DigitalPersona Pro Software is a DCOM application. In order for DigitalPersona Pro Server 3.x or 4.x to communicate with Pro Workstation 3.x correctly on Windows 2003 SP1 and above, you will need to configure DCOM to enable Server/Workstation communication and authentication on each Windows Server running DigitalPersona Pro Server. This is necessary only if your environment includes Pro Workstation 3.x.

(For additional information about DCOM, see <http://support.microsoft.com/?kbid=892500>.)

1. Click **Start**, point to **Administrative Tools**, and then click **Component Services**.



2. Expand the **Component Services\Computers** container.
3. Expand the **My Computer** container.

4. Expand the **DCOM Config** container.
5. Right-click **DPHost**, and then click **Properties**.
6. On the **Security** tab, in the **Launch and Activation Permissions** area, choose **Customize** and click **Edit**.
7. Click **Add** and type *Distributed COM Users* and click **OK**.
8. Click **Allow** for the Remote Activation permissions.
9. Click **OK** twice to accept the changes.

Additionally, “Domain Users” and “Domain Computers” need to be added to the “Distributed COM Users” group by following these steps in every domain:

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Expand the **Domain** container.
3. Expand the **Builtin** container.
4. Right-click **Distributed COM Users**, and click **Properties**.
5. On the **Members** tab, click **Add** and type *Authenticated Users*.
6. Click **OK** twice to accept the changes.

Effects of These Settings

All DCOM interfaces in Windows Server 2000 and Windows Server 2003 were configured, by default, to grant remote access permissions and remote activation permissions to anonymous (unauthenticated) users. This created opportunities for remote attacks to the system.

Windows Server 2003 SP1 and later versions introduced enhanced default security settings for the DCOM protocol. Specifically, SP1 introduces more precise rights that give an administrator independent control over local and remote permissions for launching, activating, and accessing COM servers. In Windows Server 2003 SP1 and above, all DCOM interfaces, by default, are configured to grant remote access, remote launch, and remote activation permissions only to administrators.

This change affects DigitalPersona Pro software, because it must provide services for all users, not just Domain Administrators. This is resolved by administrators explicitly granting remote access and remote activation permissions to the DCOM service to every authenticated user.

Granting these permissions lowers the security level on the domain as it creates opportunities for remote attacks to the system by domain users using the DCOM interfaces. However, it is still a higher security level than previously for Windows Server 2000 and Windows Server 2003 prior to SP1, because it does not allow anonymous access to DCOM interfaces which greatly reduces the possibility of attacks outside the firewall.

Pro Server Installations with Windows 98 Workstations

For installations running Pro Workstation running on Windows 98 workstations, administrators must make the following changes on each Windows Server 2003/2008 server:

NOTE: If you have a mixed environment of Windows 98 workstations with Windows 2000, or XP, then you need to perform all steps described in this document.

1. Click **Start**, point to **Administrative Tools**, and then click **Component Services**.
2. Expand the **Component Services\Computers** container.
3. Right-click **My Computer**, and then click **Properties**.
4. On the **COM Security** tab, click **Edit Limits** in the **Launch and Activation Permissions** area.
5. Click **Add**, type **Anonymous Logon** and click **OK**.
6. Click **Allow for the Remote Access** permissions.
7. Click **OK** twice to accept the changes.
8. Expand the **My Computer** container.
9. Expand the **DCOM Config** container.
10. Right-click **DPHost**, and then click **Properties**.
11. On the **Security** tab, choose **Customize** and click **Edit** in the **Launch and Activation Permissions** area.
12. Click **Add**, type **Anonymous Logon** and click **OK**.
13. Click **Allow** for the **Remote Activation** permissions.
14. Click **OK** twice to accept the changes.

NOTE: The results of these changes differ than that explained on the previous page for environments with Windows Server 2000 and XP only. The security level of the Domain - with regard to anonymous DCOM access - returns to the same level as prior to installing SP1. DigitalPersona Pro is not alone affected by SP1. Other applications affected include anti-virus, firewall, back-up and many other categories (including Microsoft Exchange 2003). For more information, visit (<http://support.microsoft.com/kb/896367>).