Distributed Transaction Coordinator

By Archiveddocs

Archived: 2026-04-05 21:49:18 UTC

Applies To: Windows Server 2003 with SP1

The Distributed Transaction Coordinator (DTC) service coordinates transactions that update two or more transaction-protected resources, such as databases, message queues, files systems, and so on. These transaction-protected resources may be on a single computer or distributed across many networked computers.

- Users of any computers that participate in DTC transactions, either directly or through other computers.
- System administrators of networks that use DTC components to perform transactions across networks.

In Windows Server 2003 Service Pack 1, DTC provides the administrator with greater control over the network communication between computers. By default, all network communication is disabled.

In order to manipulate the communication settings, the DTC security settings properties page has been enhanced. To see the page, use the following procedure:

1. Open the **Component Services** snap-in Microsoft Management Console (MMC).
2. In the console tree, click the **Computers** folder.
3. In the results pane, right click **My Computer** and then click **Properties**.
4. Click the **MSDTC** tab, and then click **Security Configuration**.

The table below defines the new fields in the property page, along with the registry keys affected for the different settings. All the registry keys related to MSDTC are located in the following registry key:

```
MyComputer\HKEY_LOCAL_MACHINE\Software\Microsoft\MSDTC
```

Warning

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. These registry keys might not be supported in future releases.

The following table tells you where to find the MSDTC key specific values.

Setting	Description	Corresponding registry value
Network DTC Access	Determines whether DTC on the local computer is allowed to access the network. This setting must be enabled in combination with one of the other settings to enable network DTC transactions. Default setting: Off	Security\NetworkDtcAccess 0 = Off 1 = On

Allow inbound	Allows a distributed transaction that originates from a remote computer to run on this computer.
	
	Default setting: Off
		To enable this setting you must set the following registry key values to 1:
		
		`Security\NetworkDtcAccess`
		
		`Security\NetworkDtcAccessTransactions`
		
		`Security\NetworkDtcAccessInbound`
		
		To disable this setting, you only need to set the following registry key value to 0:
		
		`Security\NetworkDtcAccessInbound`

Allow Outbound	Allows the local computer to initiate a transaction and run it on a remote computer.	To enable this setting, you need to set the following registry key values to 1:
		
		`Security\NetworkDtcAccess`
		
		`Security\NetworkDtcAccessTransactions`
		
		`Security\NetworkDtcAccessOutbound`
		
		To disable this setting, you only need to set the following registry key value to 0:
		
		`Security\NetworkDtcAccessOutbound`

Mutual Authentication Required	Adds support for mutual authentication in future versions and is the highest secured communication mode. In the current versions of Windows and Windows Server, it is functionally equivalent to the	AllowOnlySecureRpcCalls = 1 FallbackToUnsecureRPCIfNecessary = 0 TurnOffRpcSecurity = 0

Setting	Description	Corresponding registry value
	Incoming Caller Authentication Required setting. This is the recommended transaction mode for clients running Windows XP SP2 and servers running a member of the Windows Server 2003 family. **WarningWarning** You cannot use the **Mutual Authentication Required** transaction mode with computers that are in a clustered environment, or any computers that are negotiating transactions with such computers. In that context, you can use the **Incoming Caller Authentication Required** transaction mode instead. In a clustered environment, the computer account for the Distributed Transaction Coordinator service specifies the cluster node's host name instead of the transaction node's host name, which prevents the authentication request from succeeding when the **Mutual Authentication Required** transaction mode is enabled.	
Incoming Caller Authentication Required	Requires the local DTC to communicate with a remote DTC using only encrypted messages and mutual authentication. This setting is recommended for servers running Windows Server 2003 that are operating in a cluster. Only Windows Server 2003 and Windows XP SP2 support this feature, so you should only use this if you know that the DTC on the remote computer runs	AllowOnlySecureRpcCalls = 0 FallbackToUnsecureRPCIfNecessary = 1 TurnOffRpcSecurity = 0

Setting	Description	Corresponding registry value
	either the Windows Server 2003 or Windows XP SP2 operating system.	
No Authentication Required	Provides system compatibility between previous versions of the Windows operating system. When enabled, communication on the network between DTCs can fall back to a non-authentication or non-encrypted communication if a secure communication channel cannot be established. This setting should be used if the DTC on the remote computer runs a Windows 2000 operating system or a Windows XP operating system earlier than SP2. This setting is also useful when the DTCs that are involved are located on computers that are in domains that do not have an established trust relationship or if the computers are part of a Windows workgroup.	AllowOnlySecureRpcCalls = 0 FallbackToUnsecureRPCIfNecessary = 0 TurnOffRpcSecurity = 1

These changes are important in order to secure any communication coming into or going out from the computer. By default, after installing Windows Server 2003 Service Pack 1, the computer will not accept or issue any network traffic and therefore will be less vulnerable to network attacks.

Additionally, the online network protocol has been upgraded to support a more securely encrypted and mutually authenticated communication mode. This helps to ensure that attackers can not intercept or take over communications between DTCs.

After installing Windows Server 2003 Service Pack 1, all network communication coming out of or getting into DTC is disabled. For example, if a COM+ object attempts to update a SQL database on a remote computer using a DTC transaction, the transaction fails. Conversely, if your computer is hosting a SQL database that components from remote computers try to access using a DTC transaction, their transactions fail.

If your transactions fail because of network connectivity, you can use MSDTC security properties, as described previously in this document, select the **Network DTC Access** check box, and then select the **Allow Inbound** and **Allow Outbound** check boxes, as appropriate.

If you want to change these setting programmatically as part of your Windows Server 2003 Service Pack 1 deployment, you can directly change the registry values that correspond to your desired setting as described in the

table in “Securing all network communication by default,” earlier in this document. After you have changed the registry settings, you must restart the MSDTC service.

If you are using Windows Firewall to protect the computers in your organization, you must add MSDTC into the exception list in the Windows Firewall settings. To do so, use the following steps:

1. In **Control Panel**, open **Windows Firewall**.
2. Click the **Exceptions** tab, and then click **Add Program**.
3. Click **Browse**, and then add **c:\windows\system32\msdtc.exe**.
4. In **Programs and Services**, select the **Msdtc.exe** check box, and then click **OK**.

Setting name	Location	Previous default value	Default value	Possible values
NetworkDtcAccess	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MSDTC \Security	1	0	0,1
NetwordDtcAccessTransactions	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MSDTC \Security	1	0	0,1
NetworkDtcAccessInbound	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MSDTC \Security	n/a	0	0,1
NetworkDtcAccessOutbound	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MSDTC \Security	n/a	0	0,1
AllowOnlySecureRpcCalls	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MSDTC	n/a	1	0,1
FallbackToUnsecureRPCIfNecessary	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft	n/a	0	0,1

Setting name	Location	Previous default value	Default value	Possible values
	\MSDTC			
TurnOffRpcSecurity	HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MSDTC	n/a	0	0,1

Source: https://technet.microsoft.com/en-us/library/cc759136(v=ws.10).aspx