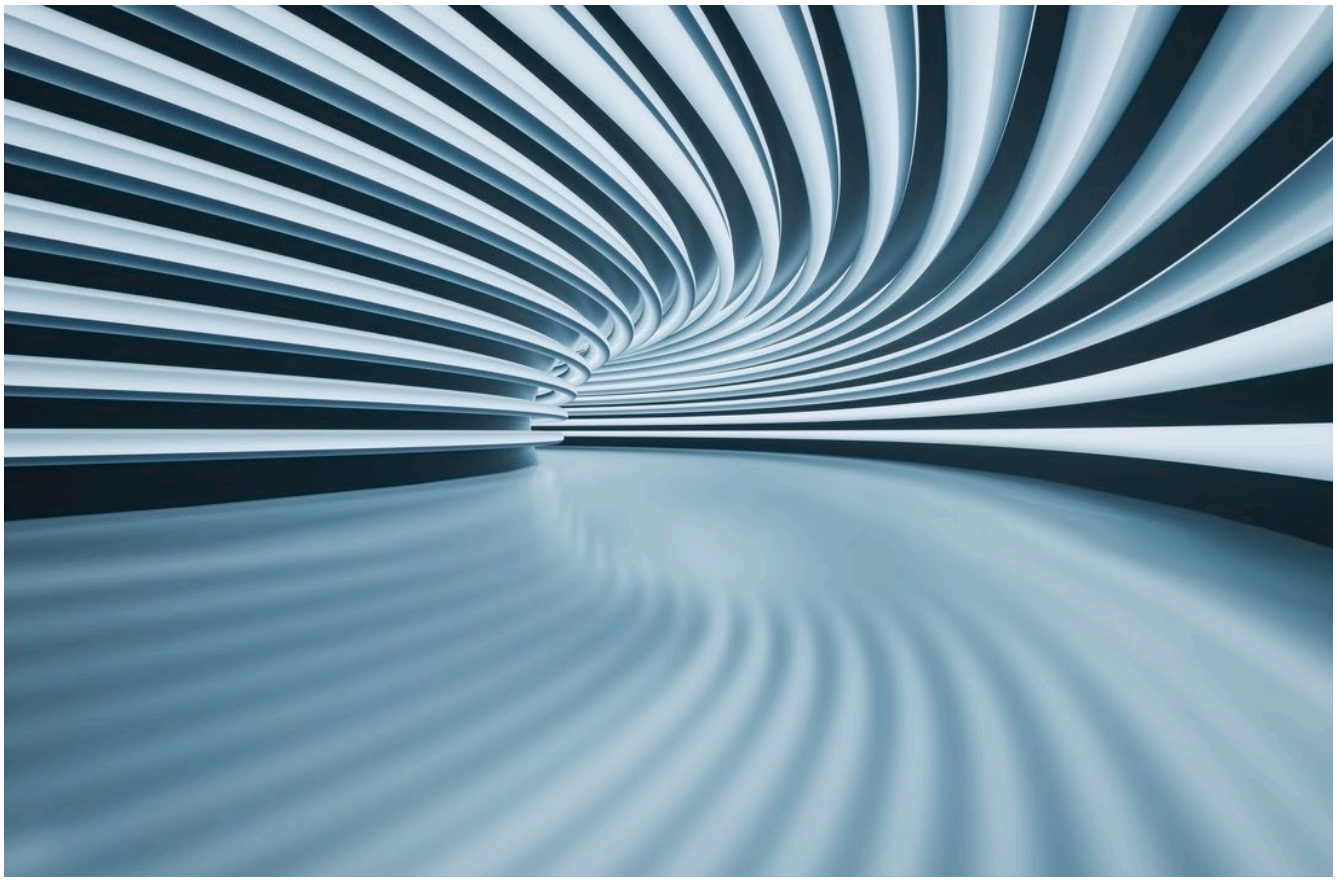


Financial & Corporate Compliance

Installation Guide

Medici™ Commercial Lending Documentation System

2024.1 (July 2024)

2023.2.1, 2023.1.3

Wolters Kluwer

Financial & Corporate Compliance

This publication was written for Medici™ Commercial Lending Documentation System

Publication Information / Version

Document Title: Medici Installation Guide
Publication Date: July 2024
Version: 2024.1, 2023.2.1, 2023.1.3

Distributed Subject to Terms of a License or other Agreement

The contents of this publication, including its appendices, exhibits, and other attachments, as updated or revised, are highly confidential and proprietary to Wolters Kluwer Financial Services, Inc. or its subsidiaries or affiliates ("Wolters Kluwer Financial Services"). This publication is distributed pursuant to a Non-Disclosure Agreement, Evaluation Agreement, License Agreement and/or other similar agreement(s) with Wolters Kluwer Financial Services, Inc. or its subsidiary or affiliate. Unless otherwise specifically provided in such agreement(s), the reproduction of this publication is strictly prohibited. Use and distribution of this publication are also subject to the responsibilities and obligations of such agreement(s), which require confidential treatment of this publication and its contents.

Information in this guide is subject to change without notice and does not represent a commitment on the part of Wolters Kluwer Financial Services.

Do Not Reproduce or Transmit

Unless otherwise specifically authorized in the agreement or license under which this publication has been provided, no part of this publication may be posted, played, transmitted, distributed, copied or reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or retaining on any information storage and retrieval system, without prior written permission from Wolters Kluwer Financial Services.

Requests for permission to reproduce content should be directed to Wolters Kluwer Customer Support, by telephone at 1-800-397-2341.

Not a Substitute for Legal Advice

This publication is intended to provide accurate and authoritative information about the subject matter covered based upon information available at the time of publication. Examples given in this publication are for illustrative purposes only.

Development of this publication and the software (including forms, disclosures, reports, and other documents generated by the software) or other products that it describes was based on Wolters Kluwer Financial Services' understanding of various laws, regulations and commentaries. Wolters Kluwer Financial Services cannot and does not guarantee that its understanding is correct.

This publication is not intended, and should not be used, as a substitute for legal, accounting, or other professional advice. Wolters Kluwer Financial Services is not engaged in providing legal, accounting or other professional services. If legal or other professional assistance is required, you should seek the services of a competent professional. We encourage you to seek the advice of your own attorney concerning all legal issues involving the use of this publication and any products described in this publication. If your interpretations or your counsel's interpretations are contrary to those expressed in this publication, you should of course, follow your/your counsel's interpretations.

The following notice is required by law:

Wolters Kluwer Financial Services' PRODUCTS AND SERVICES ARE NOT A SUBSTITUTE FOR THE ADVICE OF AN ATTORNEY.

Warranty Disclaimer

Except only for the warranties (if any) expressly set forth in the agreement(s) under which this publication is provided (i.e., your agreement or license for the described product), this publication is provided "as is", and Wolters Kluwer Financial Services makes no warranty, express, implied, by description, by sample or otherwise, and in particular and without limitation, makes no implied warranties of merchantability or fitness for purpose. No modifications to this Warranty Disclaimer are authorized unless in writing and signed by the President or a Vice President of the Wolters Kluwer Financial Services entity licensing the product described in this publication.

Attributions and Acknowledgements

All trademarks are the property of their respective owners.

Copyright Information

Contents

Introduction

Welcome to the instructions for installing Medici release 2024.1, 2023.2.1, 2023.1.3. This guide addresses new installations as well as updating existing Medici installations, from 2012.2 or higher.

All types of Medici implementations are covered: server, client, and standalone. You can successfully install this Medici release on your own using these instructions.

> **Note:** The instructions for updating from versions prior to 2012.2 are substantially different than updating from Medici 2012.2 or higher. Call Medici Support at 1-800-274-2711, ext. 1125343 before proceeding.

Quick Notes

Upgrade Summary

When updating from Medici 2012.2 or higher, your upgrade will proceed along these lines:

- Review system requirements to make sure you are up-to-date with all prerequisite software
- Perform and complete pre-install tasks, including the backup of your database and critical files
- The minimum database version is 2012.2. If the database version is less than 2012.2, you will need to update the Medici database to 2012.2.
- Install the new version of Medici (no previous release uninstall required)
- Perform some post-install configuration

New Installation Summary

If you have not already, please make sure your choice of equipment for your Medici system is supported by reviewing the system requirements. You should also have made the decision about your system and network configuration, that is, whether you are doing all of your Medici work on a single standalone workstation or working in a more complex environment with server and database servers and multiple clients. Please visit Appendix F for more details on available configurations and their capabilities if you need to.

Your new Medici installation will proceed along these lines:

- Review and complete pre-install tasks
- Install the latest version of Medici
- Perform some post-install configuration

System Requirements

The latest hardware requirements and list of supported Windows operating systems for each implementation of Medici can be found on the SupportLine web site:

- https://wolterskluwer.my.site.com/ComplianceSolutionsSupport/s/

NOTE: Only the 32-bit version of Microsoft Office is supported. The 64-bit version of Microsoft Office is not supported and cannot be used with Medici at this time.

Security Settings in Some Operating Systems

You may receive an operating system warning during installation if your current security settings are preventing the installation of Medici. You may also receive these same warnings when you try to open Medici. You may need to revisit user permissions or security policy for your operating system before installing or using this release of Medici.

Special Configuration Required for HMDA Wiz

For HMDA Wiz users, you will need to enable TLS 1.2 as well as Strong Cryptography for your Medici Client machines. Additional information on how to enable TLS 1.2 can be found at:

https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#configuring-security-via-appcontext-switches.

Note on Microsoft OLE DB Driver 18.x

Medici install requires the Microsoft OLE DB Driver (MSOLEDBSQL) version 18.2.x or newer. Please install the latest 18.2.x version or newer (current version 18.6.6 as of this release) of the MSOLEDBSQL driver prior to installing Medici.

Install the correct version from the *Prerequisites**MSOLEDBDriver* folder of the ISO or from the following Microsoft website:

https://docs.microsoft.com/en-us/sql/connect/oledb/release-notes-for-oledb-driver-for-sql-server

Note: OLE DB Driver version 19.0+ is NOT compatible (MSOLEDBSQL 19.x).

Note on .NET Framework

Installation of .NET 4.7.1 or higher is required and must be installed prior to the update and for new installations. You can install .NET 4.7.1 using the web installer at https://www.microsoft.com/en-us/download/details.aspx?id=56115.

A free .NET verification tool is available from Microsoft at http://blogs.msdn.com/b/astebner/archive/2008/10/13/8999004.aspx. You can use this tool to verify the presence or absence of a particular version of .NET Framework on your machine.

Pre-Installation Tasks

To install Medici successfully there are several pre-install tasks that must be performed first, such as setting several permissions and other configurations. The list of tasks is different for an existing install upgrade and a new install.

Database Backup

Even though the Medici installation is designed to leave your existing database intact, we highly recommend that you backup your existing Medici database before you install this upgrade. Use the Back Up task present in your version of SQL Server to back up your database.

Transactions Backup

We recommend that you backup your existing Medici *DMTransaction* folder before you install this upgrade.

Delete DM Transaction Update Folders

Delete numerical folder at *DMTransaction**Documenter Update Folder*\.

> Important: If you are upgrading from any previous version, you must delete all the numerical folders found within the *DMTransaction**Documenter Update Folder*\ location.

Custom Files Backup for Disaster Recovery

For disaster and recovery, a number of files used by Medici should be backed up before installing this release.

Server Files and Folders

Create a new folder on the same drive as your Medici server named DR Custom Server Files. Copy the following files from your existing Medici installation to this DR Custom Server Files folder:

- Multiple files in the *MediciServer* folder:
  - DMLic.lic – Your Medici license file
  - NumToText.XML (if available)
  - Server.ini
- *Userdocs* folder (if available)
- Encryption Key location – The location of this folder is specified in server.ini, located in the *MediciServer* folder. You will be prompted to enter this folder location during the server install. All the files in this folder should be backed up.

> Important: If you are not sure about the location of your Encryption Keys folder, contact Medici Support at 1-800-274-2711 ext. 1125343 or medicisupport@wolterskluwer.com before proceeding. Backup is imperative since if for any reason you lose your keys, or they become corrupted, Wolters Kluwer cannot recover them, and any data encrypted using those keys cannot be decrypted.

Client Files and Folders

On one of your client machines, create a new folder on the same drive as your Medici client named *DR Custom Client Files*. Copy the following files from your existing Medici Client installation to this *DR Custom Client Files* folder:

- Multiple files in the *MediciClient* folder:
  - CustomNPI.xml
  - LW.ini
  - Macros.ini
  - RMDisplayVars.xml
  - PDFSettings.xml
- In the *MediciClient**Databases* folder:
  - Mbnk.mdb
- Multiple files in the *MediciClient**Word Automation* folder:
  - Amort.xls
  - Bank_FindReplace.mdb
  - BankSpecific.dot
  - BankUseOnlyText.rtf
  - UFormat.ini
  - Any and all .bmp files, that is, logos

Note: Please be aware that we are no longer shipping discs containing custom content as the upgrade process preserves all customizations. If you require a copy of your custom content please, contact Medici Support.

Operating System Permissions

The person installing Medici will need to have Administrator user permissions on the Windows operating system where the installation is being performed.

Database Permissions

Database permissions and users that you established for earlier versions of Medici will work with this release. The credentials chosen at install time will need to have the *DB_Owner* access at a minimum to the database being upgraded, and *sysadmin* permissions on the SQL Server to upgrade an existing Medici database. These roles are only required during the upgrade process.

The application server's SQL credentials will need *DB_reader* and *DB_writer* access to the SQL database.

Database Backup File Location

A database file containing the details of your institution was created for you as part of the product purchase. You will need this file and its location during the Medici installation.

Note: If you are performing a remote Medici database install, the SQL Server service account must be granted access to the share where the database file is located. This service account is not the same account as your SQL Server login.

License File

As part of your product purchase, you should have obtained a Medici License Key file, *DMLic.lic*.

Store the Medici License file at a location where it can be easily accessed by the installation program. You will be prompted to enter the location of the file during the installation of the server.

Medici Encryption Keys

Encryption keys are used to encrypt and decrypt your database information and other sensitive client data that the application may use. Create a folder to house your Encryption Keys. An example folder name is *MediciKeys*. Locate the Encryption Key folder on the same machine as the Medici Application Server. You will be prompted to enter this folder location during the server install.

You must have full control over the folder location during the installation, because Medici needs to write and save files in this folder.

Warning: For security reasons, Medici creates your key files for you as part of your product purchase process. Once this process is complete, immediately make a backup of the files. If the files are lost or become corrupted, you lose access to your data within the system, such as customer information, transaction passwords and so on. If you lose your files or they become corrupted, Wolters Kluwer is not able to provide assistance in decrypting your data. The keys are unique to each institution.

Permissions

Operating System Permissions – New Installation

The person installing Medici will need to have Administrator user permissions on the Windows operating system where the installation is being performed.

Database Permissions – New Installation

The installing user should have the sysadmin rights within SQL Server to create a new Medici database. You should have remote SQL permissions to perform a remote database installation.

Note: These permissions are needed by the login being used for SQL Server access. These permissions must be granted to that login on the SQL Server instance where the install is being performed.

DM Transaction Path

Medici uses the *DMTransaction* folder to create the transaction files and output documents for all loan transactions. Prior to the installation, you must create a *DMTransaction* folder. This folder can be created on your local machine if you are doing a standalone installation.

If you want to share the transactions across a network on a network share for multiple Medici clients, you will need to create the *DMTransaction* folder on a shared network resource, for example, *Fileserver**Sharename*\. When creating the folder, you need to have full control permissions to the *DMTransaction* folder and subfolders, and the *DMTransaction* folder must be shared. Additionally, each Medici user needs to have the same network access permissions to this folder so all Medici clients can see and access documents generated by all other clients.

Note: Any machine that houses the *DMTransaction* folder needs to have its free disk space monitored on a routine basis. The transaction files increase in direct relation to the number of loan documents created.

Installing Medici

The installation will be similar whether you are beginning with a new installation or are upgrading an earlier version of Medici. The Medici installation will collect information in the following order:

- Install Choices
- Database (if selected)
- Server (if selected)
- Client (if selected)
- Finishing the install
- Post-install configuration

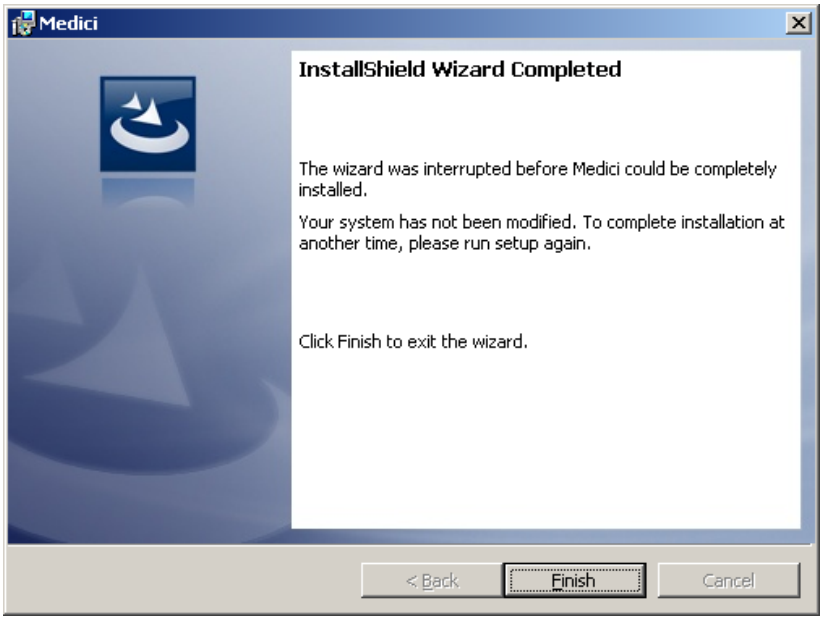
Note: If these features are spread across multiple machines for your Medici configuration, you will need to install the features in the following order: Database, Server, Client.

The choices you make as to which features to install will depend on your selected or existing configuration. If your server and database are hosted on separate machines, you will need to only install the needed features. For standalone installations, you will need to install all three features. For server configurations on a network, your client machines of course only need the client.

Canceling or Interrupting the Medici Install

You have the option to cancel or to interrupt the Medici installation, both new and upgrades, over the course of the installation. Click **Cancel** or the X Windows control available on the top right corner any of the installation screens. You will receive a message asking you to confirm that you wish to cancel the installation.

You may also receive a notice the install has been interrupted after you receive a message that one of the prerequisite software requirements is not present. You will need to correct the problem and restart the installation. Click **Finish** to exit the installation.



Install Choices

When considering how to install each feature note that only the *MediciDatabase* feature can be upgraded remotely. The *MediciServer* cannot be upgraded remotely and must be installed machine-side. The *MediciClient* cannot be upgraded remotely and must be installed machine-side.

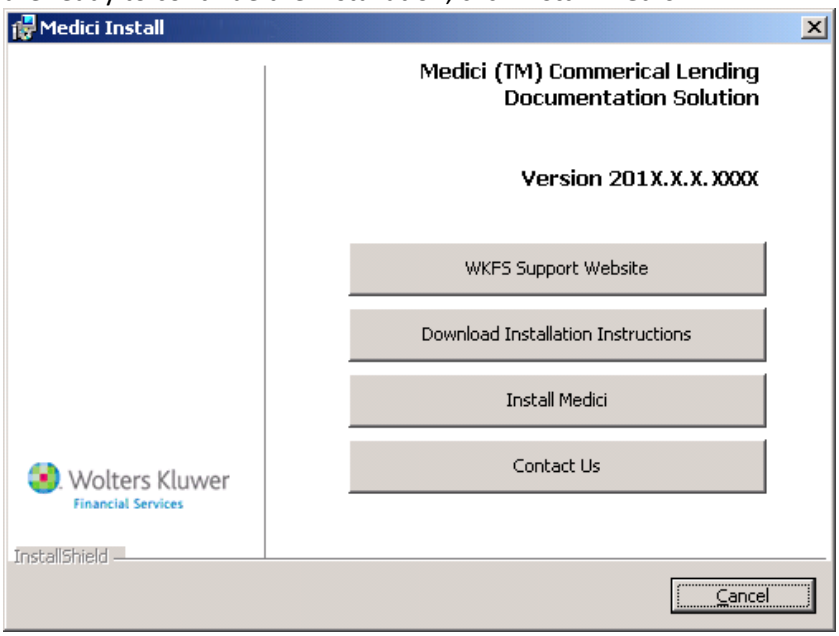
These choices are made during the installation process in the *Medici Custom Setup* option. The table below indicates which features to select for various Medici configurations:

Installation Type	Description
Standalone	Select all three features: MediciDatabase, MediciServer, and MediciClient.
Remote database (with server/client on another machine)	Select all three features: MediciDatabase, MediciServer, and MediciClient.
Separate database and server	Install the server at the server machine. The database can also be remotely installed from the server machine at the same time. Choose MediciDatabase and MediciServer. Do not choose MediciClient.
Database only	The database can be remotely installed from any machine or at the machine hosting SQL Server. Choose MediciDatabase only.
Server only	Install the server at the server machine. Choose MediciServer only. Do not choose MediciClient.
Client only	Choose only MediciClient and install at each client machine

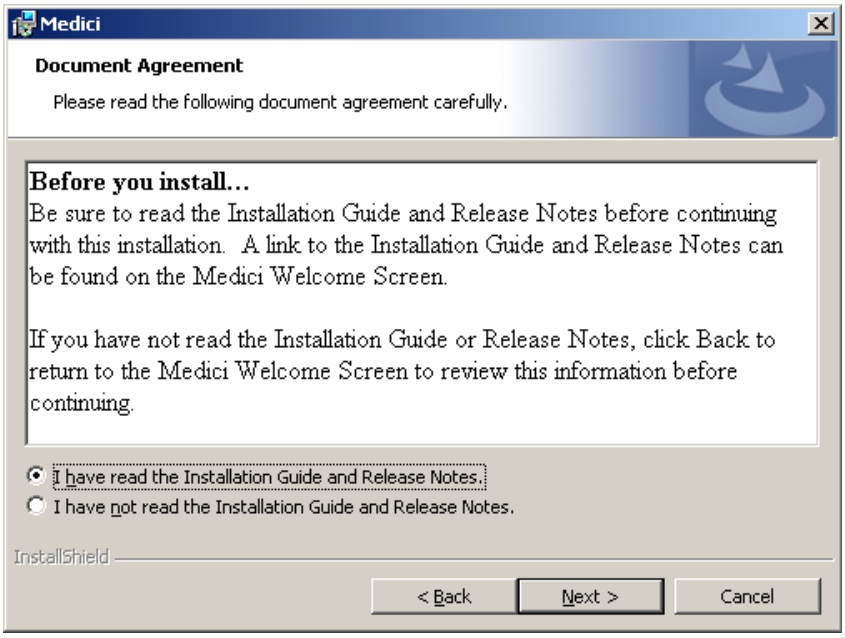
Choosing the **Client Only** feature will install just the Medici client. This option is the same as selecting Medici Client Only on the Setup Type screen.

Installing Medici

1. To begin the installation for Windows Server 2016 or later and Windows 10, right-click the ISO you downloaded for the latest release, Medici_201x.x.x.xxxx.iso, and select **Mount**.
2. From the root of the mounted virtual drive, right-click *Medici_Setup.exe* and select **Run** as Administrator.
3. The installation program will check if Microsoft .NET Framework 4.7.1 or higher is installed. The installation will halt if this prerequisite is not installed.
4. The Medici Install window will display followed shortly by the installation Welcome window. When you are ready to continue the installation, click **Install Medici**.

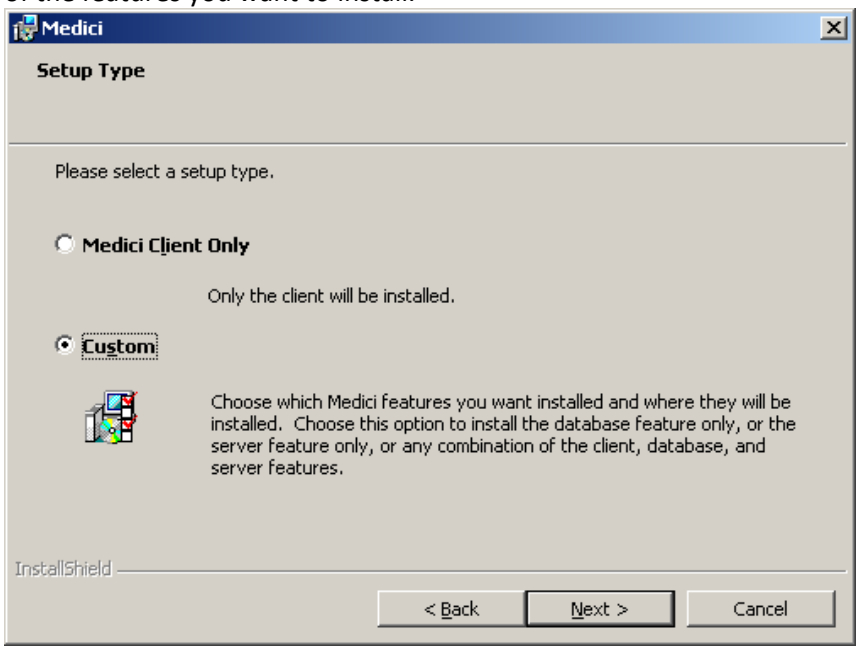


5. To proceed with the installation, you must accept the Documentation Agreement indicating you have read the release documents.

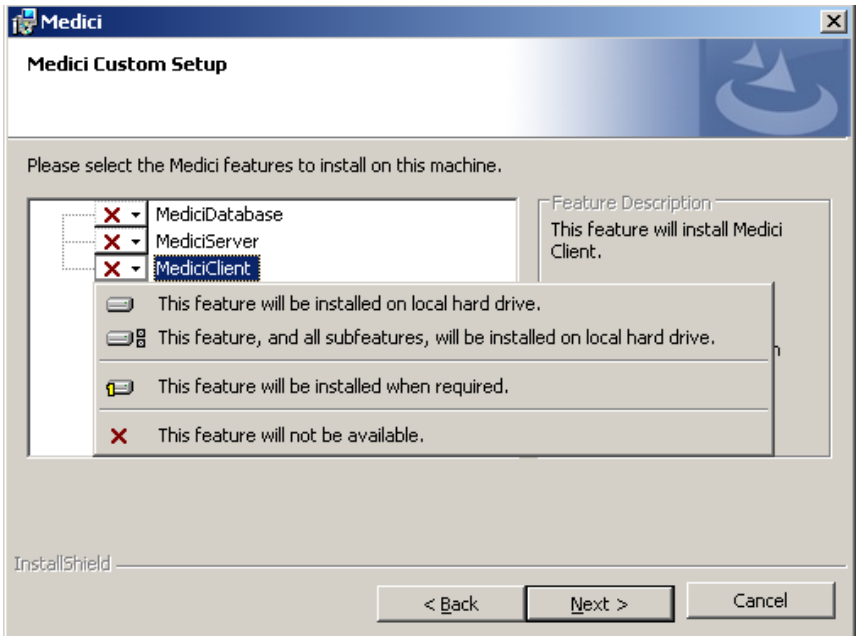


6. Click **Next**.
7. Select the Setup Type for your installation. If you are upgrading from 2010.1 or higher you will not see this screen. Each selection will give you different installation options:
   - Client. This choice will install only the Medici Client. If you choose to install only the Medici client, proceed directly to Medici Client Installation for more details.
   - Custom. This choice will be used to install different configurations of Medici server, database, and client. It allows you to select the individual feature you want to install or to select any combination

of the features you want to install.

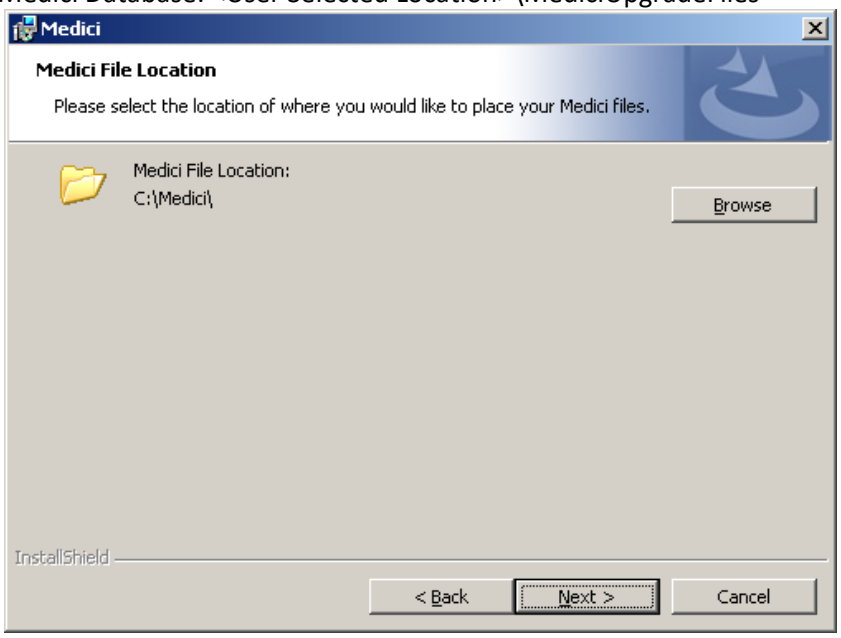


8. Click **Next**.
9. If performing a Custom installation, select the desired features that you want to install or upgrade. Refer to *Install Options* for details. If you are upgrading from 2010.1 or higher you will not see this screen.



Important: You must select all of the features you wish to install at the same time from this screen. If you install only one feature and then decide to install another later, you will first have to uninstall your original choice and re-install it along with your additional choice. It is important to understand the server/client/database configuration you wish to install or upgrade before selecting.

10. Browse to the location where you want to install Medici on your system. If you are upgrading, you may not see this screen; the installation will use your existing file location. Depending upon your configuration choices, the following folders will be created:
    - Medici Client: <User Selected Location>\MediciClient
    - Medici Server: <User Selected Location>\MediciServer
    - Medici Database: <User Selected Location>\MediciUpgradeFiles



Note: If you are installing onto a 64-bit operating system, you cannot choose a 64-bit designated file area for the installation of Medici. You must choose a 32-bit compatible area.

11. Click **Next**.

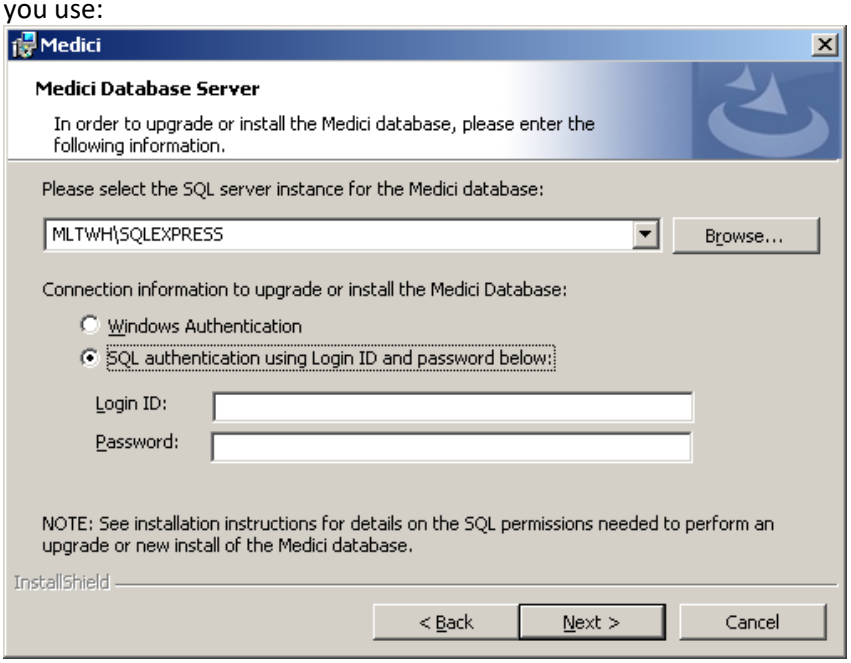
From this step onwards the installation will proceed on the basis of the choices you made on the Setup Type and Medici Custom Setup screens.

Database Installation

This section applies to both new and upgrade installations for the database.

1. Select the existing local SQL server instance from the drop-down for creating or upgrading a Medici database or browse to the instances on the network. You can also type in the name of the SQL server instance. The instance path should include the machine name hosting it. Select the authentication type

you use:

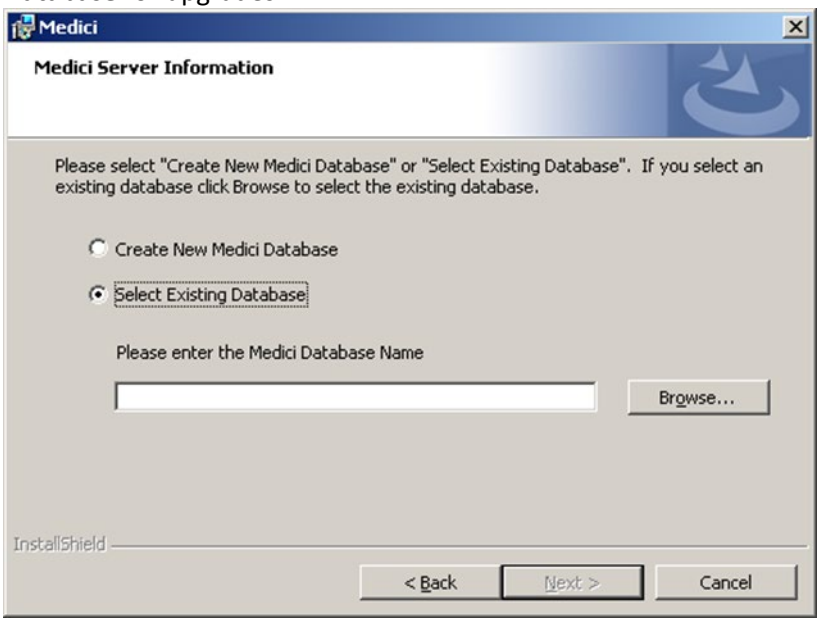


- Windows Authentication. The credentials of the user currently logged into the machine from where this install is being performed will be used. This option is selected by default.
- SQL Authentication. The Login ID must be a valid SQL Server Login that has access rights to the Medici SQL Server Database.

For an existing database upgrade, the credentials entered must have *DB_Owner* rights at a minimum on the database being upgraded and sysadmin on the SQL server. For a new install, the credentials entered must have *sysadmin* rights

2. Click **Next**.
3. The install will verify the SQL Database connection and will display one or more error messages if a connection cannot be made. You will need to edit your login or authentication type until the verification is successful.

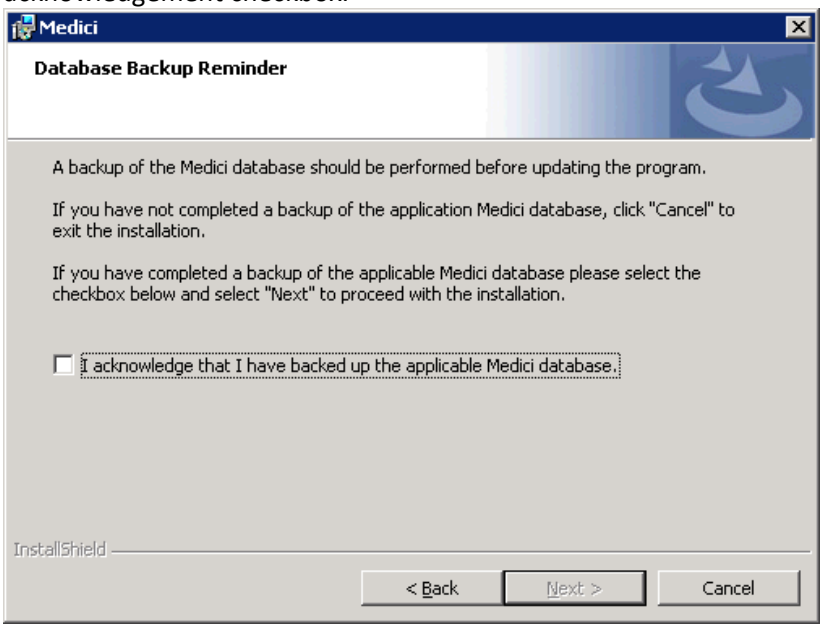
4. Next you will be asked to select **Create New Medici Database** for new installs or **Select Existing Database** for upgrades.



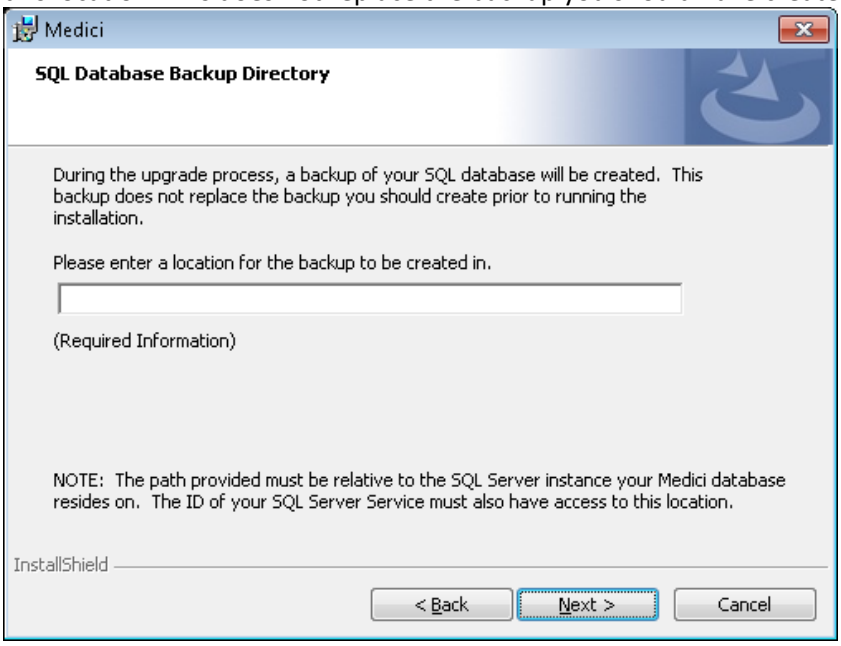
- If you are doing a **new install**, you will select Create New Medici Database and proceed to the For New Databases section of this guide for the next steps you need to perform after clicking Next.
- If an **existing database** is chosen, you will need the database catalog name. Click Browse to locate an existing database from the SQL server instance. The minimum database version is 2012.2. If the database is less than 2012.2, an error warning displays, and the installation is interrupted.

5. Click **Next**.
6. On selecting a database for upgrade, the install will verify if it is a valid Medici database. If it cannot verify the database, you will receive an error. Please review your database selection and try again. Once the verification is successful, the install will ask to verify that a backup of the database has been created prior to proceeding. After confirming that the database has been backed up, select the

acknowledgement checkbox.



7. Click **Next**.
8. Enter a location for a backup of your SQL database. The path must be relative to the SQL Server instance your Medic database resides on. The ID of your SQL Server Service must also have access to this location. This does not replace the backup you should have created prior to installation.

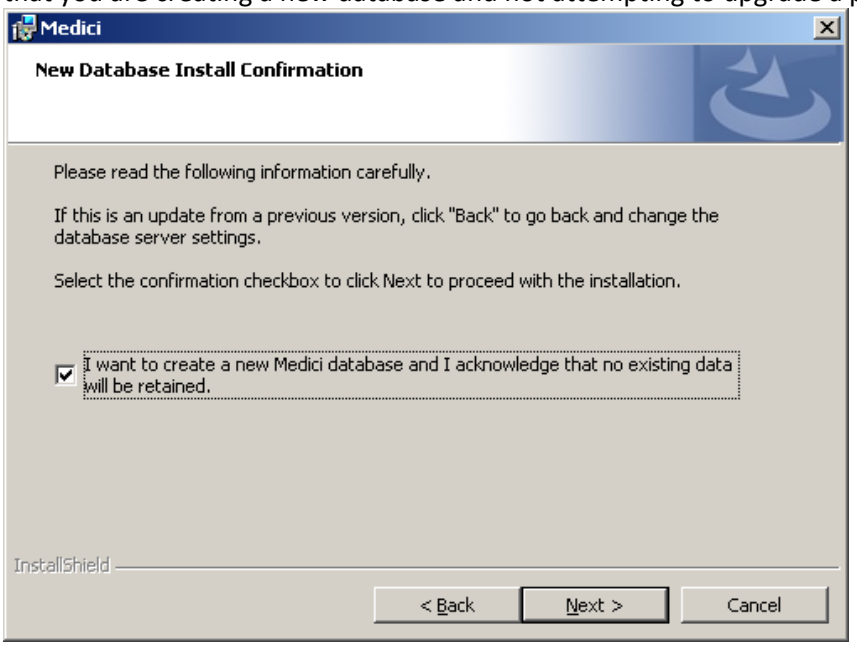


9. Click **Next**.

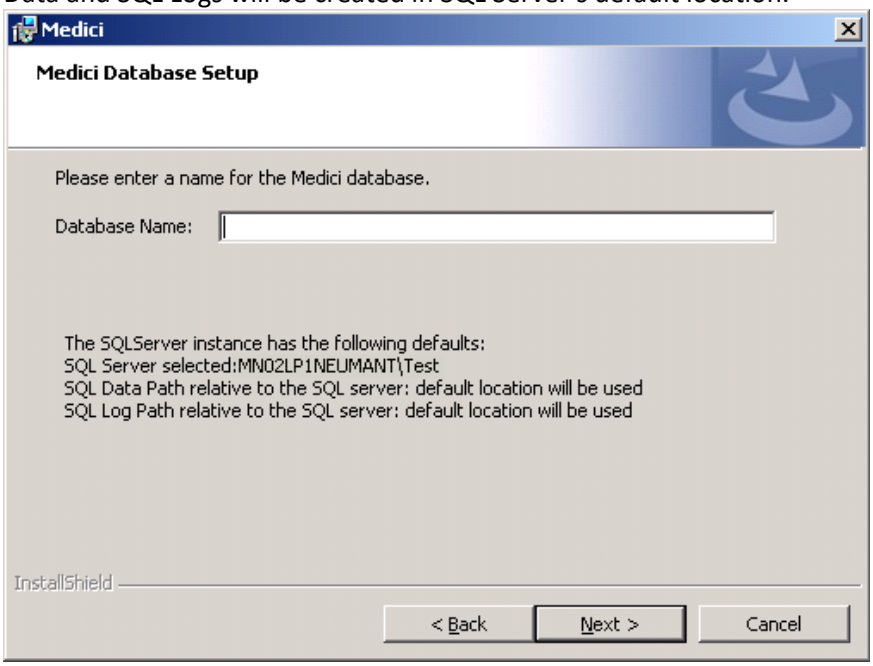
This completes the database feature install data collection for Medici. If you are doing an upgrade database-only install, you will receive the *Ready to Install* screen. If you are doing a new database install, you will proceed with your new database installation. If you are also installing the Medici application server, you will proceed to collect the information needed for the Server Installation.

For New Databases

1. After you have indicated you want to create a new Medici database, you will need to acknowledge that you are creating a new database and not attempting to upgrade a previous installation.

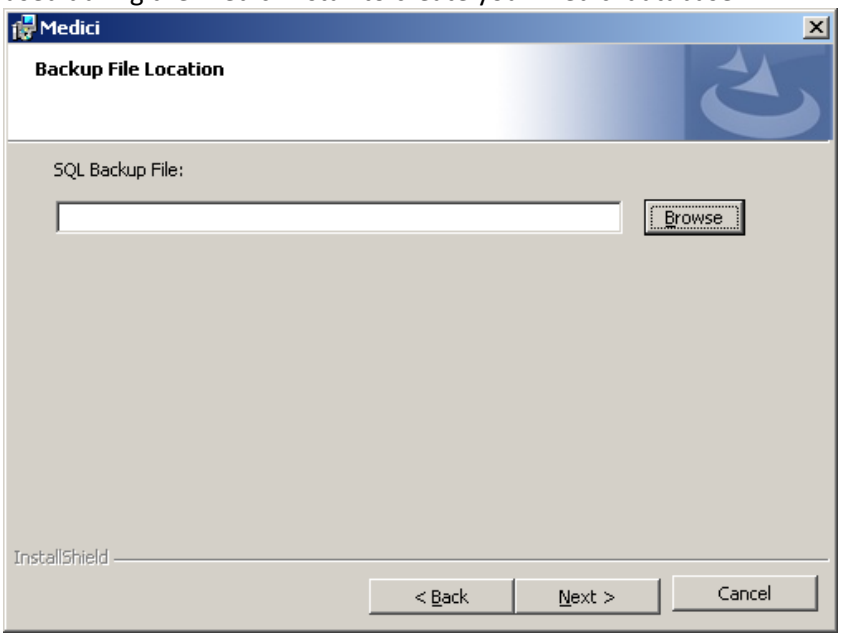


2. Click **Next**.
3. Enter the name of the database you want to create for the Medici application. The screen displays the fully qualified SQL Server instance name where the Medici database will be installed. Also note the SQL Data and SQL Logs will be created in SQL Server's default location.



4. Click **Next**.

5. Browse to the location of the database backup file, with extension .bak, created for your install by the Wolters Kluwer Professional Services as part of the purchase process. The selected backup file will be used during the Medici install to create your Medici database.



Note: If the .bak file is on a separate machine, you must have access permissions to it. The user profile under which the SQL Server instance is running needs access to this location. The user profile the install is running under, likely your own, does not need access to this location.

6. Click **Next**.
7. The install will check if the selected backup file is valid and will display an error message if the selected file is not a .bak file or you do not have permissions. Please make corrections and proceed again.

This completes the new database feature install data collection for Medici. If you are doing a database-only install, you will receive the Ready to Install screen and can proceed with your database installation. If you are also installing the Medici application server, you will proceed to collect the information needed for the Medici application server.

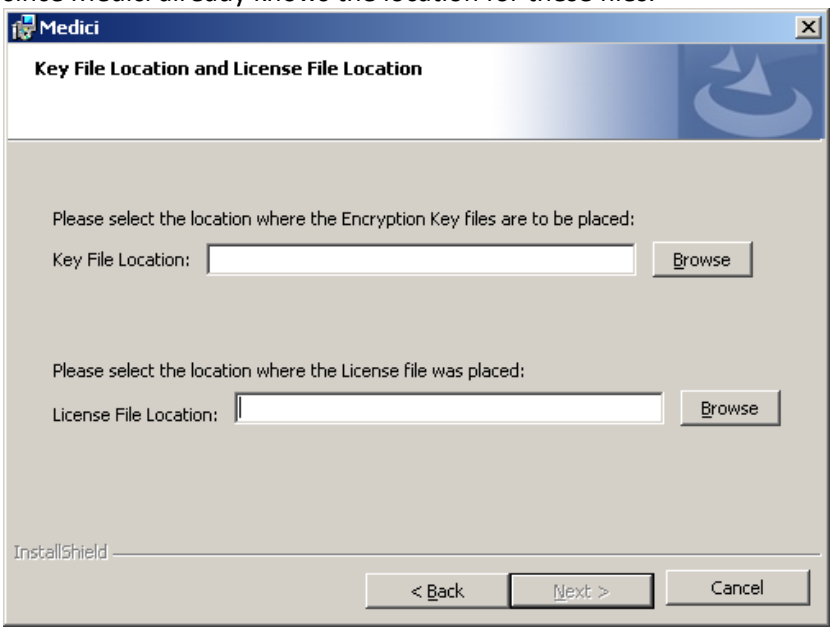
Server Installation

The Medici server installation process and steps are applicable if you have chosen to install the Medici Server feature on the Medici Custom Setup screen. This applies to both new and upgrade installations.

Note: For a new installation a version of SQL server or SQL Server Express must be installed and accessible during the server install. The Medici server requires this connection and the installation will fail without it.

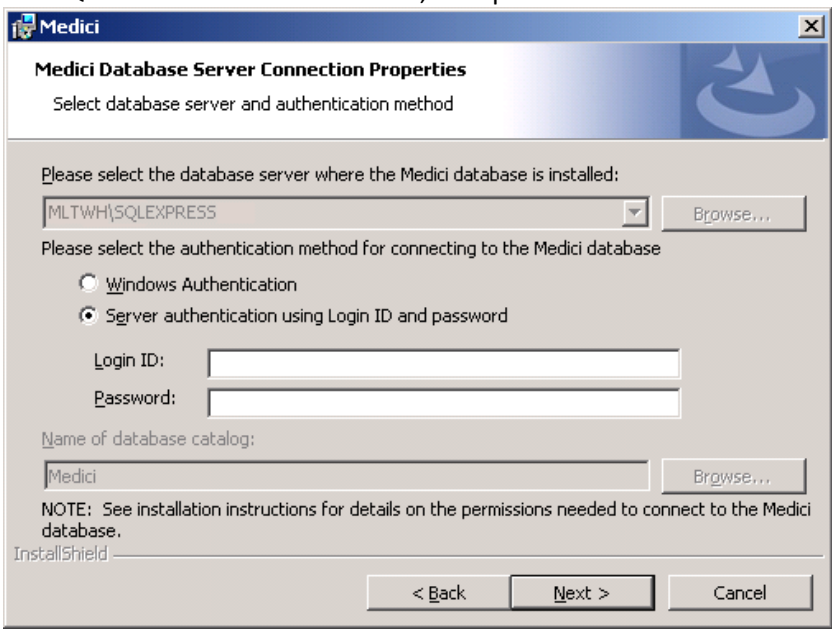
1. As noted in the pre-installation section of this guide, you will need the location for your Encryption Key files and the file location for your license file. This information is required for both new and upgrading institutions. Use Browse to navigate to the locations. If you are upgrading, you may not see this screen

since Medici already knows the location for these files.



2. Click **Next**. The install will check for both the Encryption Key folder and the License file. You will receive an error if either is not found. You may need to edit your path.

3. Once the Encryption Key folder and license file are verified, you will be asked for the name of the SQL Server instance hosting the Medici database. Use the drop-down list to select an instance on the same machine running the install, or click **Browse** to select other network locations. Note that in all cases, if the SQL Server is a named instance, the specific name of the instance must be included.



Note: The option to select the database server and the database catalog will be disabled if you have also chosen to install the database feature, as we have already collected this data. The login credentials gathered here will be used by the Medici application for connectivity.

4. Select the authentication type you want the Medici application to use to connect to the SQL server.
    - Windows Authentication. The credentials of the currently logged in user will be used. This option is selected by default. This same identity will also be the identity used by the COM+ application which you will need to configure after the install is completed.
    - SQL Authentication. The credentials entered into the Login ID and Password fields will be used. The Login ID must be a valid SQL Server Login that has access rights to the Medici SQL Server Database.

Note: The user should have the *db_datareader* and *db_datawriter* permissions on the Medici database.

5. Click **Browse** to select the Medici database from the selected SQL Server. Click **Next**. The install will now verify the SQL connection and will display an error message if the connection is not verified. Edit your connection information until the install can verify a successful connection with the SQL database.

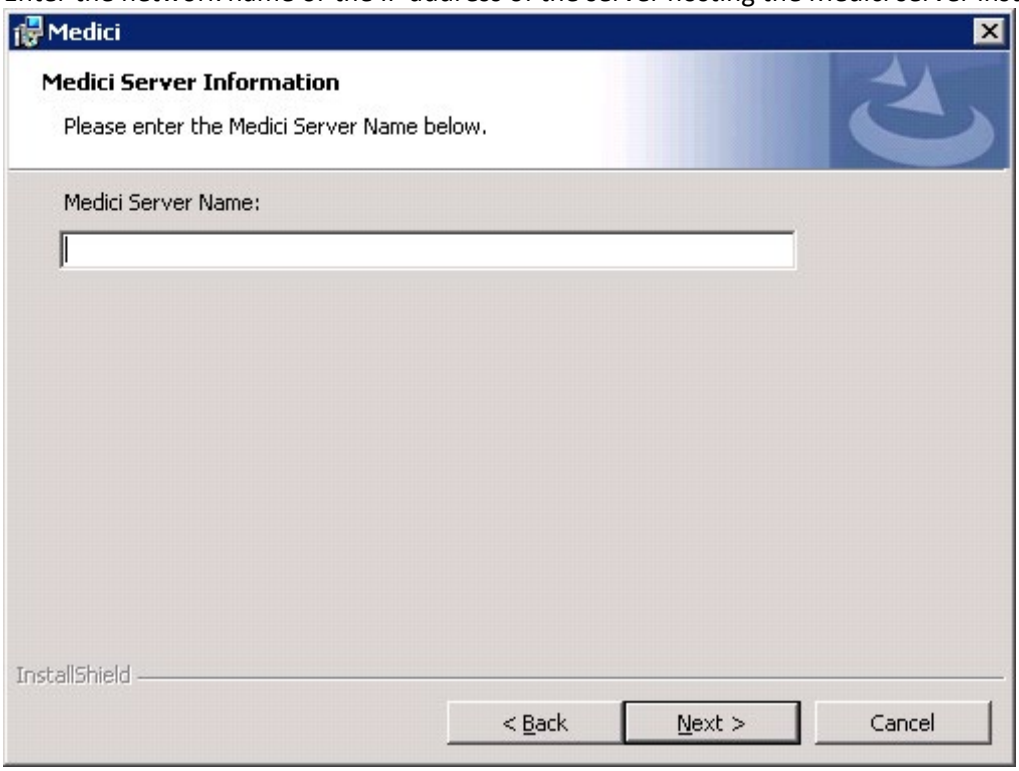
This completes the collection of information needed for the installation of the Medici server. If you are installing the Medici client feature you will proceed to collect the information needed for the Medici client installation, otherwise you will receive the Ready to Install screen.

Client Installation

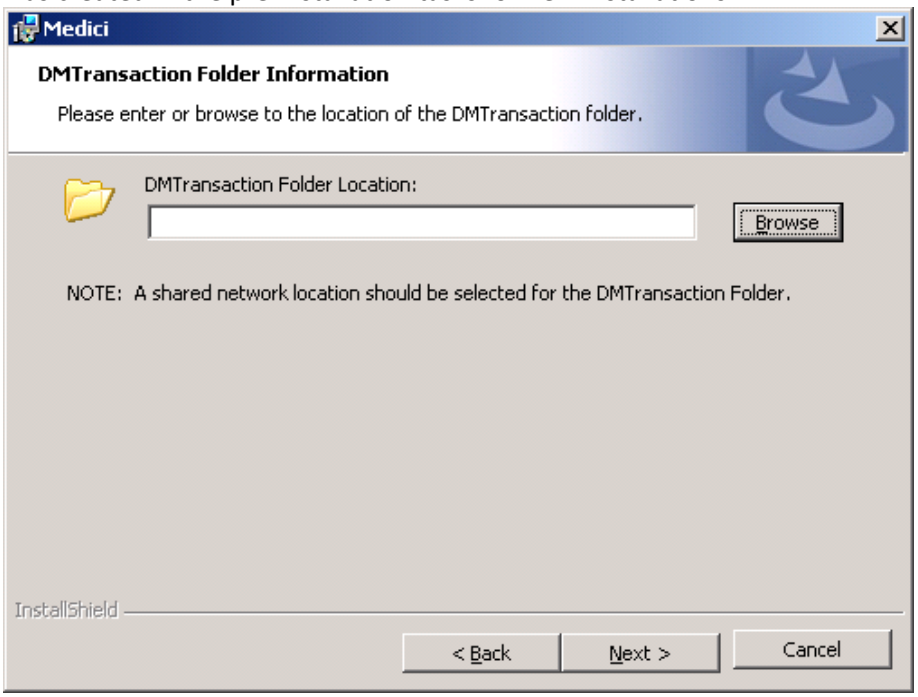
These instructions apply to both new and upgrading institutions. To install the client:

Note: If you selected to install or upgrade the Medici server as part of your installation selection, you will not see the screen in Step 1 since the installation has already collected this information. You will only see the screen in Step 1 if you are strictly installing only the client.

1. Enter the network name or the IP address of the server hosting the Medici server installation.

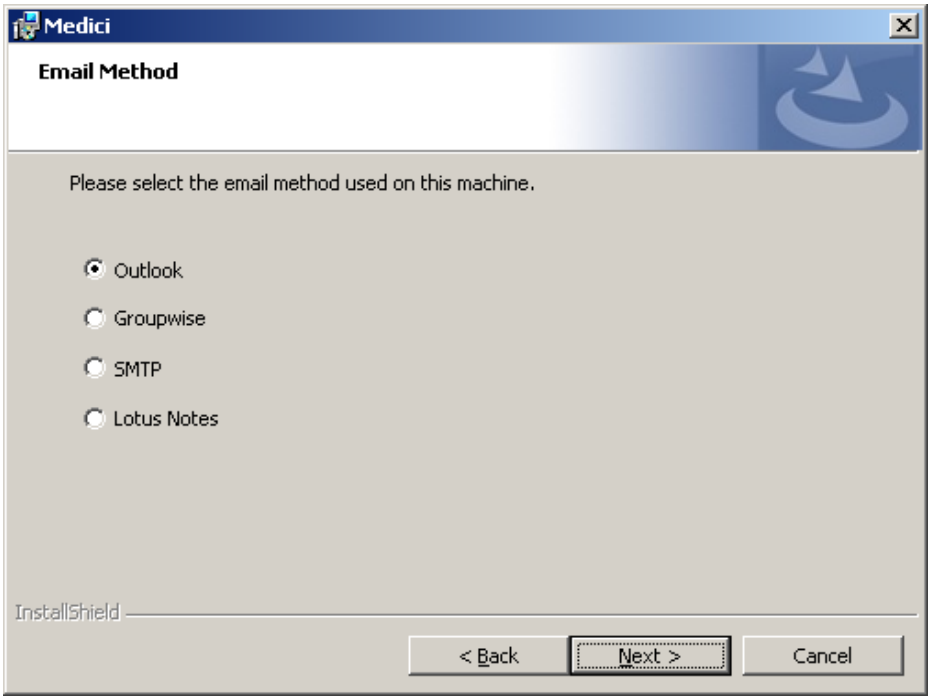


2. Click **Next**.
3. Select the *DMTransaction* folder by clicking Browse. This folder already exists for upgrading users and was created in the pre-installation tasks for new installations.



Note: For most configurations the DMTransaction folder should be on a shared network location so all Medici clients can access and share transactions.

4. Click **Next**. The install will verify if the *DMTransaction* folder exists and will display an error message if it cannot find the folder or if the installing user does not have write access to the folder. Please make corrections until the verification is successful.
5. After a successful verification you will next be asked to select the preferred method that you want to use to send emails from Medici.



6. Click **Next**.
7. If you selected SMTP as the email method on the Email Method screen, you will need to:
   - Enter the port number of the SMTP server in the Port # field.
   - Enter the name of the SMTP gateway or IP address of the server in the Server field.
8. Click **Next**. This completes the collection of information for the client install.

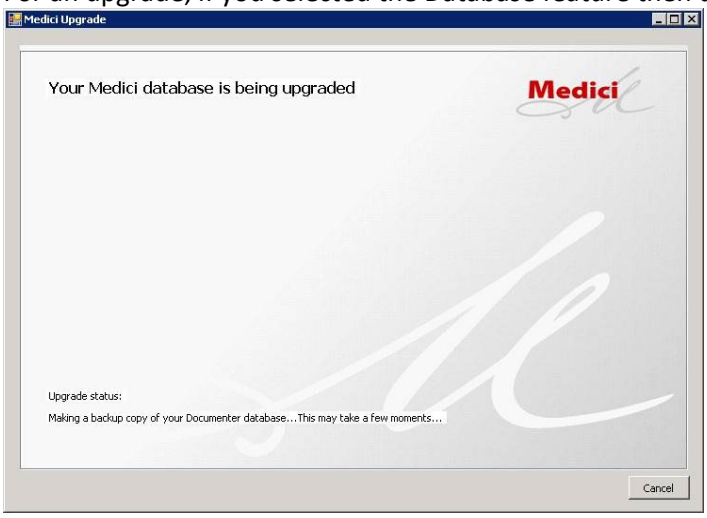
A few more steps are required for the installation to complete.

Finishing the Installation

After entering information for your selected Medici features, you will see the **Ready to Install the Program** screen.

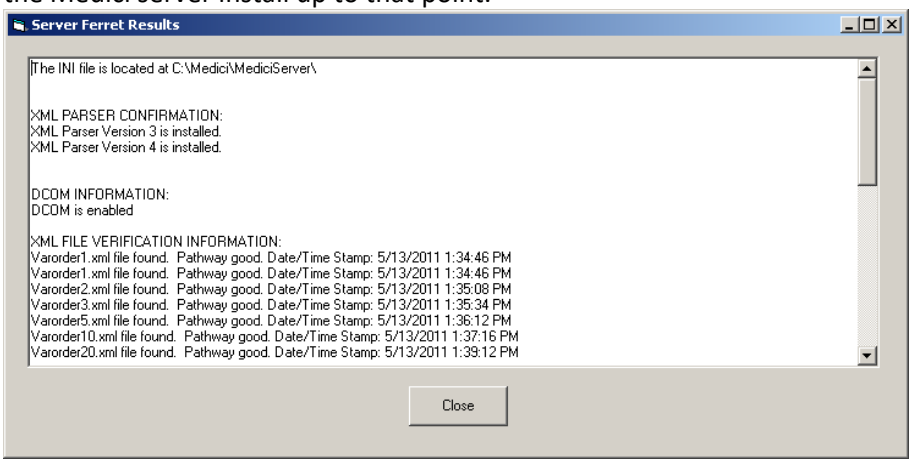
1. Click **Install**. This begins the installation of Medici based on the options you have chosen.

2. For an upgrade, if you selected the Database feature then the install will upgrade your database.

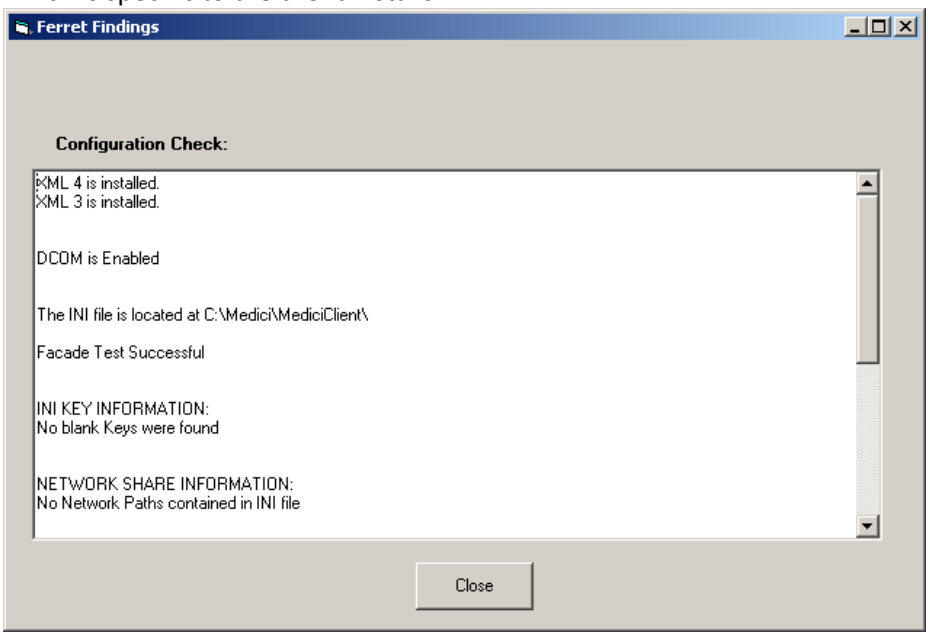


Note: The Medici Upgrade window may appear behind the install screen. You may have to look behind the install screen to see if the upgrade is finished.

3. If your install includes the server feature, you will receive some status information from a utility named Server Ferret. The purpose of the dialog boxes is to give you more detailed information about the Medici server install up to that point.



4. You may also receive some status information labeled Ferret Findings. These are from the SQL Ferret, which is specific to the client installs.



5. Please read the information from any ferret, especially looking for any warnings flashing in red text at the top of the box. If you find any, please contact SupportLine. Click **Close** after reviewing and the installation will continue. Do not cancel out of the installation if you receive any warnings.
6. Once Medici is installed, you will see the last screen informing you the installation of Medici is complete. Click **Finish** to complete the installation and proceed to post-install configuration.

Post-Installation Configuration

After installing this latest Medici release, you will need to perform some tasks before using the Medici application.

Update DM Transaction Folder for Upgrades

If you are installing multiple clients, you only need to perform the steps in this section once after the first client install. Do not repeat the steps for every client. The purpose of these steps is to make certain the updated custom files get automatically copied over to any new client workstations that may be added to your Medici environment at a later date.

1. Create a new folder called *1.0* in the *DMTransaction**Documenter Update Folder*\ location.
2. Place the following files from an upgraded client into the *1.0* folder:
   - From the *MediciClient* folder:
     a. CustomNPI.xml
     b. Macros.ini
     c. RMDisplayVars.xml

d. PDFSettings.xml

- From the *MediciClient**Database* folder:
  a. Mbnk.mdb
- From the *MediciClient**Word Automation* folder:
  a. Amort.xls
  b. Bank_FindReplace.mdb
  c. Bank_Specific.dot
  d. BankUseOnlyText.rtf
  e. Logo001.bmp and any other logo files
  f. Uformat.ini

Note: You will need to use files from an upgraded client and not the files created during the pre-install process for Disaster Recovery. Some of the files may be modified during the upgrade process.

Exclude the Medici Client Directory and DM Transaction from Anti-Virus Scanning

Anti-virus software that performs real-time file scanning while running on a machine that hosts the Medici Client negatively impacts the performance of Medici. Therefore, exclude the Medici Client directory, and all child directories, from any real-time anti-virus file scanning. Additionally, the remote *DMTransaction* path also needs to be excluded from A-V scanning on each machine running the Medici client.

Permissions to the Medici Client Directory and DM Transaction

Medici users need to have full control permissions to the Medici Client directory, and all child directories. Additionally, Medici users need to have full control permissions to the *DMTransaction* directory and all child directories.

Configure Component Services

COM+ configuration differs depending on the current version of your operating system. Follow the additional configuration steps in *Appendix B* to configure COM+ for Windows Server 2003, SP 1 and above. Complete only the section that applies to your environment.

Appendix D demonstrates how to configure user rights for the COM+ components following an installation of the Medici Server.

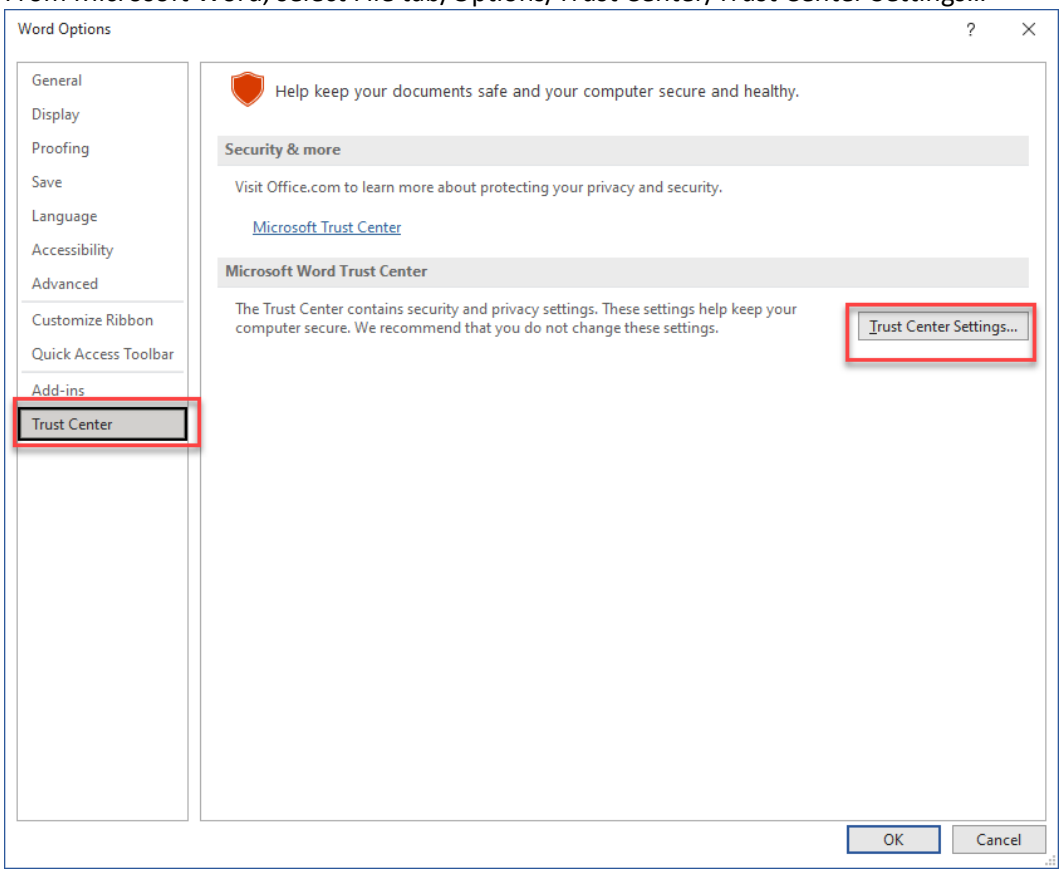
Note: You should only configure COM+ if the Medici Server exists on a separate machine from the Medici Client.

Microsoft Word Settings for Medici

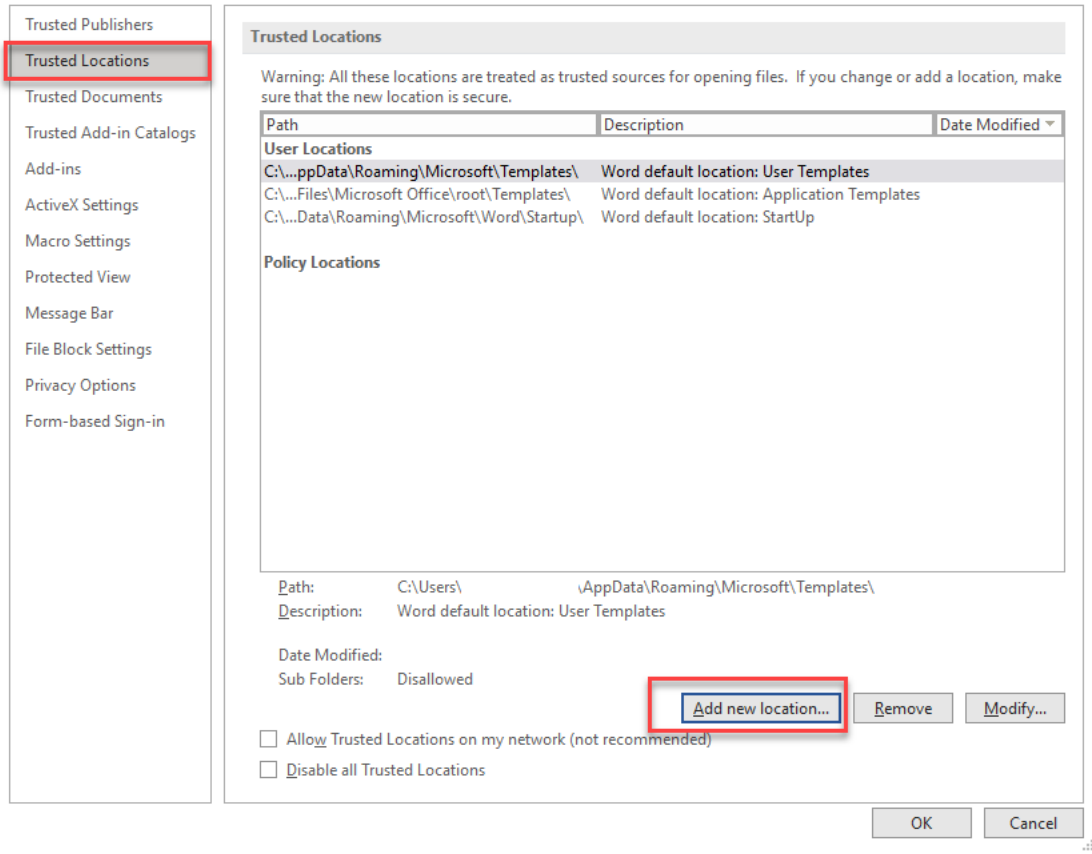
Update Trusted Locations

The following changes will need to be made for each user of Medici for Trusted Locations, ActiveX Settings, Macro Settings, and Protected View in Microsoft Word Trust Center Settings:

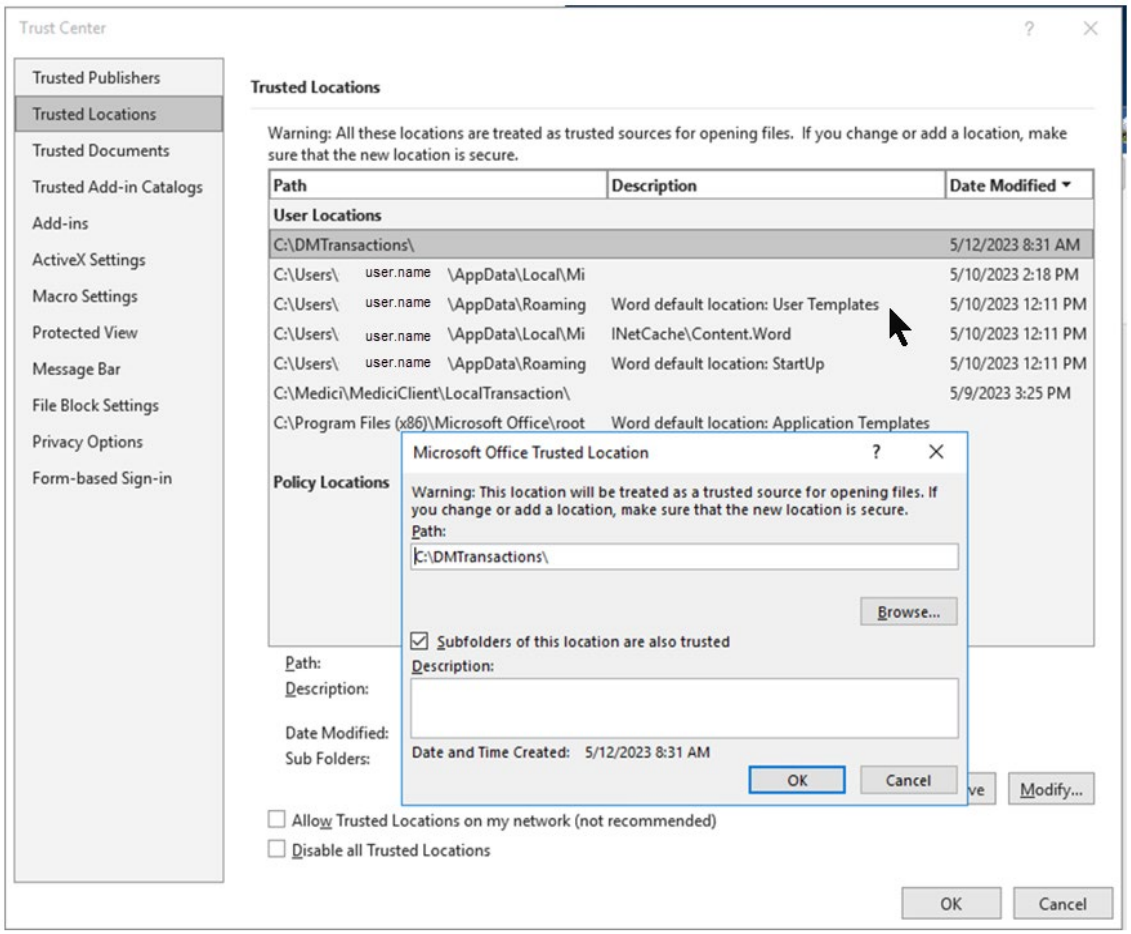
- From Microsoft Word, select File tab/Options/Trust Center/Trust Center Settings…



- Select Trusted Locations/Add new location…



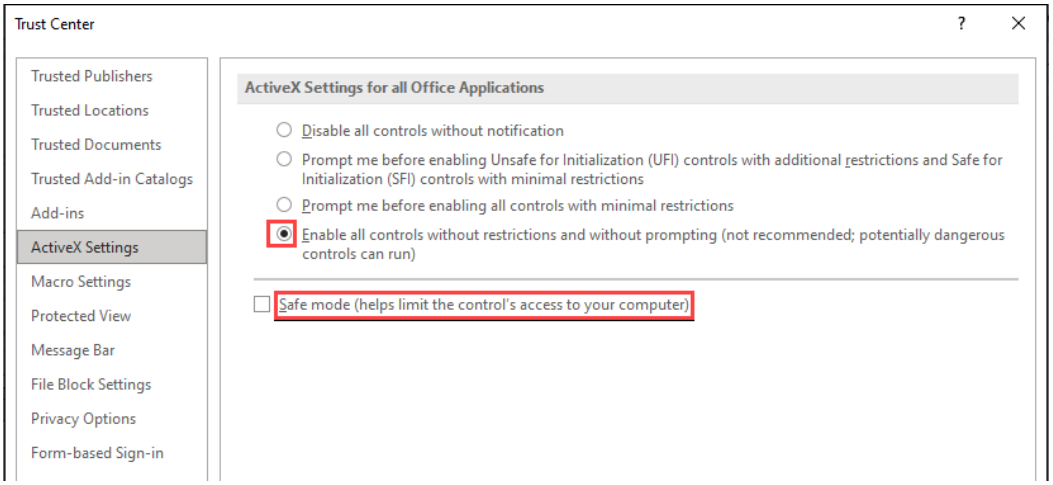
- Add updated trusted locations. Browse and add the following:
  - For Standalone
    (1) C:\DMTransactions\
  - For Client Machines
    (1) C:\Medici\MediciClient\LocalTransaction\
    (2) C:\Program Files (x86)\Microsoft Office\root\Templates\
    (3) C:\Users\user.name\AppData\Roaming\Microsoft\Templates\
    (4) C:\Users\user.name\AppData\Roaming\Microsoft\Word\Startup\
    (5) C:\Users\user.name\AppData\Local\Microsoft\Windows\
- Select checkbox for Subfolders of this location are also trusted.
- Select OK.
- Repeat for each location.
- Do not close out of Trust Center Settings.



Medici Word Settings ¬– ActiveX Settings

Next, update the ActiveX Settings for Microsoft Word.

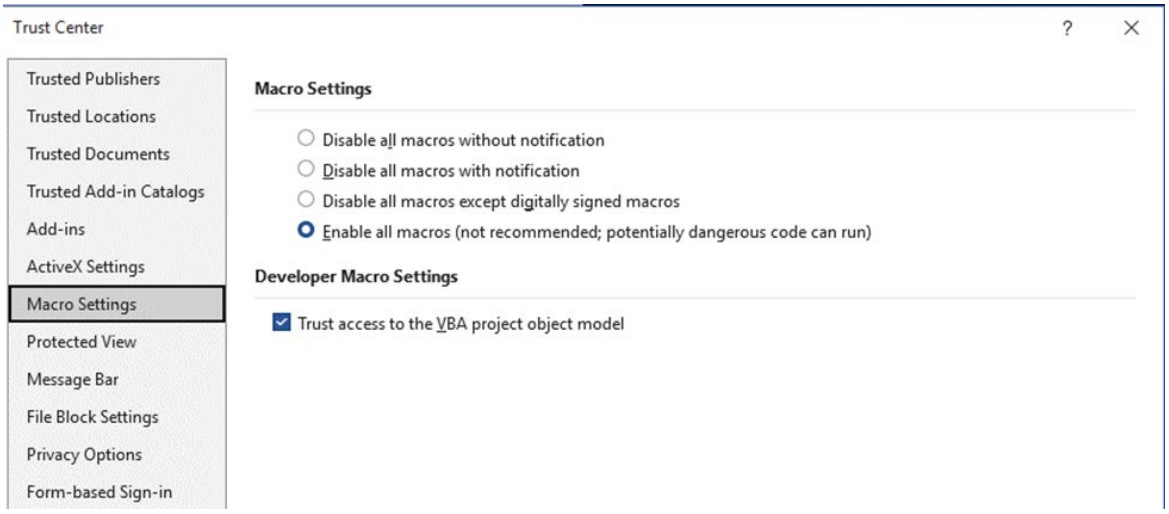
1. From Trust Center Settings…(Microsoft Word, select File tab/Options/Trust Center/Trust Center Settings…)
2. Select ActiveX Settings.
3. Select radio button for Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run).
4. Uncheck the box for Safe mode (helps limit the control's access to your computer).
5. Do not close out of Trust Center Settings.



Medici Word Settings ¬– Macro Settings

Next, update the Macro Settings.

1. From Trust Center Settings…(Microsoft Word, select File tab/Options/Trust Center/Trust Center Settings…)
2. Select radio button for Enable all macros (not recommended; potentially dangerous code can run).
3. Check the box for Trust access to the VBA project object model.
4. Do not close out of Trust Center Settings.



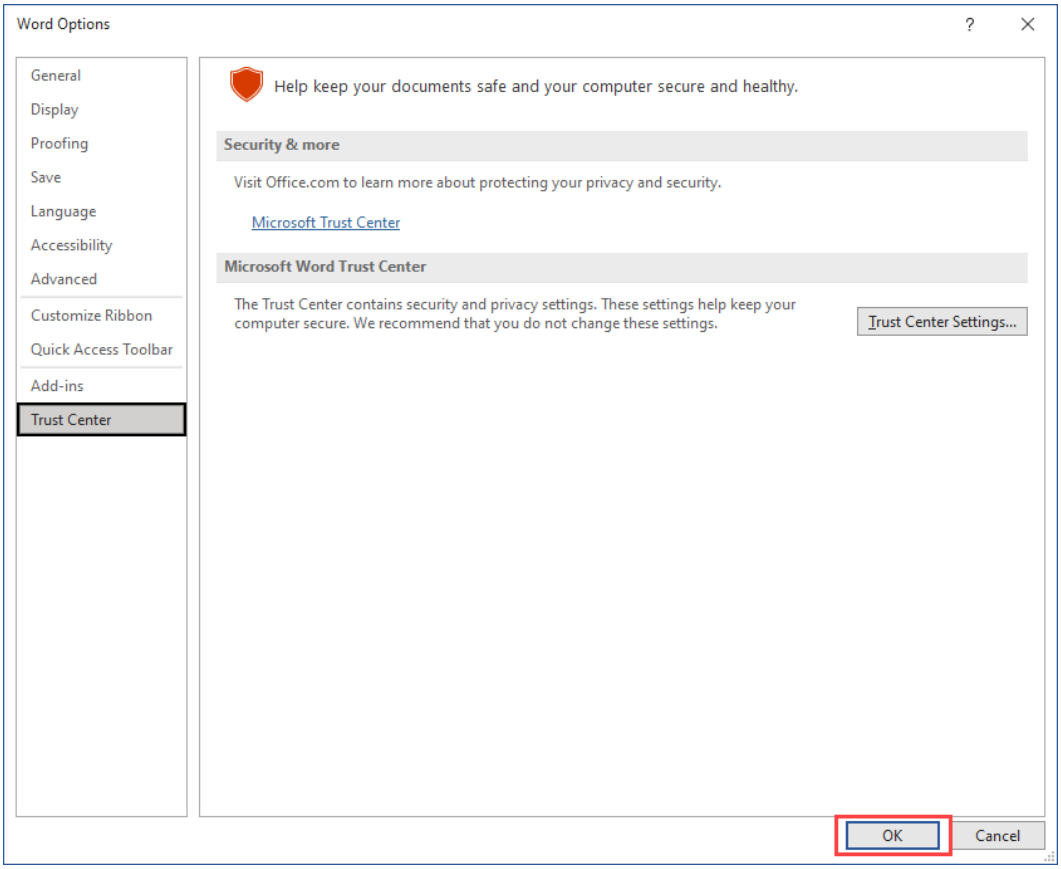
Medici Word Settings ¬– Protected View

Next, update Protected View.

1. Uncheck the following:
   - Enable Protected View for files originating from the Internet.

- Enable Protected View for files located in potentially unsafe locations.
- Enable Protected View for Outlook attachments.

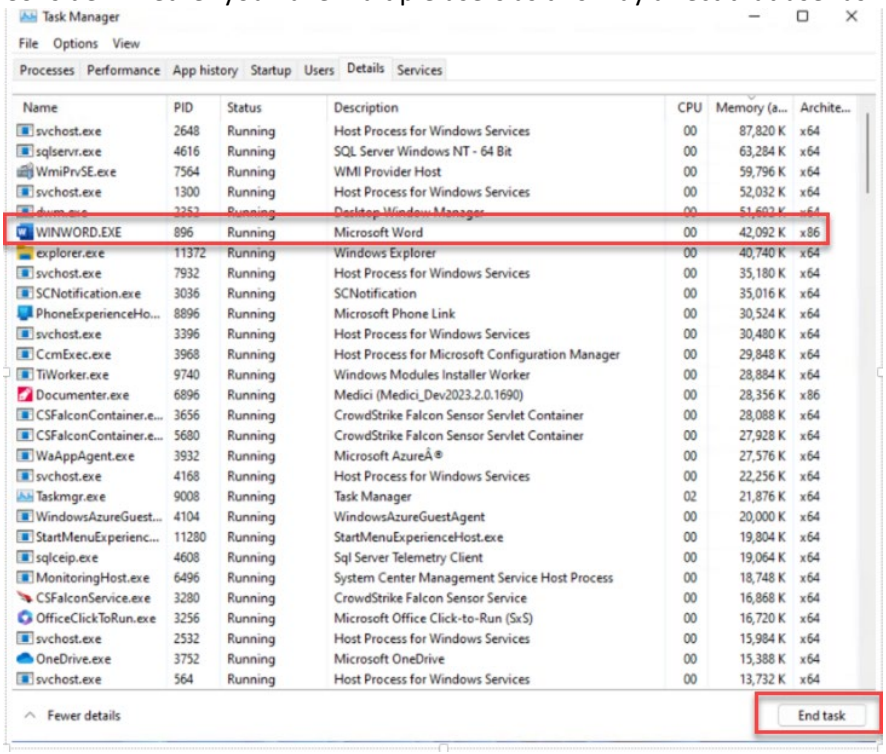
2. Select **OK**.
3. Select **OK** from Trust Center.



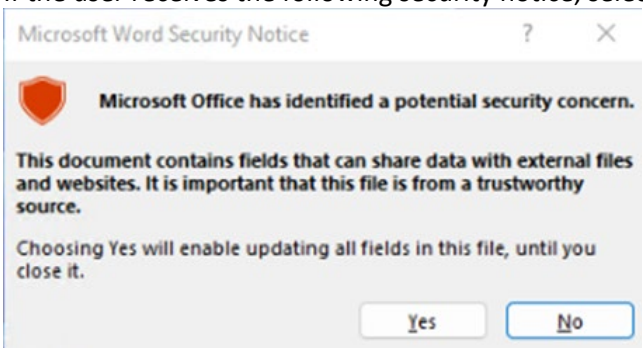
Troubleshooting Medici Word Settings

1. If a user leaves the Medici application open and unused for some time (+/- 30 mins) and then tries to generate documents, a 'Permission Denied' or a 'Disable Macros' will appear.

2. Restart the computer. You may also have to use Task Manager to end the Medici and Word processes. Consider whether you have multiple users as this may affect that user as well.



3. Verify Microsoft Word settings.
4. Open Medici, recall transaction, and generate documents. You may need to unlock the transaction that was open when the error message occurred.
5. If the user receives the following security notice, select **Yes**:



Uninstalling Medici

This section describes how to remove (un-install) the Medici application. The un-install behavior described in this section is only applicable to Medici 2021.1, 2020.2.1, and 2020.1.2.

This uninstall feature uses the Add/Remove Program option available in the Control Panel of the Windows operating system. If you are familiar with removing other applications in Windows, you will find that removing the Medici application involves similar steps.

Some files and folders remain behind when uninstalling Medici features:

- Uninstalling the Medici Server:
  - The backup folders and all the contents of the backup folders are retained. These are the folders and files you saved to the Custom Files folder in the pre-install section of this guide.
  - NumToText.xml — If you have edited this file, an upgrade or un-installation does not change or remove this file. You can find the file in the root directory of the Medici Server, for example, C:\Medici\MediciServer.
  - License file — This file, DMLic.lic, is not overwritten or removed by an upgrade or un-installation. You can find the file in the MediciServer folder.
  - Encryption Keys folder — This folder and its contents are not overwritten or removed by an upgrade or un-installation.
  - Server.ini — This file is not removed.
- Removing the Medici Database:
  - Existing Medici databases are never removed or overwritten.
  - If you choose to remove a Medici database feature, the only files removed are the database upgrade utility files.
  - SQL backup files are your property, and are not removed by the un-installation process.
  - A log file is created during the installation/un-installation process. The log file is not removed during un-installation. If errors occur as you remove Medici, you might find useful information in the log file. The SQL log is found in Log Path relative to the SQL Server.
- Removing the Medici Client:
  - The DMTransaction folder is never removed or overwritten.
  - The Client files that are not overwritten or removed by the install:
    - mBnk.mdb
    - Bank_FindReplace.mdb
    - BankSpecific.dot
    - Logo001.bmp or other logo files
    - macros.ini
    - uformat.ini
    - Barcoding info.xml
    - Amort.xls
    - lw.ini
    - BankUseOnlyText.rtf
    - RMDisplayVars.xml

The un-install process will create a backup of important Medici files. These files are saved in <Medici Install folder>\Install_Backup\<Version Number>\<Date>\<Time>\.

Example: C:\Medici\Install_Backup\10_2_0_1271\4_9_2011\23_35_41\

The un-installation of any Medici feature does not uninstall any files that were not installed as a part of the Medici feature. So, if you uninstall a Medici feature, any file remains as is, so long as the file was added after the Medici feature was installed.

To Uninstall Medici

To remove Medici:

1. From the Windows Start button, select Control Panel, Add or Remove Programs.
2. From the Currently Installed Programs list, click the Medici application.
3. Click **Change/Remove**.

Appendices

Appendix A: Windows Server 2012 for COM+ and the Medici Application Server

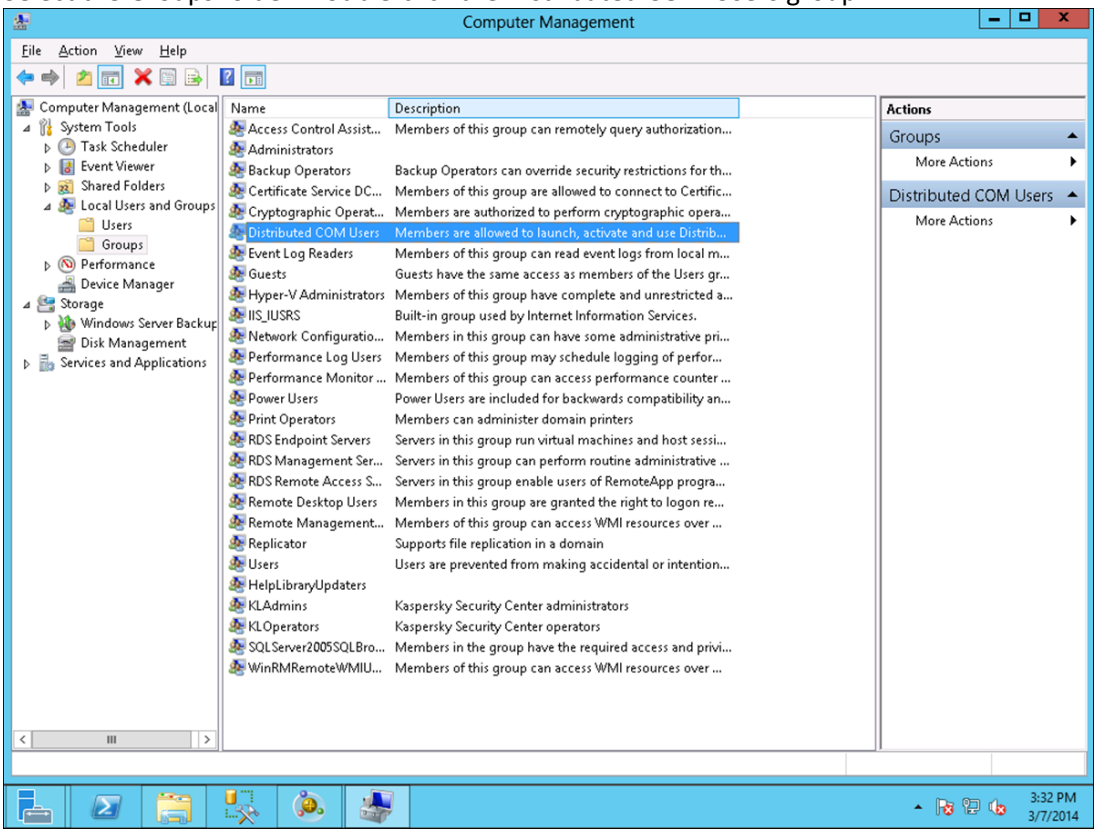
You must set up your server as an application server and not just a file server. To enable COM+, add a Domain Level Group to the Distributed COM Users group local to your Windows Server 2012 machine and add a new role to the Medici COM+ component containing the Distributed COM Users group as a user.

Note: These instructions are additional instructions for the Distributed COM Configuration performed for the standard Application Server installation. You still need to ensure that you enable COM+ and that you have configured the Identity tab of the COM+ Component.

Add a Domain Level Group to the Distributed COM Users Group

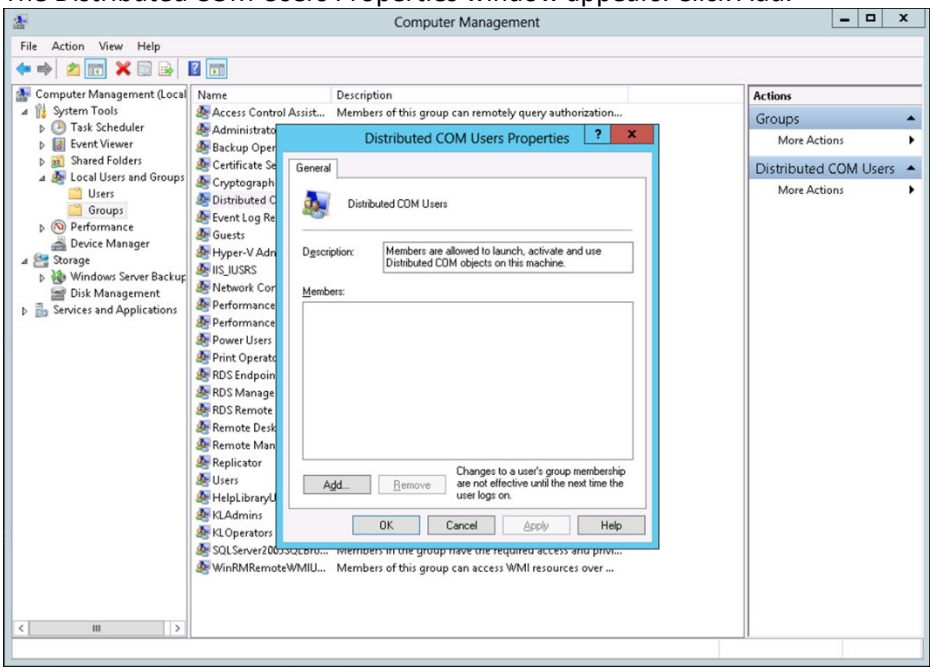
1. Open Computer Management, select Start, and Control Panel. Double-click Administrative Tools and Computer Management.

2. To access the Distributed COM Users group, expand the System Tools, Local Users and Groups nodes. Select the Groups folder. Double-click the Distributed COM Users group.

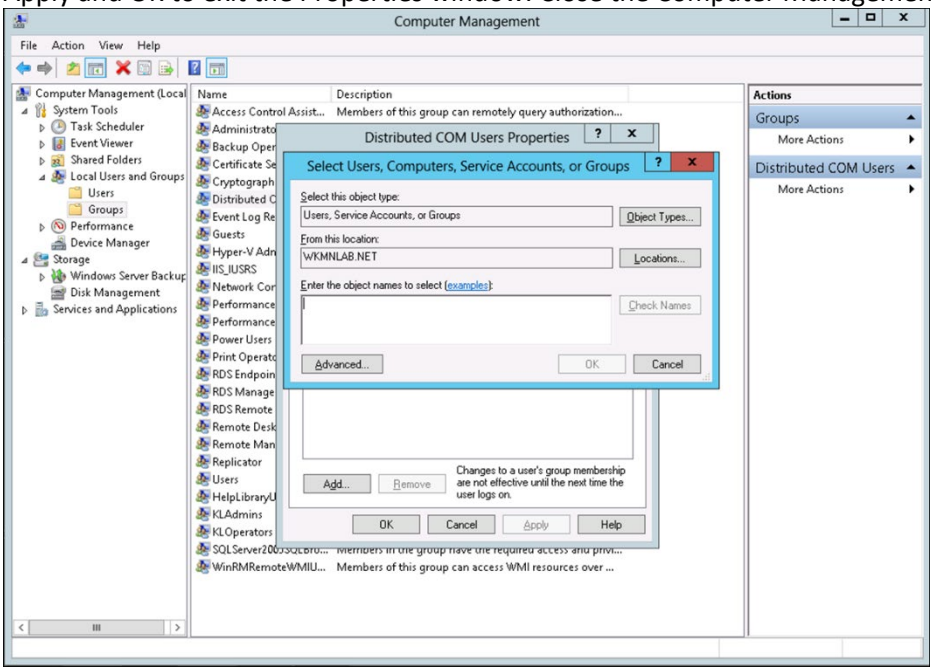


Note: Microsoft added this group to facilitate granting access to users of Distributed COM components.

3. The Distributed COM Users Properties window appears. Click Add.



4. The Select Users, Computers, or Groups window appears. Verify the object type is Users or Groups or select Object Types to change it. Add your Medici Group to the Distributed COM Users group by entering its name in the object names box. Select Check Names. Click OK to exit this window. Click Apply and OK to exit the Properties window. Close the Computer Management window.



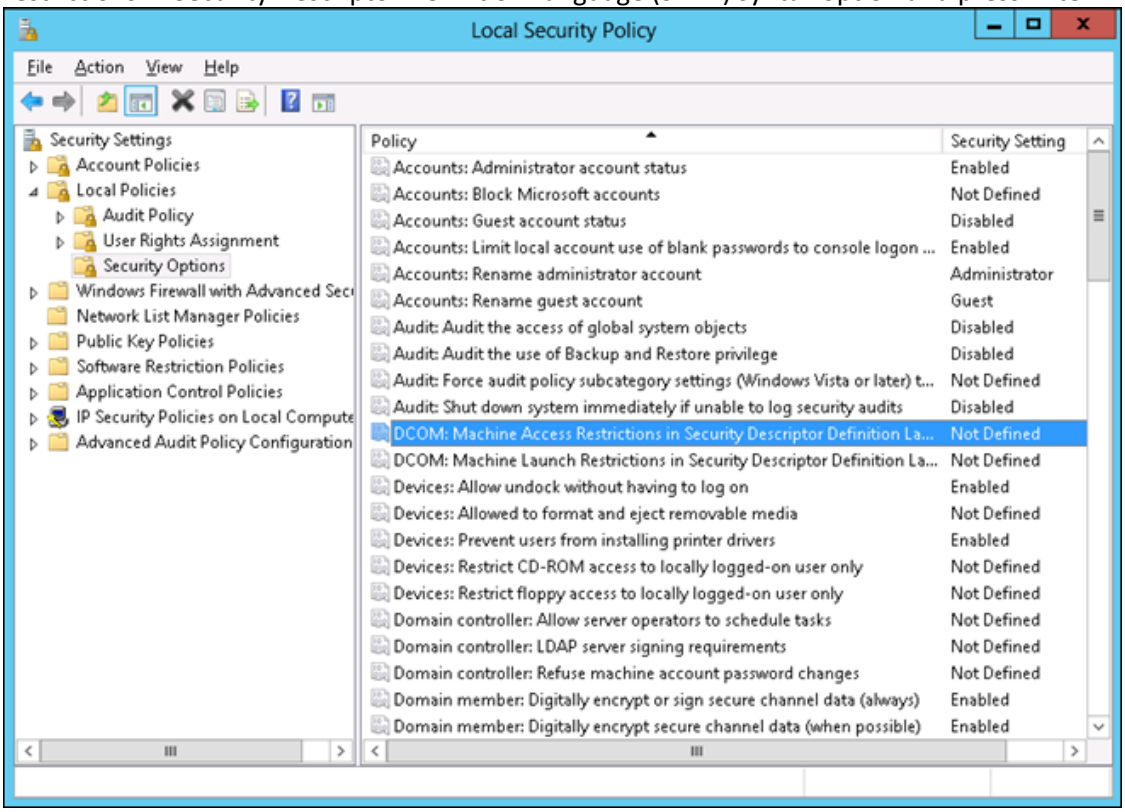
Note: The Medici Group should be the same group you use to maintain access to the shared network location DMTransaction path. This allows for easier maintenance if you need to add users to Medici.

Grant Remote and Local Access

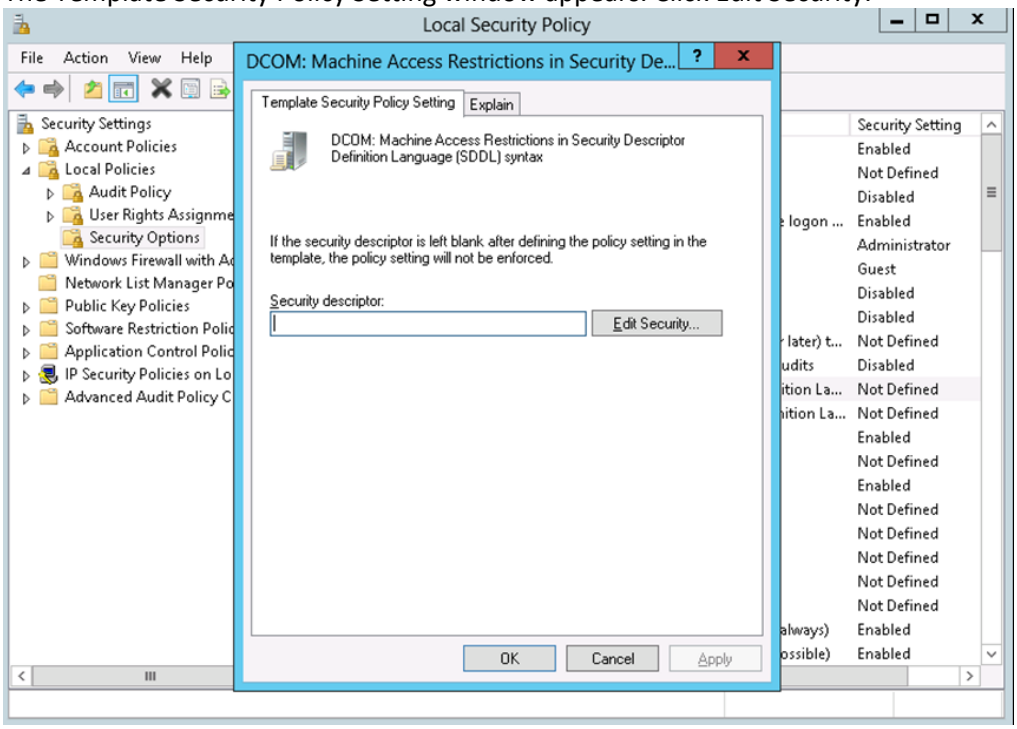
If you are unable to use the Distributed COM Users group, you need to set up a Medici Users group directly into the role of the Medici COM+ component, instead of adding the Medici Users group to the Distributed COM Users group and then adding the Distributed COM Users group to the role of the Medici COM+ component.

If you need to add the Medici Users group directly to role of the Medici COM+ Component, you must follow these additional steps to grant Remote and Local Access to Distributed COM+ components for this group.

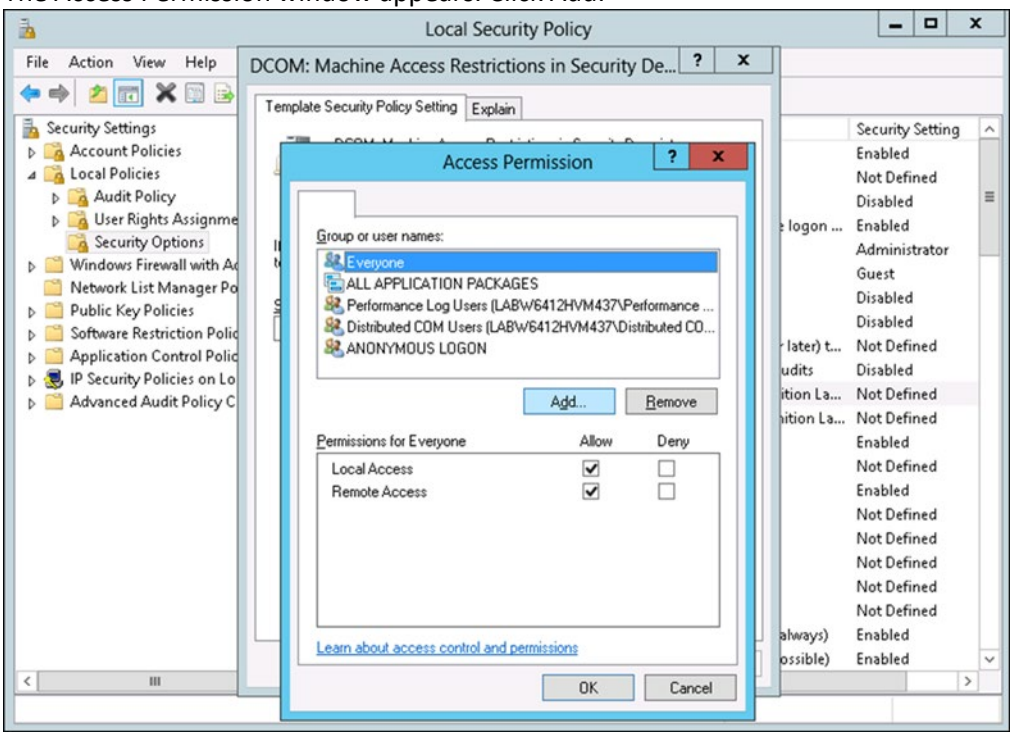
1. Open the Local Security Policy on the server hosting the Medici Application Server.
2. Expand Local Policies and select the Security Options folder. Select the DCOM: Machine Access restrictions in Security Descriptor Definition Language (SDDL) syntax option and press Enter.



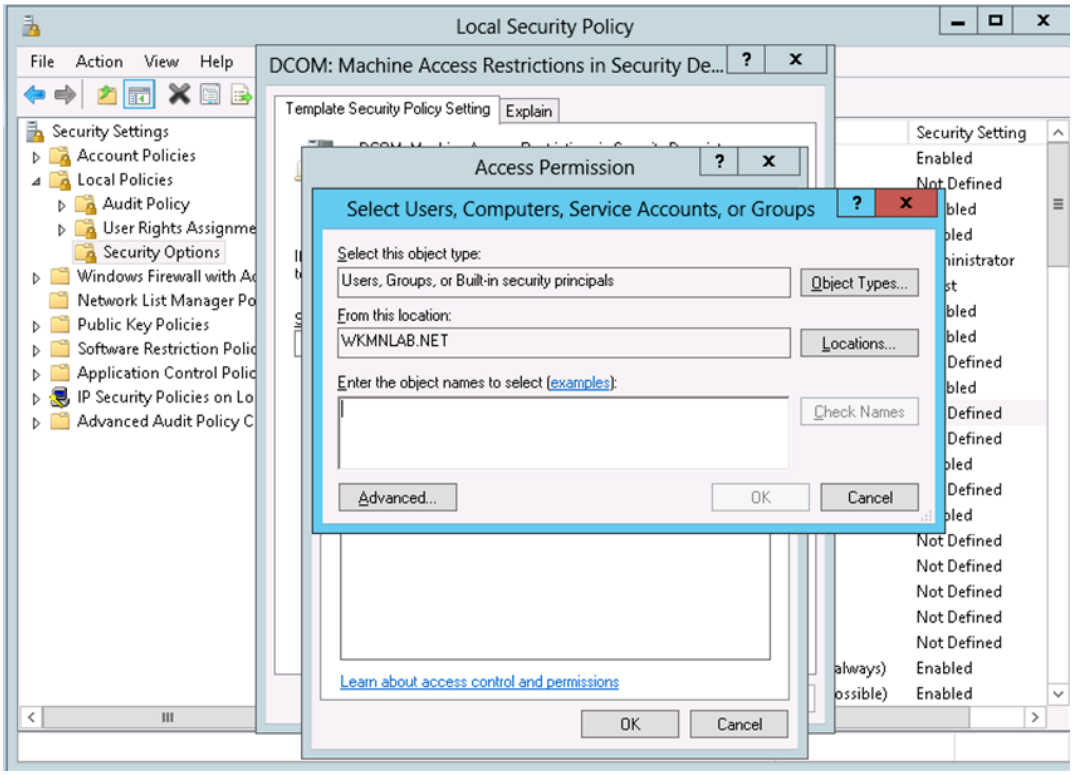
3. The Template Security Policy Setting window appears. Click Edit Security.



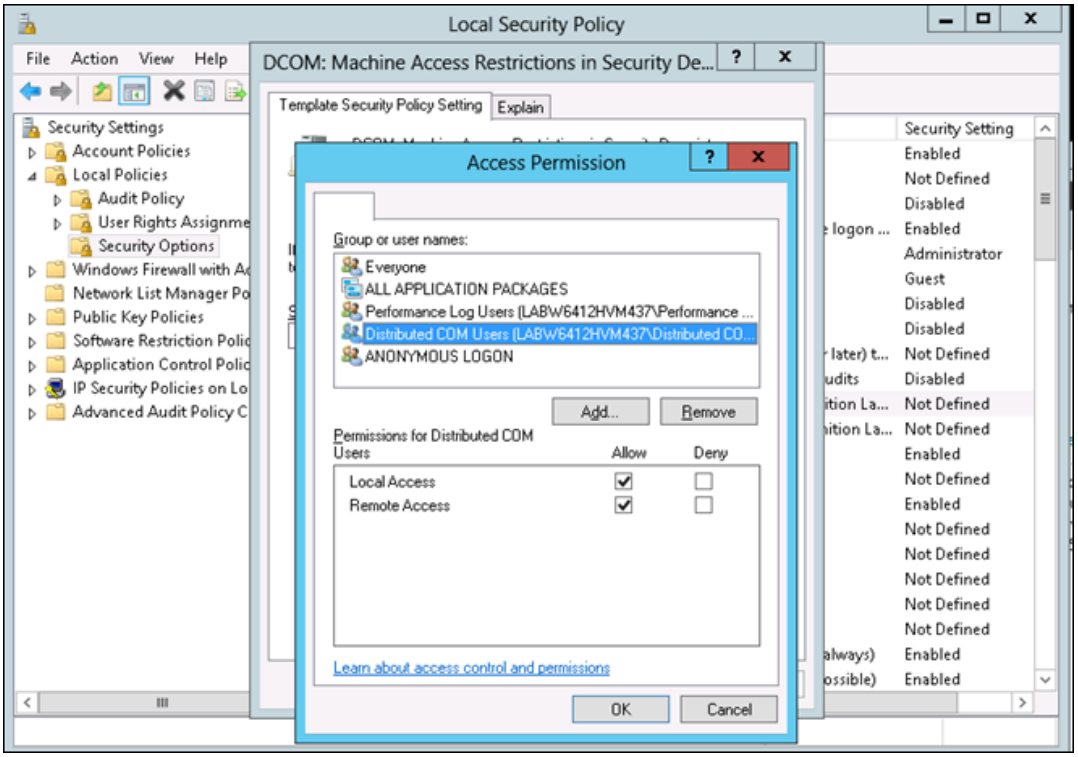
4. The Access Permission window appears. Click Add.



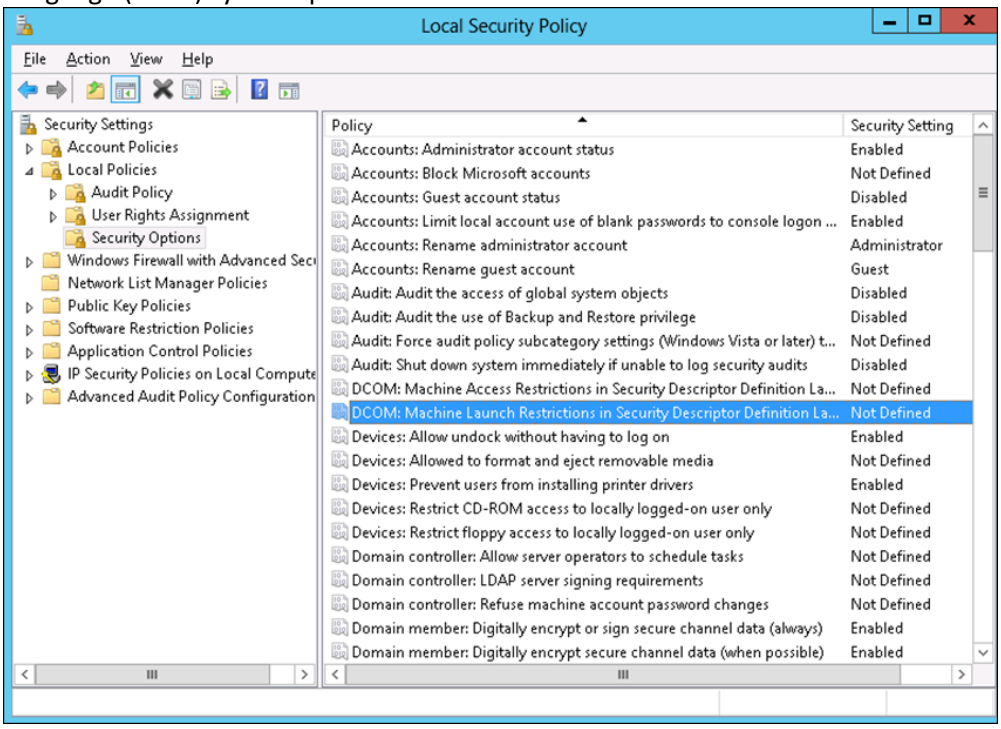
5. The Select Users or Groups window appears. Enter the Medici Users group in the Enter the object names to select box and click OK.



6. In the Access Permission window for the newly added group, select both the Local Access and Remote Access check boxes in the Allow column and click OK.



7. Click OK again to exit the Template Security Policy Setting window.
8. Repeat steps 2-7 for the DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax option.



Appendix B: Enabling COM+ for Windows Server 2016

The Application Server role has been removed by Microsoft from Windows Server 2016. It is needed by Medici and you will need to restore it by manually setting the registry value that allows COM+ remote access.

The Application Server role has been removed by Microsoft from Windows Server 2016. It is needed by Medici and you will need to restore it by manually setting the registry value that allows COM+ remote access. To do this:

1. In the Windows Server Start search box, type regedit, and click regedit.exe in the results list.
2. Locate the following subkey in the Registry Editor:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3
3. Right-click the RemoteAccessEnabled DWORD.
4. In the Value data box, enter 1.
5. Click OK.

Note: Additional information can be found at https://support.microsoft.com/en-us/help/3182294/0x80004027-error-when-you-try-to-remotely-access-com-object-after-you..

Appendix C: Medici System Configurations

There are different ways to configure Medici. Larger institutions often network all the various features on different machines: the SQL Server on one machine, the Medici Server on a second machine, the DMTransaction folder for the output files on a third machine, and then the client feature on individual workstations. Other institutions may choose to house the SQL server and Medici Server on one box, with the DMTransaction folder on a separate file server.

Based on the number of machines you want to use to run Medici, there are different configuration options:

3-Tier Configuration

Perform a 3-Tier installation if you want to have three separate machines running the three main features of the Medici application: one for the Database, one for the Medici Server, and one for each of the Medici Client workstations.

2-Tier Configuration

Perform a 2-Tier installation if you want to split the three main Medici features of Database, Medici Server and Medici Client between two separate machines, which you may accomplish in a variety of ways.

1-Tier Configuration or Stand-Alone Implementation

Perform a 1-Tier installation if you want to have all three Medici features on one machine: Medici Client, Medici Server and Database.

Note: *4-Tier Configuration* - The placement of the DMTransaction folder can create an extra “tier” for any of the above configurations if the folder is located on a different machine. The transaction folder is shared and typically exists on a network file server, so it is accessible to all client machines.

Any machine that houses the DMTransaction folder needs to have its disk free space monitored over time. The transaction files increase in direct relation to the number of loan documents created.

Changing Configuration during Upgrade

To change your existing configuration as part of your upgrade, first uninstall the previous release of Medici from all machines and when installing the new release of Medici, select your new configuration.

Appendix D: Medici Configuration Settings Utility

Overview

The Medici Configuration Settings Utility is designed to help customers set/change configuration settings which can affect how the Medici Application behaves. The configuration settings are applied system-wide and not on a user-by-user or desktop-by-desktop basis.

Installation

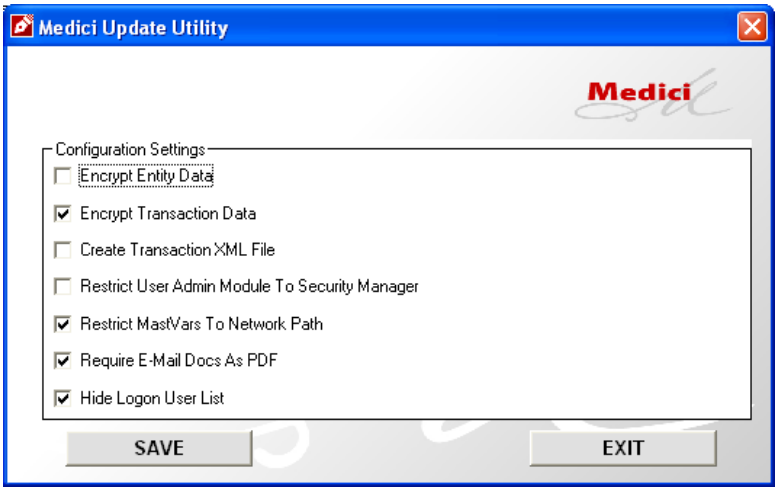
No installation is necessary. The "Configuration Settings.exe" is a stand-alone application that works with an existing Medici installation. The utility can be run from either an installed client (desktop) or from the

application server where the Medici Server Application is installed. It is recommended the utility be used by a Medici system administrator, and the tool be used from a location that has limited access to general users.

Running the Utility

Double-click the "Configuration Settings.exe" to launch the utility. The following screen will appear and the settings on the initial screen will reflect the current configuration settings in your environment.

The Utility Main Screen will reflect the current configuration settings in your Medici System. Your settings may differ from this graphic.



Settings

The settings you can make and their descriptions are provided below.

Encrypt Entity Data: No longer used.

This item is a relic and is no longer in use. Changing the setting on this will not affect anything in the Medici Application. Primary entity information (SSN/TIN) is automatically encrypted when entered into the Medici system.

Encrypt Transaction Data:

Specific data items in each transaction that are considered as "non-public information" (SSN/TIN, names of parties to a transaction, etc.) are encrypted when stored in the transaction data store. Should anyone gain access to the specific data store for a transaction, this sensitive information will be encrypted and will be useless.

- TRUE (checked): The data considered "non-public" is encrypted when at rest in the specific transaction data store.
- FALSE (unchecked): The data considered "non-public" is not encrypted when at rest in the specific transaction data store.
- DEFAULT: False

Create Transaction XML File:

Each transaction in the Medici system is represented in an XML format, and that XML contains all the information pertinent to the transaction. Normally, this data is written out to a file with a ".xml" extension and resides in the specific folder for each transaction. By setting this item to "False" (unchecked), the XML data will be stored only in the Medici database and will never be stored as a file on disk. This can improve your overall security for transaction data.

- TRUE (checked): The xml data will be written to a file stored with the transaction on disk
- FALSE (unchecked): The xml data is stored in the Medici database, and is never written as a file to disk.
- DEFAULT: True

Restrict User Admin Module to Security Manager:

The "Security Manager Role" is intended to designate a specific user as someone that only deals with the User Admin module, where security settings and user permissions are configured in the Medici Application. A user designated as a Security Manager does not have access to any other part of the Medici Application; this role specifically limits a user to accessing only the User Admin module, regardless of the permissions you grant the user or the group you assign the user into.

Note the following:

- A user that is designated as both an Admin user and a Security Manager still has access to all areas of the application.
- By setting this item to "True", the Use Admin module will only be accessible to users designated as a Security Manager. If you turn this item on and have not designated a user as a Security Manager, then no one will have access to the User Admin module.
- TRUE (checked): Access to the User Admin module in Medici is available only to users that are designated as Security Managers. No other users (not even an Admin user) will be able to access the module.
- FALSE (unchecked): Access to the User Admin module is available to Security Managers, Admins and any other users that have been granted specific permissions to access the User Admin module.
- DEFAULT: False
- A user that is designated as both an Admin user and a Security Manager still has access to all areas of the application.
- By setting this item to "True", the Use Admin module will only be accessible to users designated as a Security Manager. If you turn this item on and have not designated a user as a Security Manager, then no one will have access to the User Admin module.

Restrict MastVars to Network Path

Each transaction in Medici contains its own data store for information about that transaction. This data store can be used for processing on the local client desktop during document generation after which it is moved back to the shared network directory for the transactions. This can improve performance during document generation. However, if you are concerned about any security or maintenance issues which might arise from having this data store on local desktops, you can configure Medici so that the data store will never be moved onto or saved on the local client machine.

- TRUE (checked): The transaction data store will not be moved to or used from the local client desktops.
- FALSE (unchecked): The transaction data store will be used from the local client desktops during document generation.
- DEFAULT: False

Note: Setting this item to True may adversely affect performance during document generation in the Medici system. If you elect to use this setting, we recommend that you test the performance during document generation.

Require Email Docs as PDF

This item is a relic and is no longer in use. Changing the setting on this will not affect anything in the Medici Application. Primary entity information (SSN/TIN) is automatically encrypted when entered into the Medici system. Instead, controlling the format of email attachments can be controlled on a user or group basis form the Medici User Admin module. Use the settings for "Disable PDF Format" and "Disable Office Format."

Hide Logon User List

When Medici is configured to have users logon by entering a Medici Username and Password, the application provides a drop-down list of available Medici Usernames from which the user can select. Some customers may feel this represents a potential security issue, since anyone attempting to login to the system would be shown a list of valid usernames. This setting will change the Medici logon so that no user names are shown. A user attempting to logon to the Medici application will have a logon available, but there will be no drop-down list of usernames. Instead, the user will need to enter in the correct username for their logon.

- TRUE (checked): The logon form will not contain a dropdown list of available Medici usernames.
- FALSE (unchecked): The logon form will contain a dropdown list of available Medici usernames.
- DEFAULT: False

Note: If Medici is configured to use single-sign-on authentication, this setting has no effect.

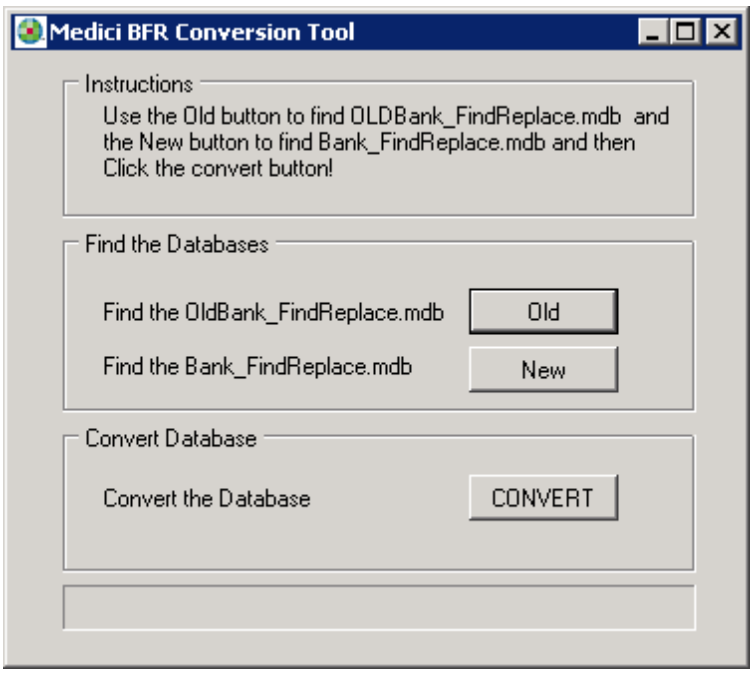
Transaction ID Maximum Length

The Medici application has a limit on the length of the name that can be used for a transaction. Historically, this has been 30 characters. To allow customers greater flexibility in their transaction naming conventions, customers can now configure Medici to accept longer transaction names. This setting can be used to configure the length of transaction names to be up to 64 characters. If this setting is changed to a value less than the minimum length or more than the maximum length listed below, Medici will automatically adjust the allowable length.

- MINIMUM LENGTH: 30 is the minimum value for this setting
- MAXIMUM LENGTH: 64 is the maximum value for this setting.
- DEFAULT: The default Transaction ID length is 30 characters.

Appendix E: Bank Find and Replace

For this activity, you will use the Medici BFR conversion tool.



Run the Conversion Tool

1. To run the conversion tool, on a client machine browse to the MediciClient folder, typically located under C:\Medici, or to the folder you indicated during the install.
2. Double-click Medici Conversion Tool.exe. The main screen appears.
3. Click Old and browse to the Bank_FindReplace.mdb which you backed up in the pre-install steps. Note that the label next to the Old button indicates the filename is OldBank_FindReplace.mdb but you did not need to rename the file when you backed it up.
4. Click New and browse to the Word Automation folder, typically under C:\Medici\MediciClient\Word Automation. Select Bank_FindReplace.mdb.
5. Click CONVERT to start the conversion process.
6. When the conversion is complete, the conversion complete message appears.
7. Click OK to exit the Medici BFR Conversion Tool.

Wolters Kluwer

About Wolters Kluwer

Wolters Kluwer (EURONEXT: WKL) is a global leader in information, software, and services for professionals in healthcare, tax and accounting, financial and corporate compliance, legal and regulatory, and corporate performance and ESG. We help our customers make critical decisions every day by providing *expert solutions* that combine deep domain knowledge with specialized technology and services.

Wolters Kluwer reported 2022 annual revenues of €5.5 billion. The group serves customers in over 180 countries, maintains operations in over 40 countries, and employs approximately 20,000 people worldwide. The company is headquartered in Alphen aan den Rijn, the Netherlands.

For more information, visit https://www.wolterskluwer.com, follow us on LinkedIn, Twitter, Facebook, and YouTube.

For Self-service: https://wolterskluwer.my.site.com/ComplianceSolutionsSupport/s/
Product Download Site: https://compliancedownload.wolterskluwer.com/
Customer Service: (800) 552-9410 *Available Monday through Friday, 8:00 a.m. to 7:00 p.m., Eastern time.*

Medici SupportLine:
Phone: (800) 274-2711 ext. 1125343
Available Monday through Friday, 8 a.m. to 8 p.m., Eastern time.
Email: medicisupport@wolterskluwer.com

Wolters Kluwer