

CenTran 5 Getting Started Guide

dormakaba

dormakaba Welcome

dormakaba is the world's leading manufacturer and supplier of high security, electronic safe locks. Its complete line of self powered, battery, and mechanical locks meets virtually every safe lock requirement. dormakaba is dedicated to satisfying end-user needs for security, safety, and convenience. We welcome you to the world of dormakaba security and the Cencon lock.

[Manual Conventions](#)

[Trademarks](#)

Table Of Contents

[The CenTran Service Package](#)

[Cencon Security System Product Overview](#)

[System Requirements](#)

[PC Hardware Installation](#)

[Before Installing the CenTran Software](#)

[Software Installation and Setup](#)

[Install Service](#)

[Create ODBC Database Connection \(Microsoft SQL\)](#)

[Configure the CenTran Service](#)

[Configuration File - system.serviceModel / bindings Section](#)

[Configuration File - system.serviceModel / services Section](#)

[Configuration File - system.serviceModel / behaviors Section](#)

[Set Up CenTran Server Certificates](#)

[Guided Certificate Installation](#)

[Using An Already Installed Server Certificate](#)

[Using A Server Certificate Provided In A File](#)

[Creating A Server Certificate](#)

[Self-Guided Certificate Installation](#)

[Set Up CenTran Management Security](#)

[Set Up CenTran Logging](#)

[Set Up CenTran Management Web Access](#)

[Set Up CenTran Event Logging](#)

[Install / Start the CenTran Service](#)

[Configure the CenTran Service using CenTran Configuration Manager](#)

[Setup Keybox](#)

[Select ODBC Database Connection](#)

[Set Company Number](#)

[Set File Settings](#)

[Start Transaction Processing](#)

[View Web Service XML Settings](#)

[View Web Service JSON Settings](#)

[View Web RSS Feed Settings](#)

[View CenTran Agent Settings](#)

[View CenTran Event Log](#)

[View CenTran Agent Persistent Connections](#)

[Stop Transaction Processing](#)

[Configure the CenTran Service using Web Management Interface](#)

[Log on to CenTran Management](#)

[Setup Keybox](#)

[Select ODBC Database Connection](#)

[Set Company Number](#)

[Set File Settings](#)

[Start Transaction Processing](#)

[View Web Service XML Settings](#)

[View Web Service JSON Settings](#)

[View Web RSS Feed Settings](#)

[View CenTran Agent Settings](#)

[View CenTran Event Log](#)
[View CenTran Agent Persistent Connections](#)
[Stop Transaction Processing](#)
[Stop / Uninstall the CenTran Service](#)
[Appendix A - Beta Expiration](#)
[Appendix B - Troubleshooting: Check Certificates](#)
[Appendix C - Troubleshooting: Check Run Time Error](#)

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Manual Conventions

This CenTran Getting Started Guide contains information on the installation and set up of the hardware and software required to manage locks. Some conventions that are followed are:

- The Smart Keys needed for a particular operation will be shown beside the flowcharts that describe the operation.
- Input to the PC will be shown in **bold type**.
- The screen samples may not look exactly as they do on your system depending on which version of the Windows operating system you are using.
- Highlighted items:

Note

Indicates a point to consider.

Helpful Hint

Indicates a technique or method that works well.

Caution

Indicates the need for care and caution to be observed during a procedure or process.

Warning

Indicates the possibility of loss of data or system integrity.

Before reading the CenTran Getting Started Guide, you should be familiar with basic Windows concepts and techniques. For detailed information, refer to your Windows documentation.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Trademarks

The following items are trademarks or registered trademarks of dormakaba in the United States and/or other countries.

- Cencon System 2000
- Cencon
- PowerStar Technology
- Smart Key

Adobe and Adobe Reader are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

IBM is a registered trademark of International Business Machines Corporation ("IBM") in the United States and/or other countries.

iButton is a registered trademark of Dallas Semiconductor.

Microsoft, Windows, and Windows Server are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Notice: The information in this manual is subject to change without notice and does not represent a commitment on the part of dormakaba. dormakaba shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Introducing CenTran 5

CenTran 5 Getting Started Guide

The CenTran Version 5 Package

The CenTran 5 implementation package includes:

- The CenTran Version 5 Install source (DVD, USB drive, or download)
- CenTran 5 Getting Started Guide
- CenTran 5 XML Programming Manual - Included on install source (DVD, USB drive, or download) in electronic format
- CenTran 2 Programming Guide - Included for legacy CenTran use on install source (DVD, USB drive, or download) in electronic format

If you are missing any of the above items, contact dormakaba Customer Service at 1(800) 950-4744

CenTran 5 System Requirements

To use the CenTran program, the following minimum hardware and software requirements must be met:

- IBM® compatible PC that is capable of running the Windows® OS's listed below and has an available USB port for the dormakaba USB Key Box.

Note

The Cencon KeyBox requires a fully compliant USB 2.0 connection. Some computers, especially laptops and notebooks, may not provide sufficient power for the Cencon KeyBox. In these cases it may be necessary to use a powered USB hub to attach the Cencon Key Box. On laptops or notebooks with "power saving" features that turn off USB power, the computer's Operating System (OS) could disconnect from the Cencon Key Box. In this instance, after awakening the computer and CenTran 5 software, unplug and re-plug the USB cable between the computer and the Cencon Key Box.

Note on Virtual Machines

It is recommended that the CenTran program be installed on a dedicated physical server. However, CenTran will operate correctly when installed in a virtual machine that fully emulates an IBM-compatible PC that meets all of the system requirements detailed in this section.

Important Note: Many virtual hosting services will not allow the attachment of USB devices directly to the physical machine hosting a given virtual machine. When the CenTran program is running under such a host, the Cencon USB KeyBox must be attached through a secure, fully USB-2.0-compliant USB-redirection solution.

- 4 GB RAM Minimum (8 GB RAM or higher is recommended.)
- If your install source is a DVD, a DVD Drive is needed. The install source can be a DVD, USB drive, or download.
- Hard Disk Drive with at least 50 megabytes disk space free
- **Please note that systems running more than 25,000 locks should run at higher than 4 GB RAM to ensure optimal system performance. (Please refer to Appendix D of the Cencon Reference Manual for more information.)**

Important Note

If you are upgrading from a previous version of Cencon and CenTran, you should also allow ample disk space for database growth.

- Windows® 7 32/64-bit, 8.1 32/64 bit, 10 32/64 bit, Windows® 2008 R2 Server 64-bit, 2012 R2 Server 64 bit, or Windows Server 2016, with 4.5.1 or higher .NET Framework.
 - You must be logged into Windows® with Admin authority
- **An installed Database Management System (DBMS):**
 - **Either Microsoft® SQL Server® 2008 R2, 2012 R2 Server 64 bit, 2014 R2 Server, 2016, or 2017 (including the SQL Server® Express, Standard, or Enterprise Editions).**
 - The DBMS installation does not have to be on the same computer as CenTran. You will need to have a valid ODBC connection to the DBMS for CenTran to use.
 - The above computer requirements do not include the requirements for the DBMS. If the DBMS is being run on the same computer as CenTran, then the total requirements will be the requirements of CenTran plus those of the DBMS.
 - The requirements of the DBMS installation will vary depending on the number of locks and users being used by Cencon and CenTran and the number of Cencon and CenTran installations connected to that DBMS.
 - A full installation of SQL Server® typically also requires .NET Framework 3.5; how this is obtained and installed will depend on the version of SQL Server® being installed and the version of Windows® on which it is being installed.

Note

If you do not have an existing Microsoft® SQL Server® database, you can download a free copy of the latest Microsoft® SQL Server® Express Edition from the Microsoft® web site at <http://www.microsoft.com/express/sql/default.aspx> You should also download and install the SQL Server®

Management Studio.

Be sure to read the related Microsoft® information on system requirements and prerequisites for these components. Contact dormakaba Technical Support for additional information.

Note - The screens shown in the CenTran Software manuals were captured on a Windows® 7 system. Your screens may look slightly different.

Important Note

CenTran 5 also requires an operational Cencon 5 system and associated database, either locally or on a network accessible computer. It is not compatible with previous versions of Cencon System 2000 software.

PC Hardware Installation

Note

The Cencon Key Box is not included with the CenTran 5 program package and must be purchased separately if not already installed on your PC system. See the Cencon 5 Getting Started Guide for Key Box installation instructions.

Important Note

Running the Cencon 5 software and the CenTran 5 software concurrently on a PC system is not recommended.

Before Installing the CenTran 5 Software

Warning

If you have not already contacted dormakaba Customer Service at 1(800) 950-4744 in preparation for your installation of CenTran 5, you must do so at this time to review minimum system requirements and database setup for your installation of CenTran 5, and to perform data validity checks on any current Cencon data.

Warning

During the CenTran 5 configuration process, you will be required to enter a unique four digit Company Number/ID. If you are a branch of a larger company, this ID must be identical to that used for all other Cencon and CenTran installations by your company. It is helpful to determine what the four-digit number is before you begin the installation process.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Cencon ATM Cash Vault Security System Product Overview

CenTran Version 5 Getting Started Guide

The Challenge

While the front of ATMs are accessed by customers with individual cards and PINs, the back of the ATM is often accessed by service personnel from multiple companies all using the same lock combination. Bank employees, cash replenishers, technical service reps, repair personnel all using the same combination to open an ATM safe poses a significant security risk.

The Solution

The Cencon ATM Cash Vault Security System from dormakaba is designed to combat insider theft from ATMs through the combined use of lock hardware, systems software and Smart Keys. The Cencon system offers total access control and accountability with its One Time Combination feature. The One Time Combination is dispatched from a central location and cannot be reused at a later date, thus eliminating temptation.

The Cencon ATM Cash Vault Security System allows locks located anywhere in the world to be controlled and monitored from one central location.

The central location consists of

- A database describing locks, lock administration personnel, lock service personnel, lock access details and history.
- dormakaba software that
 - Manages the creation and distribution of One Time Combinations(OTC).
 - Tracks the status of each lock and user.
 - Provides audit capability.
 - Can be used interactively by a human Dispatcher or programmatically by customer applications such as IVR or Web base interfaces.

The software provided by dormakaba consists of

- Cencon Interactive Application: Interactive Central Point of Control
 - Used to create, distribute, manage One Time Combinations (OTC).
- CenTran Service: Background Central Point of Control
 - Used by customer, 3rd party applications to create, distribute and manage OTCs.
- CenTran Web Services: Used by customer web applications to communicate with CenTran Service.
- CenTran Agent
 - Remote lock management: Allows CenTran Service to communicate with ATM lock, streamlining lock administration.
- Key Box Agent
 - Remote key management: Allows CenTran Service to communicate with remote key boxes, supporting decentralized lock personnel.

The Cencon ATM Cash Vault Security System supports three Modes of Operation:

FLM Mode

Designed for First Line Maintenance (FLM) personnel such as cash replenishers, technical service reps, repair personnel, the FLM mode of the Cencon lock permits the dispatch center to give a One Time Combination (OTC) for ATM lock access to a technician "on the fly." FLM personnel are each issued a Smart Key and call their dispatch center to request a One Time Combination. Once used, this combination will not function again, thus ensuring absolute access control. Once the Cencon unit is locked, a Close Seal code is displayed on the lock's LCD. Entering this Close Seal into the dispatch center's computer documents that the Cencon lock is locked and secure.

Route Mode

While permitting the same access control as FLM Mode, Route Mode additionally permits pre-defined routes for armored cash replenishers. Route personnel are each issued a Smart Key. A route of locks, along with an OTC for each lock on the route, may be assigned by a dispatch center permitting route personnel to access a series of locks without contacting their dispatch center at each individual lock. Route personnel can either call their dispatch center at the end of the shift to report the Close Seals, or the Close Seals can be read from the Smart Key by the Cencon software.

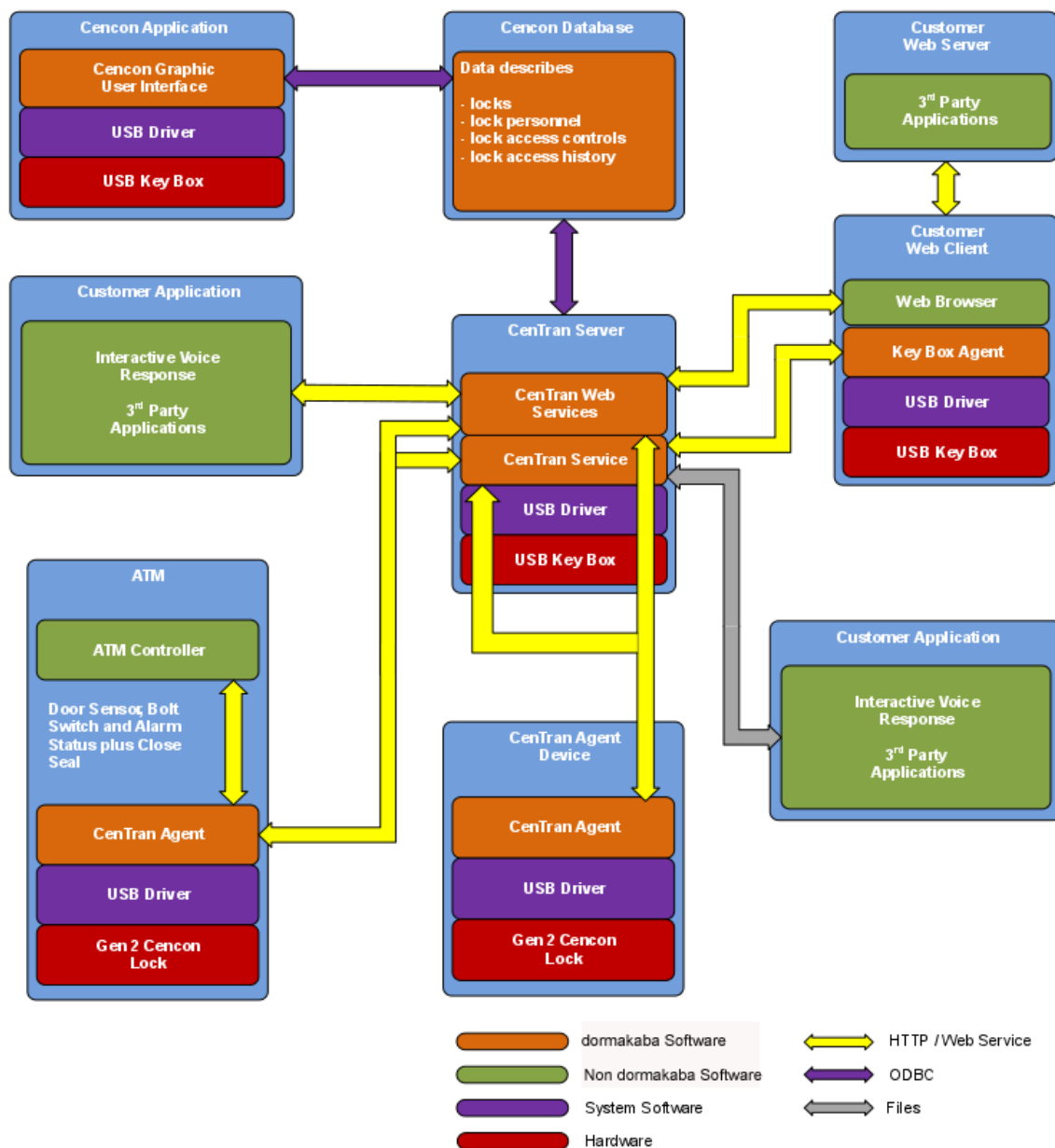
Bank Mode

Bank Mode is designed for bank personnel who may need access to the Cencon system lock but do not wish to operate through a dispatch center. Smart Keys and combinations are issued to bank personnel who may unlock the Cencon lock at any time. An internal audit trail tracks all activity of bank personnel just as it does for FLM and Route personnel. dormakaba Cencon software permits bank administrators to manage Bank Mode on site. Bank users may be added or deleted and audit trails may be downloaded from the lock.

High Level Overview of Cencon ATM Cash Vault Security System Component Architecture

The Cencon ATM Cash Vault Security System consists of several components whose method of use will vary depending on the business model of the supported enterprise. Presented here is a brief high level overview of the Cencon ATM Cash Vault Security System components.

Cencon ATM Cash Vault Security System Component Architecture



Cencon Database:

- Defines locks to be controlled, monitored and audited.
- Defines personnel allowed to access locks.
- Defines Personnel allowed to control access to locks.
- Contains access history for each lock.

Cencon Application:

- Interactive, graphical Windows application used to manage the Cencon Database contents.
- Requires a Cencon Key Box be attached to a USB port of the same computer.

CenTran Service:

- Available for use by customer applications to manage the Cencon Database contents.
- Applications communicate with the service via files or HTTP / Web Services.
- Runs in background as a Windows Service.

CenTran Web Services:

- Available for use by web applications to manage Cencon Database contents.

Customer Application Using CenTran Service Command File:

- The CenTran Service performs actions against the Cencon Database per commands imbedded in files.
- Results of those actions are reported in output files created by the CenTran Service.

Customer Application Using CenTran Web Services:

- The CenTran Service performs actions against the Cencon database per commands received via the CenTran Web Services.
- Results of those actions are reported to the customer application via the CenTran Web Services.

CenTran Agent:

- Allows CenTran Service to monitor lock in a real time manner.
- Runs on the ATM in the background as a Windows Service.

Key Box Agent:

- Allows CenTran Service access to Cencon Key Boxes on remote systems.
- Runs on remote Web Client systems in background as a Windows Service.

Customer Web Client:

- Customer developed web browser based user interface used to manage Cencon Database contents as well as Cencon Smart Keys via the CenTran Web Services.
- Can be located remotely.

Cencon ATM Cash Vault Security System Components and Business Processes

Examples of Business Processes Supported by Cencon ATM Cash Vault Security System Components:

1. FLM (First Line Maintenance) Operations with human Dispatcher:
 1. FLM personnel reaches ATM and contacts Dispatcher requesting OTC.
 2. Dispatcher generates OTC via Cencon interactive application, gives OTC to FLM personnel.
 3. FLM personnel opens and closes lock, recording the Close Seal.
 4. FLM personnel gives Close Seal to Dispatcher who enters it into Cencon database via Cencon interactive application.
2. Route Operations with human Dispatcher:
 1. Before starting route, Route personnel contacts Dispatcher and requests OTCs for each lock on route.
 2. Dispatcher generates OTCs via Cencon interactive application, gives OTCs to Route personnel.
 3. Route personnel opens and closes each lock on route, recording Close Seals.
 4. When the Route has been completed, the Close Seals are given to the Dispatcher who enters them into the Cencon database via Cencon interactive application.
3. FLM Operations with IVR (Interactive Voice Response) system:
 1. FLM personnel reaches ATM, calls IVR system and requests OTC.
 2. IVR system generates OTC via CenTran Command File interface and reports OTC to FLM person.
 3. FLM personnel opens and closes lock, recording the Close Seal.
 4. FLM personnel calls IVR system and enters Close Seal.
 5. IVR system records Close Seal in Cencon database via CenTran Command File interface.

Though business processes will vary between companies there are core lock management tasks that will be used in every enterprise such as:

- Create User and Initialize Smart Key
- Delete User
- Dispatch Lock
- Open / Close physical lock
- Close Lock in Cencon database
- Reassign Lock
- Audit Lock
- Audit Key
- Audit Cencon Database

The following lists describe for a few of the core lock management tasks one possible flow of control through the Cencon ATM Cash Vault Security System components.

Create User and Initialize Smart Key:

- Dispatcher ->
- Customer Web Client ->
- CenTran Web Services ->
- CenTran Service ->
- CenTran Web Services ->
- Key Box Agent (writes KEY) ->
- CenTran Service ->
- CenTran Web Services ->
- Customer Web Client

Note:

- Customer Web Client & Key Box Agent will probably be on same location but do not have to be
- Customer Web Client does NOT require a Keybox on the same system

Dispatch Lock(s):

- Dispatcher ->
- Customer Web Client ->
- CenTran Web Services ->
- CenTran Service ->
- Cencon Database ->
- CenTran Service ->
- CenTran Web Services ->
- Customer Web Client ->
- Dispatcher receives OTC
- Dispatcher transmits OTC to FLM/Route personnel

Lock is physically opened and closed:

- Service personnel calls Close Seal in to the Dispatcher who "Closes Lock" in the Cencon Database. The component flow is the same as that described for Dispatch Lock(s).
 - OR
- CenTran Agent Service on ATM uses CenTran Web Services to report Closure to CenTran Service and "Closes Lock" in the Cencon Database programmatically:
 - Lock is closed ->
 - CenTran Agent ->
 - CenTran Web Services ->
 - CenTran Service ->
 - Cencon Database ->
 - CenTran Service ->
 - CenTran Web Services ->
 - CenTran Agent

Introducing CenTran 5

CenTran 5 Getting Started Guide

The CenTran Version 5 Package

The CenTran 5 implementation package includes:

- The CenTran Version 5 Install source (DVD, USB drive, or download)
- CenTran 5 Getting Started Guide
- CenTran 5 XML Programming Manual - Included on install source (DVD, USB drive, or download) in electronic format
- CenTran 2 Programming Guide - Included for legacy CenTran use on install source (DVD, USB drive, or download) in electronic format

If you are missing any of the above items, contact domakaba Customer Service at 1(800) 950-4744

CenTran 5 System Requirements

To use the CenTran program, the following minimum hardware and software requirements must be met:

- IBM® compatible PC that is capable of running the Windows® OS's listed below and has an available USB port for the domakaba USB Key Box.

Note

The Cencon KeyBox requires a fully compliant USB 2.0 connection. Some computers, especially laptops and notebooks, may not provide sufficient power for the Cencon KeyBox. In these cases it may be necessary to use a powered USB hub to attach the Cencon Key Box. On laptops or notebooks with "power saving" features that turn off USB power, the computer's Operating System (OS) could disconnect from the Cencon Key Box. In this instance, after awakening the computer and CenTran 5 software, unplug and re-plug the USB cable between the computer and the Cencon Key Box.

Note on Virtual Machines

It is recommended that the CenTran program be installed on a dedicated physical server. However, CenTran will operate correctly when installed in a virtual machine that fully emulates an IBM-compatible PC that meets all of the system requirements detailed in this section.

Important Note: Many virtual hosting services will not allow the attachment of USB devices directly to the physical machine hosting a given virtual machine. When the CenTran program is running under such a host, the Cencon USB KeyBox must be attached through a secure, fully USB-2.0-compliant USB-redirection solution.

- 4 GB RAM Minimum (8 GB RAM or higher is recommended.)
- If your install source is a DVD, a DVD Drive is needed. The install source can be a DVD, USB drive, or download.
- Hard Disk Drive with at least 50 megabytes disk space free
- **Please note that systems running more than 25,000 locks should run at higher than 4 GB RAM to ensure optimal system performance. (Please refer to Appendix D of the Cencon Reference Manual for more information.)**

Important Note

If you are upgrading from a previous version of Cencon and CenTran, you should also allow ample disk space for database growth.

- Windows® 7 32/64-bit, 8.1 32/64 bit, 10 32/64 bit, Windows® 2008 R2 Server 64-bit, 2012 R2 Server 64 bit, or Windows Server 2016, with 4.5.1 or higher .NET Framework.
 - You must be logged into Windows® with Admin authority
- **An installed Database Management System (DBMS):**
 - **Either Microsoft® SQL Server® 2008 R2, 2012 R2 Server 64 bit, 2014 R2 Server, 2016, or 2017 (including the SQL Server® Express, Standard, or Enterprise Editions).**
 - The DBMS installation does not have to be on the same computer as CenTran. You will need to have a valid ODBC connection to the DBMS for CenTran to use.
 - The above computer requirements do not include the requirements for the DBMS. If the DBMS is being run on the same computer as CenTran, then the total requirements will be the requirements of CenTran plus those of the DBMS.
 - The requirements of the DBMS installation will vary depending on the number of locks and users being used by Cencon and CenTran and the number of Cencon and CenTran installations connected to that DBMS.
 - A full installation of SQL Server® typically also requires .NET Framework 3.5; how this is obtained and installed will depend on the version of SQL Server® being installed and the version of Windows® on which it is being installed.

Note

If you do not have an existing Microsoft® SQL Server® database, you can download a free copy of the latest Microsoft® SQL Server® Express Edition from the Microsoft® web site at <http://www.microsoft.com/express/sql/default.aspx> You should also download and install the SQL Server®

Management Studio.

Be sure to read the related Microsoft® information on system requirements and prerequisites for these components. Contact dormakaba Technical Support for additional information.

Note - The screens shown in the CenTran Software manuals were captured on a Windows® 7 system. Your screens may look slightly different.

Important Note

CenTran 5 also requires an operational Cencon 5 system and associated database, either locally or on a network accessible computer. It is not compatible with previous versions of Cencon System 2000 software.

PC Hardware Installation

Note

The Cencon Key Box is not included with the CenTran 5 program package and must be purchased separately if not already installed on your PC system. See the Cencon 5 Getting Started Guide for Key Box installation instructions.

Important Note

Running the Cencon 5 software and the CenTran 5 software concurrently on a PC system is not recommended.

Before Installing the CenTran 5 Software

Warning

If you have not already contacted dormakaba Customer Service at 1(800) 950-4744 in preparation for your installation of CenTran 5, you must do so at this time to review minimum system requirements and database setup for your installation of CenTran 5, and to perform data validity checks on any current Cencon data.

Warning

During the CenTran 5 configuration process, you will be required to enter a unique four digit Company Number/ID. If you are a branch of a larger company, this ID must be identical to that used for all other Cencon and CenTran installations by your company. It is helpful to determine what the four-digit number is before you begin the installation process.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Software Installation and Setup

CenTran 5 Getting Started Guide

Complete the following steps to install the software:

1. Check the PC Date and Time Properties (date, time, time zone, DST adjustment setting) from the Control Panel to ensure accuracy. Adjust, if necessary, before proceeding.
2. Ensure that no other programs are running.
3. If you have a previous version of Cencon installed, you should ensure that data has been archived in accordance with the customer archive requirements and then backup the current Cencon database.
4. If your install source is a DVD, insert the Cencon 5 Install DVD in the appropriate drive. The install source can be a DVD, USB drive, or download. If you have autorun enabled on your system, the Cencon 5 Installation screen will be displayed. Otherwise, double click **Autorun.exe** from the CenTran 5 install source (DVD, USB drive, or download) root directory, and the CenTran 5 Installation screen will be displayed.

The CenTran Version 5 Software Installation dialog is loaded and the Main Menu is displayed:



5. From the Main Menu, click on the **Install** button.
6. Depending on your operating system, either the 32 or 64-bit CenTran install page is displayed:

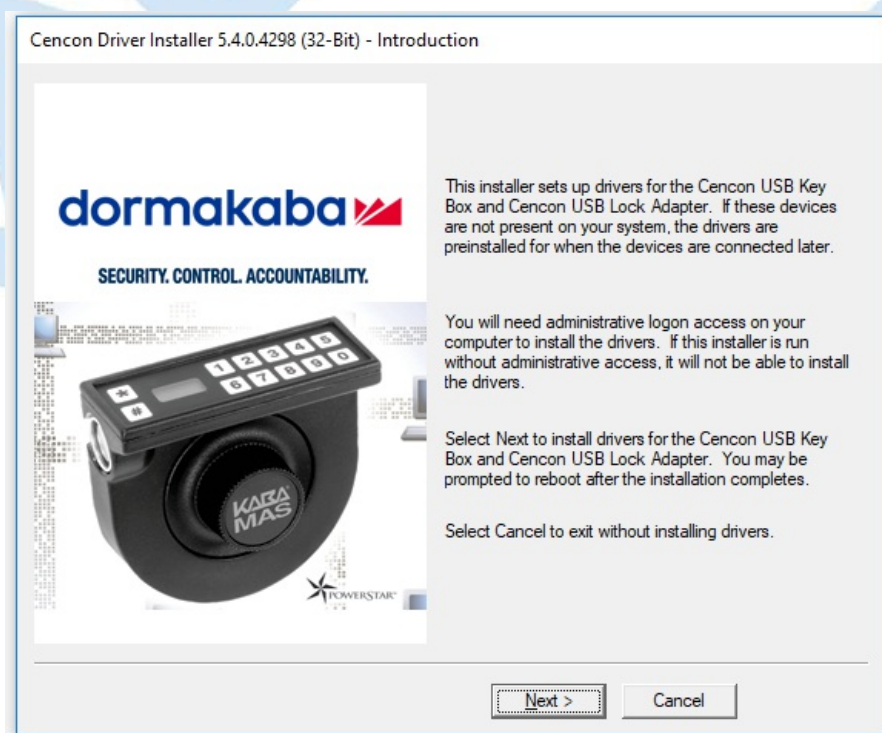


7. Install Microsoft® SQL Server® 2012 Native Client 11.0 ODBC Driver

Install the Microsoft® SQL Server 2012 Native Client 11.0 ODBC Driver on your system if you have not already done so. Using the default SQL ODBC Driver available with Windows will result in slow performance. If you have a more recent SQL installation from Microsoft than SQL Server 2012 use that SQL ODBC Driver. To install the provided SQL ODBC Driver select the **SQL ODBC Driver** button.

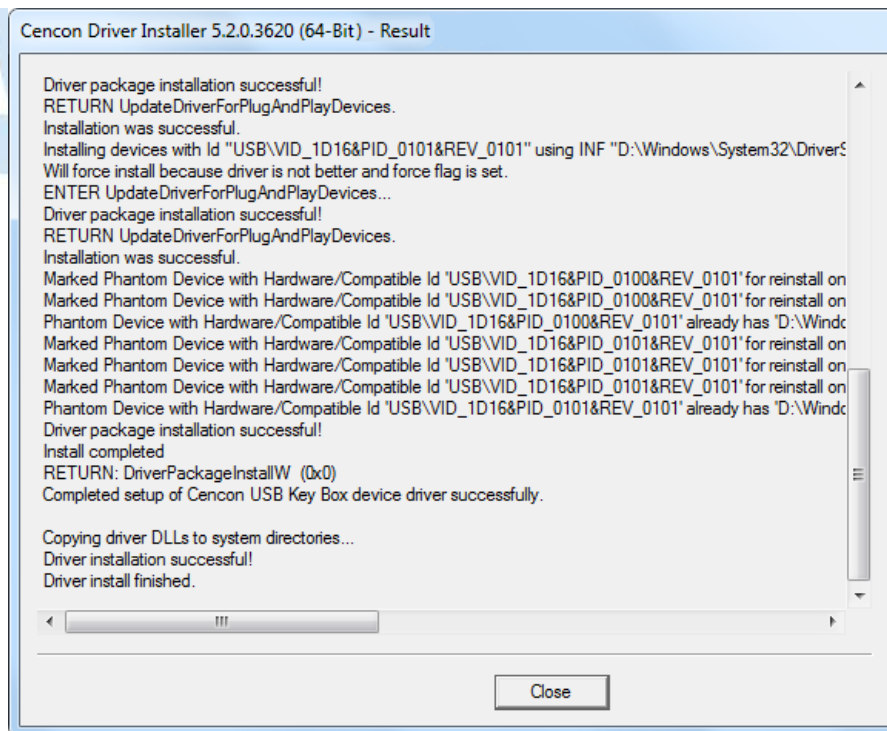
8. Install Cencon USB KeyBox and Cencon Lock Adapter Device Drivers

Install the Cencon USB KeyBox and Cencon Lock Adapter device drivers by clicking on the Windows Drivers button. The button will state either **Windows 32 Bit Drivers** or **Windows 64 Bit Drivers** depending on if you have a 32 or 64 bit operating system. The Cencon Driver Installer application will be launched by clicking on the button.



Click on **Next** to begin installing drivers. The Cencon Driver installer will update existing drivers as needed. It will also preinstall the drivers if you do not have a Cencon USB KeyBox or Cencon Lock Adapter attached yet. You will be prompted for Windows operating system authorization several times as the drivers are installed. You will need to select **Yes** for each one of these approval dialogs. You must have administrative rights on the operating system you are installing drivers to. The driver install can take several minutes, depending on your computer performance.

Once the driver installation is complete, you should see a result page similar to the following:



9. Next, click on the **CenTran** button on the CenTran install page.

Note

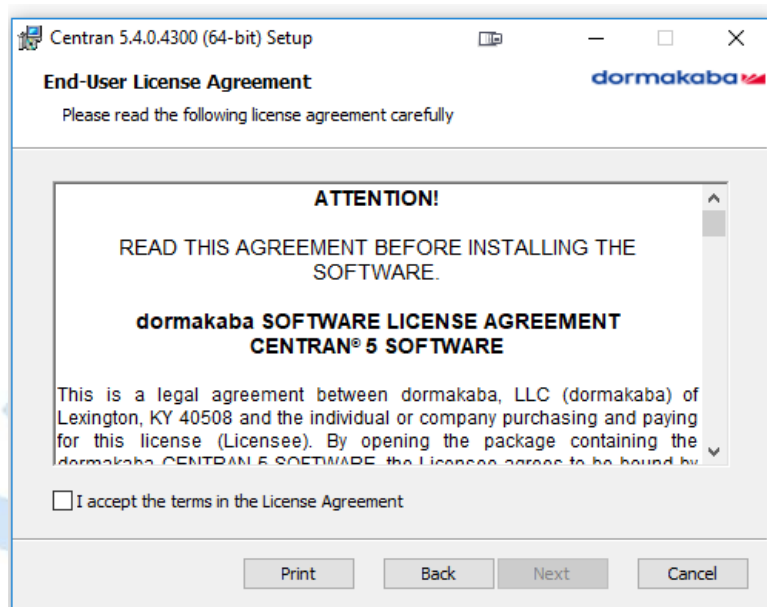
CenTran® 5 only supports using the Cencon USB KeyBox. Cencon PCI or ISA Cards are no longer supported.

The "Welcome to the CenTran Setup Wizard" screen is displayed. The installer is a Windows program that will take you through the rest of the setup process:



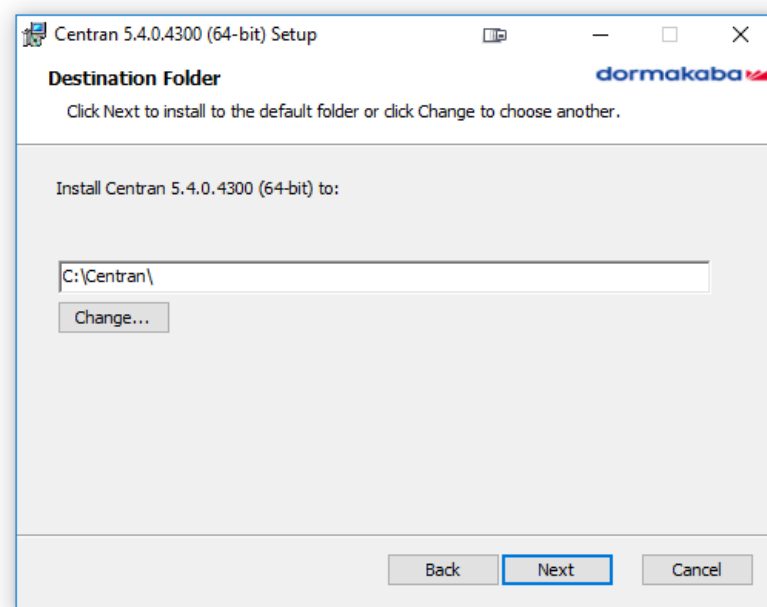
Click on **Next** to continue with the installation.

10. The Software License Agreement acceptance screen is displayed.



Read the Software License Agreement and then click the **I accept the terms in the License Agreement** button followed by the **Next>** button.

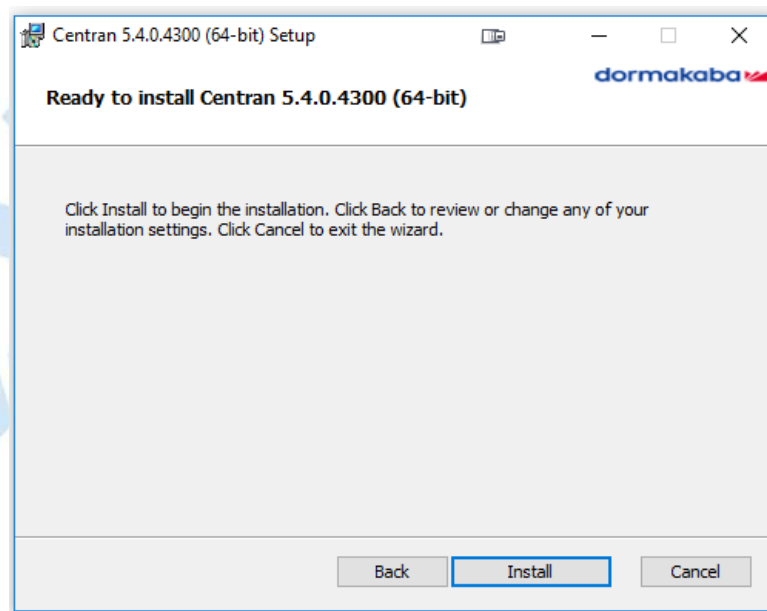
11. The Destination Folder window is displayed to allow you to select the program folder to which the CenTran 5 program will be added.



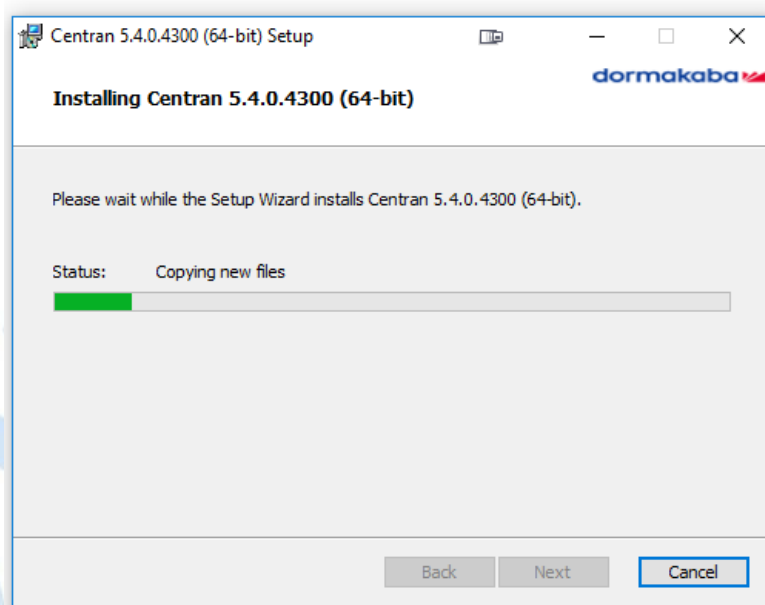
Note: The default installation directory is shown. If CenTran 5 is already installed on your system, it is recommended that you install CenTran 5 to a new directory. If you want the CenTran 5 software installed in another directory, click on the Browse button and select the new path.

Click on the **Next>** button to add the programs to the designated folder.

12. Confirm Installation - If there is anything you wish to change, click on the **<Back** button. Otherwise, click **Next>** to install the program with the designated settings.



The Setup Status screen displays the status of the installation.



The installation Complete screen is then displayed indicating that the CenTran 5 service has been successfully installed.



Click **Finish** to complete the installation process.

ODBC Connection Creation for SQL Server

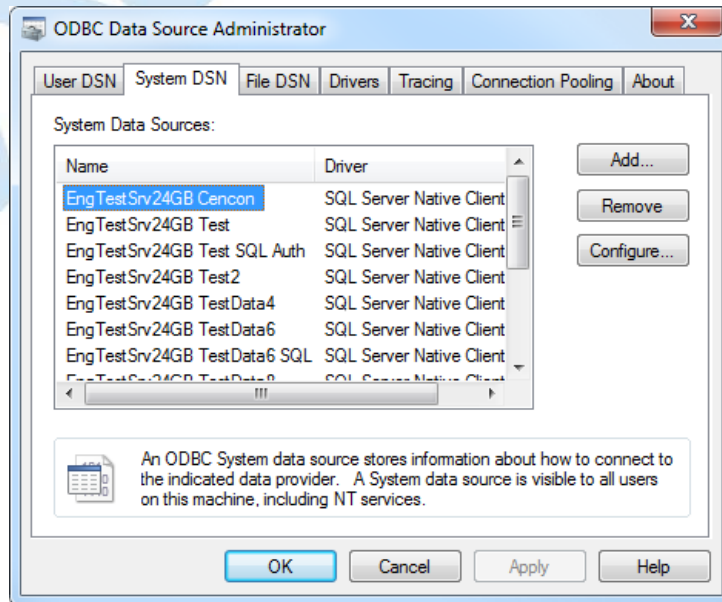
Centran Version 5 Getting Started Guide

Note

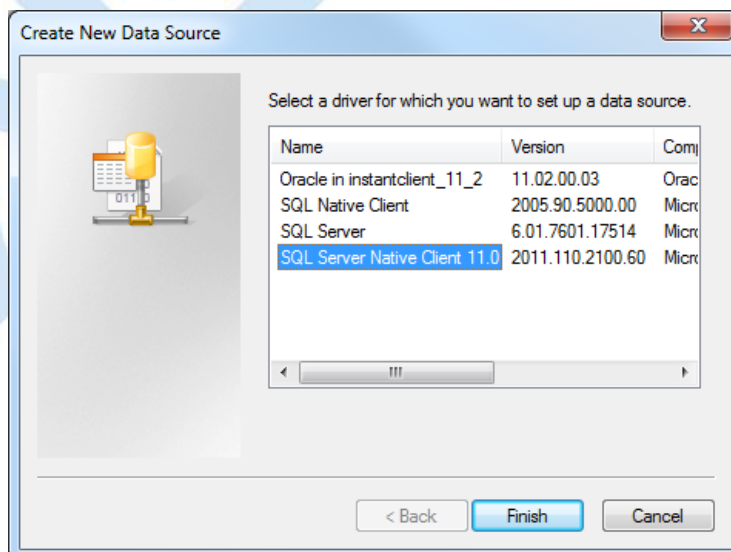
ODBC (Open Database Connectivity) is a standard C interface for accessing database management systems (DBMS). The designers of ODBC aimed to make it independent of database systems and operating systems. An application can use ODBC to query data from a DBMS, regardless of the operating system or DBMS it uses.

ODBC accomplishes DBMS independence by using an *ODBC driver* as a translation layer between the application and the DBMS. The application uses ODBC functions through an *ODBC driver manager* with which it is linked, and the driver passes the query to the DBMS.

1. Go to Control Panel/Administration Tools/Data Sources.
2. Select the System DSN tab and click **Add**.



3. Select the driver and click **Finish**.



4. Type a name and type or use the drop down to select the server and instance.
5. Click **Next**.

Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: engtestsrv24gb Test3

How do you want to describe the data source?

Description:

Which SQL Server do you want to connect to?

Server: engtestsrv24gb

Finish Next > Cancel Help

6. Select SQL Server Authentication, and enter your SQL user name and password. Click **Next**.

Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

☐ With Integrated Windows authentication.

SPN (Optional):

☒ With SQL Server authentication using a login ID and password entered by the user.

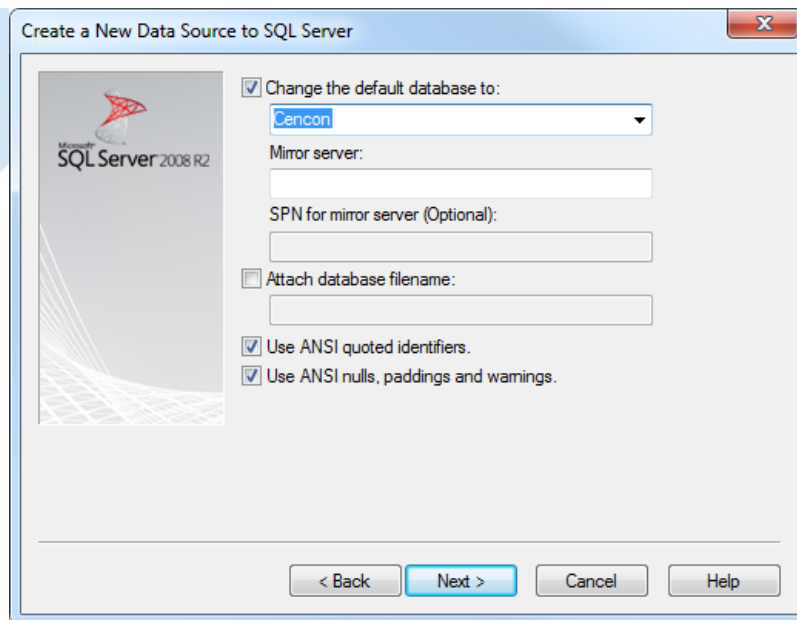
Login ID: CentranUser

Password:

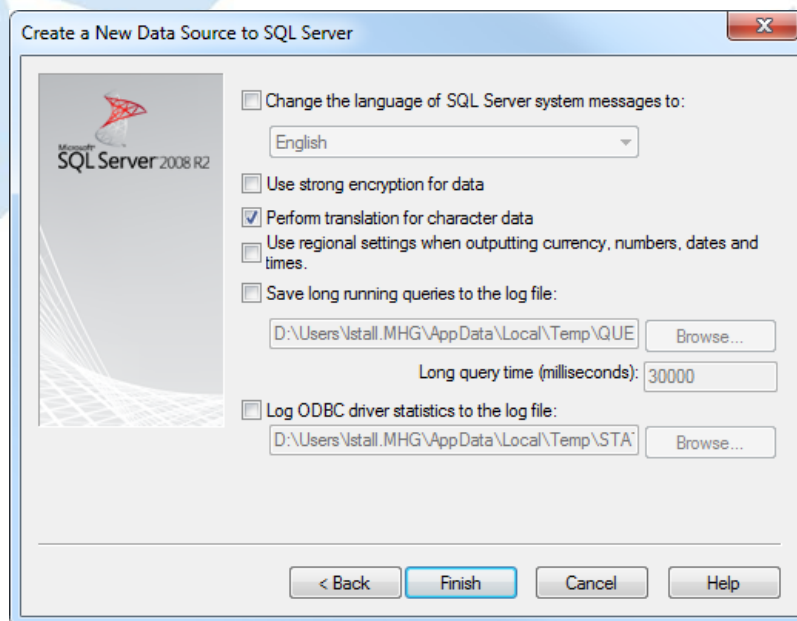
☒ Connect to SQL Server to obtain default settings for the additional configuration options.

< Back Next > Cancel Help

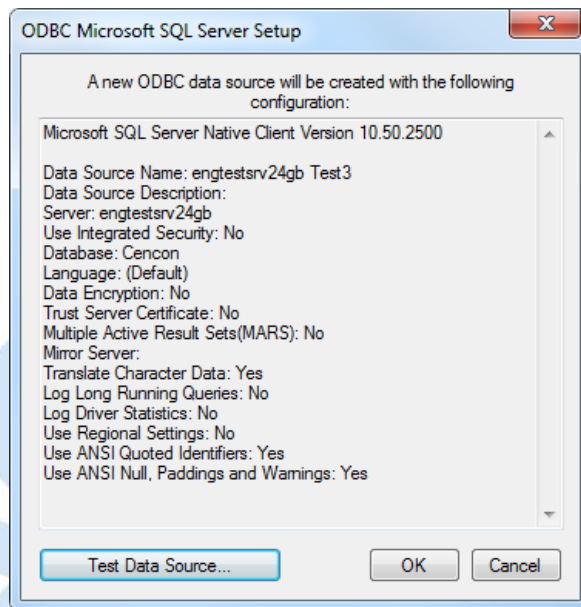
6. Make sure the database schema containing the Cencon database set set as default. Click **Next**.



7. Click **Finish**.



8. Click OK



© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Configure the CenTran Service

CenTran Version 5 Getting Started Guide

The CenTran service has some settings that are manually set in the CenTran service configuration file. This file is named **Centran.exe.config**. Depending on your system settings, the file extension may be hidden.

You can edit the **Centran.exe.config** file by double clicking on it, and a default editor will be opened. You can also edit it with the Notepad application. The file is an XML formatted text file.

The **Centran.exe.config** file contains various configuration settings. If you change settings in the CenTran service configuration file, you will need to restart the CenTran service for the settings to take effect.

There are example **Centran.exe.config** files installed with CenTran. These are contained in the **Configuration Files** directory installed within the application directory. There is one example file for using Windows authentication with the CenTran web service and one example file for using user ID / password authentication with the CenTran web service.

To use one of the example **Centran.exe.config** files, copy the file to the CenTran application directory. Any changes to the **Centran.exe.config** file must be made before starting the CenTran service. If you make changes to the **Centran.exe.config** file while the CenTran service is already running, the changes will not be read until next time the CenTran service is started.

Warning

When the CenTran service is upgraded from a previous version, the previous configuration file is retained from the previous installation. If new CenTran endpoints or communications methods have been added that the old configuration file does not have support for, those endpoints or communications methods will not be available with the old configuration file.

If new CenTran endpoints or communications methods from an upgrade need to be used, then you will need to replace the previous configuration file with one of the example configuration files and re-set up your CenTran settings.

You may want to retain a copy of your previous configuration file in a different location, to compare to the new settings you apply to CenTran.

appSettings Section

These settings are specific to the CenTran service. Some of these settings are configured manually. A link to an [overview](#) of these settings is provided below.

system.serviceModel Section Group

These settings are related to the web service communications provided by CenTran. These entries are defined by the Microsoft Windows Communication Foundation. Detailed information about how these settings are used is beyond the scope of this manual. You can look up Microsoft Windows Communication Foundation documentation for more information. Additional documentation is available at: [Windows Communication Foundation Configuration Schema](#)

Links to [overviews](#) of these settings is provided below.

Configuration File Section Descriptions:

The following sections can be edited within the CenTran configuration file:

- [Configuration File - system.serviceModel / bindings Section](#)
- [Configuration File - system.serviceModel / services Section](#)
- [Configuration File - system.serviceModel / behaviors Section](#)

Configuration File - system.serviceModel / bindings Section

CenTran Version 5 Getting Started Guide

The **bindings** section is part of the system.serviceModel section group used to configure Windows Communication Foundation (WCF) settings. This section defines the various communications settings to be used by the web service endpoints provided by CenTran. The following is a brief overview of this section.

- **webHttpBinding:**

This subsection contains settings for REST model of web service communications. Each **binding** listed within this section defines how a web service endpoint does its communications across HTTP or HTTPS, using standard HTTP GET and POST operations.

This type of web service communications is easily accessed from web browsers and web sites. It does not have the flexibility of operations that SOAP web service communications has.

The **security** section under each **binding** defines the type of encryption and user authentication to be used with the web service endpoint.

- **wsHttpBinding:**

This subsection contains settings for SOAP web service communications. Each **binding** listed within this section defines how a web service endpoint does its communications using SOAP (Simple Object Access Protocol).

This type of web service communications is not easily accessible from web browsers and web sites. However, it has a much greater degree of flexibility and possible options than REST web service communications. An example of these options provided by SOAP is WS-ReliableMessaging, which allows support for handling network failures.

The **security** section under each **binding** defines the type of encryption and user authentication to be used with the web service endpoint.

There are many other types of web service communication bindings available. These two are given as defaults for use by CenTran, but others could potentially be used.

© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Configuration File - system.serviceModel / services Section

CenTran Version 5 Getting Started Guide

The **services** section is part of the system.serviceModel section group used to configure Windows Communication Foundation (WCF) settings. It is used to define the specific web service endpoints provided by CenTran. The following is a brief overview of this section.

- **service:**

Each **service** section defines the web service endpoints provided for a service from CenTran. Within a **service** section is a set of **endpoint** entries. Each **endpoint** entry defines a web service URI and method of communications provided by CenTran.

The service names can be one of the following:

- **Centran.CentranService**

This is the main web service implemented by CenTran, using XML message formatting. Any access to operations of this web service contract must have some form of user authentication, otherwise access will be refused (except for the Version and Hello operations). The default behavior used with this web service is **centran_service_behavior** already defined in the example CenTran configuration files.

- **Centran.CentranService.JSON**

This is the main web service implemented by CenTran, using JSON message formatting. Any access to operations of this web service contract must have some form of user authentication, otherwise access will be refused (except for the Version and Hello operations). The default behavior used with this web service is **centran_service_json_behavior** already defined in the example CenTran configuration files.

- **Centran.CentranFeedsService**

This is the RSS feeds web service implemented by CenTran. The operations provided by this web service contract are intended to support web RSS feeds to query alert information from CenTran. Encryption and user authentication are not needed for this web service contract. Encryption is recommended, however. The default behavior used with this web service is **centran_feeds_service_behavior** already defined in the example CenTran configuration files.

- **Centran.CentranAgentService**

This is the web service for operations supporting the CenTran Agent Service running on ATM console systems for remote access to Cencon locks. The operations provided by this web service contract are used to update status of locks in response to lock events detected by the CenTran Agent Service. Encryption and user authentication are not needed for this web service contract. Encryption is recommended, however. The default behavior used with this web service is **centran_agent_service_behavior** already defined in the example CenTran configuration files.

Each **endpoint** entry has the following items that it defines:

- **address**

This is the address or URI that is provided by the web service. It can specify localhost to default to the current host server base address or can define a different address. This can also be used to define a different TCP port for the address.

- **binding**

This is the type of binding used to define the communications used for the web service endpoint. The defaults for CenTran are **webHttpBinding** or **wsHttpBinding**.

- **bindingConfiguration**

This is the specific configuration of binding that is being used by the web service endpoint. This name must match one of the names defined from the matching **binding** section. This is used to define the encryption and user authentication used for the web service endpoint.

- **contract**

This is the name of the web service contract implementation calls within CenTran that is to be made accessible through the web service endpoint. The contracts that CenTran provides can be one of the following:

- **Centran.ICentran**

This is the main web service contract implemented by CenTran for XML formatted data. It defines access to the Centran.CentranService web service.

- **Centran.ICentranJSON**

This is the main web service contract implemented by CenTran for JSON formatted data. It defines access to the Centran.CentranService.JSON web service.

- **Centran.ICentranFeeds**

This is the RSS feeds web service contract implemented by CenTran. It defines access to the Centran.CentranFeedsService web service.

- **Centran.ICentranAgent**

This is the web service contract for operations supporting the CenTran Agent Service running on ATM console systems for remote access to Cencon locks. It defines access to the Centran.CentranAgentService web service.

- **behaviorConfiguration**

This specifies what additional settings are to be used by the web service endpoint. These additional settings are defined by **behavior** entries under the **behaviors / endpointBehaviors** section. Default settings for endpoint behaviors are already defined in the example CenTran configuration files.

Configuration File - system.serviceModel / behaviors Section

CenTran Version 5 Getting Started Guide

The **behaviors** section is part of the system.serviceModel section group used to configure Windows Communication Foundation (WCF) settings. It is used to define additional settings for the web service endpoints provided by CenTran.

The following is a brief overview of this section.

- **endpointBehaviors**

This section defines endpoint behaviors used by the web service endpoints. This includes if help support is to be generated for a specific endpoint.

- **serviceBehaviors**

This section defines the web service behaviors for each web service provided by CenTran. This includes what certificate is used for encryption with a web service provided by CenTran, under the **serviceCredentials** section. The **serviceCredentials** section has two entries:

- **serviceCertificate**

This section defines what certificate is used by the web service for communications encryption. It is composed of the following entries:

- **findValue**

This is the unique value used to find the certificate in the indicated certificate store. The way this value is used is determined by the **x509FindType** that is set. In the case of **FindByThumbprint**, this value will be composed of a unique hexadecimal thumbprint value associated with the desired certificate.

- **storeLocation**

This specifies if the certificate is stored associated with the current user account or with a system account. For the CenTran service to access the certificate, this must be set to **LocalMachine** to indicate a system account.

- **storeName**

This specifies the store name that the certificate is in. For the CenTran service, this must be **My** to indicate the certificate store for personal certificates.

- **x509FindType**

This indicates how the certificate is to be uniquely identifies, based off of various values associated with the certificate. The recommended default is **FindByThumbprint**.

The CenTran Configuration Manager has support for creating self signed certificates for use by the CenTran service. You can also use a server certificate as provided by your network certificate authority server. Using a certificate as provided by your network certificate authority server is the preferable way to set up your network security.

Whatever the source of your CenTran server certificate, you can specify the certificate within the configuration file manually, or you can set it using the CenTran Configuration Manager.

The CenTran server certificate must have a name matching the way you are going to address the CenTran web service. If it is by server name, then the certificate name must match the server name. If it is by IP address, then the certificate name must match the IP address.

- **userNameAuthentication**

This section defines the internal method of support for user names and passwords implemented by CenTran. The default settings for this entry should not be changed from what is provided with the example CenTran configuration files.

Set Up CenTran Server Certificates

CenTran 5 Getting Started Guide

For a web service to make use of encryption or user authentication, it requires a server certificate to be configured for use by that web service. The operation and concepts behind certificates and the Transport Layer Security Protocol (TLS) are beyond the scope of this manual. The following is a link to describe some of these concepts:

[SSL/TLS Strong Encryption: An Introduction](#)

Ideally, your organization will have a server configured to be a certificate authority for managing the security of communications on your network. If you do not have support for managing certificates on your network, you can set up a self signed certificate and distribute it manually to the systems that are going to be accessing the CenTran web service.

To assist with this process, the CenTran Configuration Manager has support for creating certificates and configuring them in the CenTran configuration file for you.

The CenTran Configuration Manager supports the creation of a self signed certificate authority (CA) certificate. It can then use this CA certificate to create a signed CenTran Web Service Server certificate. The CenTran Configuration Manager can then be used to update the CenTran configuration file with information describing the signed CenTran Web Service Server certificate.

Exported Agent Configuration and CA Certificate Files

When the CenTran configuration file is updated with a CenTran server certificate, the CenTran Configuration Managers exports three files to a directory named **AgentConfigurations** under the CenTran installation directory:

- A CenTran Agent configuration file, configured for a persistent connection to this CenTran server
- A Cencon Key Box Agent configuration file, configured for a persistent connection to this CenTran server
- A Certificate Authority certificate file, containing the public key certificate that issued the CenTran server's server certificate

The CenTran Agent configuration file and the certificate can be imported into an installation of the CenTran Agent Configuration Manager and used to configure agents.

To set up CenTran server certificates, select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu. Then select the **Certificates** tab. You should see the following:

CenTran Configuration Manager 5.3.0.4156 (64-Bit)

Certificates

Service Security

Service

USB Keybox Setup

Database Settings

Security Settings

Input / Output File Settings

CenTran Status

Web XML Service Settings

Web JSON Service Settings

Web RSS Feed Settings

CenTran Agent Settings

CenTran Event Log

Agent Connections

Certificate Authority

Selected Certificate Authority:

Certificate Authority Name:

Certificate Authority Organization:

Certificate Authority Title:

Certificate Authority Thumb Print:

CenTran Web Service Server Certificate

Selected CenTran Certificate:

Certificate Name:

Certificate Organization:

Certificate Title:

Certificate Thumb Print:

Update Certificates

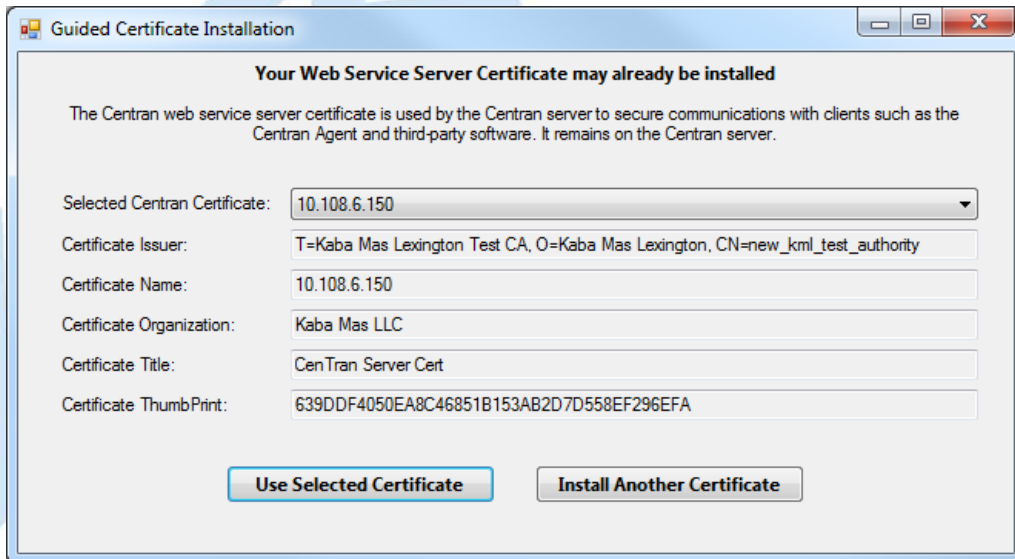
Select [Guide Me](#) to be guided through the certificate installation process, or [I'll Guide Myself](#) to use the unguided process.

Guided Certificate Installation

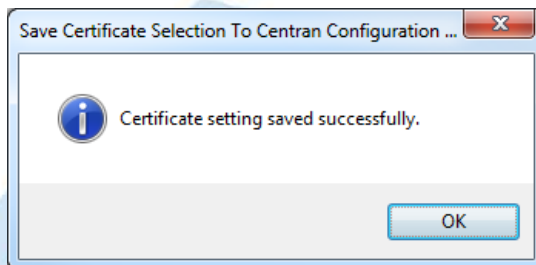
The guided certificate installation process takes the user through several common scenarios for installing a server certificate for the CenTran server.

Using An Already Installed Server Certificate

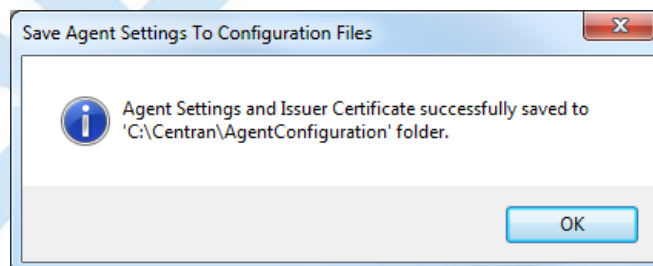
The first of these common scenarios involves using a certificate already created and installed on the server machine:



The pull-down menu is populated with server certificates installed on the local machine that are named with the DNS name of the machine or an IP address assigned to the machine. As an item is selected in the list, the fields describing the certificate are filled in on the form. If the user selects an item and clicks **Use Selected Certificate**, the certificate will be installed in the configuration file for the CenTran Server, and a message will be displayed indicating the fact:



Click **OK** to close the prompt. Example CenTran Agent and Cencon Key Box Agent configuration files, along with the public key version of the CenTran server certificate, are now exported, and a message is displayed to indicate the fact:



Click **OK** to close the prompt. The server certificate for the CenTran server is now set up.

Centran Configuration Manager 5.3.0.4156 (64-Bit)

Certificates

Service Security
Service
USB Keybox Setup
Database Settings
Security Settings
Input / Output File Settings
Centran Status
Web XML Service Settings
Web JSON Service Settings
Web RSS Feed Settings
Centran Agent Settings
Centran Event Log
Agent Connections

Certificates

Certificate Authority

Selected Certificate Authority:

Certificate Authority Name: new_kml_test_authority

Certificate Authority Organization: Kaba Mas Lexington

Certificate Authority Title: Kaba Mas Lexington Test CA

Certificate Authority Thumb Print: 601F6D2D476E97B64B87D3CB213E8ADCC701029A

Centran Web Service Server Certificate

Selected Centran Certificate:

Certificate Name: 10.108.6.150

Certificate Organization: Kaba Mas LLC

Certificate Title: CenTran Server Cert

Certificate Thumb Print: 639DDF4050EA8C46851B153AB2D7D558EF296EFA

Update Certificates

Guide Me **I'll Guide Myself**

Using A Server Certificate Provided In A File

The second common scenario involves the use of a server certificate which has been provided in a certificate file.

Guided Certificate Installation

Your Web Service Server Certificate may already be installed

The Centran web service server certificate is used by the Centran server to secure communications with clients such as the Centran Agent and third-party software. It remains on the Centran server.

Selected Centran Certificate: 10.108.6.150

Certificate Issuer: T=Kaba Mas Lexington Test CA, O=Kaba Mas Lexington, CN=new_kml_test_authority

Certificate Name: 10.108.6.150

Certificate Organization: Kaba Mas LLC

Certificate Title: CenTran Server Cert

Certificate ThumbPrint: 639DDF4050EA8C46851B153AB2D7D558EF296EFA

Use Selected Certificate **Install Another Certificate**

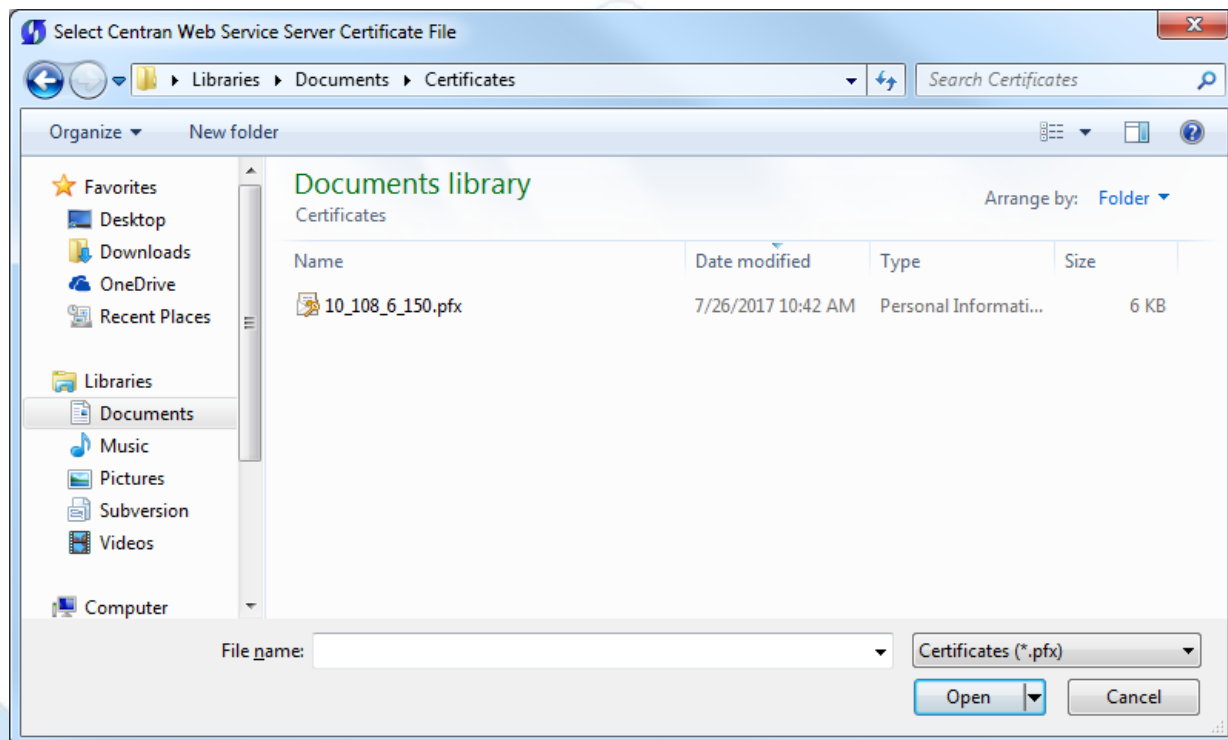
In this case, the user selects **Install Another Certificate** instead of selecting and using an already installed certificate. A message is displayed:

Guided Certificate Installation

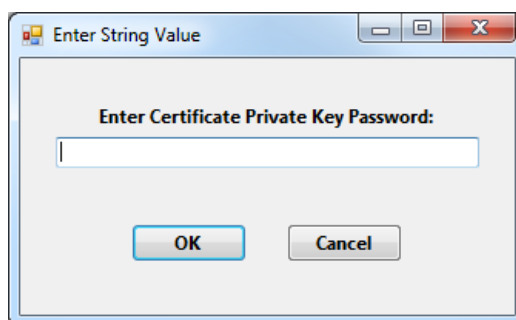
Have you been given a file with a server certificate to install?

Yes **No**

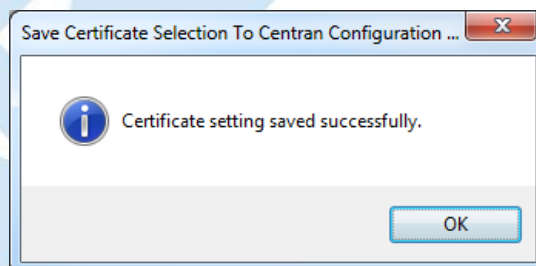
Click **Yes** to be prompted for the location of the file containing the certificate. This file should be a Personal Information Exchange file with an extension of **pfx**:



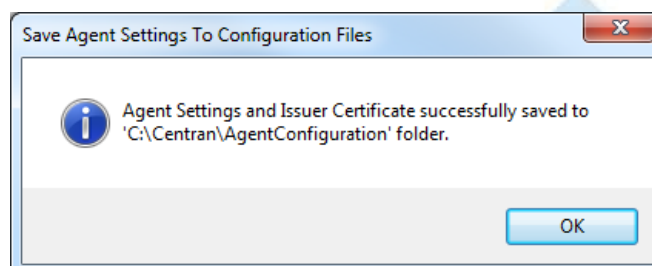
Navigate to the directory containing the file using the Open File dialog, select the file, and click **Open**. Because this file contains the private key with which the server secures communications, it will be protected by a password, for which a password prompt will be displayed:



Enter the password and click **OK**. The certificate in the file will be installed on the system and the the CenTran server configuration will updated to use it. A message will be displayed indicating the fact:



Click **OK** to close the prompt. Example CenTran Agent and Cencon Key Box Agent configuration files, along with the public key version of the CenTran server certificate, are now exported, and a message is displayed to indicate the fact:



Click **OK** to close the prompt. The server certificate for the CenTran server is now set up.

Centran Configuration Manager 5.3.0.4156 (64-Bit)

Certificates

Service Security

Service

USB Keybox Setup

Database Settings

Security Settings

Input / Output File Settings

Centran Status

Web XML Service Settings

Web JSON Service Settings

Web RSS Feed Settings

Centran Agent Settings

Centran Event Log

Agent Connections

Certificate Authority

Selected Certificate Authority:

Certificate Authority Name: new_kml_test_authority

Certificate Authority Organization: Kaba Mas Lexington

Certificate Authority Title: Kaba Mas Lexington Test CA

Certificate Authority Thumb Print: 601F6D2D476E97B64B87D3CB213E8ADCC701029A

Centran Web Service Server Certificate

Selected Centran Certificate:

Certificate Name: 10.108.6.150

Certificate Organization: Kaba Mas LLC

Certificate Title: CenTran Server Cert

Certificate Thumb Print: 639DDF4050EA8C46851B153AB2D7D558EF296EFA

Update Certificates

Guide Me

I'll Guide Myself

Creating A Server Certificate

The third common scenario for installing the CenTran server certificate involves creating a new, self-signed certificate. This option is provided if the user selects **Install Another Certificate** in the existing server certificate dialog:

Guided Certificate Installation

Your Web Service Server Certificate may already be installed

The Centran web service server certificate is used by the Centran server to secure communications with clients such as the Centran Agent and third-party software. It remains on the Centran server.

Selected Centran Certificate: 10.108.6.150

Certificate Issuer: T=Kaba Mas Lexington Test CA, O=Kaba Mas Lexington, CN=new_kml_test_authority

Certificate Name: 10.108.6.150

Certificate Organization: Kaba Mas LLC

Certificate Title: CenTran Server Cert

Certificate ThumbPrint: 639DDF4050EA8C46851B153AB2D7D558EF296EFA

Use Selected Certificate

Install Another Certificate

and **No** when asked if a certificate has been provided in a file:

Guided Certificate Installation

Have you been given a file with a server certificate to install?

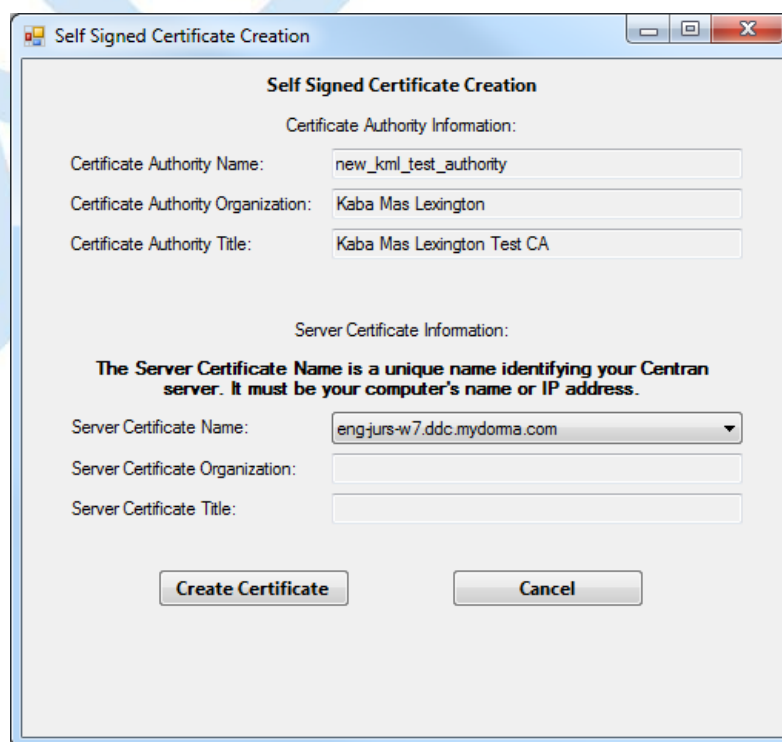
Yes

No

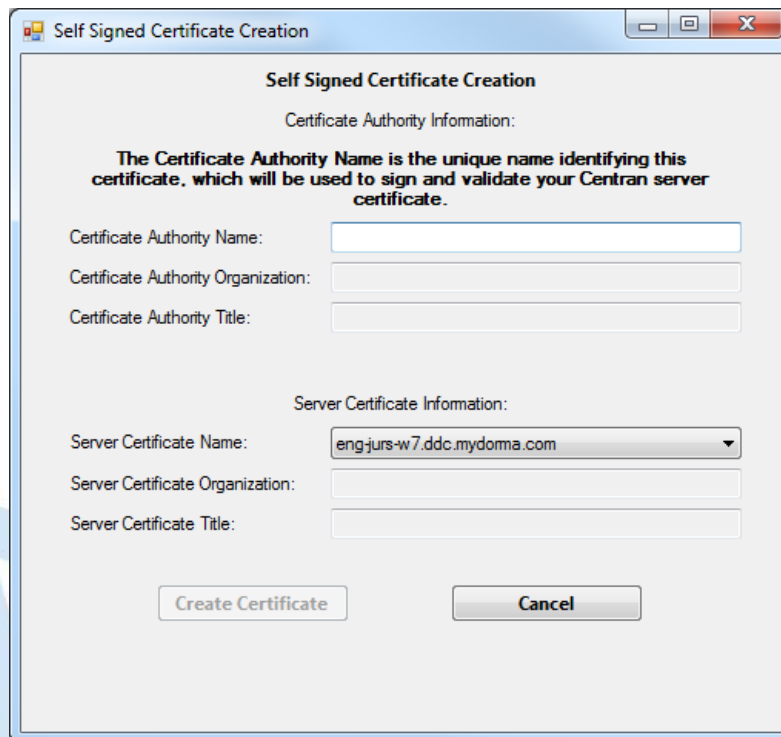
Before a server certificate can be created, a Certificate Authority certificate must exist. A prompt is provided to check whether a Certificate Authority certificate already exists:



All of the Certificate Authority certificates on the local machine that can be used to create certificates are listed. If one is selected and **Use Selected Certificate** is clicked, a dialog for entering the information needed to create the server certificate is displayed, with the Certificate Authority certificate's information filled in:



If, instead, **Install Another Certificate** is clicked, the dialog for entering the information needed to create the server certificate is displayed, with no Certificate Authority certificate's information filled in. In this case, the user must enter information for both a new Certificate Authority certificate and a new CenTran server certificate:



Self Signed Certificate Creation

Certificate Authority Information:

The Certificate Authority Name is the unique name identifying this certificate, which will be used to sign and validate your Centran server certificate.

Certificate Authority Name:

Certificate Authority Organization:

Certificate Authority Title:

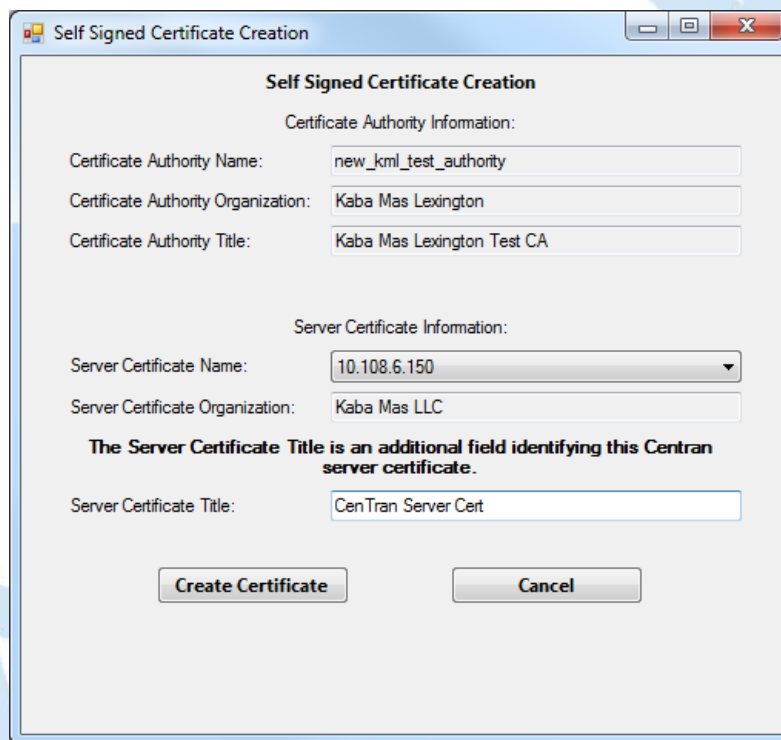
Server Certificate Information:

Server Certificate Name:

Server Certificate Organization:

Server Certificate Title:

Note that descriptive text is displayed above each field while it is being filled in. Also, the certificate name field for the CenTran server certificate must be a valid name or IP address for the CenTran server machine, so that field is a pull-down menu containing only those values.



Self Signed Certificate Creation

Certificate Authority Information:

Certificate Authority Name:

Certificate Authority Organization:

Certificate Authority Title:

Server Certificate Information:

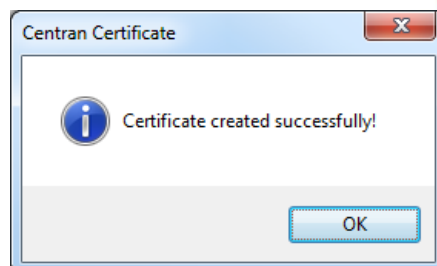
Server Certificate Name:

Server Certificate Organization:

The Server Certificate Title is an additional field identifying this Centran server certificate.

Server Certificate Title:

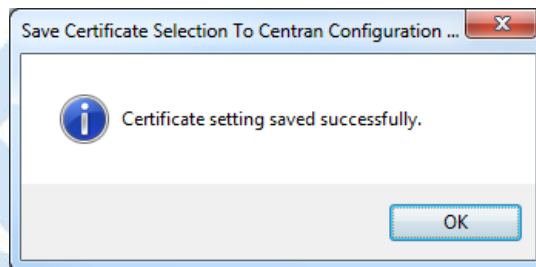
Fill in the fields with the appropriate values and Click **Create Certificate**. A message will be displayed indicating success. (If the Certificate Authority was also created, a message for that will also be displayed.)



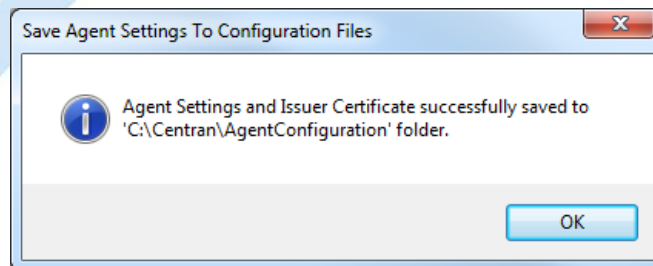
Centran Certificate

 Certificate created successfully!

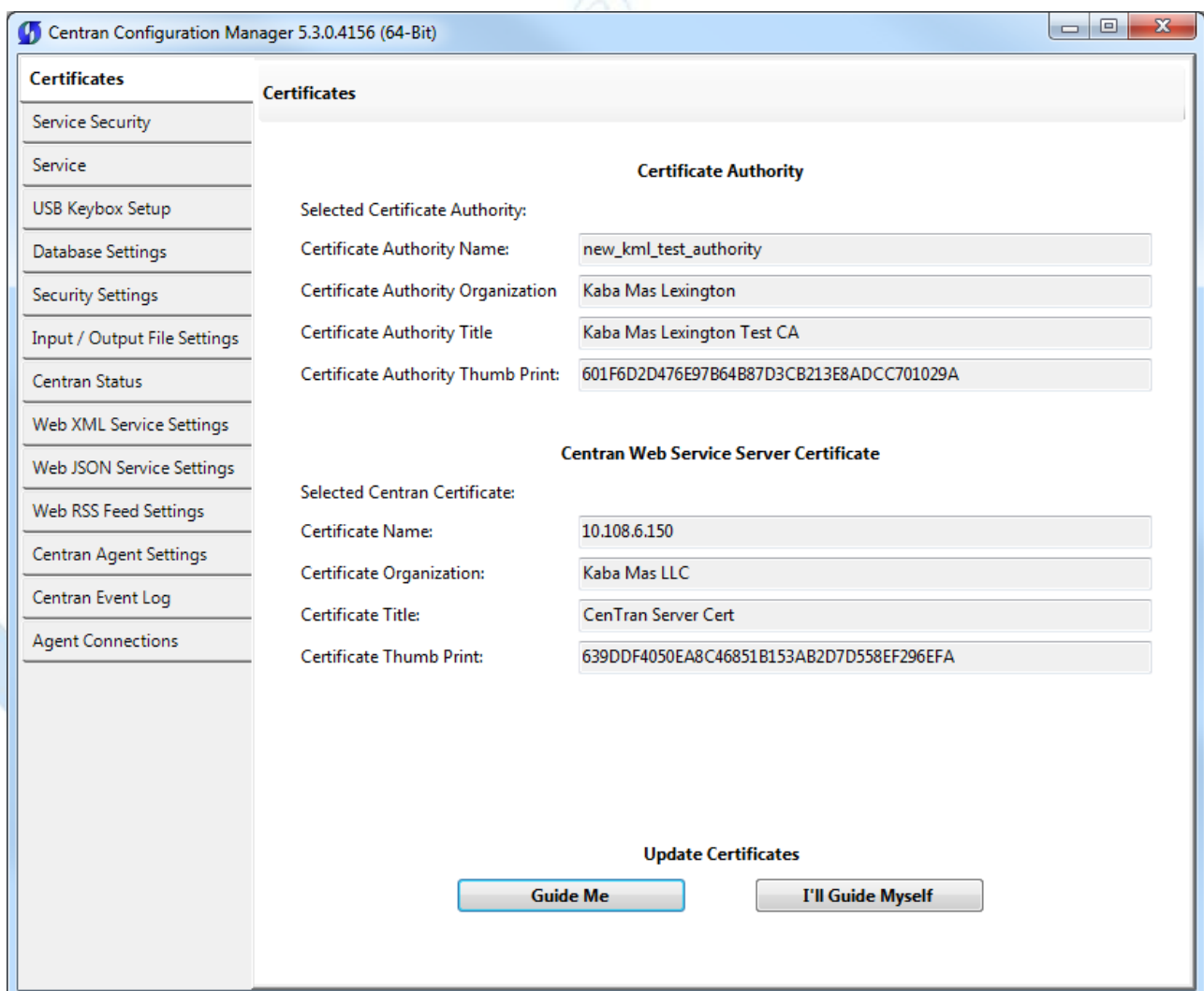
Click **OK** to close the prompt(s). The CenTran configuration will be updated with the new server certificate, and a message will be displayed indicating the fact:



Click **OK** to close the prompt. Example CenTran Agent and Cencon Key Box Agent configuration files, along with the public key version of the CenTran server certificate, are now exported, and a message is displayed to indicate the fact:



Click **OK** to close the prompt. The server certificate for the CenTran server is now set up.



Self-Guided Certificate Installation

This dialog allows the user to work more freely with certificates. For example, from this dialog it is possible to create server certificates to be used on other machines.

Self Signed Certificates

Certificate Authority

Selected Certificate Authority:

Certificate Authority Name:

Certificate Authority Organization:

Certificate Authority Title:

Certificate Authority Thumb Print:

Create Certificate Authority Self Signed Certificate **Export Public Key...**

Centran Web Service Server Certificate

Selected Centran Certificate:

Certificate Name:

Certificate Organization:

Certificate Title:

Certificate Thumb Print:

Create / Update Centran Web Service Certificate **Export Public Key...**

Centran Configuration File

Configuration File:

Save Certificate Selection To Centran Configuration File

You can select an existing certificate authority certificate to sign with, or create a new one.

To use an existing CA certificate select any certificate in the local machine root authority store that you have a private key for from the dropdown menu labeled **Selected Certificate Authority**.

To create a new CA certificate complete the **Certificate Authority Name**, **Certificate Authority Organization** and **Certificate Authority Title** fields with the desired data and select **Create Certificate Authority Self Signed Certificate**.

A new certificate authority (CA) certificate will be created. The **Selected Certificate Authority** pulldown and the **Certificate Authority Thumb Print** fields will be filled in. The new CA certificate will also be placed in the local machine trusted root certification authorities store.

Self Signed Certificates

Certificate Authority

Selected Certificate Authority: new_kml_test_authority

Certificate Authority Name: new_kml_test_authority

Certificate Authority Organization: Kaba Mas Lexington

Certificate Authority Title: Kaba Mas Lexington Test CA

Certificate Authority Thumb Print: 601F6D2D476E97B64B87D3CB213E8ADCC701029A

Create Certificate Authority Self Signed Certificate **Export Public Key...**

Centran Web Service Server Certificate

Selected Centran Certificate:

Certificate Name:

Certificate Organization:

Certificate Title:

Certificate Thumb Print:

Create / Update Centran Web Service Certificate **Export Public Key...**

Centran Configuration File

Configuration File: C:\Centran\Centran.exe.config

Save Certificate Selection To Centran Configuration File

An existing signed certificate can be used as the CenTran Web Service Server Certificate or a new signed certificate can be created using the selected certificate authority (CA) certificate.

To use an existing signed CenTran Web Service Server Certificate select from the **Selected Centran Certificate** pulldown the desired certificate. All fields, including those in the **Certificate Authority** section, will be completed with the appropriate data for the selected certificate.

To create a new signed CenTran Web Service Server Certificate first enter the name you will use to access CenTran in the **Certificate Name** field.

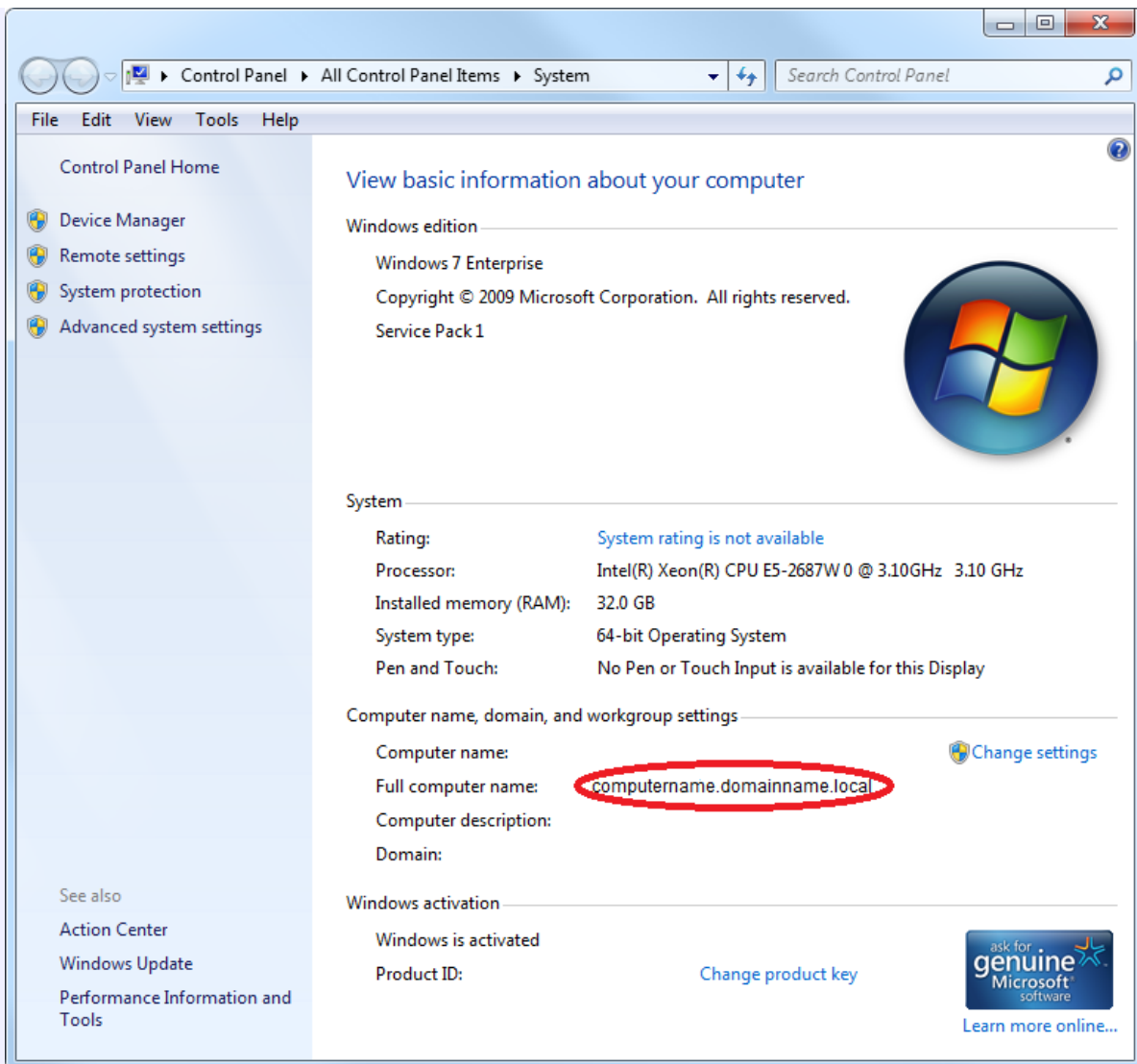
Important Note - CenTran Server Network Address

It is very important that this name matches how you are going to address CenTran in a browser. If this is by server name, then the server name needs to be the name of the certificate. If it is by IP address, then the IP address needs to be the name of the certificate.

If you are accessing the CenTran web service on a company intranet using Windows Active Directory and a Domain Name Server (DNS), it is recommended to use the fully qualified server name for the certificate. This will look like the following: **computername.domainname.local**

If you are accessing the CenTran web service on a company intranet using Windows Active Directory and a Domain Name Server (DNS) and you do not use the fully qualified computer name, then your proxy server may block network access.

You can find the CenTran server full computer name under the Windows computer properties dialog. This can be accessed by right clicking on **Computer** in the Start Menu or File Explorer and selecting **Properties** from the context menu.



If you are going to be accessing the CenTran web service on a network without a Domain Name Server, then you will use the IP address of the CenTran web service. For IPv4 this will look like the following: **192.168.0.111**

You can find the CenTran server IP address by opening a command prompt and entering the following command: **ipconfig**

Look for **IPv4 Address** in the text returned for the CenTran server address.

If you are accessing the CenTran web service exposed to the internet, then the security certificate used and the name of the certificate will be the same as your web site. Consult with your IT department for the proper certificate configuration in this case.

Important Note - CenTran Server Firewall

If your CenTran server is running either the Windows network firewall software or an antivirus vendor network firewall software, then the following ports (depending on the configuration that you have set) must be made available:

Default Port	Usage	Setting Location
80	Web Service HTTP	Configuration File: <system.serviceModel><services><service><endpoint> address property
443	Web Service HTTPS	Configuration File: <system.serviceModel><services><service><endpoint> address property
53004	CenTran Agent Persistent Connections	Configuration File: <appSettings><add> key="PersistentAgentConnectionsPort" value="port number"

Enter the organization name and title as desired, and select **Create / Update CenTran Web Service Certificate**. The certificate will be created, and selected in the dropdown menu labeled **Selected CenTran Certificate**.

Self Signed Certificates

Certificate Authority

Selected Certificate Authority: new_kml_test_authority

Certificate Authority Name: new_kml_test_authority

Certificate Authority Organization: Kaba Mas Lexington

Certificate Authority Title: Kaba Mas Lexington Test CA

Certificate Authority Thumb Print: 601F6D2D476E97B64B87D3CB213E8ADCC701029A

Create Certificate Authority Self Signed Certificate Export Public Key...

Centran Web Service Server Certificate

Selected Centran Certificate: 10.108.6.150

Certificate Name: 10.108.6.150

Certificate Organization: Kaba Mas LLC

Certificate Title: CenTran Server Cert

Certificate Thumb Print: 639DDF4050EA8C46851B153AB2D7D558EF296EFA

Create / Update Centran Web Service Certificate Export Public Key...

Centran Configuration File

Configuration File: C:\Centran\CenTran.exe.config

Save Certificate Selection To Centran Configuration File

Lastly, you can have the CenTran Configuration Manager set up the selected certificate in the CenTran configuration file. Select the **Save Certificate Selection To Centran Configuration File**. This will update the CenTran configuration file with information for your selected server certificate.

Any systems that are required to trust the CenTran web service through browser access will need to have the selected certificate authority (CA) certificate (not including private key) imported into the systems' local computer trusted root certification authorities store. A set of example steps of one method for accomplishing this on Windows 7 is as follows:

You can export the public keys for the CenTran certificates to certificate files (.cer) using the CenTran Configuration Manager:

Self Signed Certificates

Certificate Authority

Selected Certificate Authority: new_kml_test_authority

Certificate Authority Name: new_kml_test_authority

Certificate Authority Organization: Kaba Mas Lexington

Certificate Authority Title: Kaba Mas Lexington Test CA

Certificate Authority Thumb Print: 601F6D2D476E97B64B87D3CB213E8ADCC701029A

Create Certificate Authority Self Signed Certificate Export Public Key...

Centran Web Service Server Certificate

Selected Centran Certificate: 10.108.6.150

Certificate Name: 10.108.6.150

Certificate Organization: Kaba Mas LLC

Certificate Title: CenTran Server Cert

Certificate Thumb Print: 639DDF4050EA8C46851B153AB2D7D558EF296EFA

Create / Update Centran Web Service Certificate Export Public Key...

Centran Configuration File

Configuration File: C:\Centran\Centran.exe.config

Save Certificate Selection To Centran Configuration File

Note

You can also manually export the CenTran certificates using the Microsoft Management Console:

Export the selected certificate authority (CA) certificate:

1. Open Microsoft Management Console (Start -> Run -> mmc.exe).
2. Choose File -> Add/Remove Snap-in.
3. Choose the Certificates snap-in, and click Add.
4. In the wizard, choose the Computer Account, and then choose Local Computer.
5. Press Finish followed by OK to end the wizard.
6. Navigate to Certificates (Local Computer).
7. Select Trusted Root Certification Authorities.
8. Expand Certificates.
9. Right click the CA certificate specified in CenTran Configuration Manager.
10. Select All Tasks -> Export and follow the prompts; Do NOT export the private key; Record the specified target file name.

Note

To import the selected certificate authority (CA) certificates to a system that needs to trust the CenTran Web Services:

1. Logon to the system that is to trust the CenTran Web Services.
2. Copy the file containing the exported CA certificate onto this system.
3. Open Microsoft Management Console (Start -> Run -> mmc.exe).
4. Choose File -> Add/Remove Snap-in.
5. Choose the Certificates snap-in, and click Add.
6. In the wizard, choose the Computer Account, and then choose Local Computer.
7. Press Finish followed by OK to end the wizard.
8. Navigate to Certificates (Local Computer).
9. Right click Trusted Root Certification Authorities.
10. Select All Tasks -> Import and follow the prompts; Provide the name of the file containing the exported CA certificate.

Set Up CenTran Management Security

CenTran 5 Getting Started Guide

The CenTran Management Security Settings tab provides control over various security related attributes of the CenTran web services.

To modify these attributes select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu and click on the **Service Security** tab to access this tab page:

CenTran Configuration Manager 5.3.0.4135 (64-Bit)

CenTran Management Security Settings

Authentication Method

Type of Authentication to use for CenTran Web Services

☒ Use Windows Authentication

☐ Use Cencon User ID and Password

CenTran Management Web Access

Credentials for using CenTran Configuration Manager through Web Interface

User ID:

Password:

CenTran Agent Service Security

Protocol for CenTran Agent Service Communications

☒ Both HTTP and HTTPS should be available

☐ Only HTTPS should be available

The **Save Changes** and **Discard Changes** buttons will be enabled when any data on this tab is changed.

Clicking the **Save Changes** button will save the tab data to the CenTran configuration file.

Clicking the **Discard Changes** button will set the tab data to the values currently in the CenTran configuration file.

Clicking either the **Save Changes** button or the **Discard Changes** button will disable both buttons.

Note

If changes are saved the CenTran service must be stopped and started for the changes to take effect.

Authentication Method

Select the authentication method of **Windows Authentication** or **Cencon User ID and Password** to use to access operations in the main CenTran web services

- CenTran.CenTranService which uses XML message formatting
- CenTran.CenTranServiceJSON which uses JSON message formatting

See [CenTran Web Service Configuration](#) for CenTran web service information.

When **Windows Authentication** is selected the CenTran service must be running on a computer that is a member of a Windows logon domain on which the Windows logon user ID to be used is authorized.

When **Cencon User ID and Password** is selected the user ID and password to be used must be in the Cencon database to which the CenTran service is

connected. The Cencon User ID must be of type dispatcher, supervisor or special supervisor.

Valid Cencon User ID with invalid password in HTTP Credentials

If the Cencon User ID is specified with an incorrect password in 5 consecutive HTTP requests

- The Cencon User ID will be locked out from use in HTTP request credentials for 5 minutes.
- A message to that effect will be placed in the CenTran Event Log and in the Cencon Activity Log.

During the lockout period HTTP requests using this Cencon user ID in the credentials will return a result of "(403) Forbidden".

A user of type special supervisor can end the lockout prematurely via the "Disable User" attribute on the Cencon Client "Edit User" dialog "Access Control" tab.

Invalid Cencon User ID in HTTP Credentials

Each HTTP request in which the credentials contain an invalid Cencon User ID will be rejected returning to the sender a result of "(403) Forbidden".

If an excessive number of HTTP requests with an invalid Cencon User ID are received a message will be recorded in the CenTran Event Log and the Cencon Activity Table (CENAUD) warning of a possible denial of service attack.

CenTran Management Web Access

Define the user name and password that must be provided when accessing the CenTran Configuration Manager via a web browser.

See [Log on to CenTran Management](#) in [Configure the CenTran Service using Web Management Interface](#) for more information on the access process.

The default user name is **admin**.

The default password is **password**.

CenTran Configuration Manager 5.3.0.4135 (64-Bit)

Service Security

CenTran Management Security Settings

Authentication Method

Type of Authentication to use for CenTran Web Services

☒ Use Windows Authentication

☐ Use Cencon User ID and Password

CenTran Management Web Access

Credentials for using CenTran Configuration Manager through Web Interface

User ID:

Password: **Show**

CenTran Agent Service Security

Protocol for CenTran Agent Service Communications

☒ Both HTTP and HTTPS should be available

☐ Only HTTPS should be available

Save Changes **Discard Changes**

The button to the right of the Password field toggles between **Show** and **Hide**.

Click the **Show** button to display the password characters as they are typed.

Click the **Hide** button to hide the password characters as they are typed.

Centran Configuration Manager 5.3.0.4135 (64-Bit)

Certificates

Service Security

Service

USB Keybox Setup

Database Settings

Security Settings

Input / Output File Settings

Centran Status

Web XML Service Settings

Web JSON Service Settings

Web RSS Feed Settings

Centran Agent Settings

Centran Event Log

Agent Connections

Centran Management Security Settings

Authentication Method

Type of Authentication to use for Centran Web Services

☒ Use Windows Authentication

☐ Use Cencon User ID and Password

Centran Management Web Access

Credentials for using Centran Configuration Manager through Web Interface

User ID:

Password: [Hide](#)

Centran Agent Service Security

Protocol for Centran Agent Service Communications

☒ Both HTTP and HTTPS should be available

☐ Only HTTPS should be available

[Save Changes](#) [Discard Changes](#)

CenTran Agent Service Security

Specify whether or not the CenTran Agent web service operations can be accessed using HTTP (hypertext transfer protocol) which is not encrypted, as well as with HTTPS (Hypertext Transfer Protocol Secure) which is encrypted.

Centran Configuration Manager 5.3.0.4135 (64-Bit)

Certificates

Service Security

Service

USB Keybox Setup

Database Settings

Security Settings

Input / Output File Settings

Centran Status

Web XML Service Settings

Web JSON Service Settings

Web RSS Feed Settings

Centran Agent Settings

Centran Event Log

Agent Connections

Centran Management Security Settings

Authentication Method

Type of Authentication to use for Centran Web Services

☒ Use Windows Authentication

☐ Use Cencon User ID and Password

Centran Management Web Access

Credentials for using Centran Configuration Manager through Web Interface

User ID:

Password:

Centran Agent Service Security

Protocol for Centran Agent Service Communications

☒ Both HTTP and HTTPS should be available

☐ Only HTTPS should be available

© 1996-2017 dormakaba

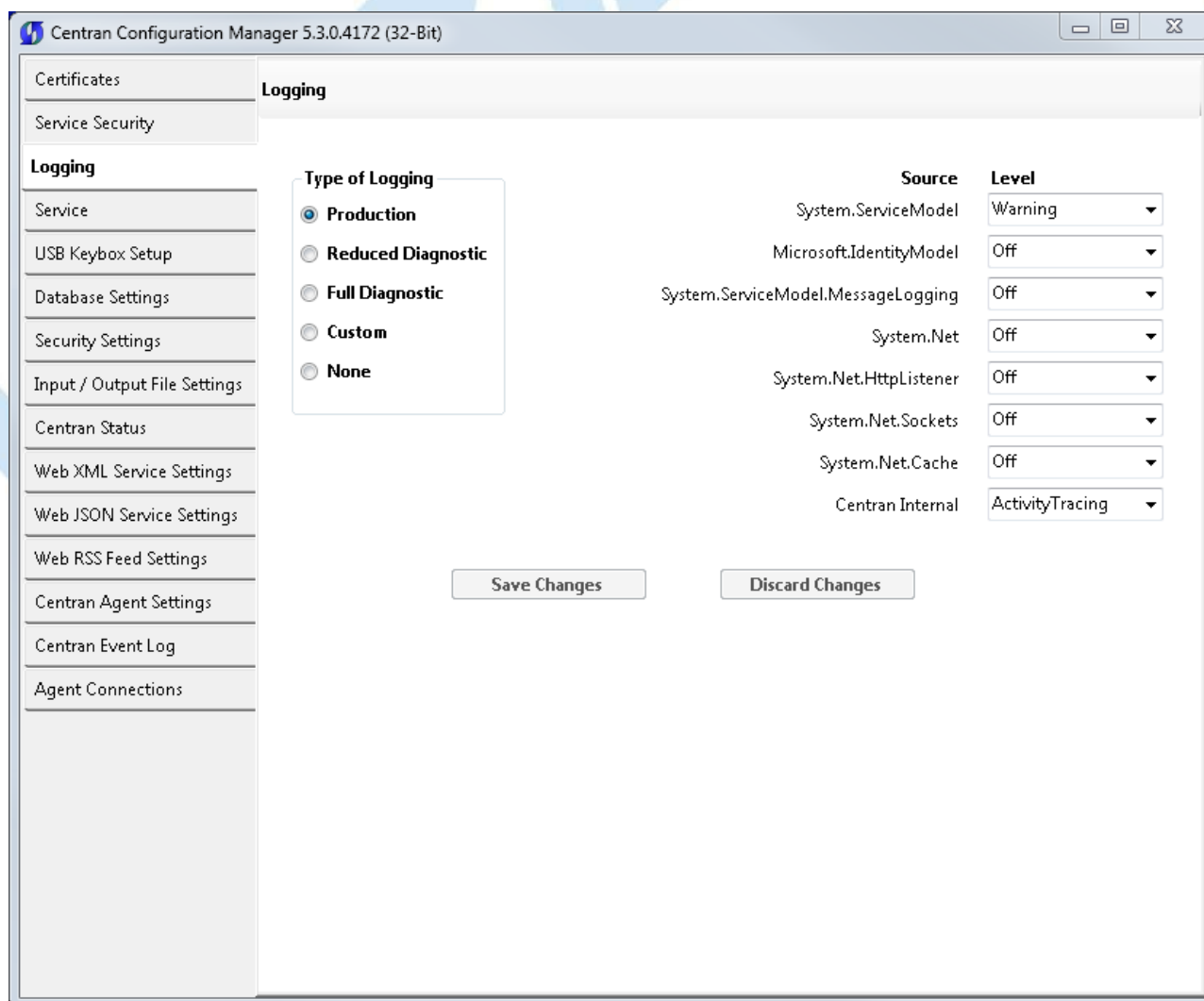
Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Set Up CenTran Diagnostics / Logging

CenTran 5 Getting Started Guide

The Logging tab provides control over the output of Windows Communication Foundation (WCF) diagnostic output for tracing operations. This may be useful for diagnosing issues with communications with the CenTran web service.

To modify these attributes select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu and click on the **Logging** tab to access this tab page:



The **Save Changes** and **Discard Changes** buttons will be enabled when any data on this tab is changed.

Clicking the **Save Changes** button will save the tab data to the CenTran configuration file.

Clicking the **Discard Changes** button will set the tab data to the values currently in the CenTran configuration file.

Clicking either the **Save Changes** button or the **Discard Changes** button will disable both buttons.

Note

If changes are saved the CenTran service must be stopped and started for the changes to take effect.

Type of Logging

The radio buttons shown under **Type of Logging** allow for quick selection of pre-defined logging settings.

- **Production:** initial / default setting. Captures limited information for diagnostics in order to maintain performance.
- **Reduced Diagnostic:** Additional information is captured. May be useful in initial problem diagnosis.
- **Full Diagnostic:** Detailed information is captured. May be useful in diagnosis of more difficult issues.
- **Custom:** Detailed information for selected WCF components is captured. May be useful in diagnosis of more difficult issues. Selecting this radio button does not change the loggers that are enabled, nor the log levels. It is used to indicate that the enabled loggers or log levels do not match any of the other predefined settings.
- **None:** No information is captured. This setting disables the capturing of any WCF diagnostic information.

Any diagnostic information for WCF events is recorded in a file named **WcfServiceTrace.svclog**. This file will be created within the application directory in

which the CenTran service is installed. The file can be viewed using the Microsoft Service Trace Viewer (SvcTraceViewer.exe). Double clicking on the file will automatically open the file in the Microsoft Service Trace Viewer.

The Microsoft Service Trace Viewer is available as a free download within the Windows Platform SDK.

Logging Sources and Logging Levels

The logging sources indicate the various WCF components or modules for which diagnostic information can be recorded. The logging level indicates the types of events for which diagnostic information will be recorded. The Log Levels are:

- Off: No information for the associated source is captured.
- Critical: Captures unexpected processing conditions.
- Error: Captures severe error conditions.
- Warning: Captures error conditions.
- Information: Captures events that mark successful processing.
- Verbose: Captures detailed information concerning successful processing.
- ActivityTracing: Captures flow between components.
- All: Captures all events. **This may degrade application performance.**

As log levels change from "Off" to "All" the event information at all prior levels is also recorded. Example: at a log level of "Warning", events that would be recorded at either the "Critical" or "Error" levels are also recorded.

For more information about WCF logging, look at the documentation provided online by Microsoft.

See [Appendix C - Troubleshooting: Check Run Time Error](#) for more information on viewing the Windows Communication Foundation (WCF) Trace log.

Message Content Logging

Once logging is enabled for **System.ServiceModel.MessageLogging**, an option is provided to also record the contents of the messages. If the "Log content of messages" checkbox is checked, then the content of WCF messages will be recorded.

Centran Configuration Manager 5.3.0.4172 (32-Bit)

Logging

Type of Logging

- ☐ Production
- ☐ Reduced Diagnostic
- ☐ Full Diagnostic
- ☒ Custom
- ☐ None

Source	Level
System.ServiceModel	Off
Microsoft.IdentityModel	Critical
System.ServiceModel.MessageLogging	Error
System.Net	Warning
System.Net.HttpListener	Information
System.Net.Sockets	Verbose
System.Net.Cache	ActivityTracing
Centran Internal	All

☒ Log content of messages

Save Changes **Discard Changes**

Set Up CenTran Management Web Access

CenTran 5 Getting Started Guide

The Service tab provides the ability to Install, Start, Stop and Uninstall the CenTran Service.

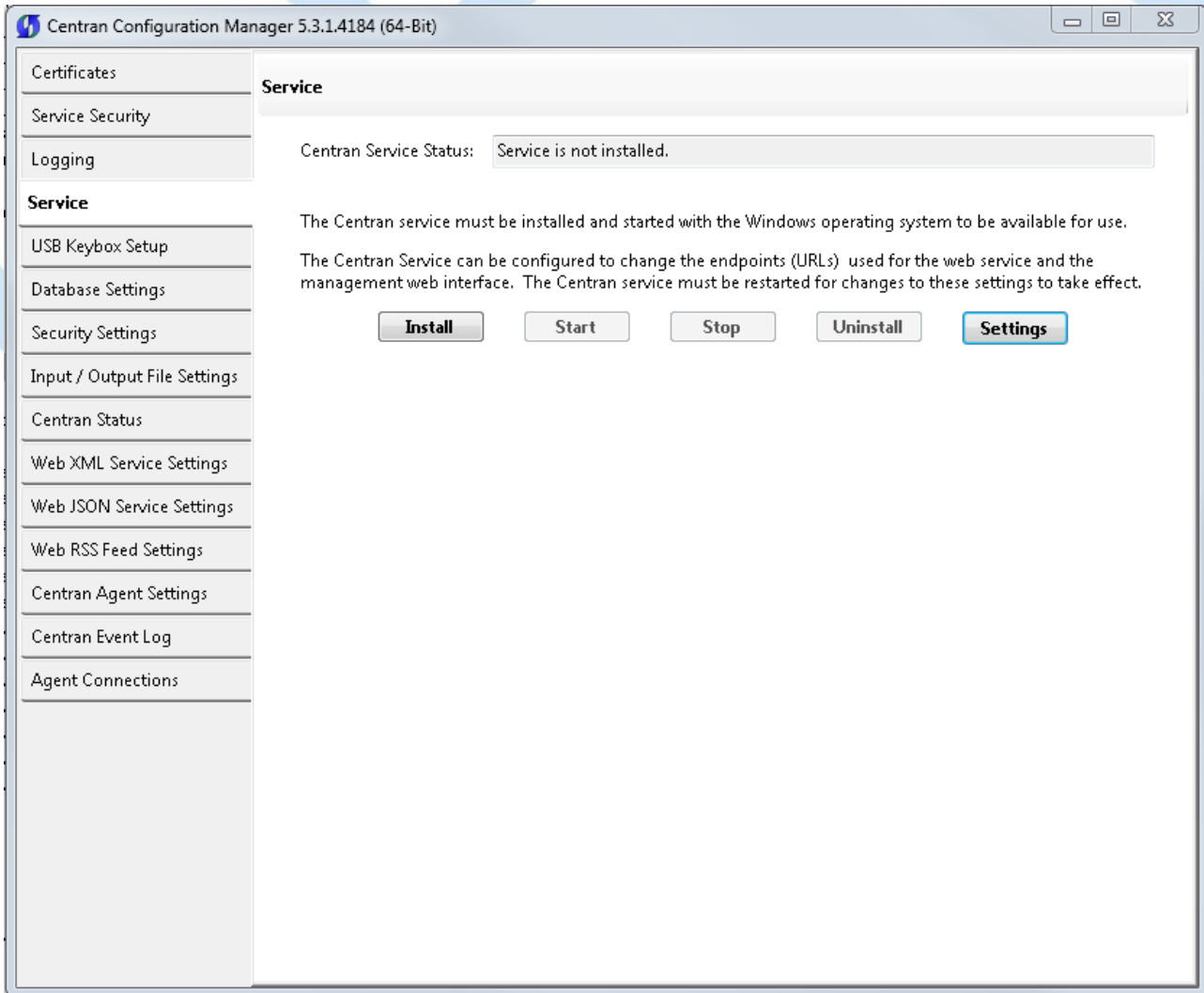
The Service tab also provides control over the URL endpoint for managing the CenTran Service over the network; as well as the ability to provide a localized (translated) web page for managing the CenTran Service.

This tab provides the information for customizing the URL endpoint for accessing the CenTran Management via the web browser and localization of the web page presented in the browser when access CenTran Management.

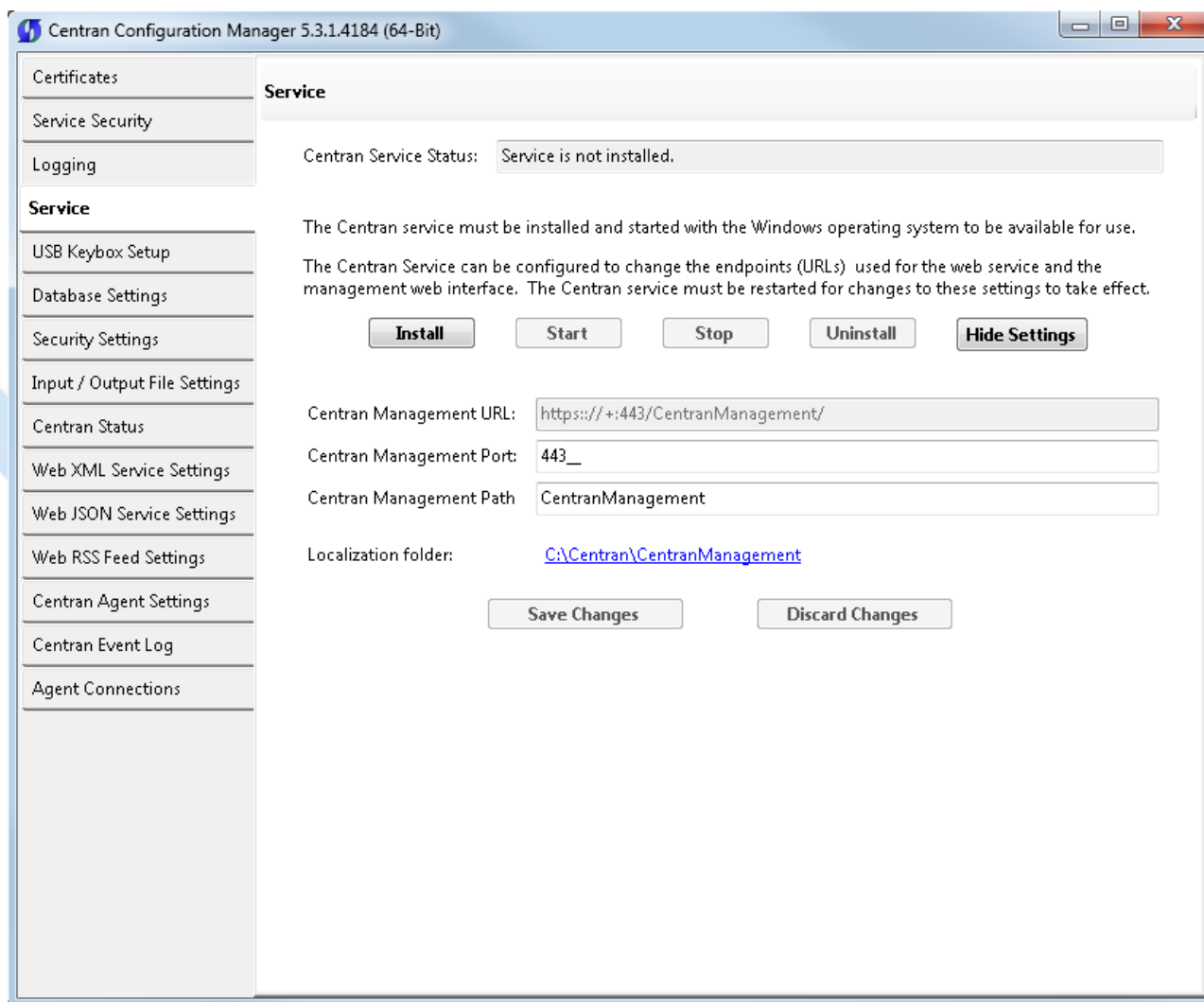
See [Install / Start the CenTran Service](#) for details on installing or starting the CenTran Service.

See [Stop / Uninstall the CenTran Service](#) for details on stopping or uninstalling the CenTran Service.

To modify the configuration settings for controlling web access to the CenTran Management application: select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu and then click on the **Service** tab to access this tab page within the application (the actual page may vary slightly based on the state of the CenTran Service):



Click on the **Settings** button to access the controls for modifying the configuration settings for the web connection to the CenTran Management application. The page will look like:



The **Save Changes** and **Discard Changes** buttons will be enabled when any data on this tab is changed.

Clicking the **Save Changes** button will save the tab data to the CenTran configuration file.

Clicking the **Discard Changes** button will set the tab data to the values currently in the Centran configuration file.

Clicking either the **Save Changes** button or the **Discard Changes** button will disable both buttons.

Note

If changes are saved the CenTran service must be (re)started for the changes to take effect.

Centran Management URL

The Centran Management URL shows the URL used to connect to the server's Centran Management application using the Web Browser. There are two parts to this URL that can be modified: the port and the path.

1. The Port: the port number to fully designate the network connection to the server's Centran Management application using the web browser. The default port is 443.
2. The Path: Default value is CentranManagement.

As the Port and Path are changed the resulting URL is updated as long as the values are valid. A warning messages will indicate if / when an invalid value is entered.

You will **NOT** be able to save invalid settings.

These settings change the URL used to access the Centran Management application in the browser.

Localization Folder

The Localization folder allows you to translate (or localize) the CentranManagement web page. To localize the CenTran Management web application:

1. Make a copy of the original CentranManagement folder. The original CenTran Management folder is named 'CentranManagement' and is in the Centran service install folder.
2. Edit the index.html in the copy folder.
3. Select the copy folder by clicking on the Localization Folder link, and
4. Navigate to the copy folder, select it, and then click on the OK button.

This setting does NOT change the URL used to access the CenTran Management application in the browser. It does change where the application loads the files used to display the CenTran Management application in the browser.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide



Set Up CenTran Event Logging

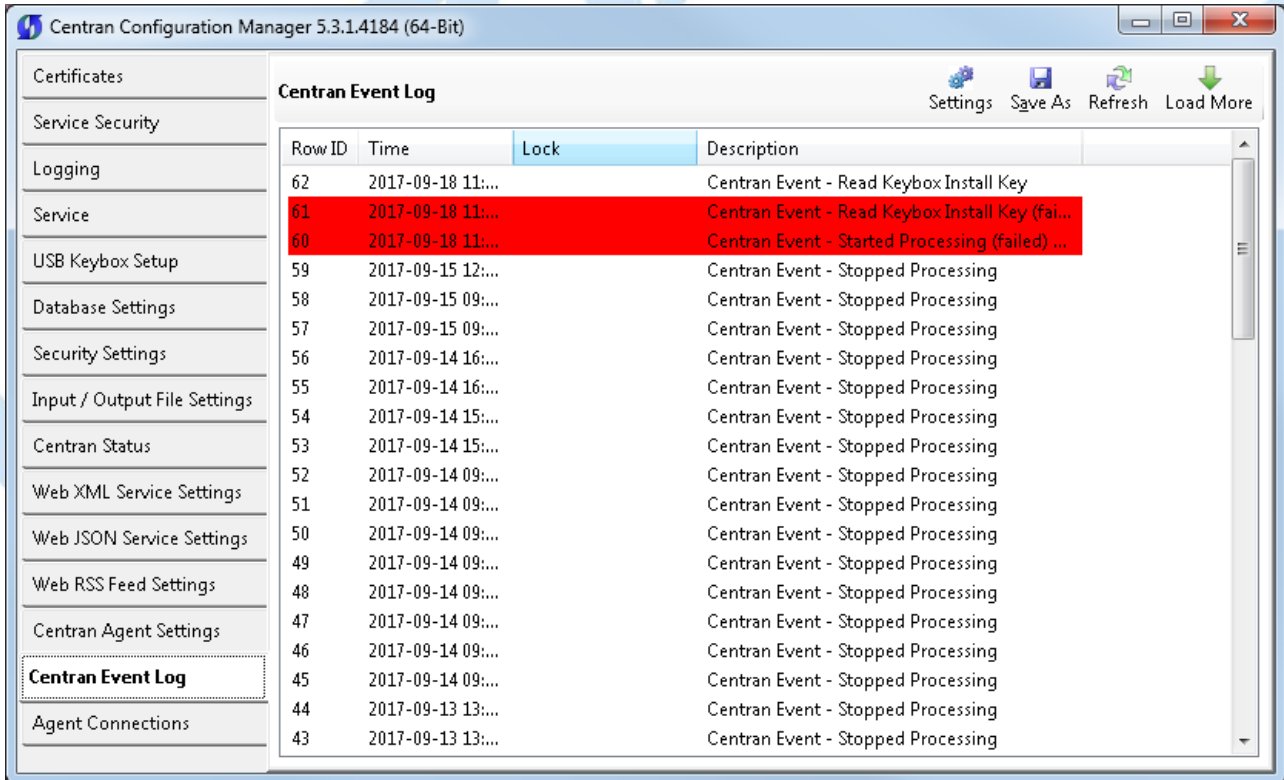
CenTran 5 Getting Started Guide

The CenTran Event Log tab provides a view of the most recent events that have been processed by the CenTran Service, and the means to refresh, save, and to load additional (older) events.

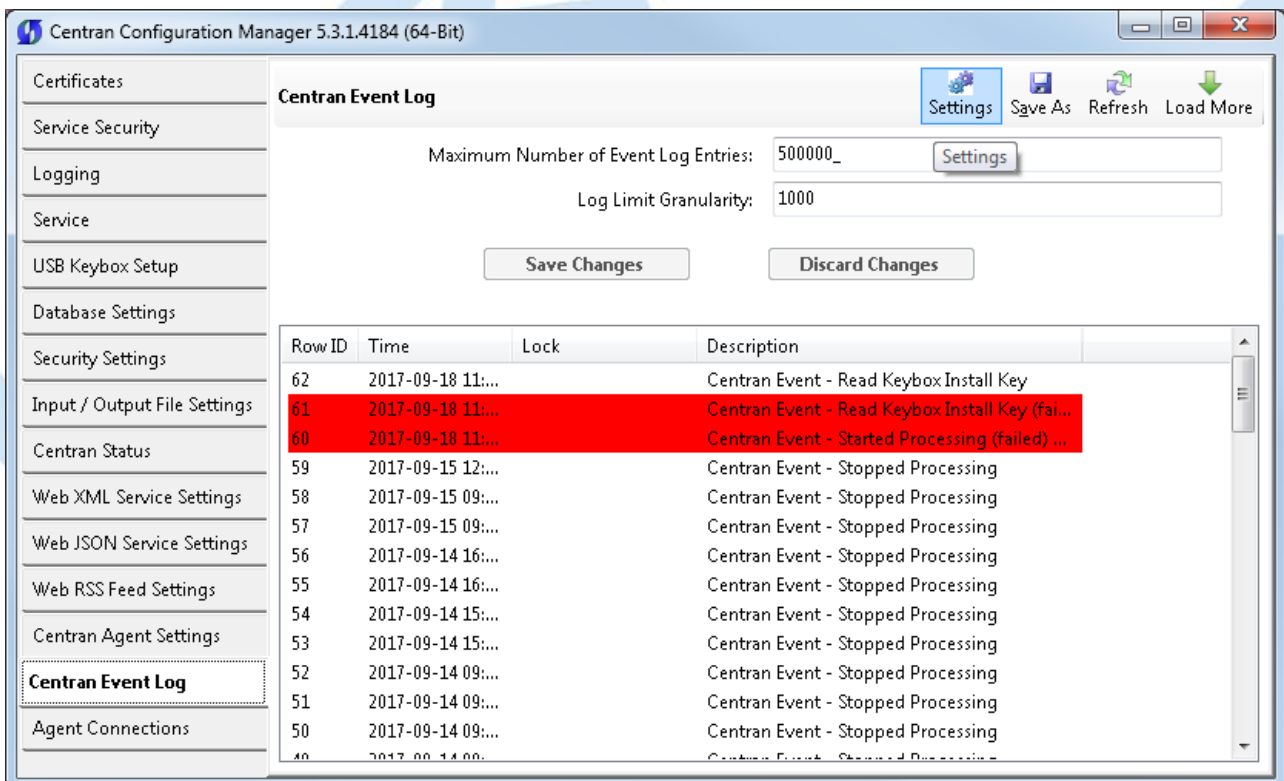
The CenTran Event Log tab also provides control over the settings to configure the maximum number of events audited and the granularity with which that maximum limit is checked.

See [View CenTran Event Log](#) for details on viewing the Audit trail.

To modify these settings select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu and click on the **CenTran Event Log** tab to access this tab page:



Click on the **Settings** button to access the controls for modifying the configuration settings for the web connection to the CenTran Management application. The page will look like:



The **Save Changes** and **Discard Changes** buttons will be enabled when either setting on this tab is changed.

Clicking the **Save Changes** button will update these settings in the CenTran configuration file.

Clicking the **Discard Changes** button will set the tab data to the values currently in the CenTran configuration file.

Clicking either the **Save Changes** button or the **Discard Changes** button will disable both buttons.

Note

If changes are saved the CenTran service must be stopped and started for the changes to take effect.

Maximum Number of Event Log Entries

This setting controls the total number of most recent audit events that are recorded. It limits the size of the Centran Event Log. Once the log reaches the set limit, it will delete the oldest audits to remain within the limit. The check for the limit size is controlled by this setting and the **Log Limit Granularity**. The event log may grow slightly larger than the set limit based upon the granularity. The lowest valid value for this setting is 10,000. The highest valid value for this setting is 1,000,000. The default value for this setting is 500,000.

Log Limit Granularity

The Log Limit Granularity determines the number of new events that must be added before the number of event log entries is checked against the limit. This "granularity" minimizes the impact on performance. The lowest valid value for this setting is 100. The highest valid value for this setting is 5,000. The default value for this setting is 1000.

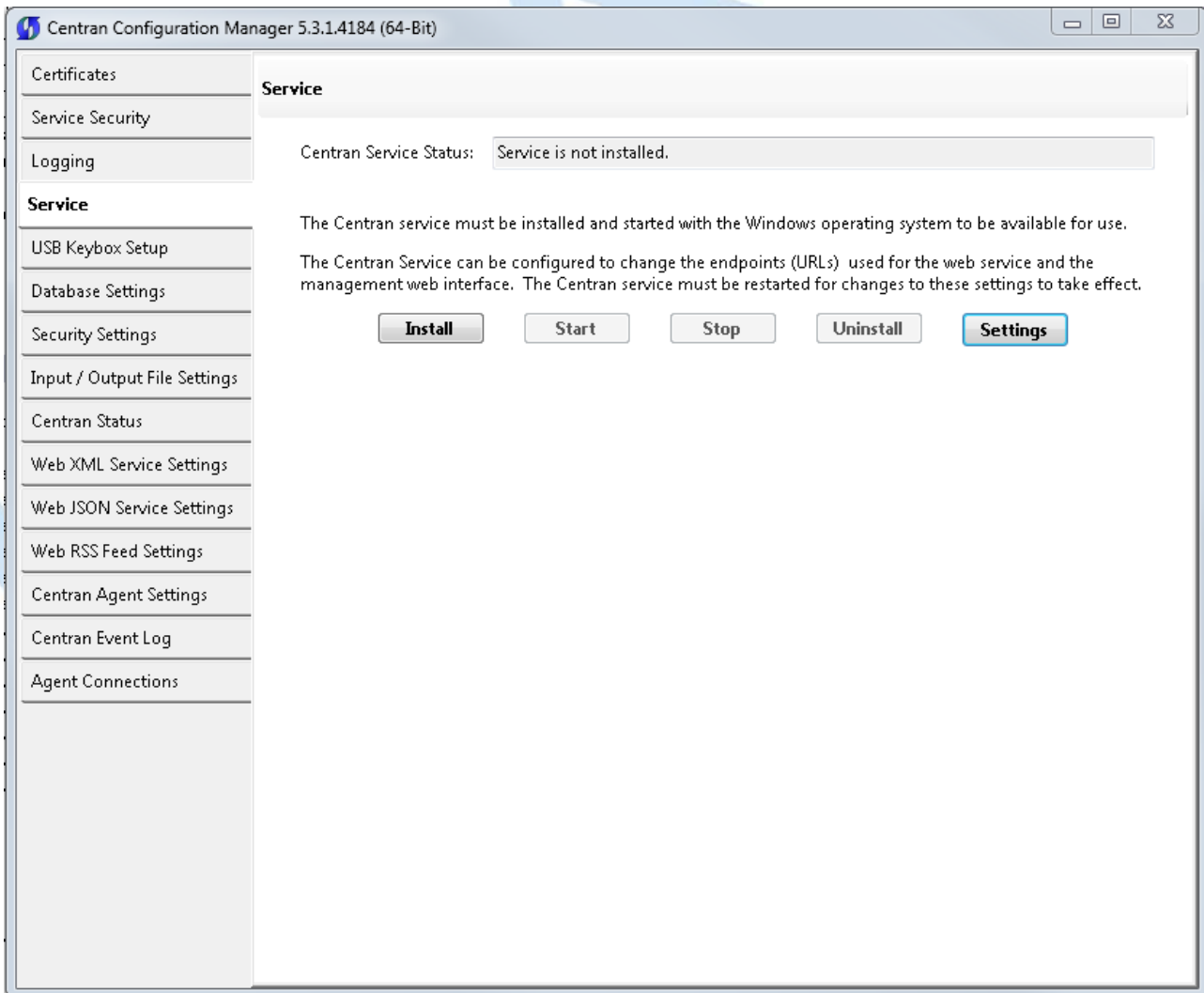
© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

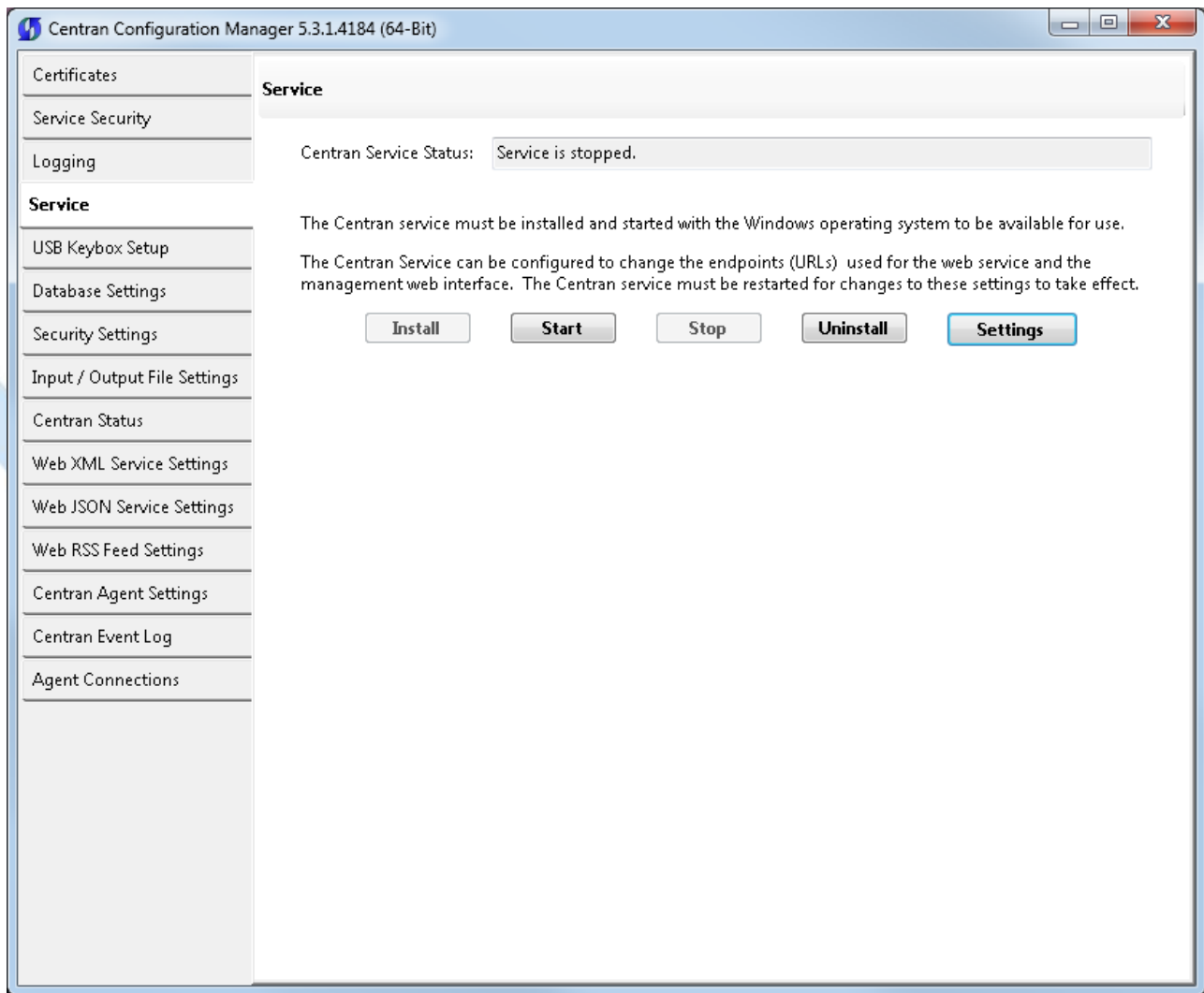
Install / Start the CenTran Service

CenTran 5 Getting Started Guide

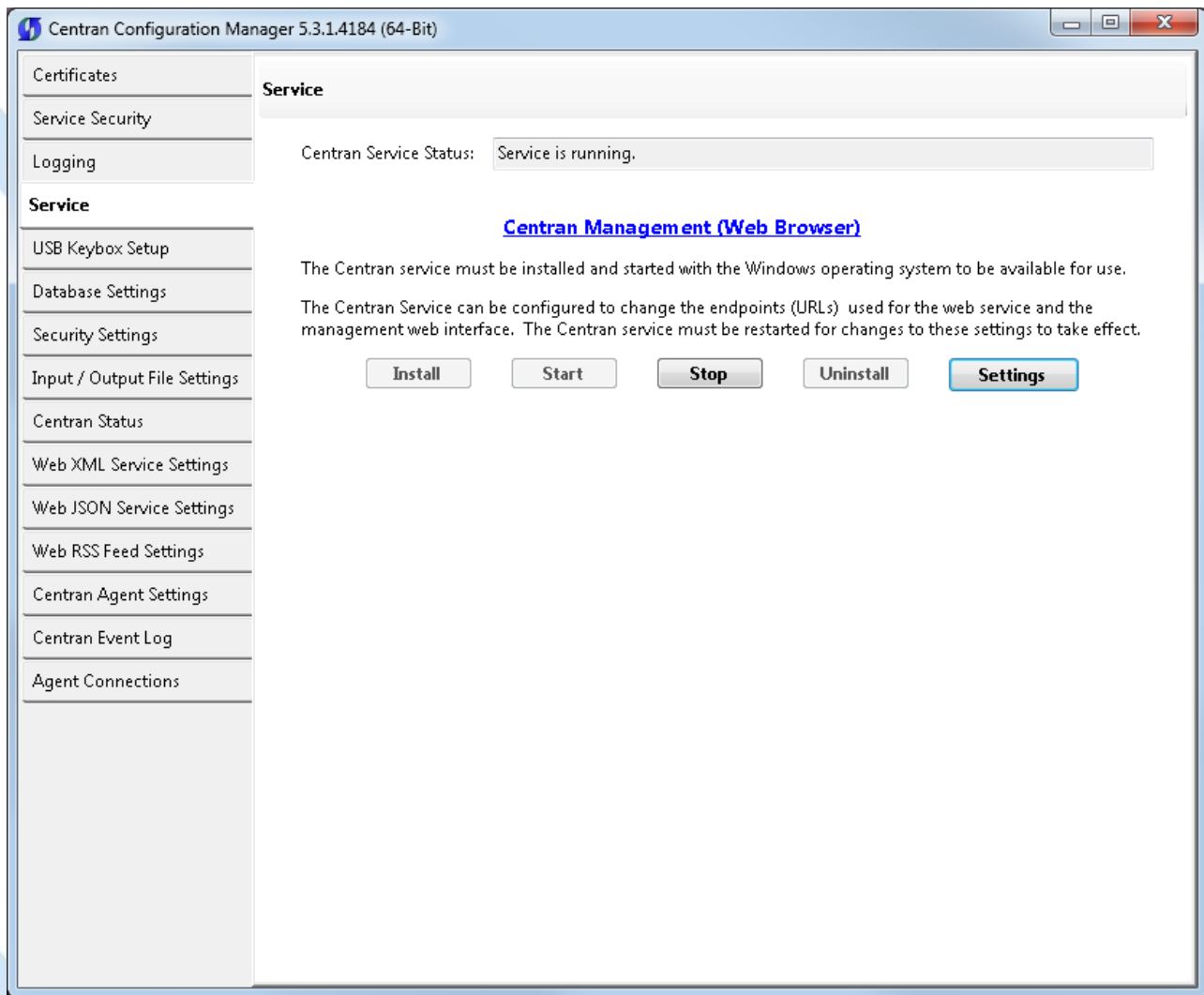
To install and start the CenTran service, select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu. Click on the **Service** tab. You should see the following tab page:



Select the **Install** button to install the CenTran service with the operating system.



Make sure you have completed any changes to the CenTran service configuration file. Select the **Start** button to start the CenTran service with the operating system.



You will now have a link available to open the CenTran Management interface in your default web browser. Your web browser must support HTML5 and CSS3. This includes the following browsers:

1. Internet Explorer 9 or higher
2. Firefox 10 or higher
3. Google Chrome 16 or higher
4. Apple Safari 5 or higher

If you are using Internet Explorer, you must have compatibility mode for intranet sites turned off under the Tools menu. Press Alt-T to open the tools menu in Internet Explorer to get to this setting.

You can now manage CenTran settings either directly through the CenTran Configuration Manager or through the web browser CenTran Management interface. You will now need to set up the CenTran settings using one of these two methods, and then you can start processing lock transactions using CenTran.

© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Configure the CenTran Service using CenTran Configuration Manager

CenTran 5 Getting Started Guide

The CenTran Configuration Manager supports directly managing a running CenTran service on the same computer. It does not support managing a CenTran service running on a different computer. To manage a running CenTran service, you must have already set up the appropriate CenTran configuration file settings and certificates. You must have also installed and started the CenTran service.

Managing the CenTran service:

The following sections describe setting up and managing the CenTran service using the CenTran Configuration Manager:

- [Setup Keybox](#)
- [Select ODBC Database Connection](#)
- [Set Company Number](#)
- [Set File Settings](#)
- [Start Transaction Processing](#)
- [View Web Service XML Settings](#)
- [View Web Service JSON Settings](#)
- [View Web RSS Feed Settings](#)
- [View CenTran Agent Settings](#)
- [View CenTran Event Log](#)
- [View CenTran Agent Persistent Connections](#)
- [Stop Transaction Processing](#)

© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Setup Keybox

CenTran 5 Getting Started Guide

Click on the **USB Keybox Setup** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

USB Keybox Setup	
Is Keybox Connected / Responding:	Present
Is Keybox Firmware Version Good:	Firmware Version is up to date
Is Keybox Setup:	USB Keybox installation has not been set up
Hardware Type:	Cencon USB Key Box
Firmware Version ID:	200712
Firmware Version:	1.3.4022 2016/04/21 14:46:48
Hardware Serial Number:	01E268DE1500003E
Device ID:	0160
Customer ID:	Brink's Route ALL BRINK'S
Kaba Mas Customer Number:	LLID#026
Kaba Mas Order Number:	2016-12-06 13:18:47Z
Device Initialization Date:	2016-12-06
Abbreviated Device ID:	0651
Abbreviated Customer ID:	0063
Device Description:	Bank FLM Route Enterprise
Max FLM Locks Restriction:	0
Max Route Locks Restriction:	0
Max Bank Locks Restriction:	0
Max Device Reinstall Restriction:	20

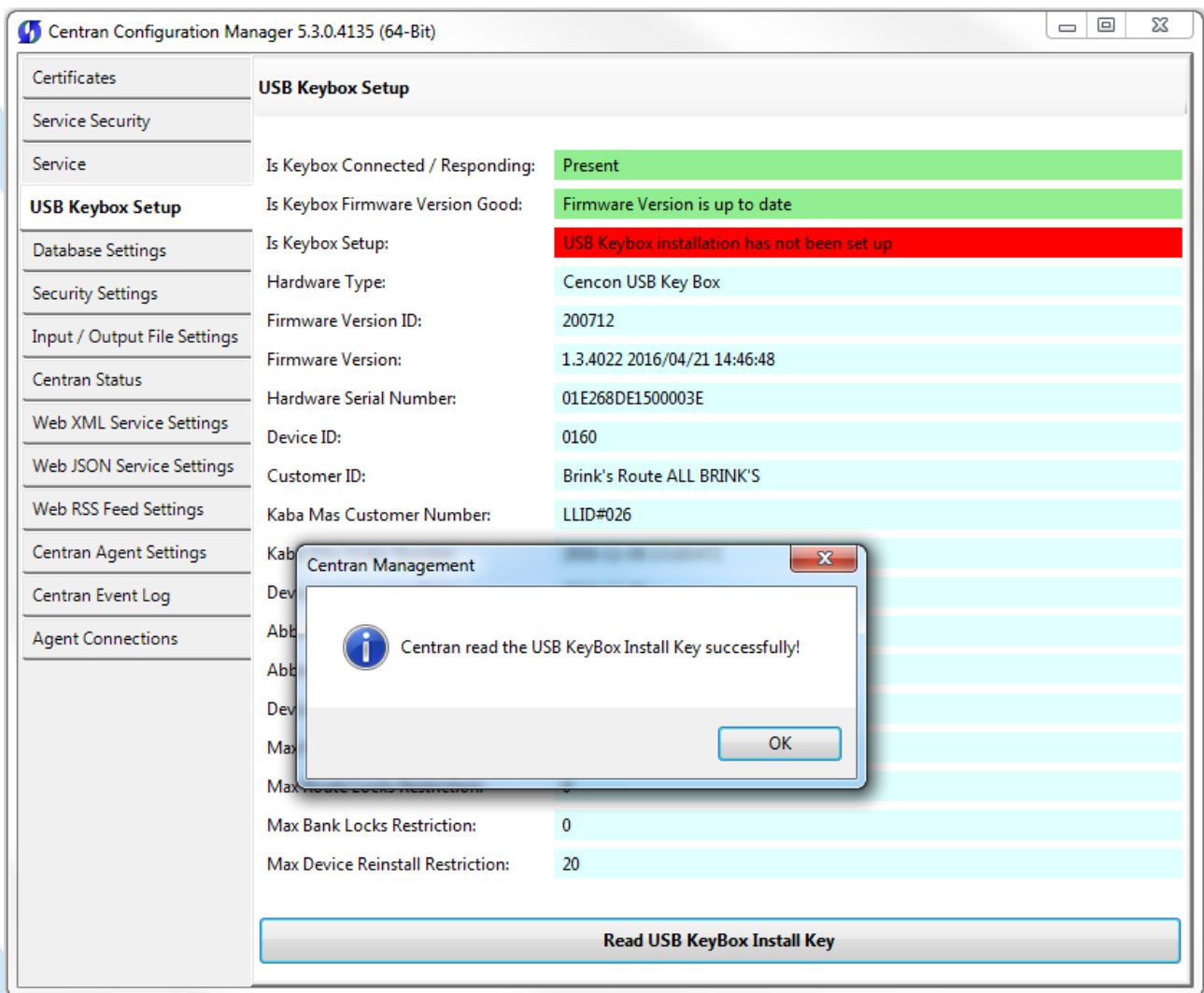
Read USB KeyBox Install Key

Place your Keybox install key in the first port of the keybox: (This will be the port farthest away from the USB connection.)



Click on the **Read USB Keybox Install Key** button on the **USB Keybox Setup** tab page.

You should see the following in the **USB Keybox Setup** tab page.



Click on the **OK** button on message box.

You should see the following in the **USB Keybox Setup** tab page.

Centran Configuration Manager 5.3.0.4135 (64-Bit)

Certificates

Service Security

Service

USB Keybox Setup

Database Settings

Security Settings

Input / Output File Settings

Centran Status

Web XML Service Settings

Web JSON Service Settings

Web RSS Feed Settings

Centran Agent Settings

Centran Event Log

Agent Connections

USB Keybox Setup

Is Keybox Connected / Responding:

Present

Is Keybox Firmware Version Good:

Firmware Version is up to date

Is Keybox Setup:

USB Keybox installation has been set up

Hardware Type:

Cencon USB Key Box

Firmware Version ID:

200712

Firmware Version:

1.3.4022 2016/04/21 14:46:48

Hardware Serial Number:

01E268DE1500003E

Device ID:

0160

Customer ID:

Brink's Route ALL BRINK'S

Kaba Mas Customer Number:

LLID#026

Kaba Mas Order Number

2016-12-06 13:18:47Z

Device Initialization Date:

2016-12-06

Abbreviated Device ID:

0651

Abbreviated Customer ID:

0063

Device Description:

Bank FLM Route Enterprise

Max FLM Locks Restriction:

0

Max Route Locks Restriction:

0

Max Bank Locks Restriction:

0

Max Device Reinstall Restriction:

20

Read USB KeyBox Install Key

Select ODBC Database Connection

CenTran 5 Getting Started Guide

Important Note

CenTran no longer runs under the permissions of the logged on user. It has been changed to run as a background service on the host server you install it on, and is independent of who is logged on. The CenTran service will run in the background even if no one is logged onto the host server.

By default, the CenTran service runs logged on under a **Local System** account. This gives it access to resources and settings on the host server you install it on. However, the **Local System** account only has access to the host server, not to resources on your network.

If the CenTran service is configured to run logged onto the default **Local System** account, you will need to use SQL authentication for CenTran to access the SQL Server database.

If the CenTran service is configured to run logged onto an account configured for it on your network domain, then that account must have administrative privileges on the host server CenTran is on.

If you use Windows authentication for CenTran's database authentication, then the account CenTran is logged onto must be a network domain account and have authorization to access the SQL Server database.

You can view and edit the CenTran service settings from the Microsoft Management Console:

- Open the Start Menu.
- Right click on **Computer**.
- Select **Manage** from the displayed context menu. You must have administrative privileges.
- The **Computer Management** console will be displayed. Expand the **Services and Applications** section on the left side.
- Select **Services** from the **Services and Applications** section.
- Locate **CenTran** from the list of services. Right click on **CenTran** and select **Properties** from the context menu.
- A service **Properties** dialog will be displayed. Select the **Log On** tab to examine the account the service is set up to log on as.

Click on the **Database Settings** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

CenTran Configuration Manager 5.3.0.4135 (64-Bit)

Database Settings

Open Database Connectivity (ODBC) Database Settings

Data Source Name:

User ID:

Is Database Administrator:

Is Database System Administrator:

Default Schema Name:

Database Management System Name:

Database Management System Version:

Server Name:

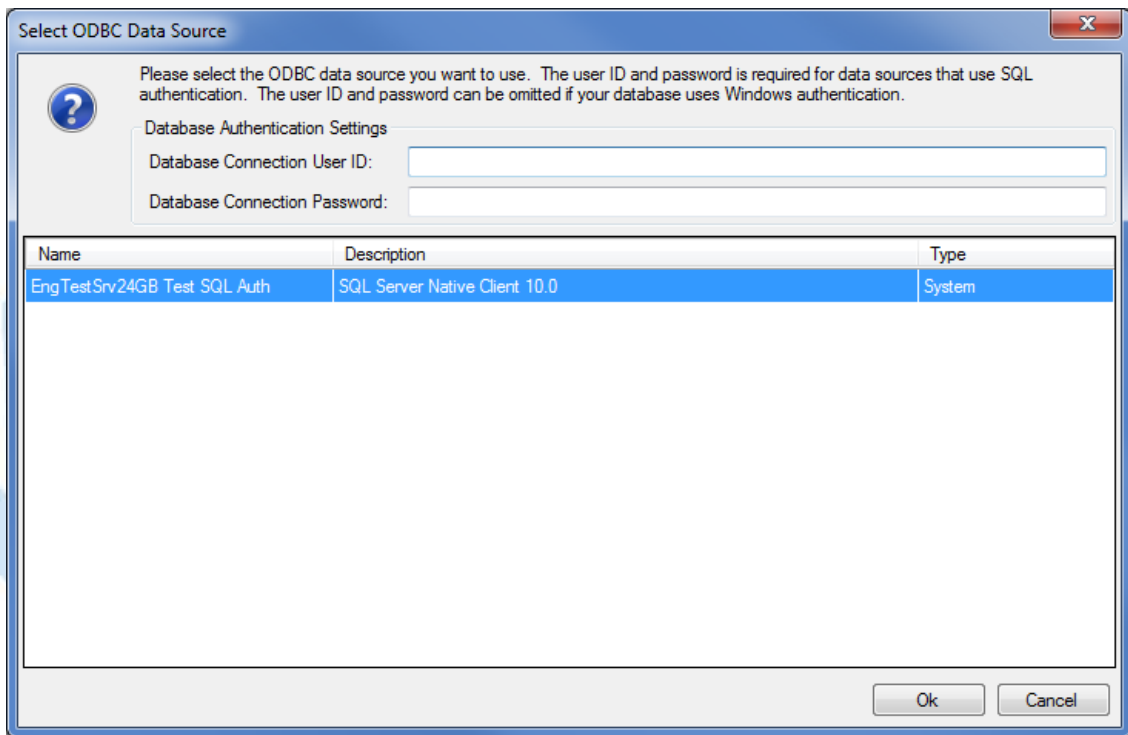
Database Name:

Instance Name:

Is Case Sensitive:

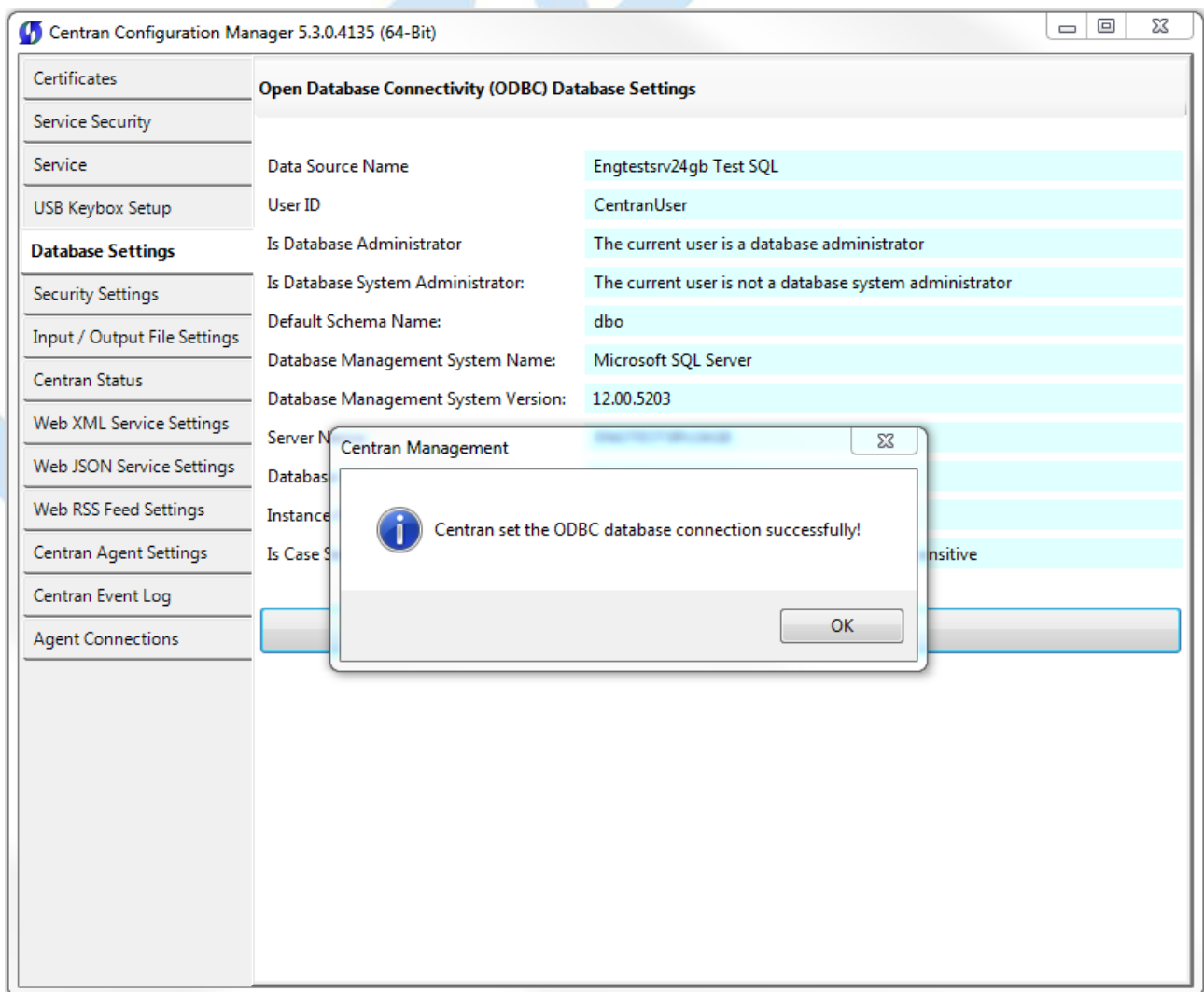
Select ODBC Data Source

You will need to have set up an ODBC database connection specifying the database you want to use. The ODBC database connection will need to be configured to use SQL authentication. Click on the **Select ODBC Data Source** button. You should see the following dialog displayed:



Select the ODBC database connection you want to use. For SQL authentication, you will also need to enter a user name and password for the CenTran service to use with the database connection.

You should see the following tab page displayed by the CenTran Configuration Manager:



Click on the **OK** button on message box.

You should see something similar to the following tab page displayed by the CenTran Configuration Manager, depending on your database configuration:

Centran Configuration Manager 5.3.0.4135 (64-Bit)

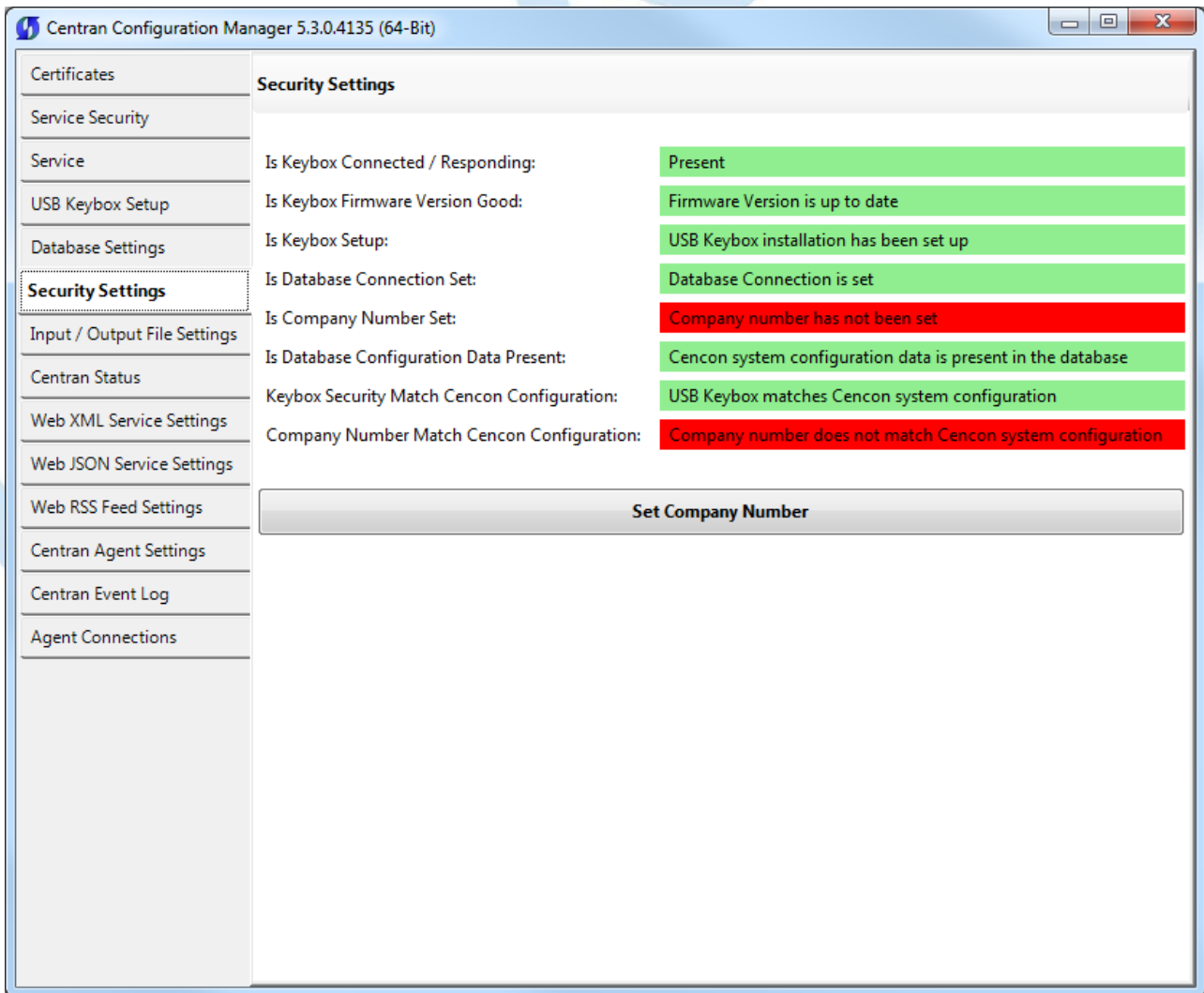
Certificates	Open Database Connectivity (ODBC) Database Settings	
Service Security		
Service	Data Source Name	Engtestsv24gb Test SQL
USB Keybox Setup	User ID	CentranUser
Database Settings	Is Database Administrator	The current user is a database administrator
Security Settings	Is Database System Administrator:	The current user is not a database system administrator
Input / Output File Settings	Default Schema Name:	dbo
Centran Status	Database Management System Name:	Microsoft SQL Server
Web XML Service Settings	Database Management System Version:	12.00.5203
Web JSON Service Settings	Server Name:	ENGTESTSRV24GB
Web RSS Feed Settings	Database Name:	Loomis
Centran Agent Settings	Instance Name	MSSQLSERVER
Centran Event Log	Is Case Sensitive:	The database is not configured to be case sensitive
Agent Connections	Select ODBC Data Source	

Set Company Number

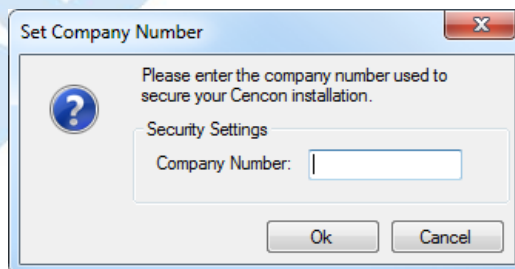
CenTran 5 Getting Started Guide

Click on the **Security Settings** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

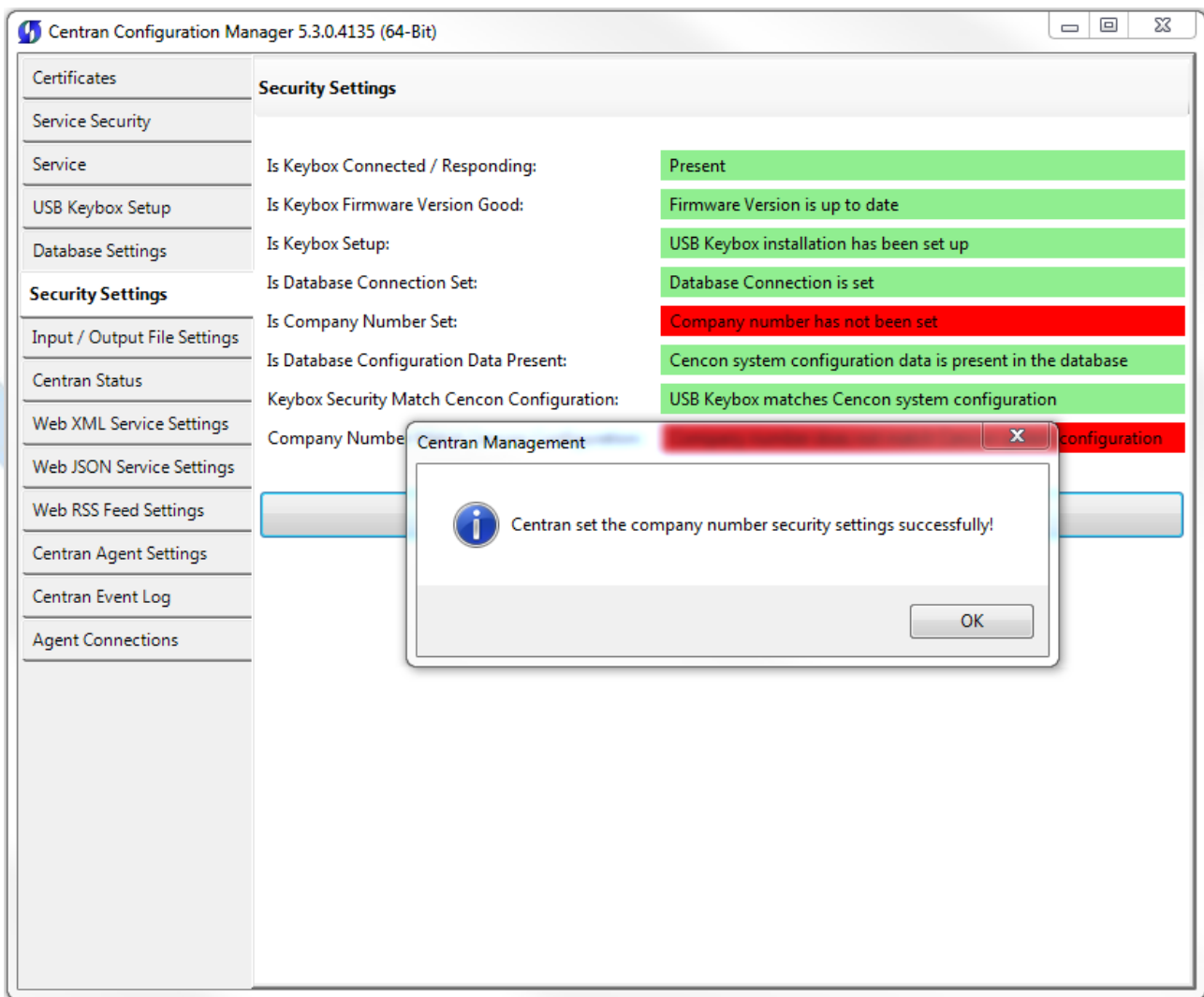


Click on the **Set Company Number** button. You should see the following dialog displayed:



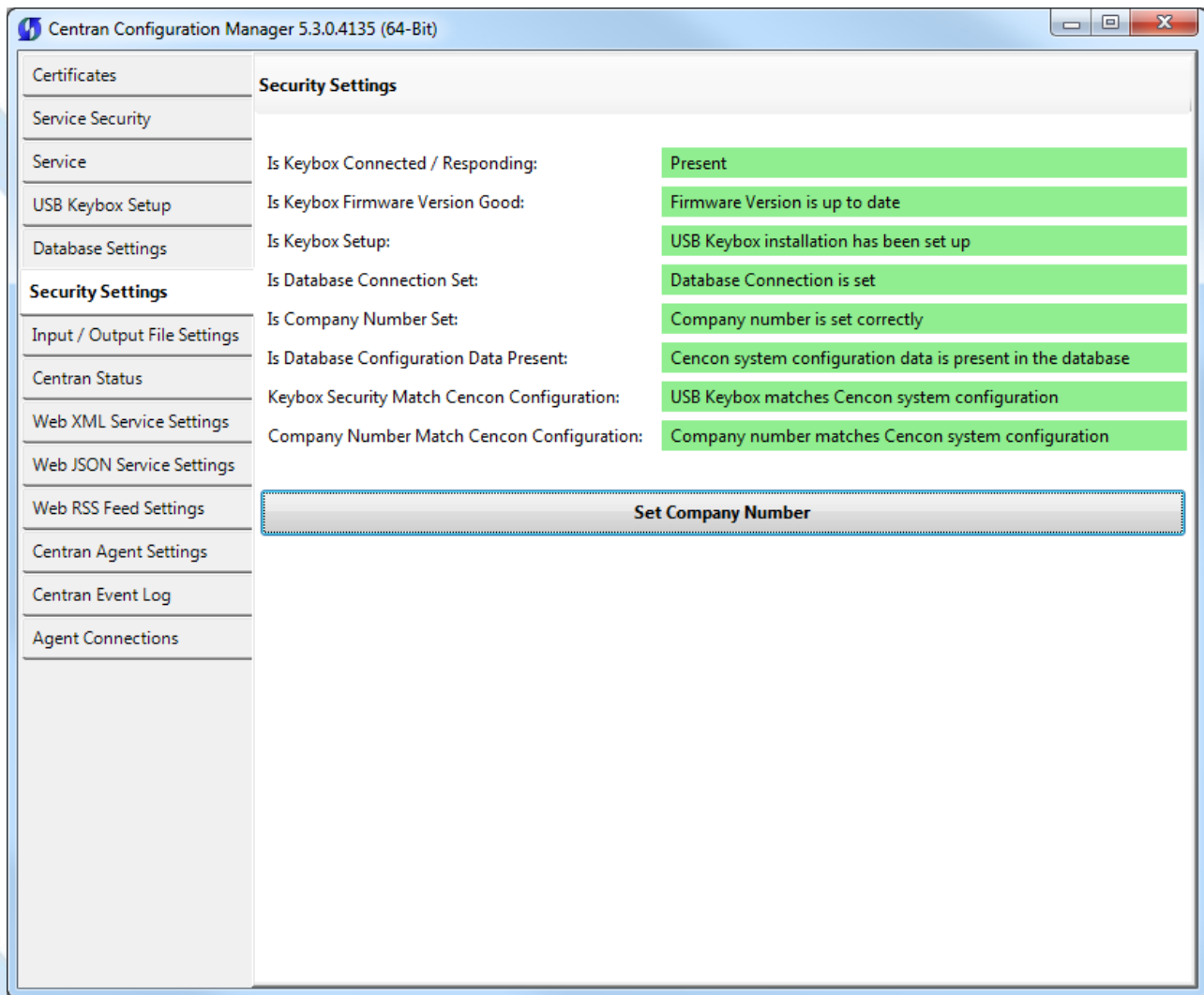
Enter the 4 digit company number you are using with Cencon. This is a sensitive piece of security information that is part your security with the Cencon system. You should record it and keep it in a secure place. The company number you enter for use by the CenTran service must match the one you are using with Cencon.

You should see the following tab page displayed by the CenTran Configuration Manager:



Click on the **OK** button on message box.

You should see the following tab page displayed by the CenTran Configuration Manager:



© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Set File Settings

CenTran 5 Getting Started Guide

Important Note

CenTran no longer runs under the permissions of the logged on user. It has been changed to run as a background service on the host server you install it on, and is independent of who is logged on. The CenTran service will run in the background even if no one is logged onto the host server.

By default, the CenTran service runs logged on under a **Local System** account. This gives it access to resources and settings on the host server you install it on. However, the **Local System** account only has access to the host server, not to resources on your network.

If you are configuring CenTran to access a shared file location on your network, not on the host server, then you will need to set up CenTran with a network domain account.

The account you set up CenTran to run logged onto must have administrative privileges on the host server CenTran is on. It must also have read / write access to the directories you are using for file input / output.

In this case, the file directories must be identified by UNC (Universal Naming Convention) paths: "\\server\share\path\"

You can not use mapped drive letters for network paths for a service. Mapped drive letters for network paths are specific to an account. They are not accessible from other accounts. If you set up a mapped drive letter for your logged on account, that does not mean that CenTran can access it from its account.

You can view and edit the CenTran service settings from the Microsoft Management Console:

- Open the Start Menu.
- Right click on **Computer**.
- Select **Manage** from the displayed context menu. You must have administrative privileges.
- The **Computer Management** console will be displayed. Expand the **Services and Applications** section on the left side.
- Select **Services** from the **Services and Applications** section.
- Locate **Centran** from the list of services. Right click on **Centran** and select **Properties** from the context menu.
- A service **Properties** dialog will be displayed. Select the **Log On** tab to examine the account the service is set up to log on as.

1. Click on the **Input / Output File Settings** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

CenTran Configuration Manager 5.3.0.4135 (64-Bit)

Input / Output File Settings

Input File Directory:	
Input File Extension:	
Delay Before Reading Input Files (Milliseconds):	10
Output File Directory:	
Output File Extension:	
Save Diagnostic Information:	Not saving diagnostics information.
Diagnostic File Path:	
Default Dispatcher ID:	CENTRAN
Force Default Dispatcher To Be Used:	Not forcing default dispatcher ID to be used for transaction processing.

Set File Settings

Set Default Dispatcher Settings

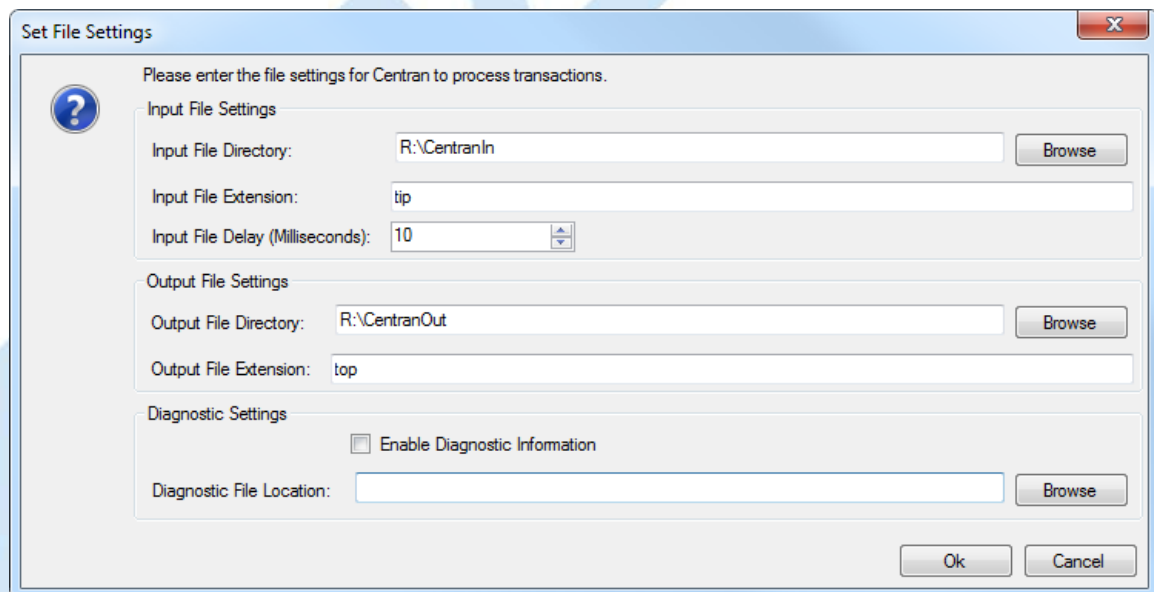
2. You will need to setup an input directory and an output directory for CenTran to receive file transactions and return the response.

- **Input Directory** - The input directory is the directory where CenTran reads transactions being sent to it. It looks in this directory for files representing lock transactions to be processed. You will need to create an input directory that you want to use for CenTran to listen for incoming file transactions.
- **Input File Extension** - The input file extension defined here is the file extension CenTran looks for when attempting to find transaction input files in the input directory that has been identified. If an input file extension is not set, then the CenTran service will attempt to read any file placed in the input directory.
- **Input File Delay** - The delay before reading next input transaction file setting is intended to allow a delay after detecting a file and before reading it. It is possible for an error in reading the input file to occur if it has not been completely written to the input directory yet. This delay allows the write of the input file to complete before the CenTran service reads the file. This delay begins when a transaction file is detected in the input directory by CenTran.
- **Output Directory** - The output directory is the directory where CenTran places the output files containing the results of processed transactions. This directory can be the same directory as the one used to contain input files. If the two directories are the same, then the files must have different extensions assigned. You will need to create an output directory that you want to use for CenTran to write output files to.
- **Output File Extension** - The output file extension is the file extension placed by CenTran at the end of output file names. The file names will be the same as the input file names, except for the file extension. If an output file extension is set, then that extension will be placed at the end of output files produced by CenTran.

Note

CenTran has been validated against the SuperSpeed RamDisk Plus software. This software allows you to use a ram disk as the file location used for transferring CenTran transaction files. This improves performance and speed of transferring CenTran transaction files, and eliminates hard drive wear from transferring CenTran transaction files. This software is available at <http://www.superspeed.com/desktop/ramdisk.php>. SuperSpeed RamDisk is a Microsoft Certified software.

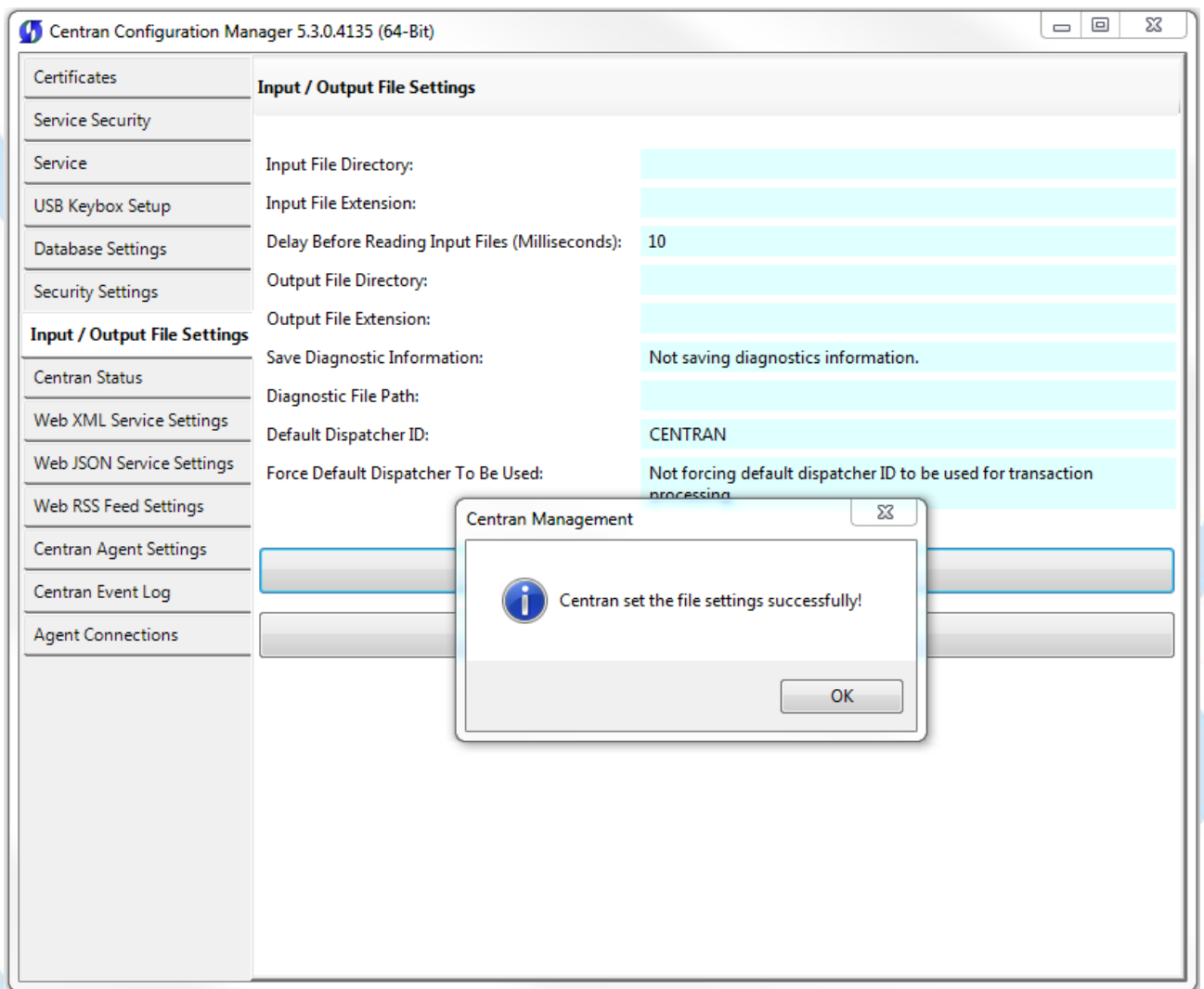
3. Click on the **Set File Settings** button. You should see the following dialog displayed:



The image shows a Windows-style dialog box titled "Set File Settings". It contains three sections: "Input File Settings", "Output File Settings", and "Diagnostic Settings". In the "Input File Settings" section, "Input File Directory" is set to "R:\CenTranIn", "Input File Extension" is "tip", and "Input File Delay (Milliseconds)" is "10". In the "Output File Settings" section, "Output File Directory" is set to "R:\CenTranOut" and "Output File Extension" is "top". In the "Diagnostic Settings" section, the "Enable Diagnostic Information" checkbox is unchecked, and "Diagnostic File Location" is empty. There are "Browse" buttons next to the directory fields and "Ok" and "Cancel" buttons at the bottom right.

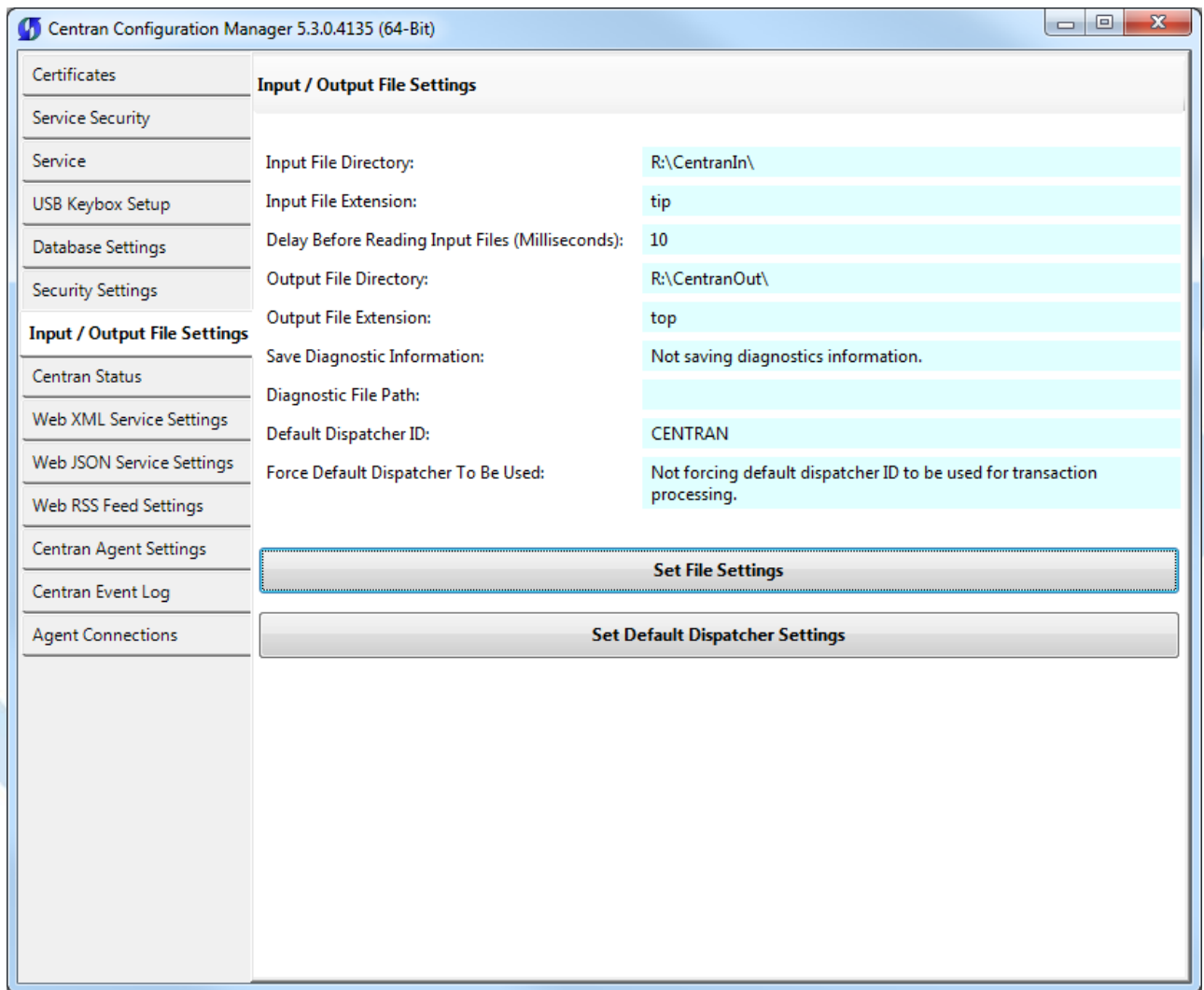
4. Enter the input and output directories and extensions for the CenTran service to process files. Optionally, you can enable CenTran to record diagnostic output to a file, but this slows down performance. Once you have entered the settings you want to use, click on the **OK** button.

You should see the following tab page displayed by the CenTran Configuration Manager:



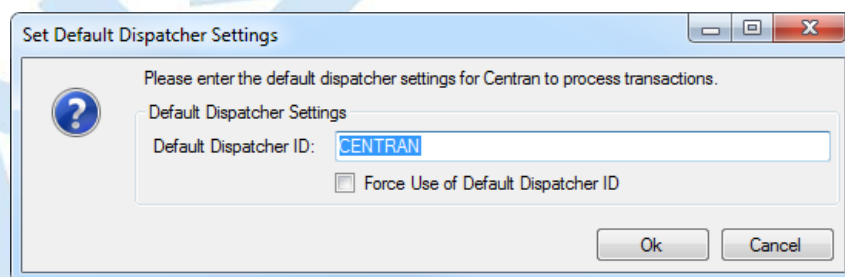
5. Click on the **OK** button on message box.

You should see the following tab page displayed by the CenTran Configuration Manager:



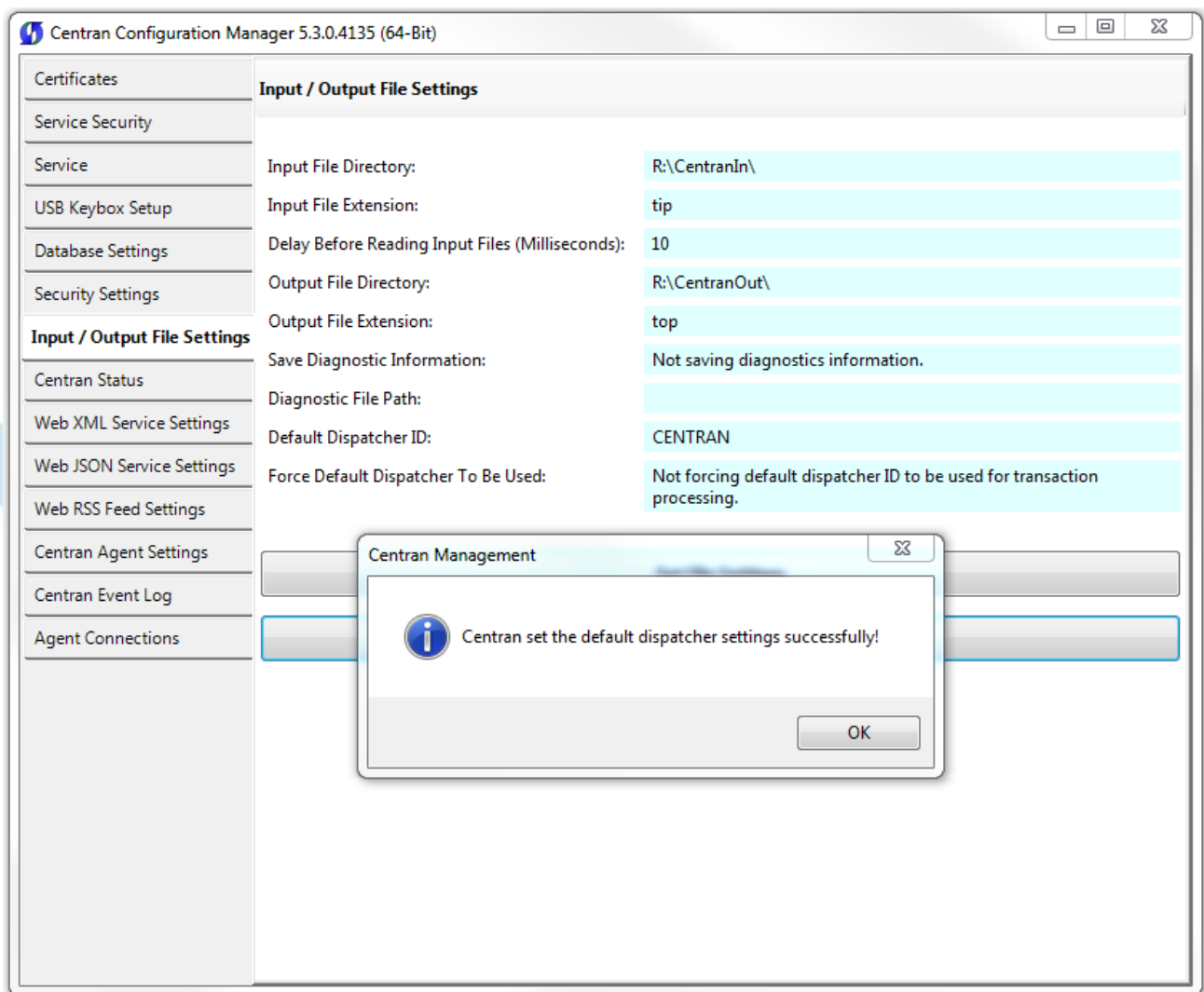
6. You will also need to set the default dispatcher ID to be used for the CenTran service when a dispatcher ID is not available for a transaction being processed. Optionally, you can force this dispatcher ID to be used instead of the dispatcher ID associated with a transaction. Click on the **Set Default Dispatcher Settings** button. You should see the following dialog displayed:

You should see the following dialog displayed:



7. Enter the default dispatcher ID you want to use. This default dispatcher ID must have been already set up under Cencon, and be present in the database. The role that the default dispatcher is assigned to will effect what authorizations the default dispatcher has. Once you have entered the default dispatcher ID you want to use, click on the **OK** button.

You should see the following message displayed by the CenTran Configuration Manager:

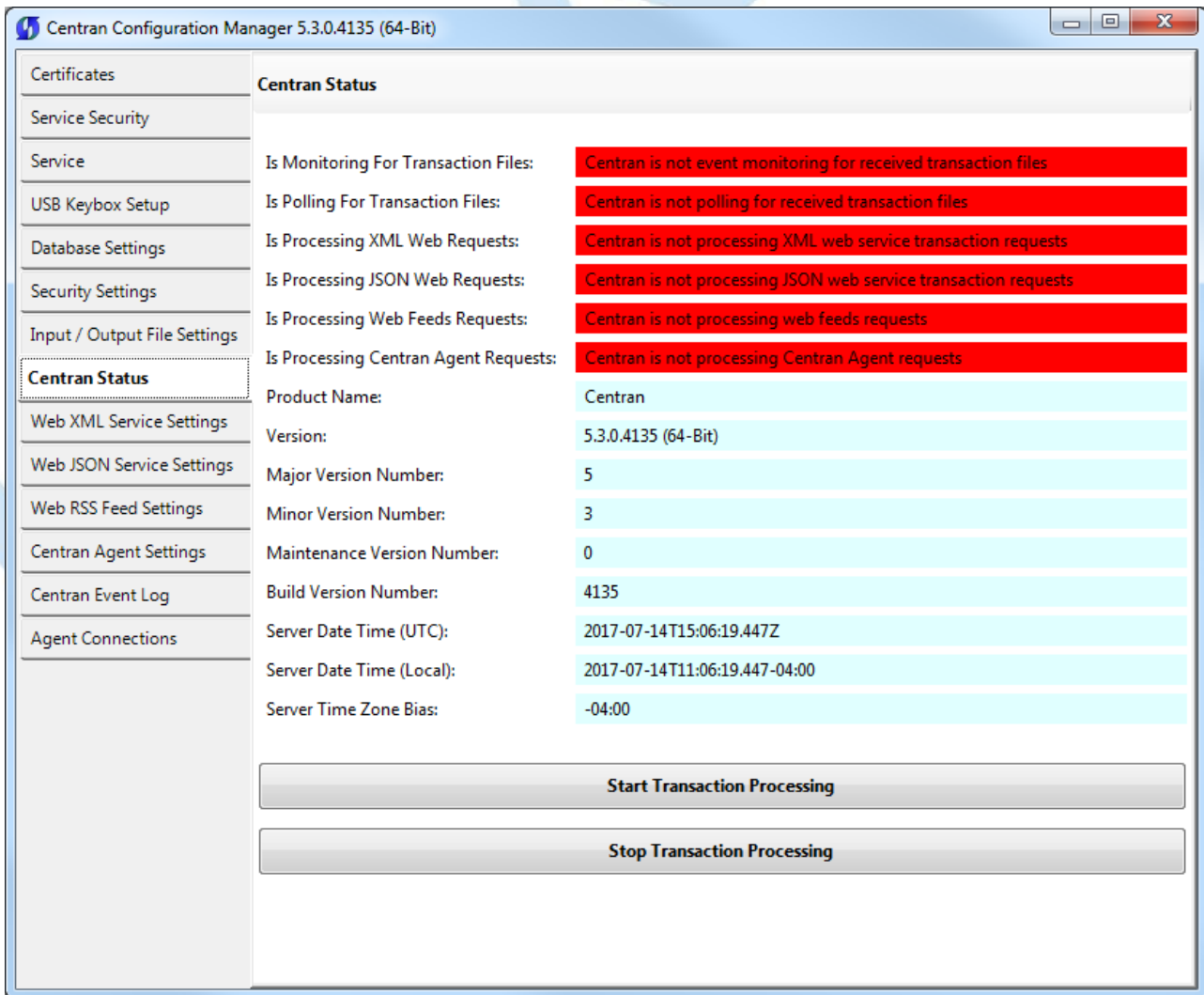


Start Transaction Processing

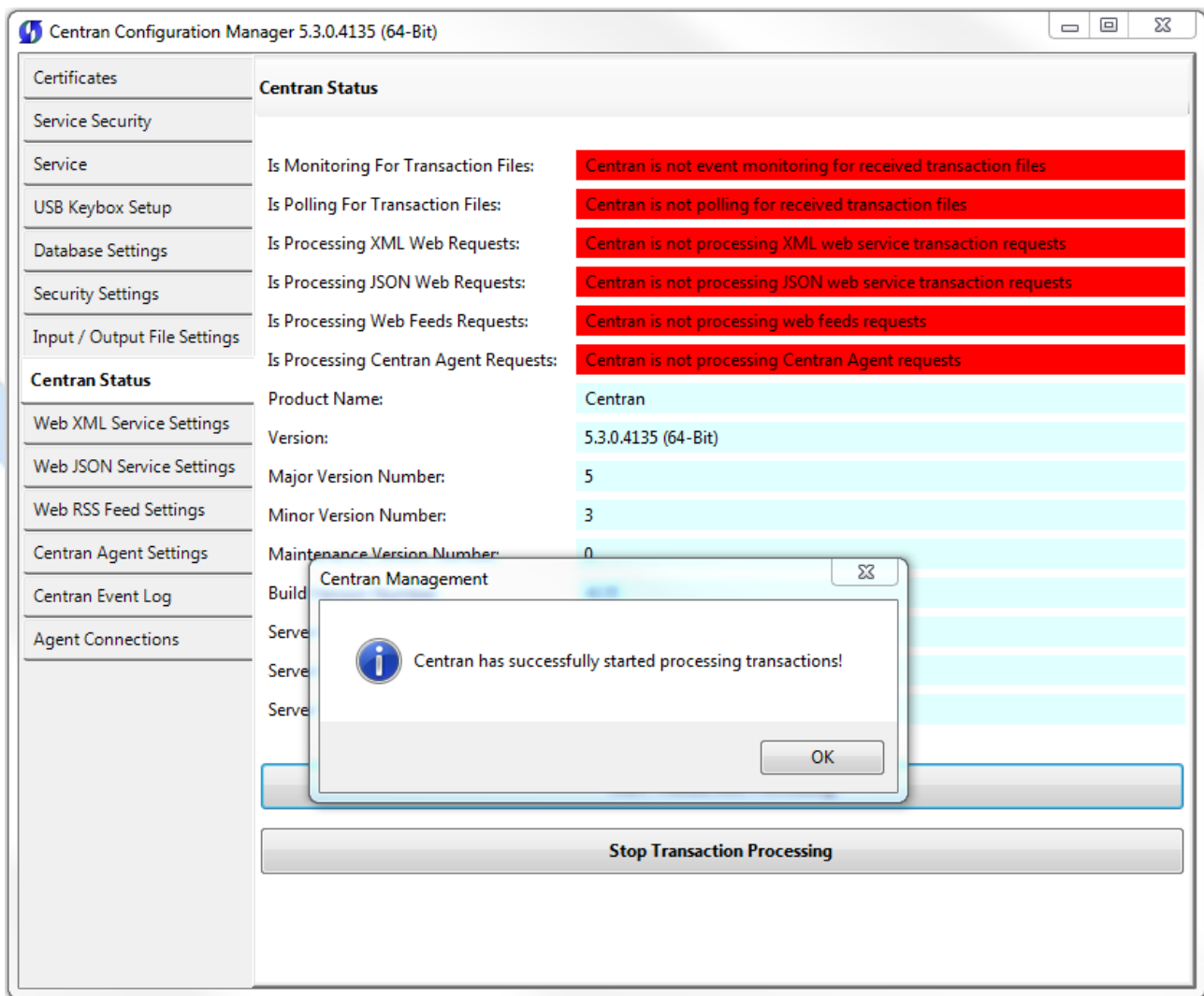
CenTran 5 Getting Started Guide

Click on the **CenTran Status** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

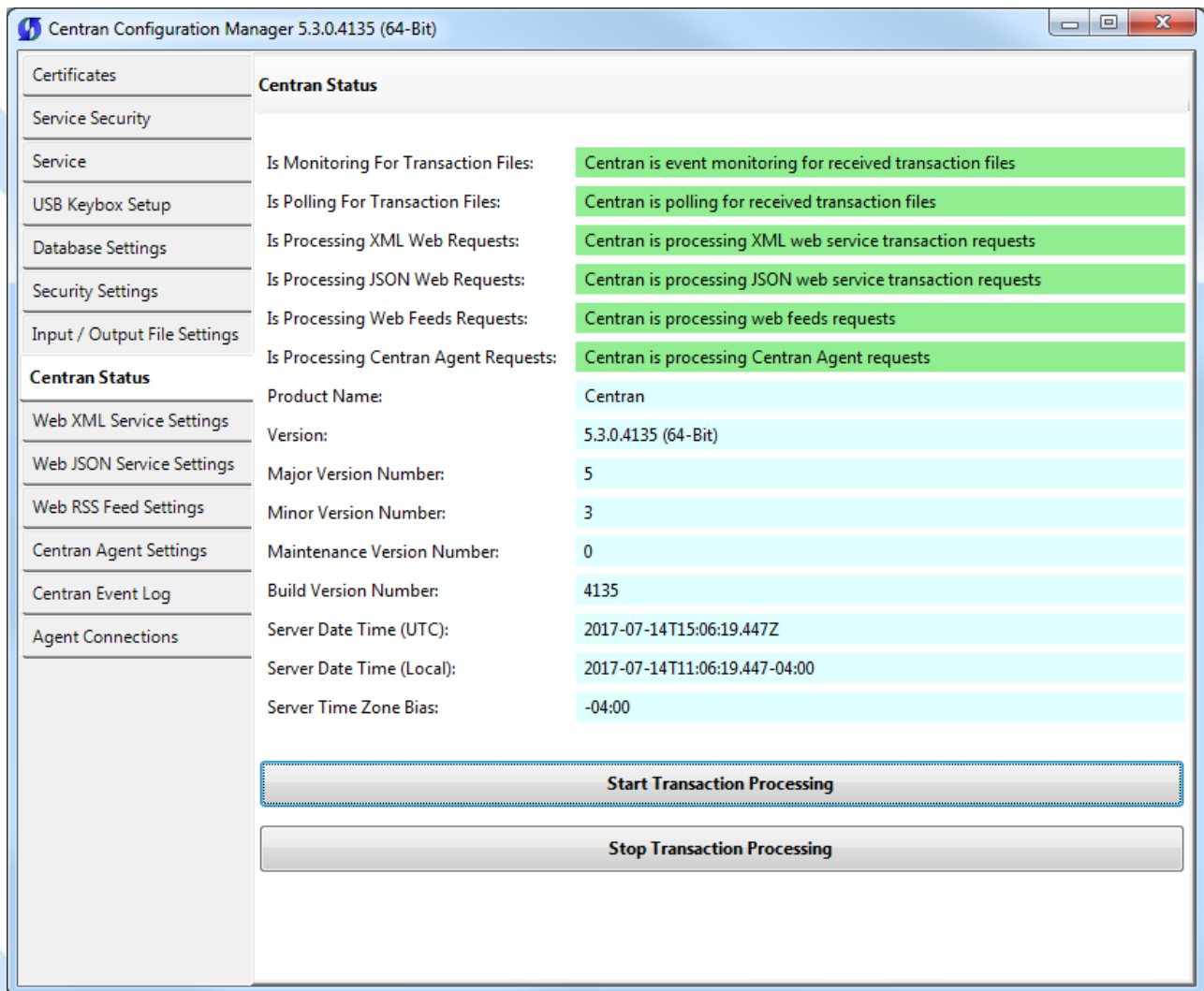


Click on the **Start Transaction Processing** button. You should see the following message dialog displayed:



Click on the message dialog **OK** button.

You should see the following tab page displayed by the CenTran Configuration Manager:



© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

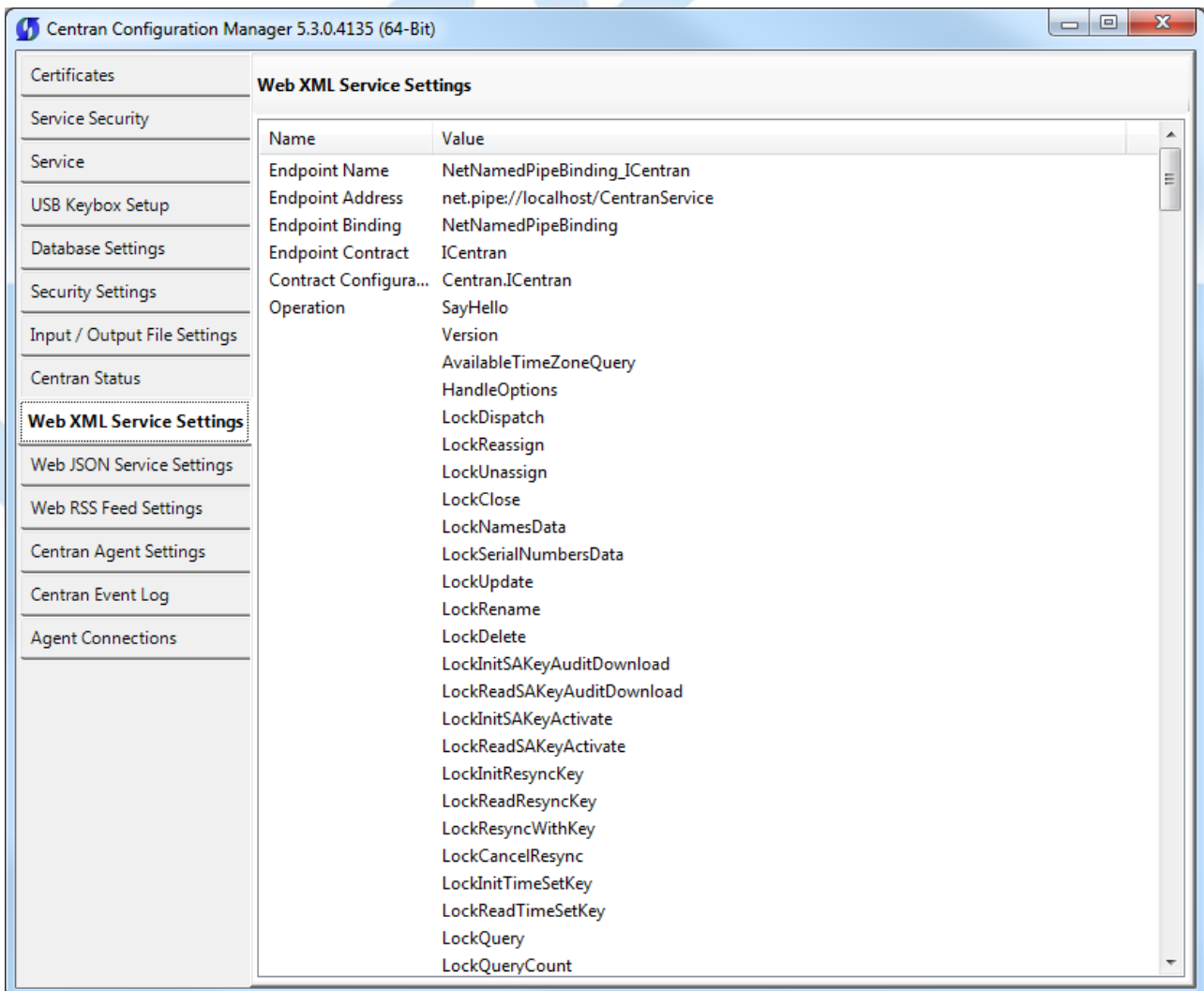
View Web Service XML Settings

CenTran 5 Getting Started Guide

The web service settings are configured in the **system.serviceModel** section of the CenTran service configuration file. The resultant web service based on the settings can be viewed while the CenTran service is processing transactions.

Click on the **Web XML Service Settings** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:



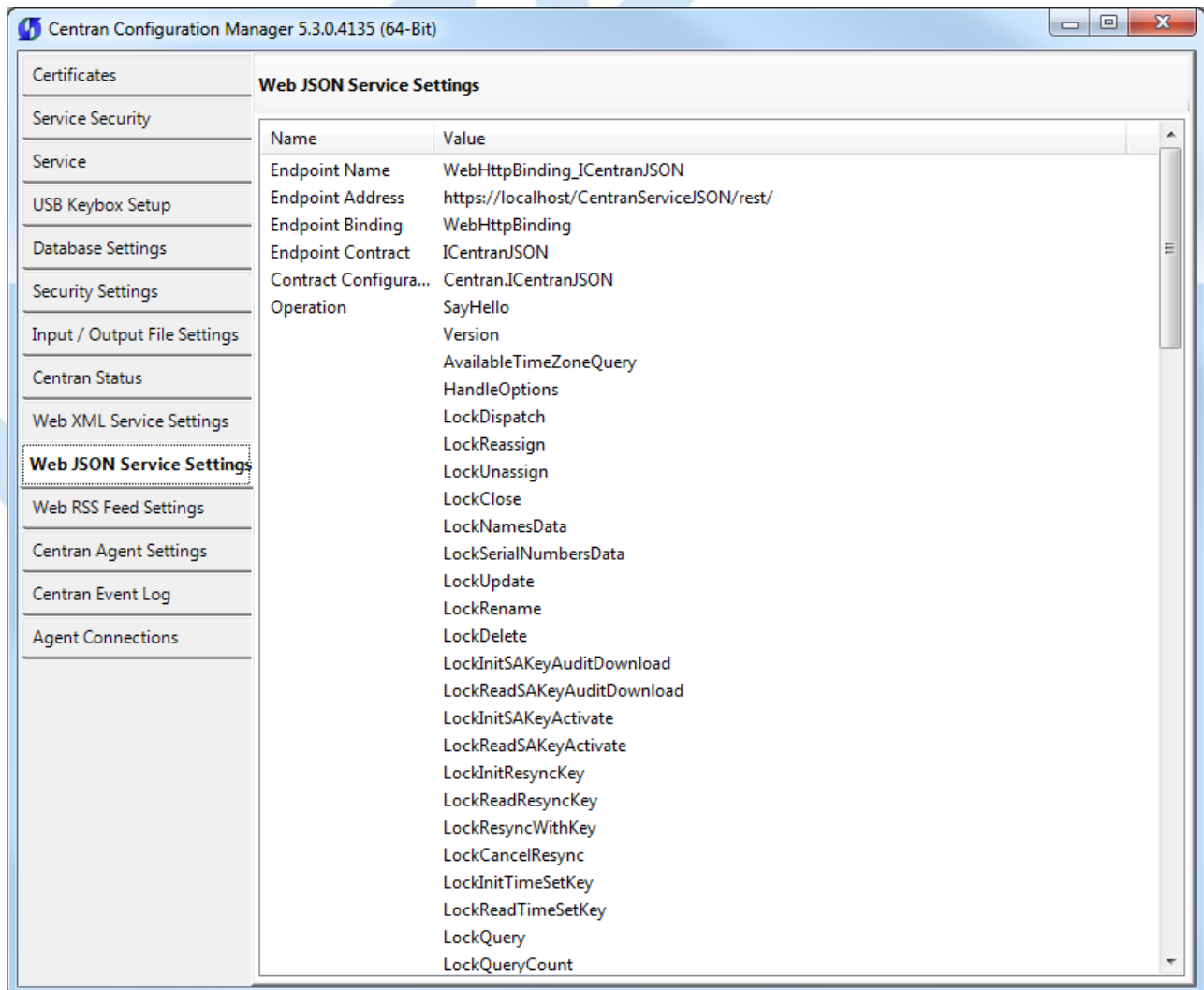
View Web Service JSON Settings

CenTran 5 Getting Started Guide

The web service settings are configured in the **system.serviceModel** section of the CenTran service configuration file. The resultant web service based on the settings can be viewed while the CenTran service is processing transactions.

Click on the **Web JSON Service Settings** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:



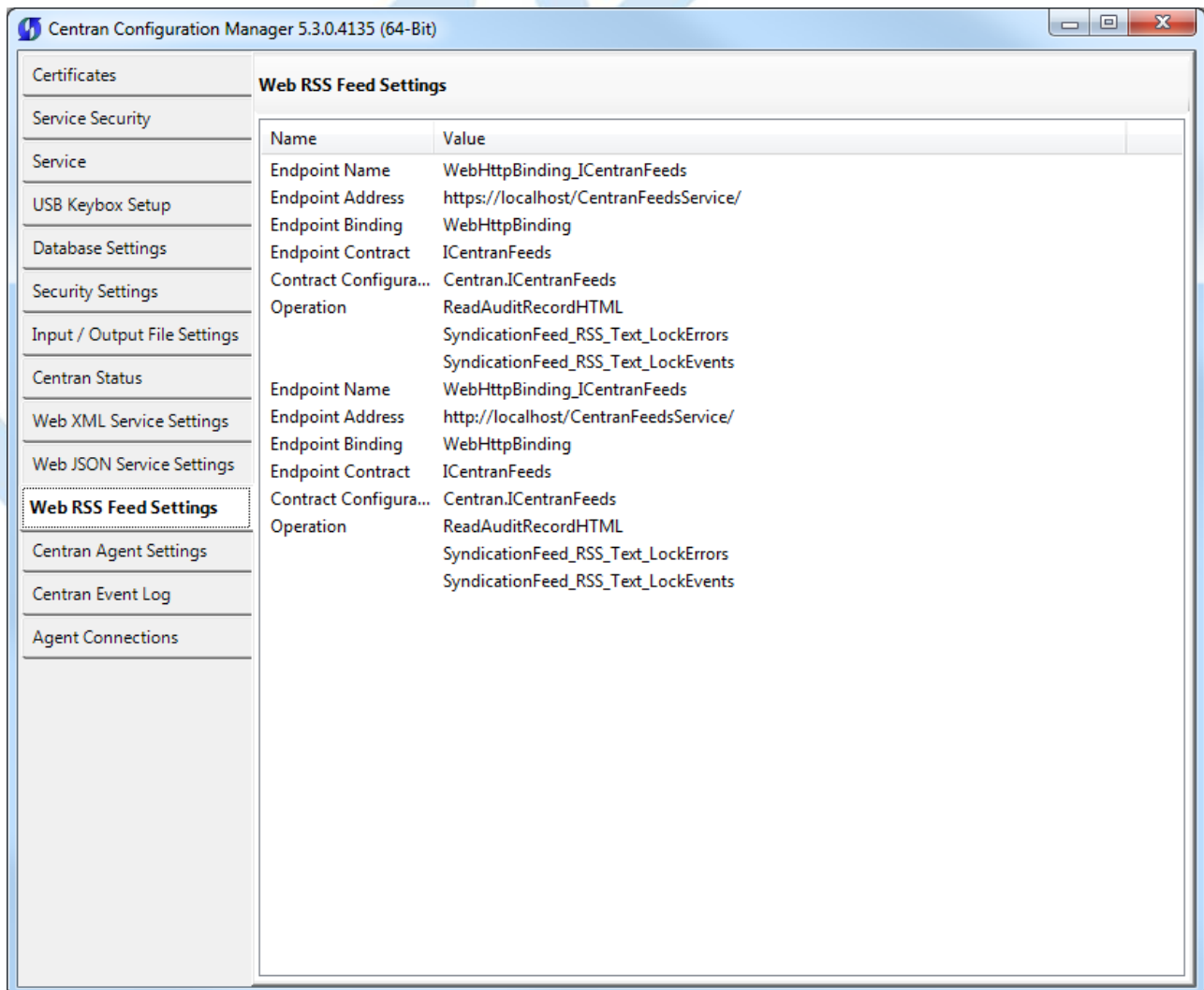
View Web RSS Feed Settings

CentTran 5 Getting Started Guide

The web rss feed settings are configured in the **system.serviceModel** section of the CentTran service configuration file. The resultant web rss feeds based on the settings can be viewed while the CentTran service is processing transactions.

Click on the **Web RSS Feed Settings** tab on the CentTran Configuration Manager:

You should see the following tab page displayed by the CentTran Configuration Manager:



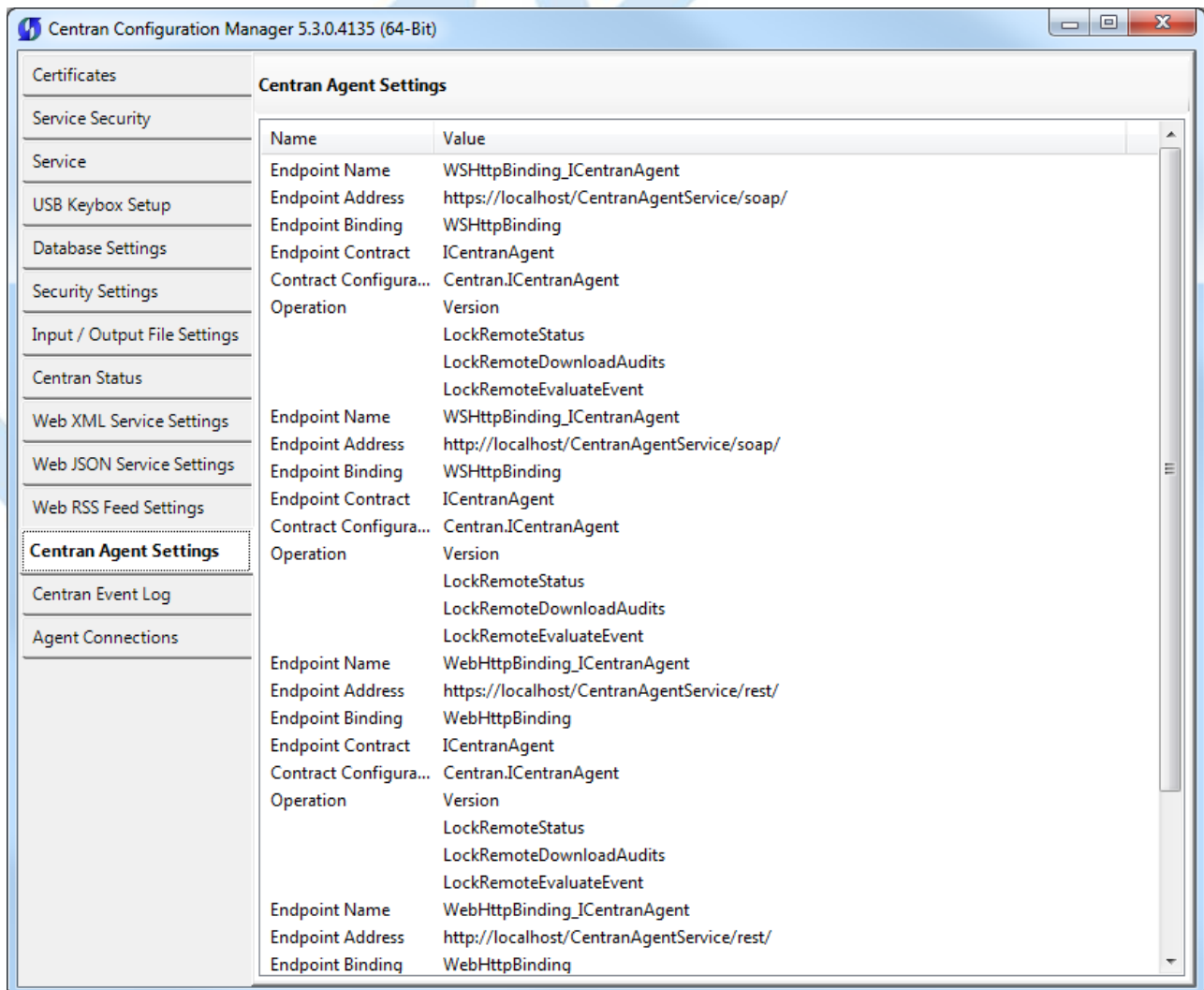
View CenTran Agent Settings

CenTran 5 Getting Started Guide

The CenTran Agent settings are configured in the **system.serviceModel** section of the CenTran service configuration file. The resultant web service based on the settings can be viewed while the CenTran service is processing transactions.

Click on the **CenTran Agent Settings** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

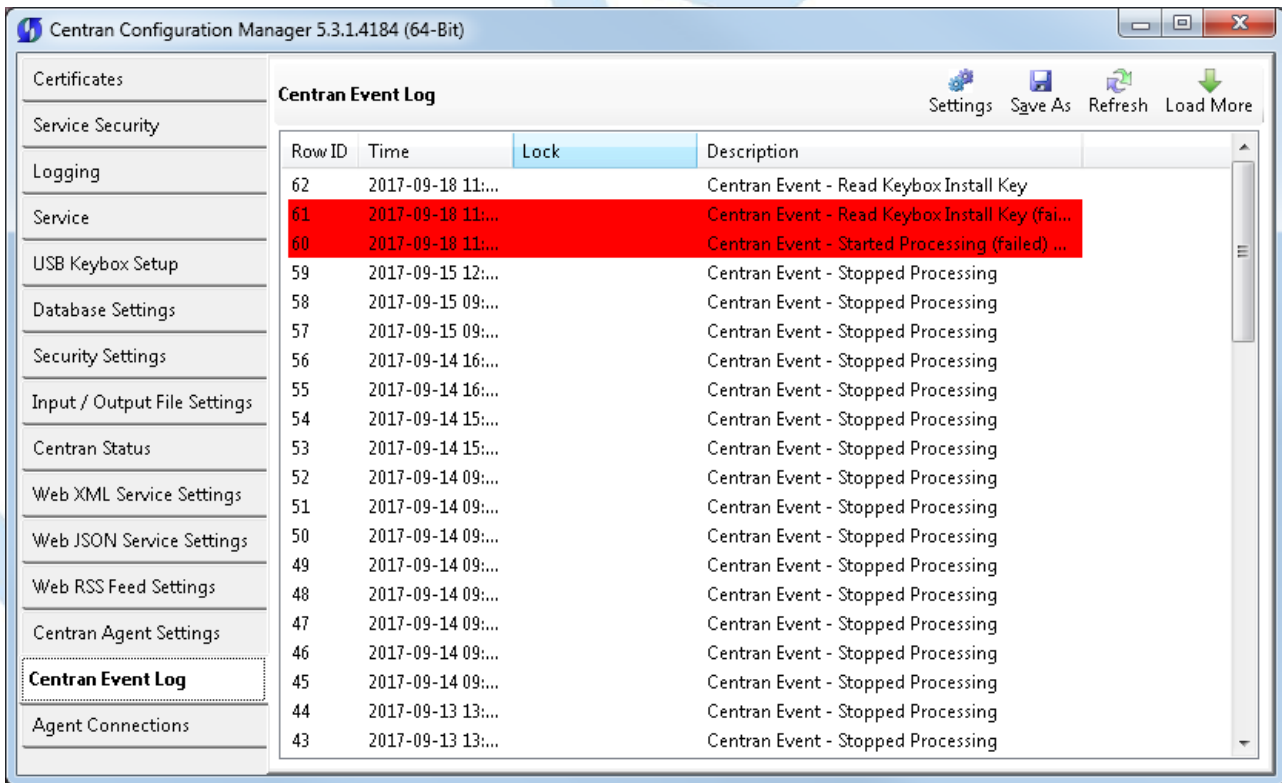


View Event Log

CentTran 5 Getting Started Guide

Click on the **CentTran Event Log** tab on the CentTran Configuration Manager:

You should see the following tab page displayed by the CentTran Configuration Manager:



The CentTran Management interface loads event log audits 100 at a time. To load additional audits for viewing, click on the **Load More** button.

You can also save the CentTran event log to an HTML file. Click on the **Save As** button to save the event log. This will display a save file dialog to allow you to choose the file to save to. The entire event log will be saved to the file.

The CentTran event log is limited in size based on the settings you made in the CentTran service configuration file. Once the event log reaches the limit you set, it will delete the oldest audits to remain within the limit when new audits are added. This occurs based off of the granularity you set in the configuration file. The event log will be allowed to grow slightly larger than the set limit based off of the granularity size used to regulate how often the check is made. Click on the **Settings** button to change these settings.

See [Setup CentTran Event Logging](#) for information on changing these settings.

Additional information is available in the CentTran event log registered with the operating system. Service start and stop events are recorded there. Additionally, if internal errors occur within CentTran, the description of the error is recorded there also. This can be accessed by opening the administrative tools section of the control panel for your computer. Under that is an item labeled **Event Viewer**. Open the **Event Viewer**, and you will see a CentTran event log under the application and services event logs section.

Also, additional information is available in the Windows Communication Foundation (WCF) diagnostic output set up from the CentTran configuration file. The default settings from the CentTran configuration file creates a diagnostic output file for Windows Communication Foundation (WCF) events, named **WcfServiceTrace.svclog**. This file will be created within the application directory the CentTran service is installed to. This file can be viewed using the Microsoft Service Trace Viewer (SvcTraceViewer.exe). Double clicking on the file will automatically open the file under the Microsoft Service Trace Viewer.

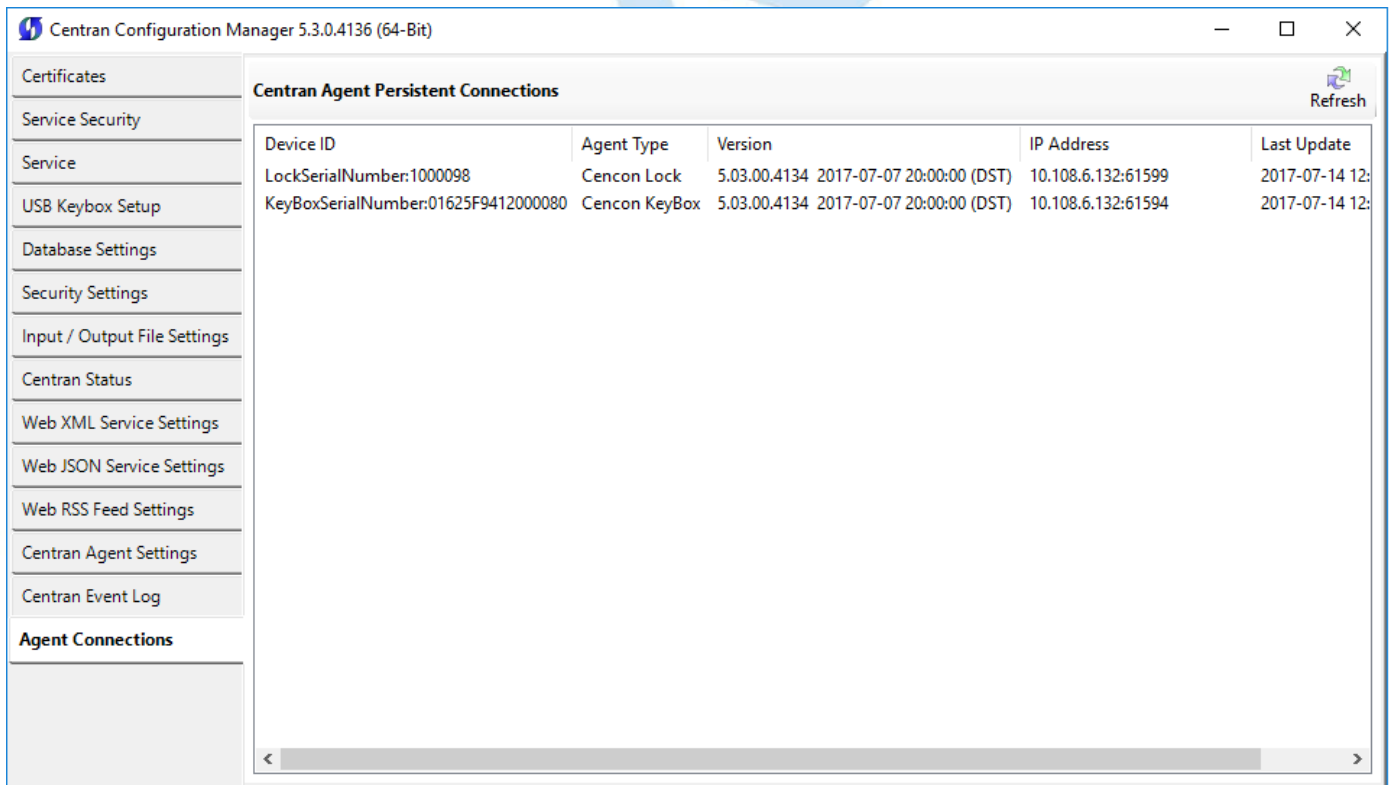
The Microsoft Service Trace Viewer is available as a free download within the Windows Platform SDK.

View CenTran Agent Persistent Connections

CenTran 5 Getting Started Guide

Click on the **Agent Connections** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:



Centran Agent Persistent Connections							Refresh
Device ID	Agent Type	Version			IP Address	Last Update	
LockSerialNumber:1000098	Cencon Lock	5.03.00.4134	2017-07-07 20:00:00 (DST)		10.108.6.132:61599	2017-07-14 12:	
KeyBoxSerialNumber:01625F9412000080	Cencon KeyBox	5.03.00.4134	2017-07-07 20:00:00 (DST)		10.108.6.132:61594	2017-07-14 12:	

The CenTran agents use persistent connections from each agent to CenTran to avoid issues with network firewalls. Connections from client systems to a server are generally permitted by firewalls, however connections initiated from outside the firewall are denied. To allow CenTran to do network operations with an agent service, the agent services set up persistent connections that are identified by the lock or keybox. CenTran can be commanded to do an operation with a lock or keybox using these identifiers.

If you are not running any firewalls between your client systems (either ATMs or Host PCs) and CenTran, then the CenTran address does not have to be configured with the client system agent services. In this case, the agent services will default to using a direct network address for operations.

© 1996-2017 dormakaba

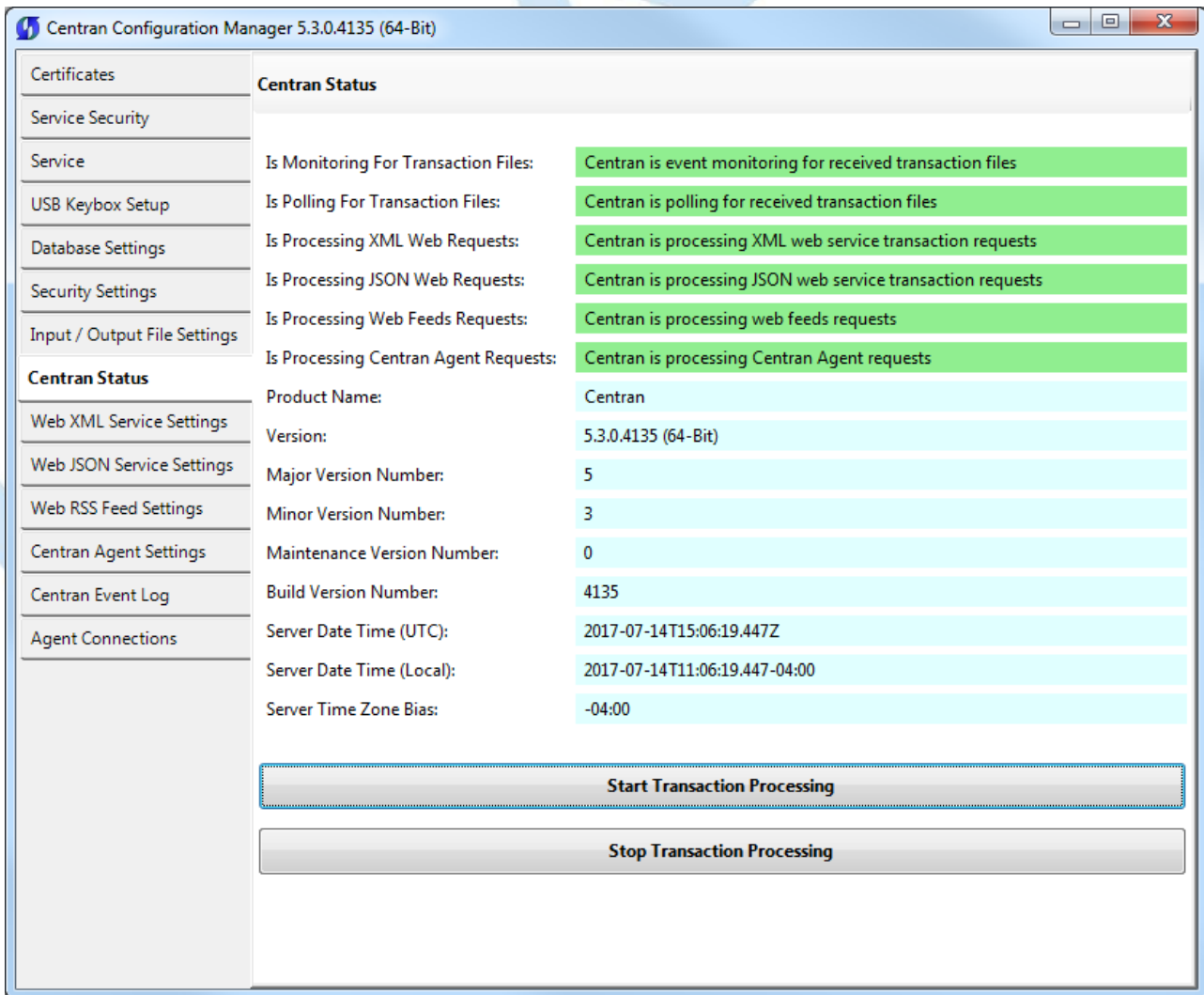
Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Stop Transaction Processing

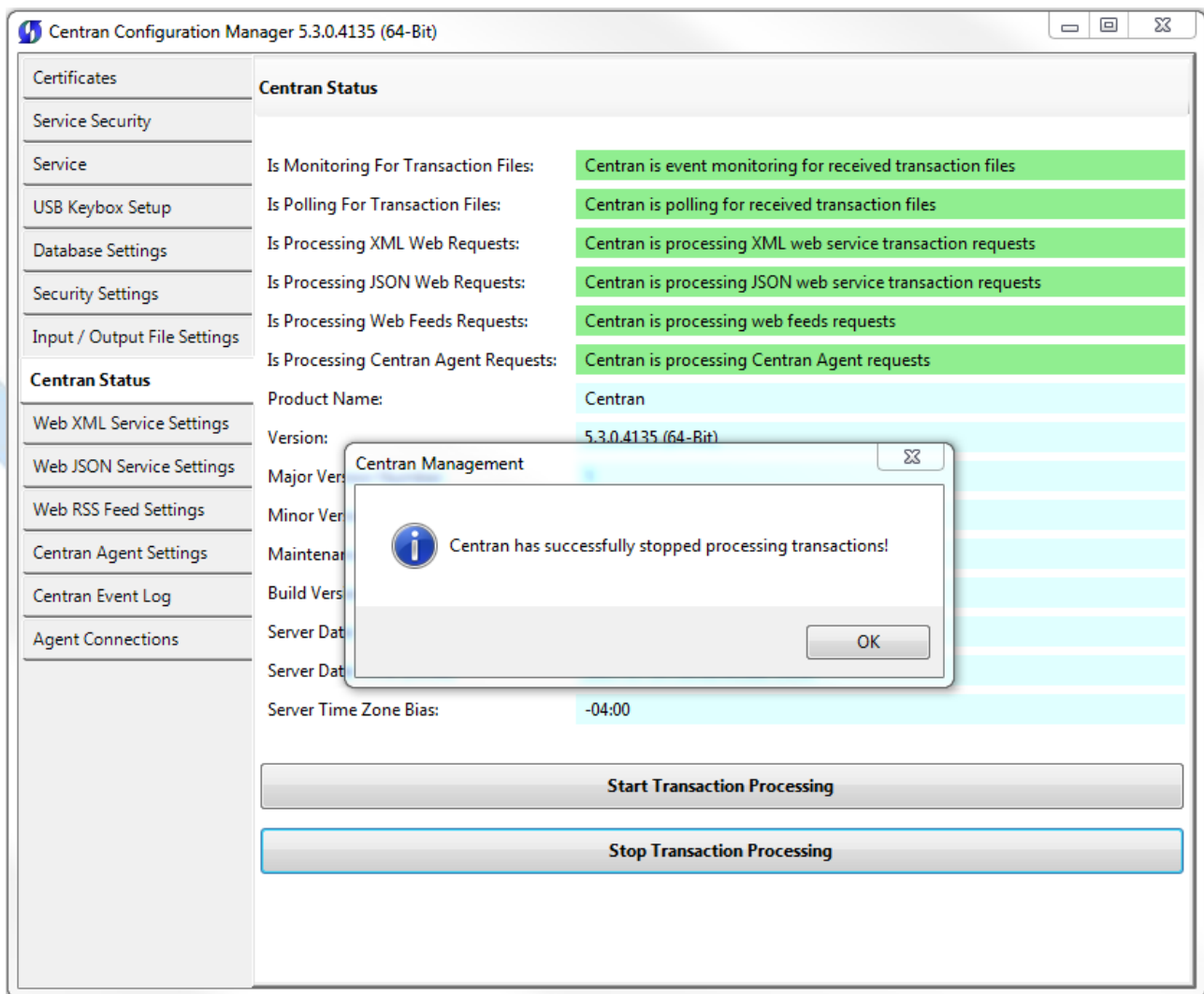
CenTran 5 Getting Started Guide

Click on the **CenTran Status** tab on the CenTran Configuration Manager:

You should see the following tab page displayed by the CenTran Configuration Manager:

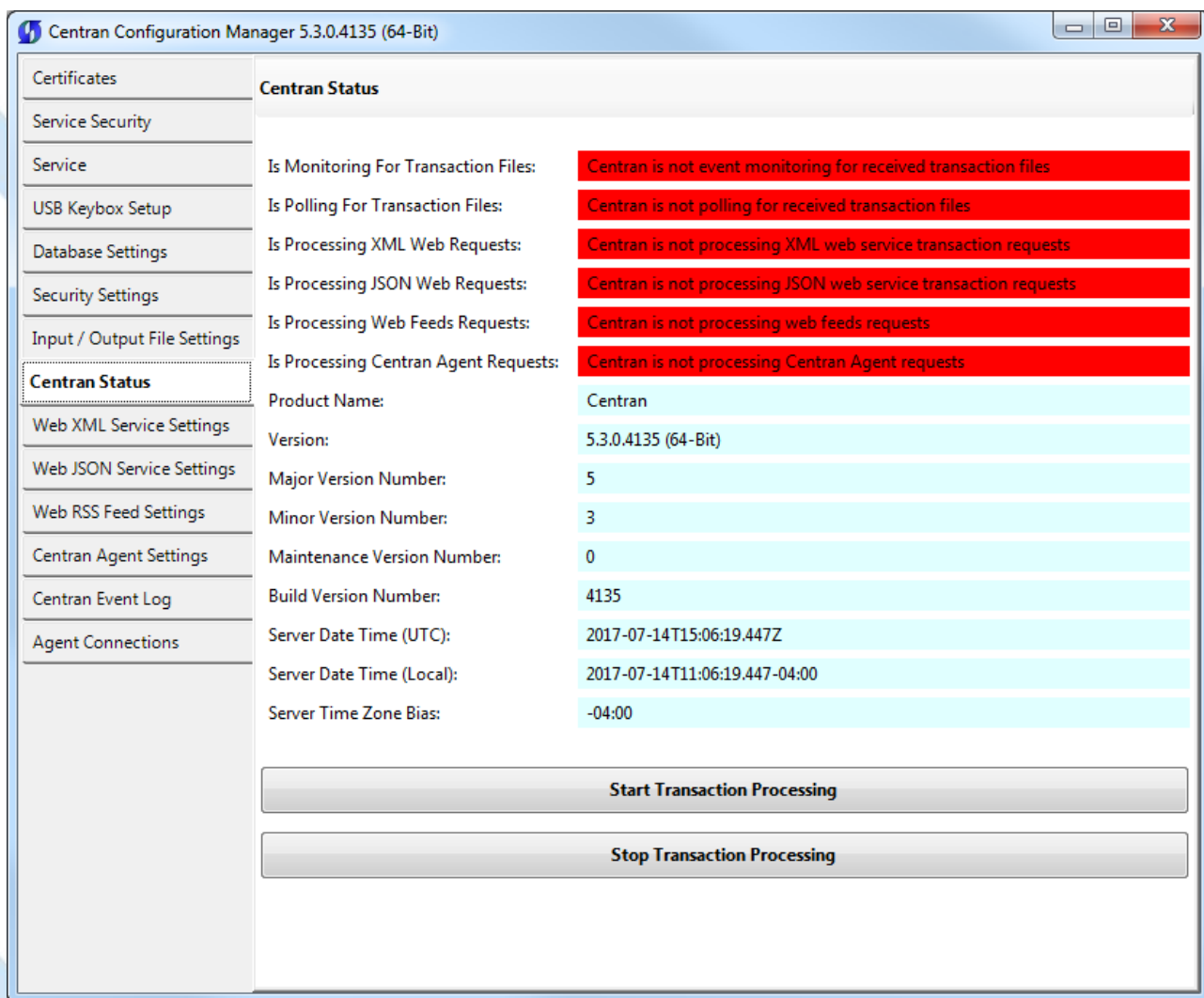


Click on the **Stop Transaction Processing** button. You should see the following message dialog displayed:



Click on the message dialog **OK** button.

You should see the following tab page displayed by the CenTran Configuration Manager:



© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Configure the CenTran Service using Web Management Interface

CenTran 5 Getting Started Guide

The web browser CenTran Management interface supports remotely managing a running CenTran service. To manage a running CenTran service, you must have already set up the appropriate CenTran configuration file settings and certificates. You must have also installed and started the CenTran service.

Managing the CenTran service:

The following sections describe setting up and managing the CenTran service using the web browser CenTran Management interface:

- [Log on to CenTran Management](#)
- [Setup Keybox](#)
- [Select ODBC Database Connection](#)
- [Set Company Number](#)
- [Set File Settings](#)
- [Start Transaction Processing](#)
- [View Web Service XML Settings](#)
- [View Web Service JSON Settings](#)
- [View Web RSS Feed Settings](#)
- [View CenTran Agent Settings](#)
- [View CenTran Event Log](#)
- [View CenTran Agent Persistent Connections](#)
- [Stop Transaction Processing](#)

© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Log on to CenTran Management

CenTran 5 Getting Started Guide

Note: To access the CenTran Management interface in a web browser, the CenTran service must be installed and started.

Your web browser must support HTML5 and CSS3. This includes the following browsers:

1. Internet Explorer 9 or higher
2. Firefox 10 or higher
3. Google Chrome 16 or higher
4. Apple Safari 5 or higher

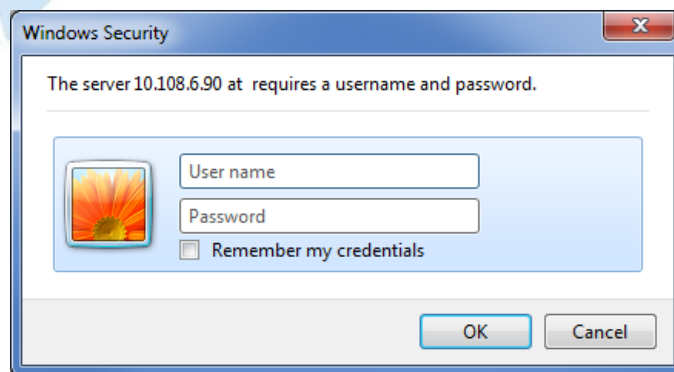
If you are using Internet Explorer, you must have compatibility mode for intranet sites turned off under the Tools menu. Press Alt-T to open the tools menu in Internet Explorer to get to this setting.

The URL of the CenTran web management interface is of the form:

`https://centran_host_server_name/CenTranManagement/index.htm`

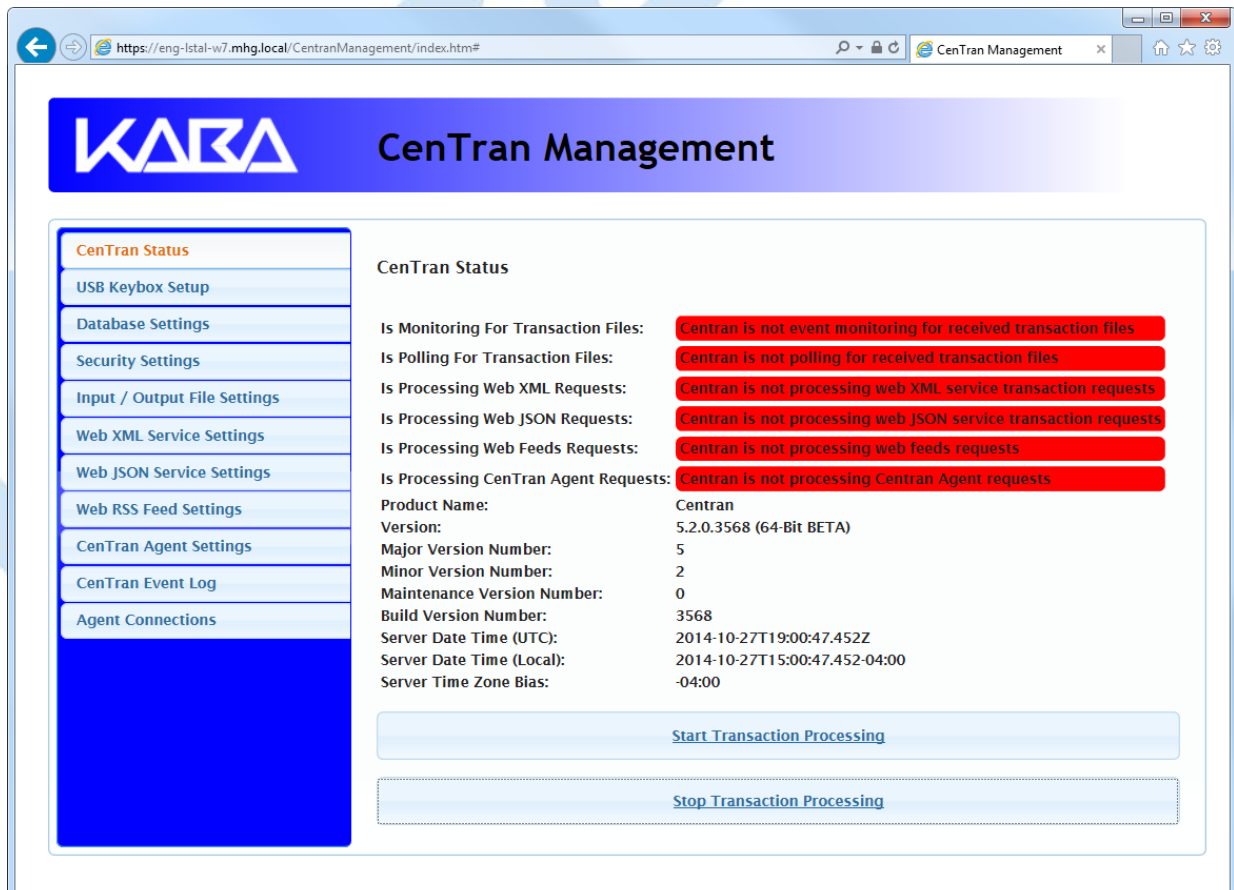
You will need to replace the `centran_host_server_name` in the URL with the name you gave the CenTran Web Service Certificate you created earlier.

Open the URL in your preferred web browser, and you should see a dialog similar to the following:



Enter the user name and password specified in the [CenTran Management Web Access](#) section of the Service Security tab in the CenTran Configuration Manager and select **OK**. The default user name is **admin**. The default password is **password**.

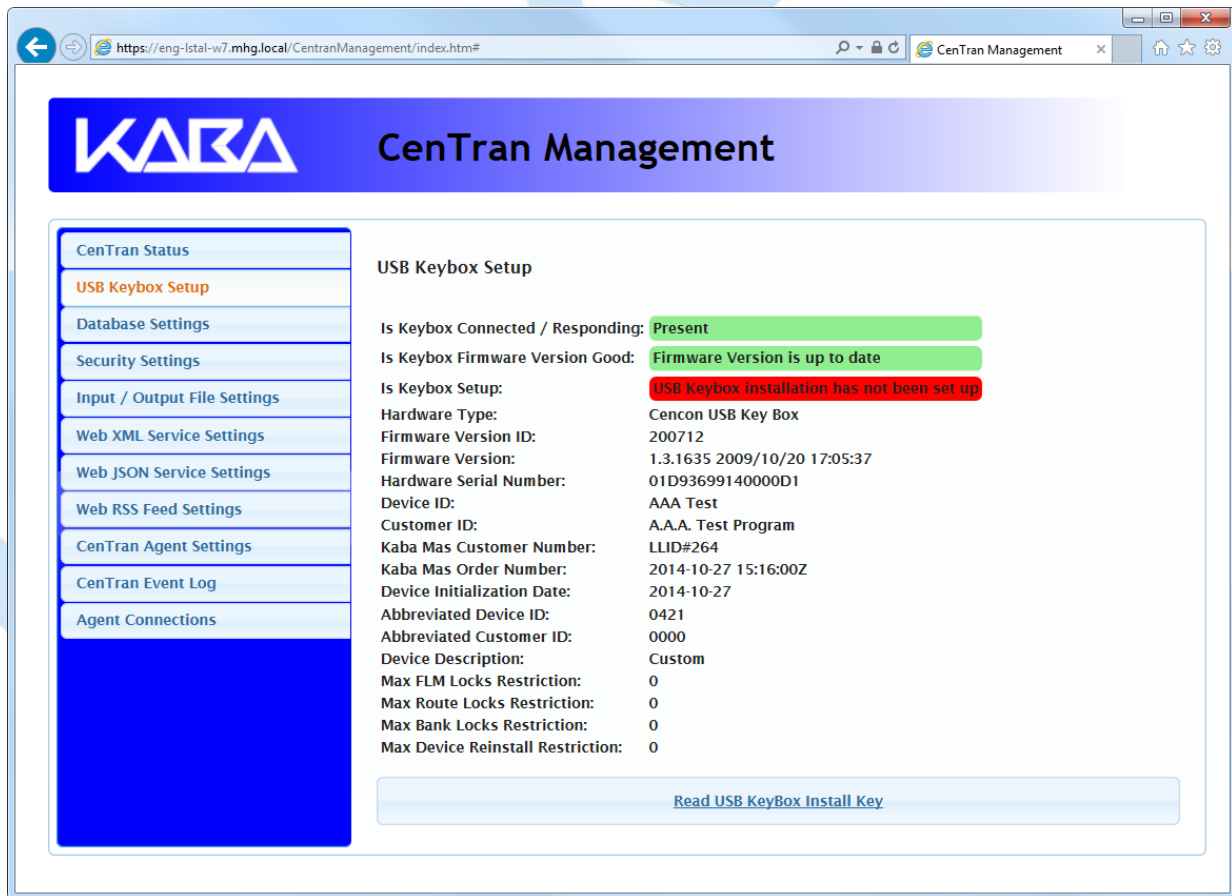
You should see the following in your web browser:



Setup Keybox

CenTran 5 Getting Started Guide

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **USB Keybox Setup** tab on the left side:
You should see the following in your web browser:

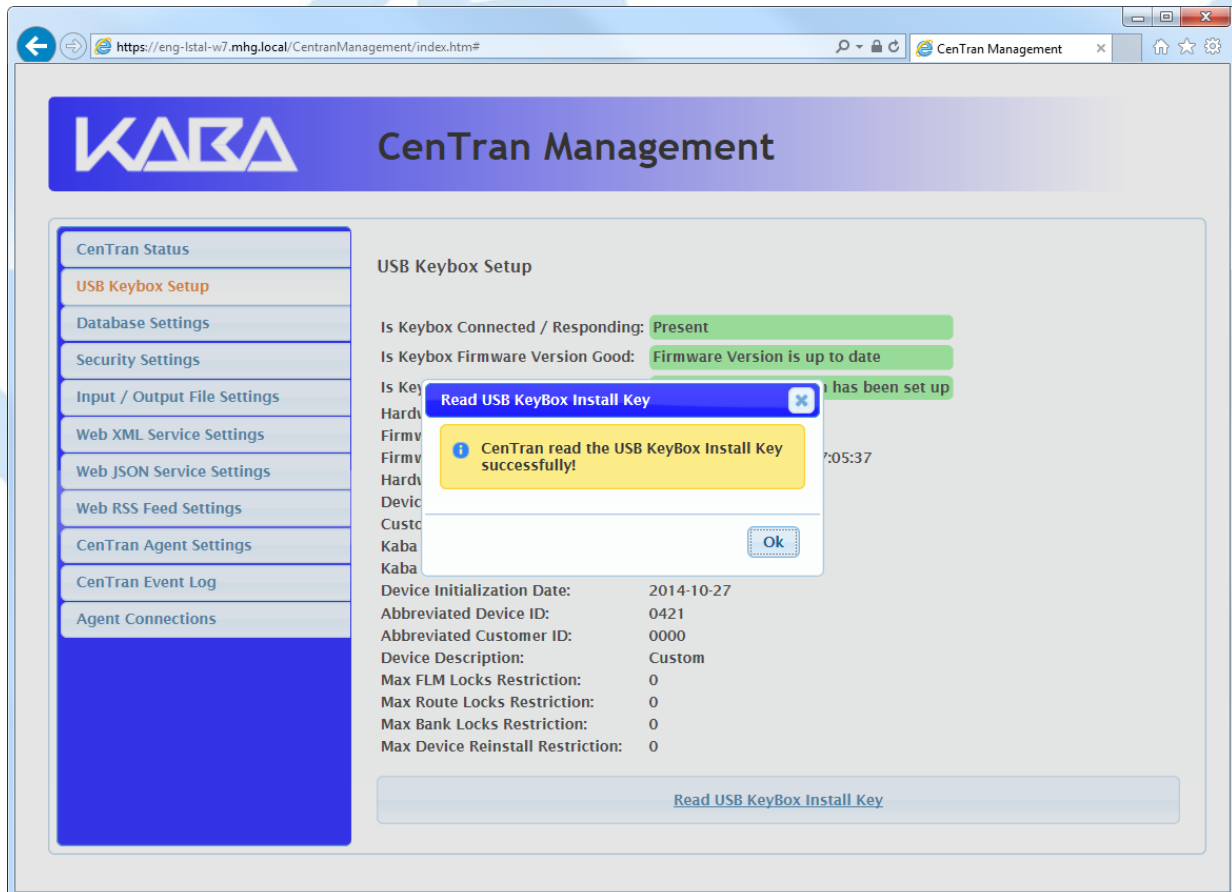


Place your Keybox install key in the first port of the keybox: (This will be the port farthest away from the USB connection.)



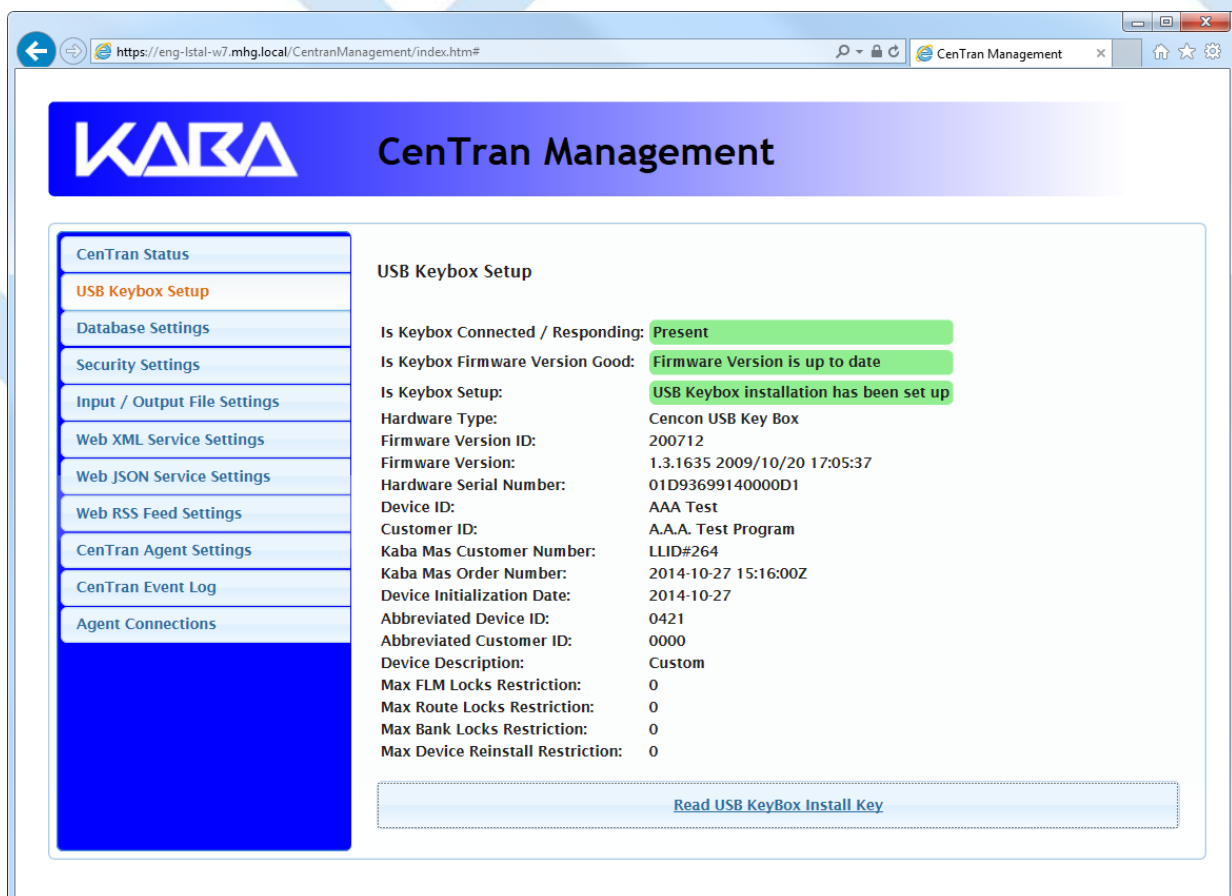
Click on the **Read USB Keybox Install Key** button on the **USB Keybox Setup** web page.

You should see the following in your web browser:



Click on the **OK** button on message box.

You should see the following in your web browser:



Select ODBC Database Connection

CenTran 5 Getting Started Guide

Important Note

CenTran no longer runs under the permissions of the logged on user. It has been changed to run as a background service on the host server you install it on, and is independent of who is logged on. The CenTran service will run in the background even if no one is logged onto the host server.

By default, the CenTran service runs logged on under a **Local System** account. This gives it access to resources and settings on the host server you install it on. However, the **Local System** account only has access to the host server, not to resources on your network.

If the CenTran service is configured to run logged onto the default **Local System** account, you will need to use SQL authentication for CenTran to access the SQL Server database.

If the CenTran service is configured to run logged onto an account configured for it on your network domain, then that account must have administrative privileges on the host server CenTran is on.

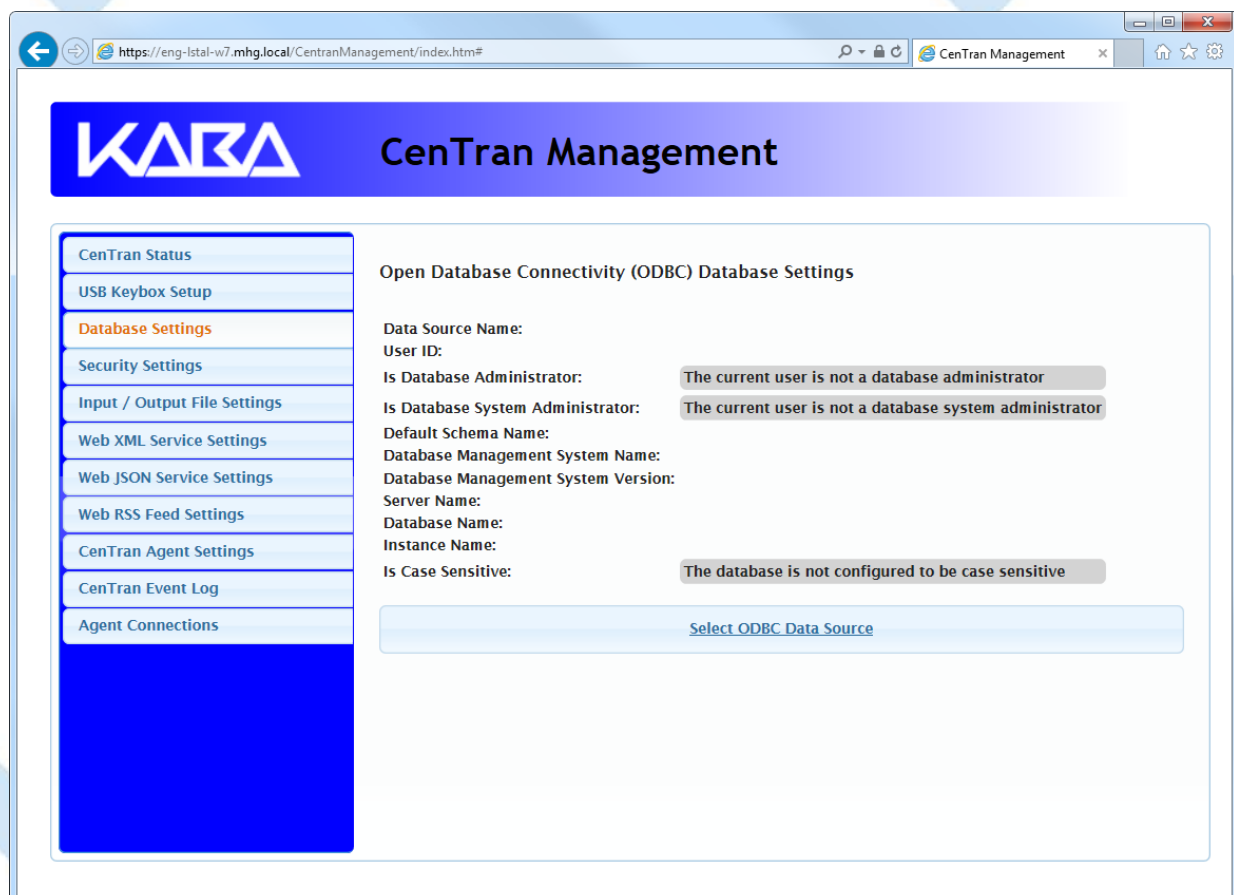
If you use Windows authentication for CenTran's database authentication, then the account CenTran is logged onto must be a network domain account and have authorization to access the SQL Server database.

You can view and edit the CenTran service settings from the Microsoft Management Console:

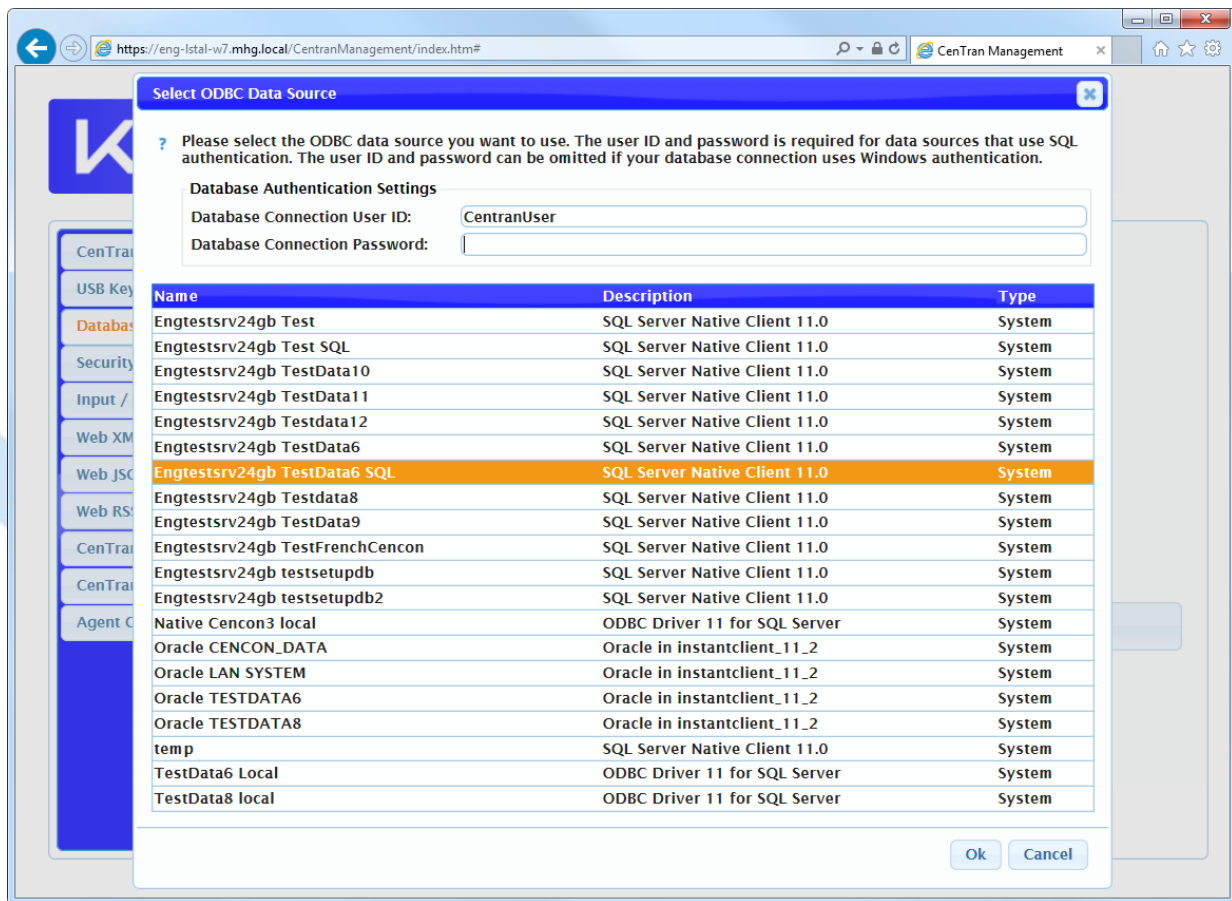
- Open the Start Menu.
- Right click on **Computer**.
- Select **Manage** from the displayed context menu. You must have administrative privileges.
- The **Computer Management** console will be displayed. Expand the **Services and Applications** section on the left side.
- Select **Services** from the **Services and Applications** section.
- Locate **CenTran** from the list of services. Right click on **CenTran** and select **Properties** from the context menu.
- A service **Properties** dialog will be displayed. Select the **Log On** tab to examine the account the service is set up to log on as.

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Database Settings** tab on the left side:

You should see the following in your web browser:

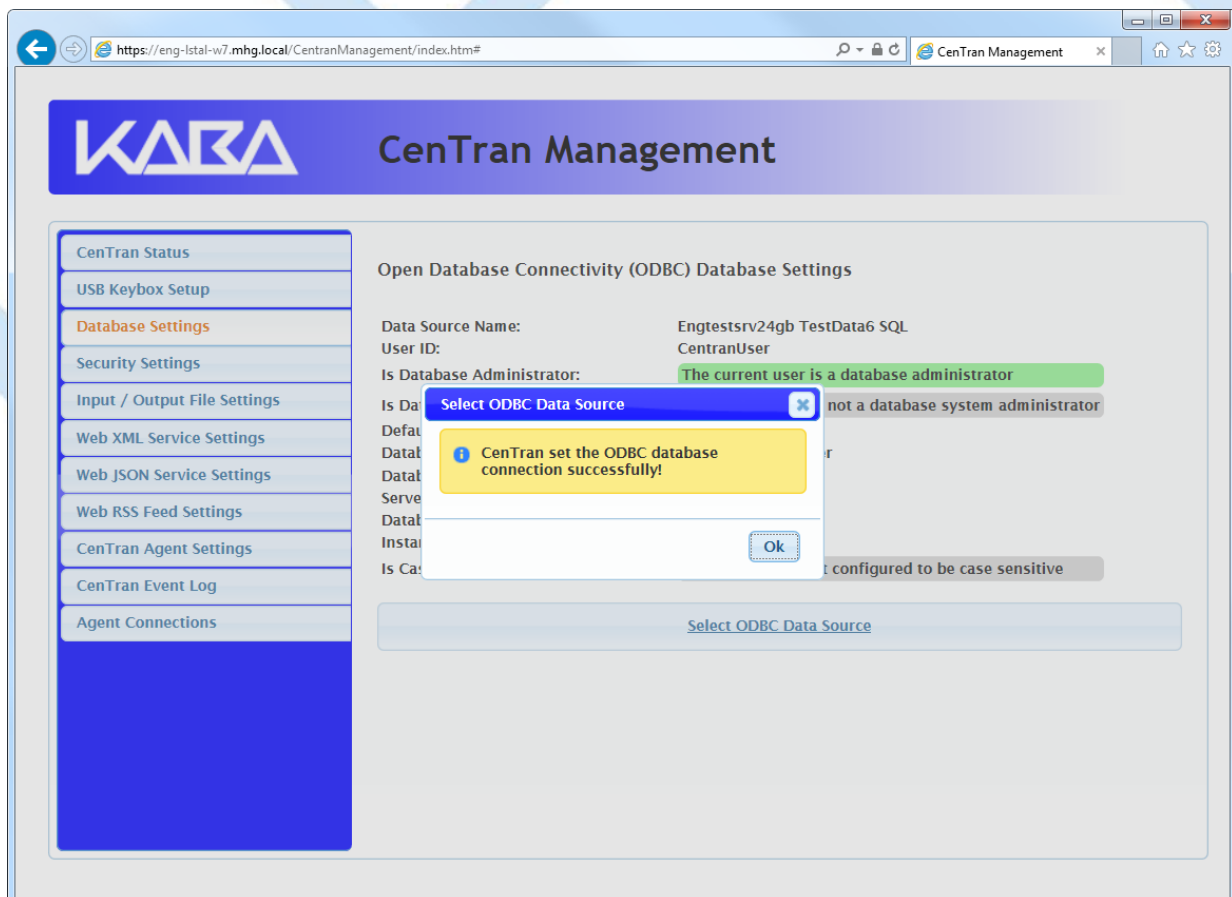


Click on the **Select ODBC Data Source** button. You should see the following dialog displayed:



Select the ODBC database connection you want to use. If you are using SQL authentication, you will also need to enter a user name and password for the CentTran service to use with the database connection.

You should see the following in your web browser:



Click on the **OK** button on message box.

You should see the following in your web browser:

[←](#)
[↻](#)
<https://eng-istal-w7.mhg.local/CenTranManagement/index.htm#>

CenTran Management

✕

🏠

★

⚙️



CenTran Management

CenTran Status

USB Keybox Setup

Database Settings

Security Settings

Input / Output File Settings

Web XML Service Settings

Web JSON Service Settings

Web RSS Feed Settings

CenTran Agent Settings

CenTran Event Log

Agent Connections

Open Database Connectivity (ODBC) Database Settings

Data Source Name:

Engtestsrv24gb TestData6 SQL

User ID:

CentranUser

Is Database Administrator:

The current user is a database administrator

Is Database System Administrator:

The current user is not a database system administrator

Default Schema Name:

dbo

Database Management System Name:

Microsoft SQL Server

Database Management System Version:

10.50.2550

Server Name:

ENGTESTSRV24GB

Database Name:

TestData6

Instance Name:

MSSQLSERVER

Is Case Sensitive:

The database is not configured to be case sensitive

Select ODBC Data Source

© 1996-2017 dormakaba

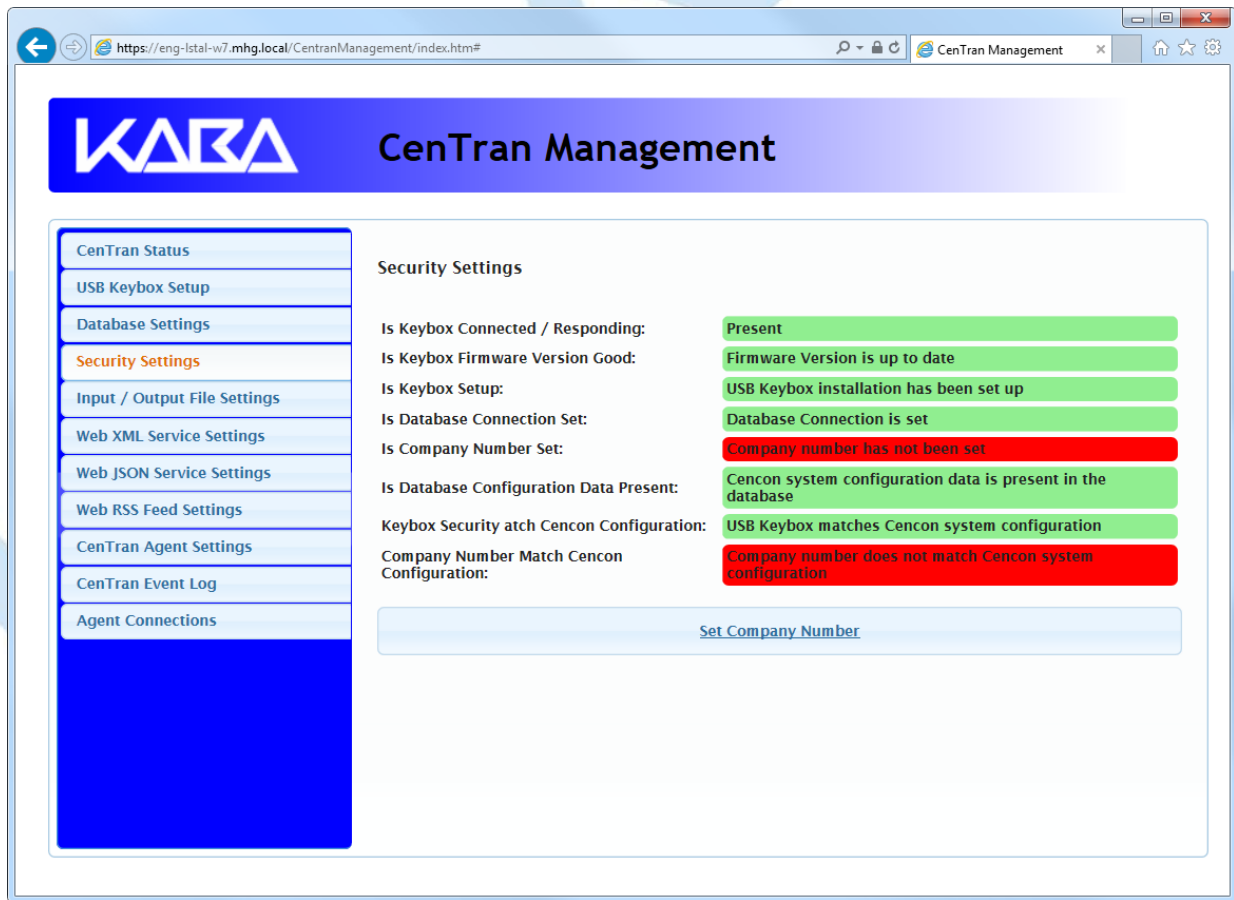
Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Page 93 of 118

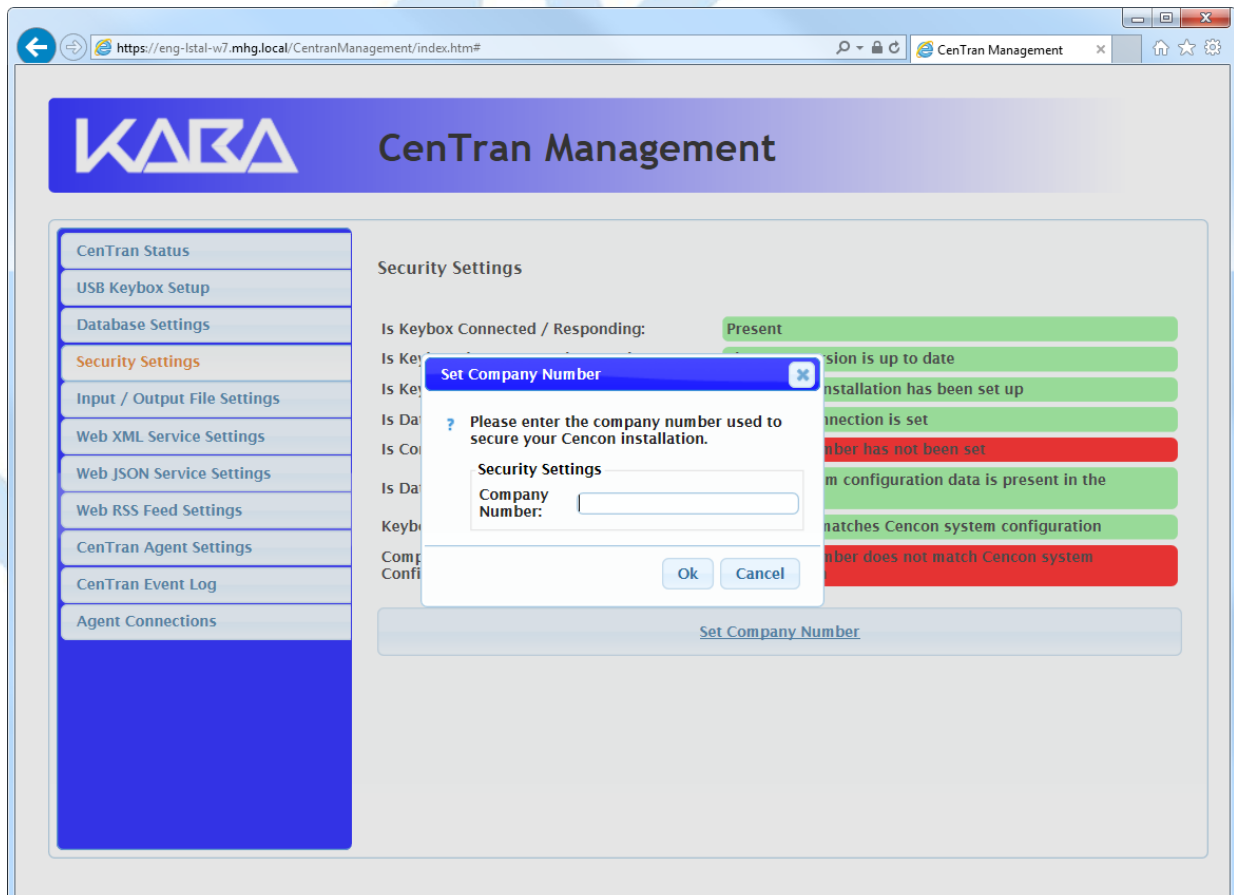
Set Company Number

CenTran 5 Getting Started Guide

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Security Settings** tab on the left side:
You should see the following in your web browser:

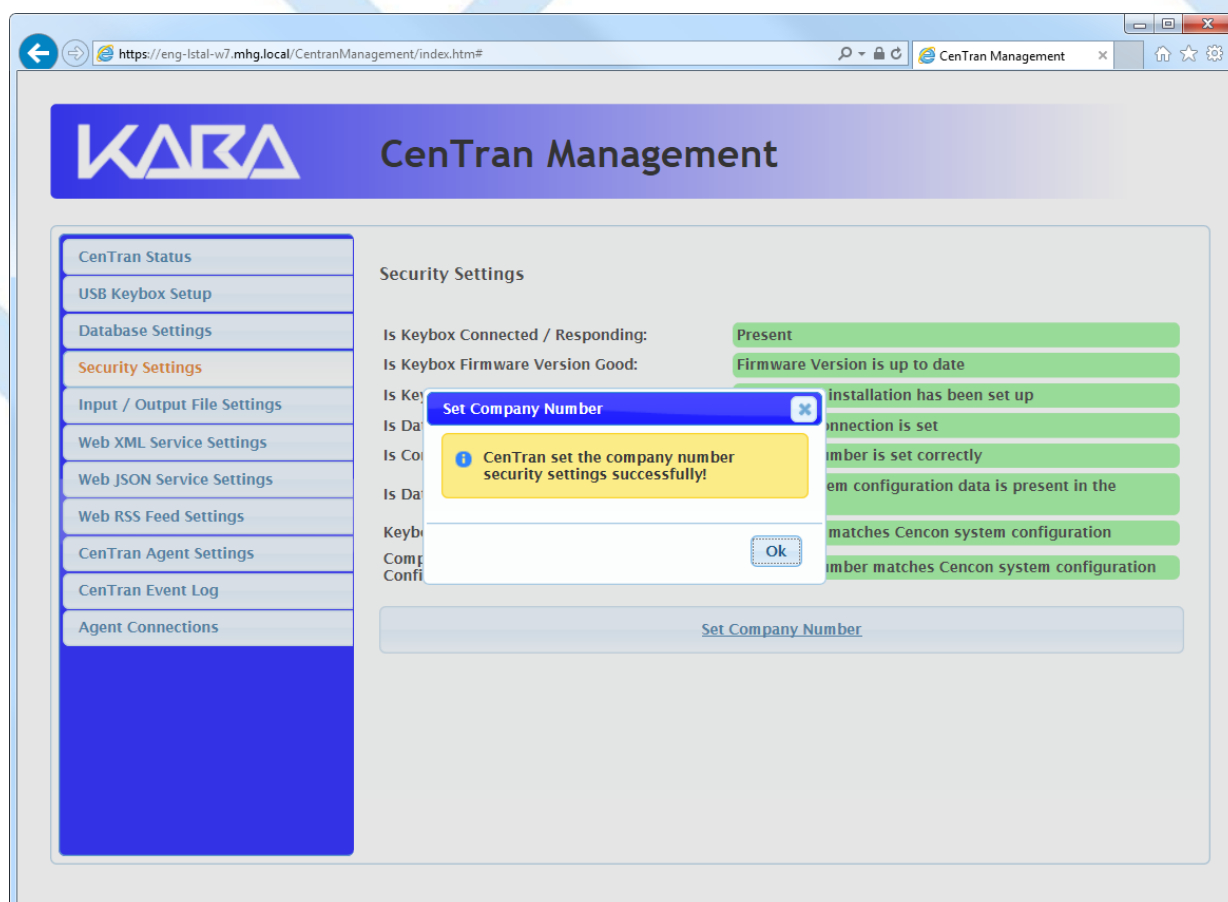


Click on the **Set Company Number** button. You should see the following dialog displayed:



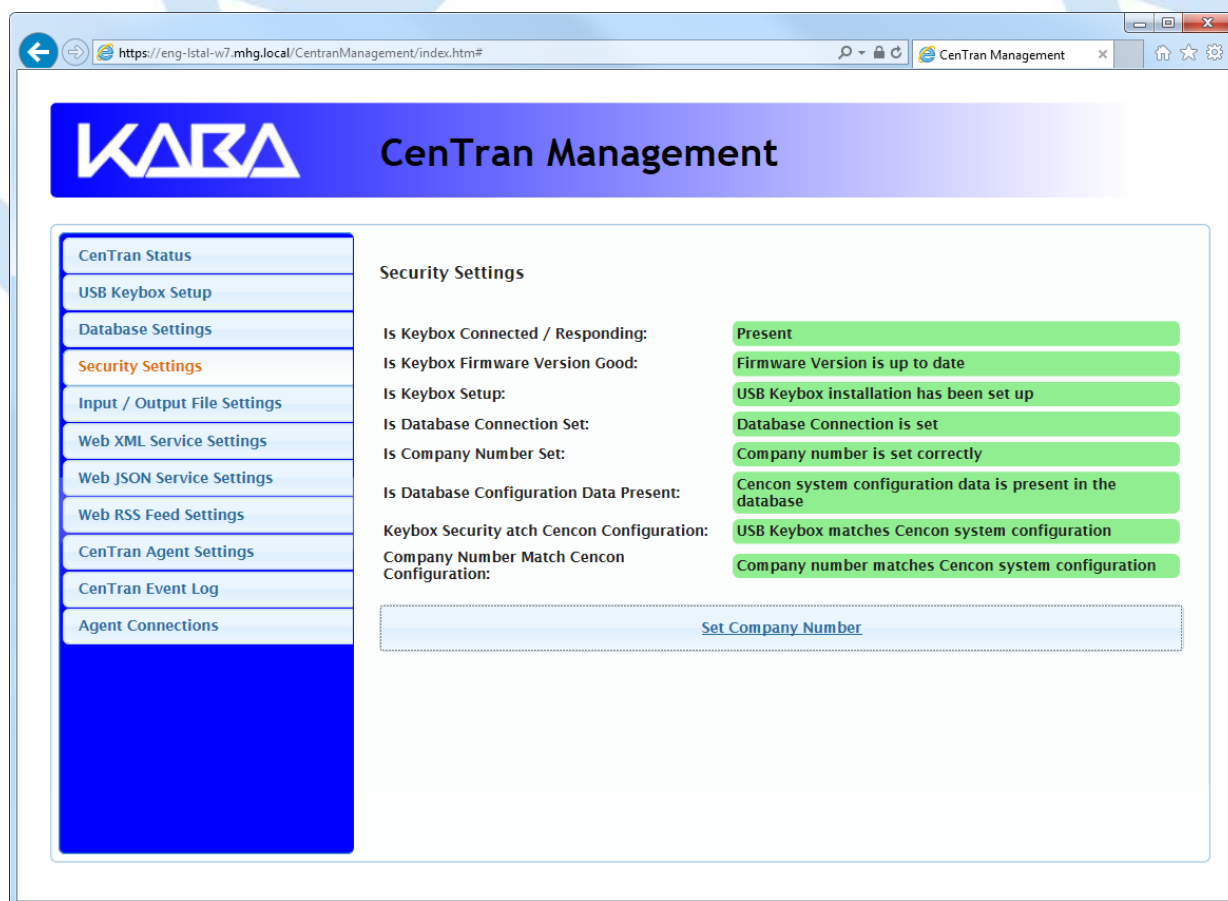
Enter the 4 digit company number you are using with Cencon. This is a sensitive piece of security information that is part your security with the Cencon system. You should record it and keep it in a secure place. The company number you enter for use by the CenTran service must match the one you are using with Cencon.

You should see the following in your web browser:



Click on the **OK** button on message box.

You should see the following in your web browser:



Set File Settings

CenTran 5 Getting Started Guide

Important Note

CenTran no longer runs under the permissions of the logged on user. It has been changed to run as a background service on the host server you install it on, and is independent of who is logged on. The CenTran service will run in the background even if no one is logged onto the host server.

By default, the CenTran service runs logged on under a **Local System** account. This gives it access to resources and settings on the host server you install it on. However, the **Local System** account only has access to the host server, not to resources on your network.

If you are configuring CenTran to access a shared file location on your network, not on the host server, then you will need to set up CenTran with a network domain account.

The account you set up CenTran to run logged onto must have administrative privileges on the host server CenTran is on. It must also have read / write access to the directories you are using for file input / output.

In this case, the file directories must be identified by UNC (Universal Naming Convention) paths: "\\server\share\path"

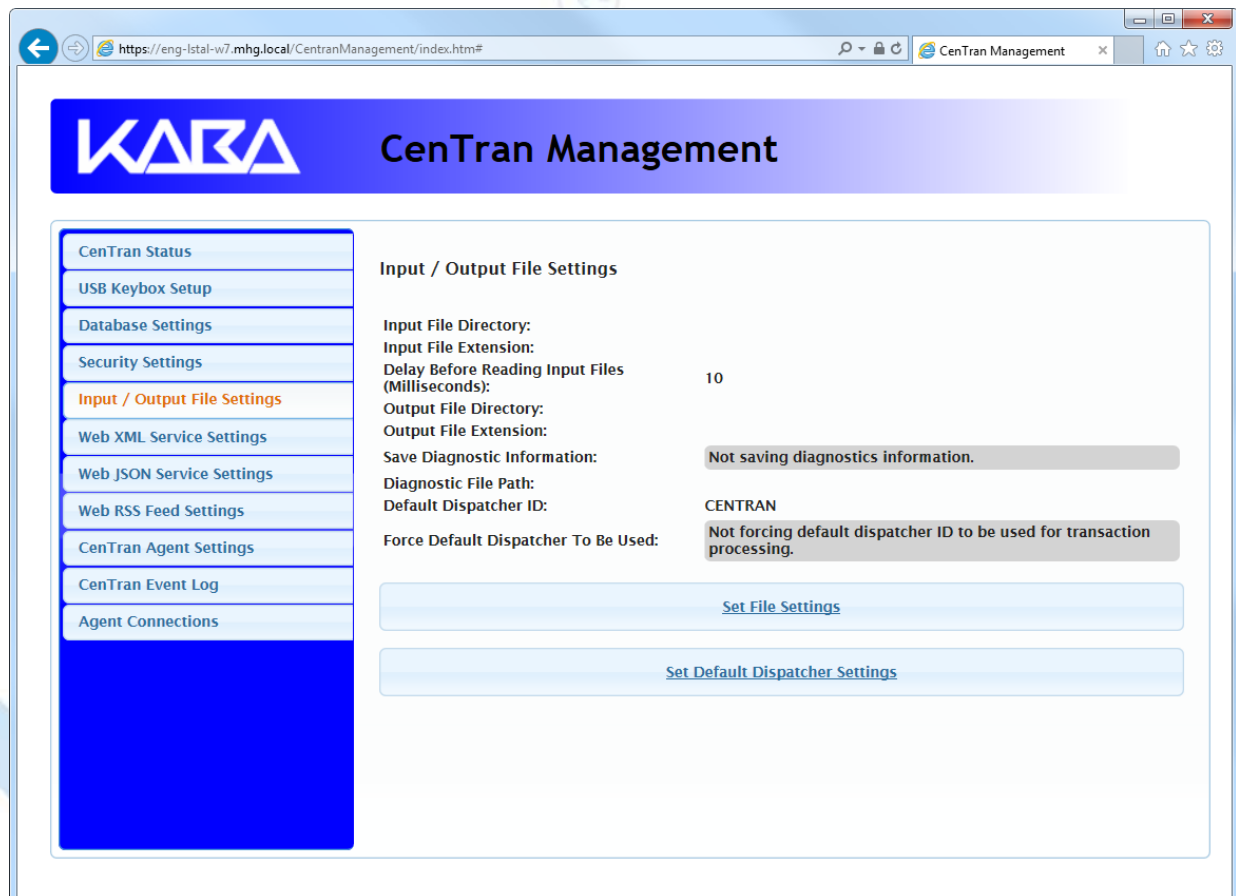
You can not use mapped drive letters for network paths for a service. Mapped drive letters for network paths are specific to an account. They are not accessible from other accounts. If you set up a mapped drive letter for your logged on account, that does not mean that CenTran can access it from its account.

You can view and edit the CenTran service settings from the Microsoft Management Console:

- Open the Start Menu.
- Right click on **Computer**.
- Select **Manage** from the displayed context menu. You must have administrative privileges.
- The **Computer Management** console will be displayed. Expand the **Services and Applications** section on the left side.
- Select **Services** from the **Services and Applications** section.
- Locate **CenTran** from the list of services. Right click on **CenTran** and select **Properties** from the context menu.
- A service **Properties** dialog will be displayed. Select the **Log On** tab to examine the account the service is set up to log on as.

1. You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Input / Output File Settings** tab on the left side:

You should see the following in your web browser:



2. You will need to setup an input directory and an output directory for CenTran to receive file transactions and return the response.

- **Input Directory** - The input directory is the directory where CenTran reads transactions being sent to it. It looks in this directory for files representing lock transactions to be processed. You will need to create an input directory that you want to use for CenTran to listen for incoming file transactions.
- **Input File Extension** - The input file extension defined here is the file extension CenTran looks for when attempting to find transaction input files

in the input directory that has been identified. If an input file extension is not set, then the CenTran service will attempt to read any file placed in the input directory.

- **Input File Delay** - The delay before reading next input transaction file setting is intended to allow a delay after detecting a file and before reading it. It is possible for an error in reading the input file to occur if it has not been completely written to the input directory yet. This delay allows the write of the input file to complete before the CenTran service reads the file. This delay begins when a transaction file is detected in the input directory by CenTran.

Note

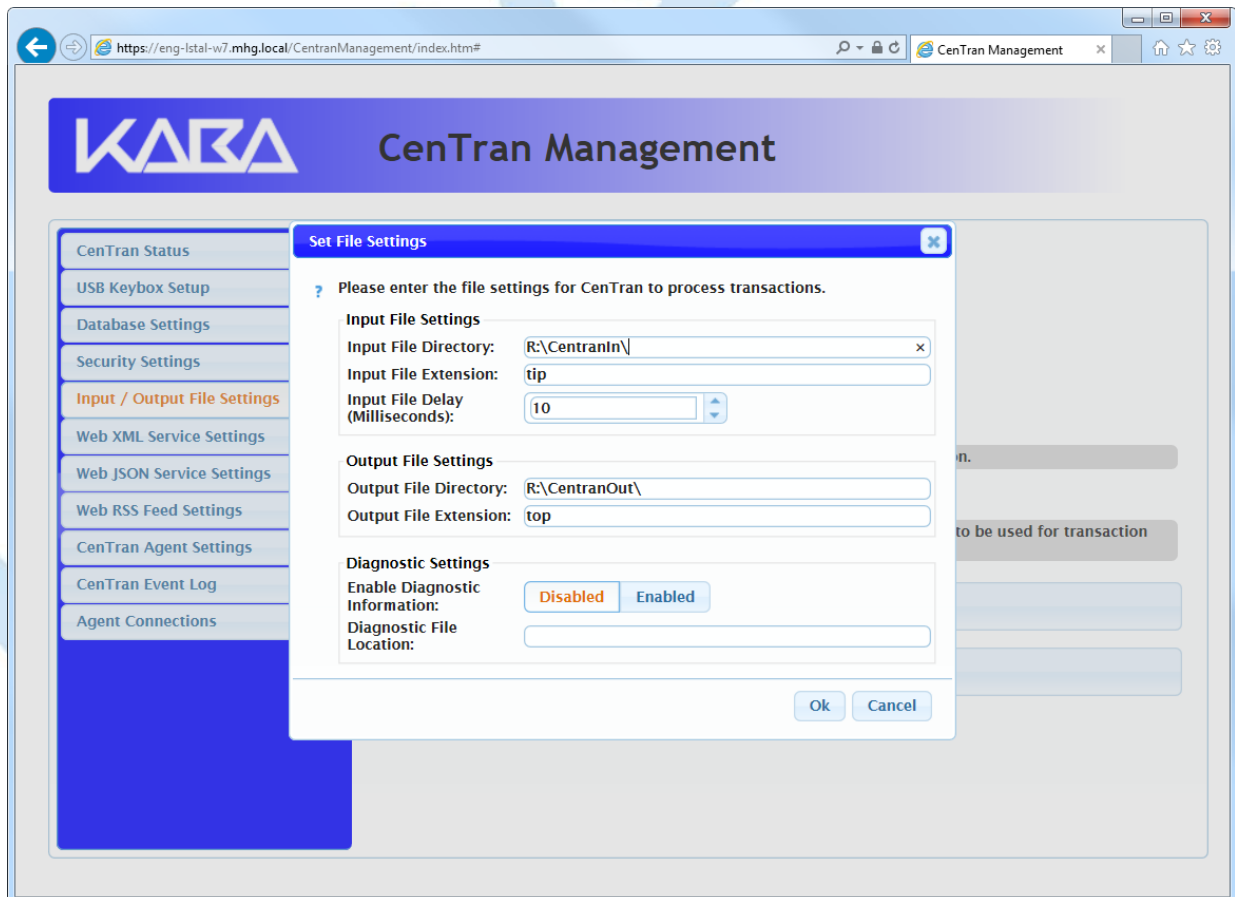
CenTran can also be used with an input file delay of zero. In this case, CenTran will attempt to detect file events for when the file is finished being written. CenTran will then immediately process the transaction file without a delay. If your file server supports CenTran detecting the file events, then an input file delay of zero can improve your CenTran performance.

- **Output Directory** - The output directory is the directory where CenTran places the output files containing the results of processed transactions. This directory can be the same directory as the one used to contain input files. If the two directories are the same, then the files must have different extensions assigned. You will need to create an output directory that you want to use for CenTran to write output files to.
- **Output File Extension** - The output file extension is the file extension placed by CenTran at the end of output file names. The file names will be the same as the input file names, except for the file extension. If an output file extension is set, then that extension will be placed at the end of output files produced by CenTran.

Note

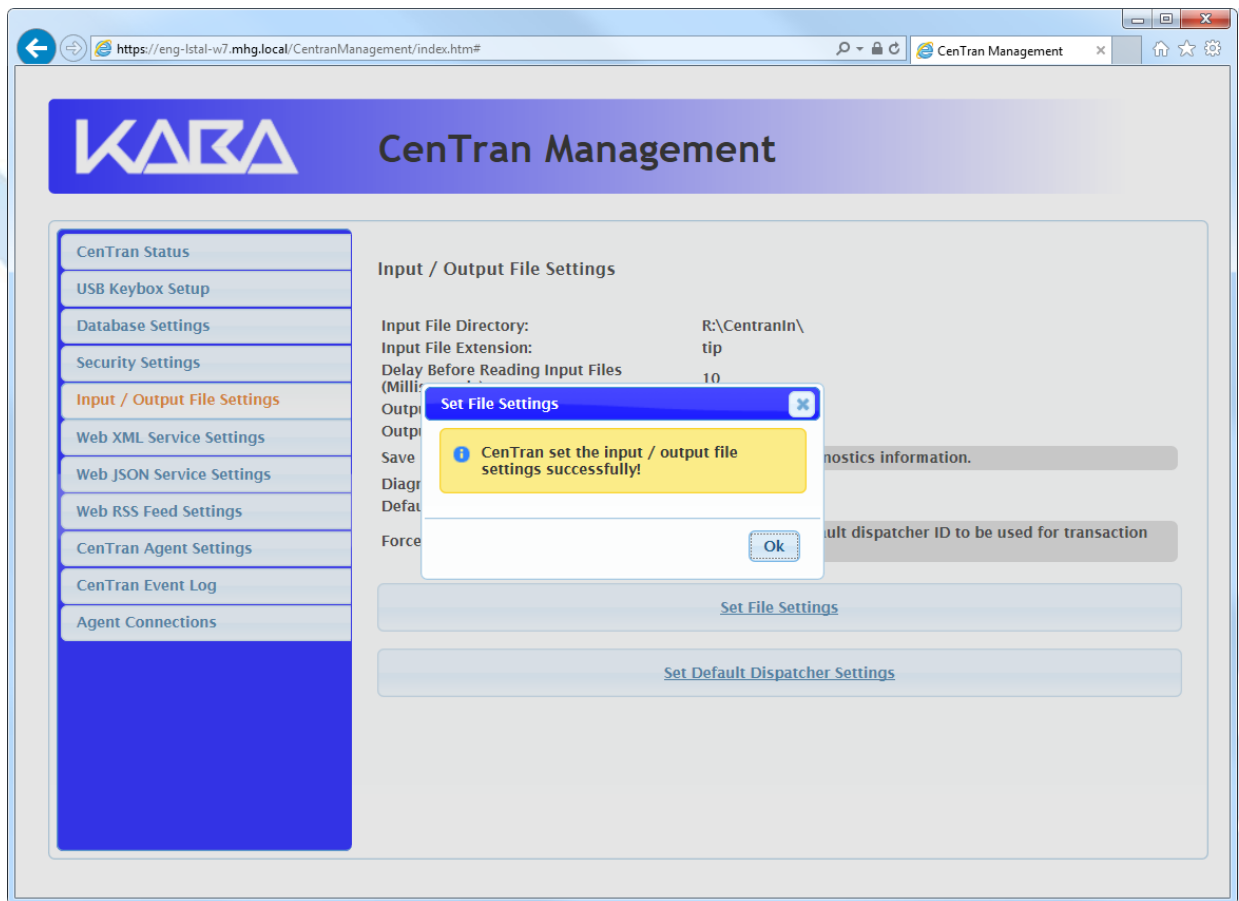
CenTran has been validated against the SuperSpeed RamDisk Plus software. This software allows you to use a ram disk as the file location used for transferring CenTran transaction files. This improves performance and speed of transferring CenTran transaction files, and eliminates hard drive wear from transferring CenTran transaction files. This software is available at <http://www.superspeed.com/desktop/ramdisk.php>. SuperSpeed RamDisk is a Microsoft Certified software.

3. Click on the **Set File Settings** button. You should see the following dialog displayed:



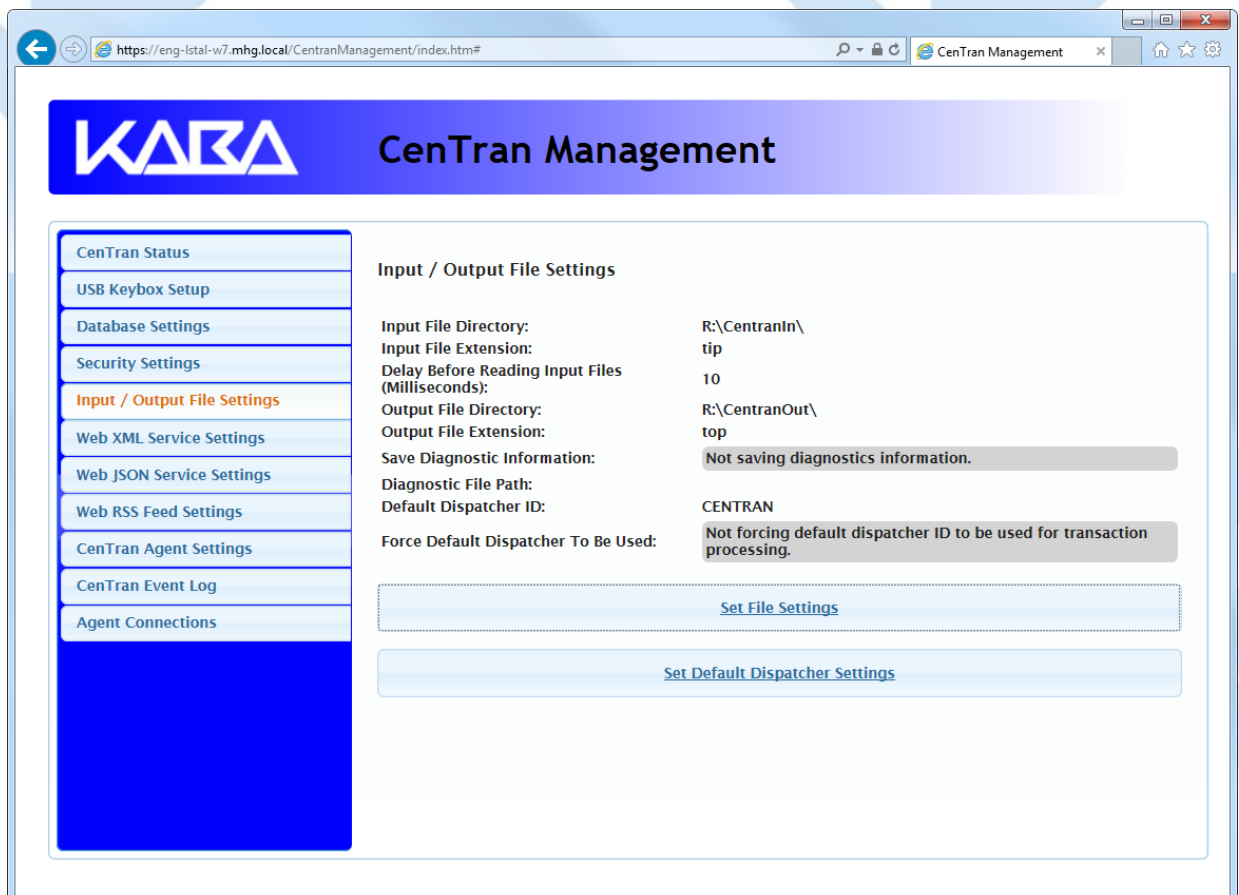
4. Enter the input and output directories and extensions for the CenTran service to process files. Optionally, you can enable CenTran to record diagnostic output to a file, but this slows down performance. Once you have entered the settings you want to use, click on the **OK** button.

You should see the following in your web browser:



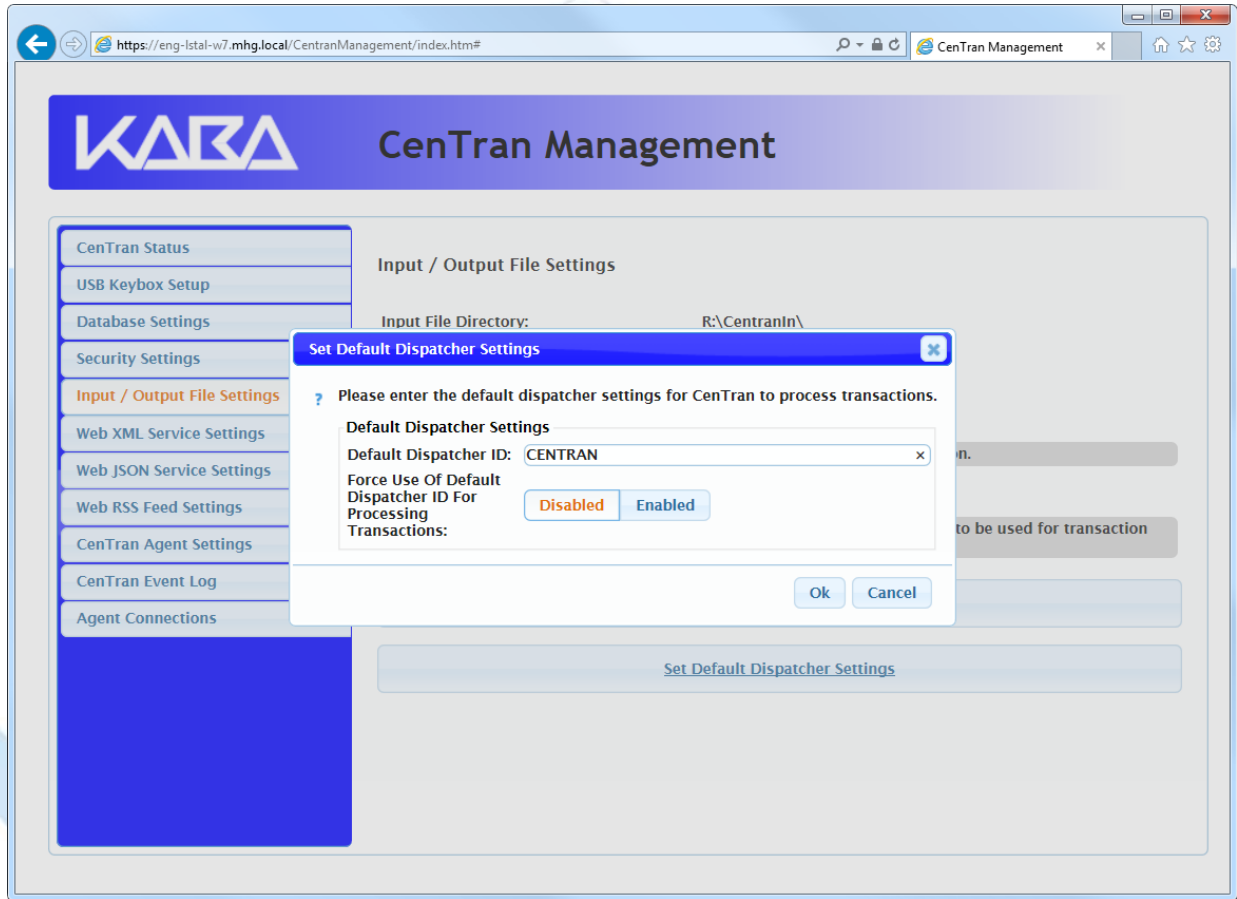
5. Click on the **OK** button on message box.

You should see the following in your web browser:



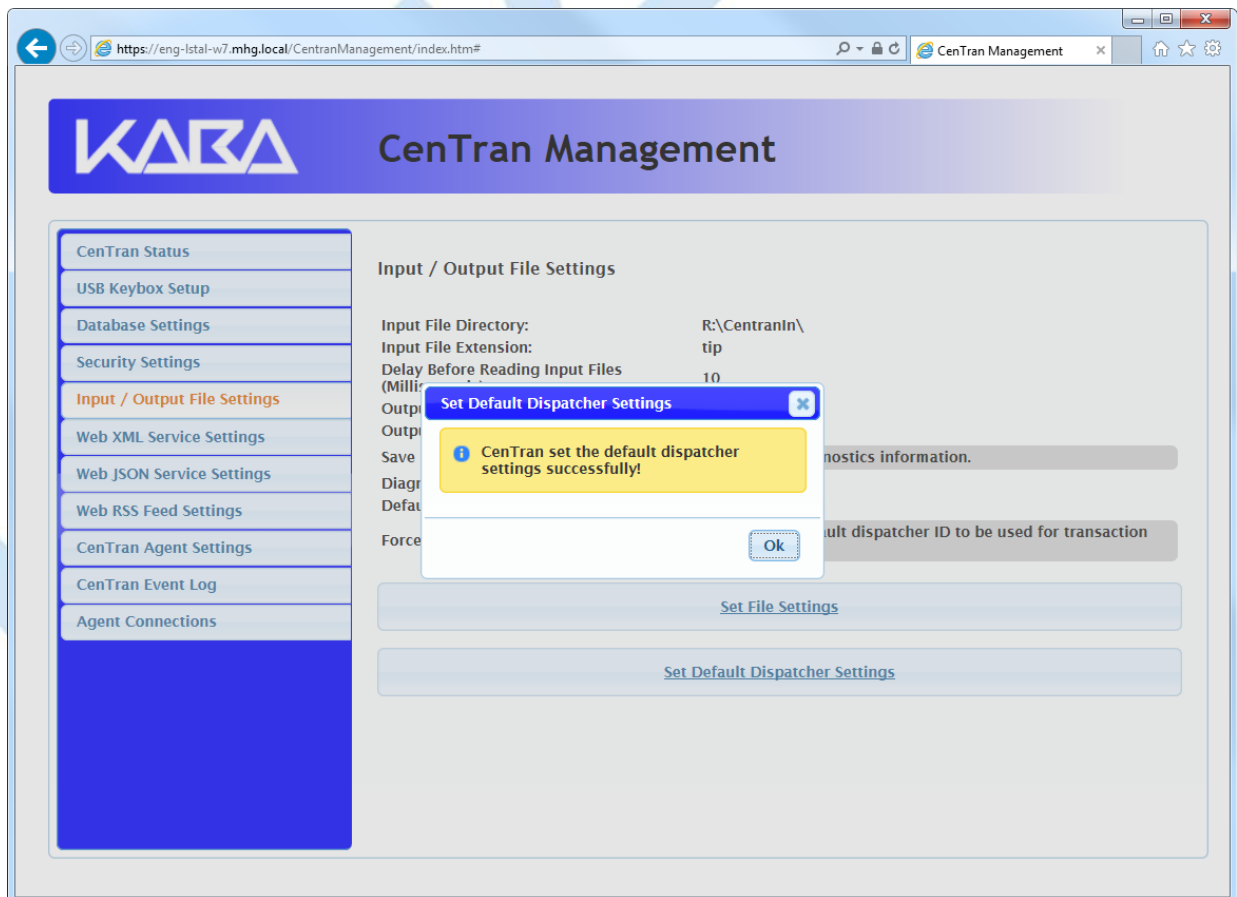
6. You will also need to set the default dispatcher ID to be used for the CenTran service when a dispatcher ID is not available for a transaction being processed. Optionally, you can force this dispatcher ID to be used instead of the dispatcher ID associated with a transaction.

You should see the following in your web browser:



7. Enter the default dispatcher ID you want to use. This default dispatcher ID must have been already set up under Cencon, and be present in the database. The role that the default dispatcher is assigned to will effect what authorizations the default dispatcher has. Once you have entered the default dispatcher ID you want to use, click on the **OK** button.

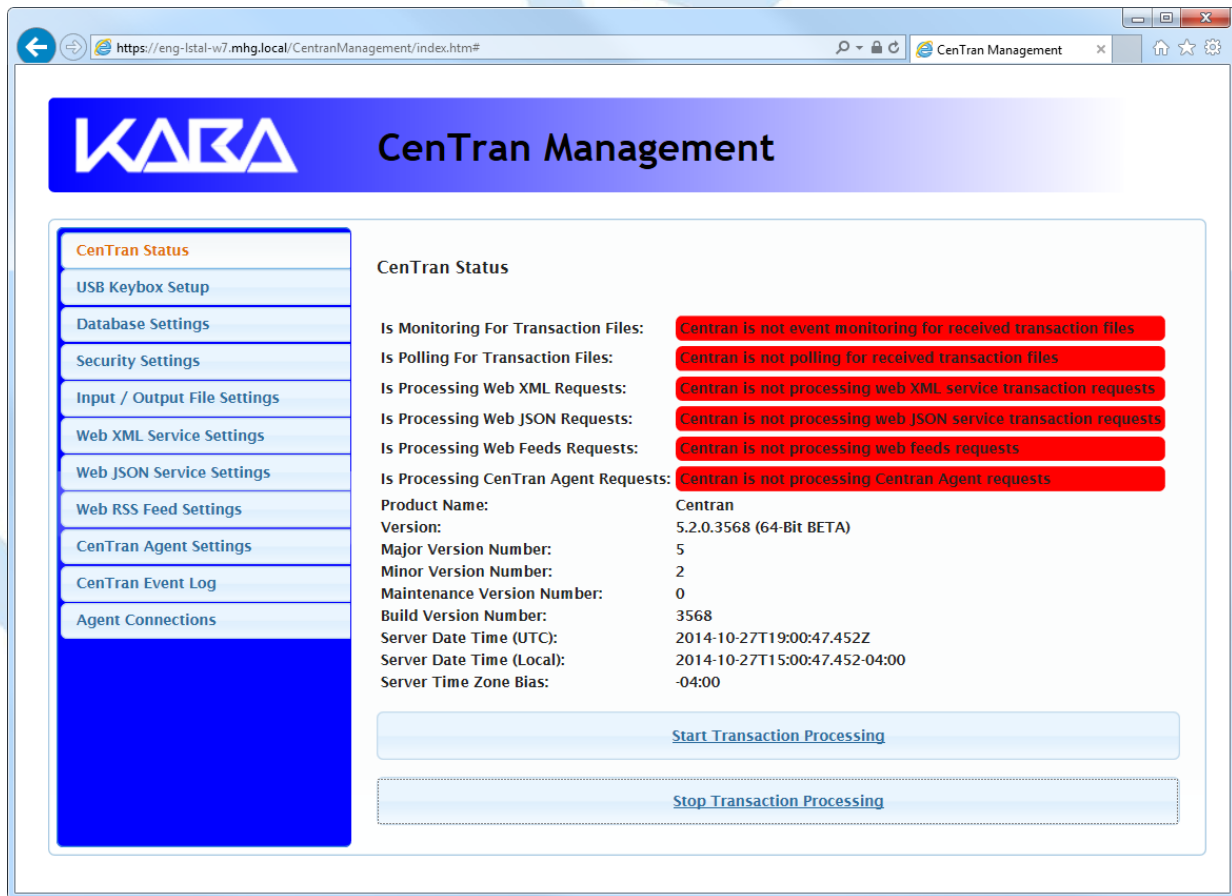
You should see the following in your web browser:



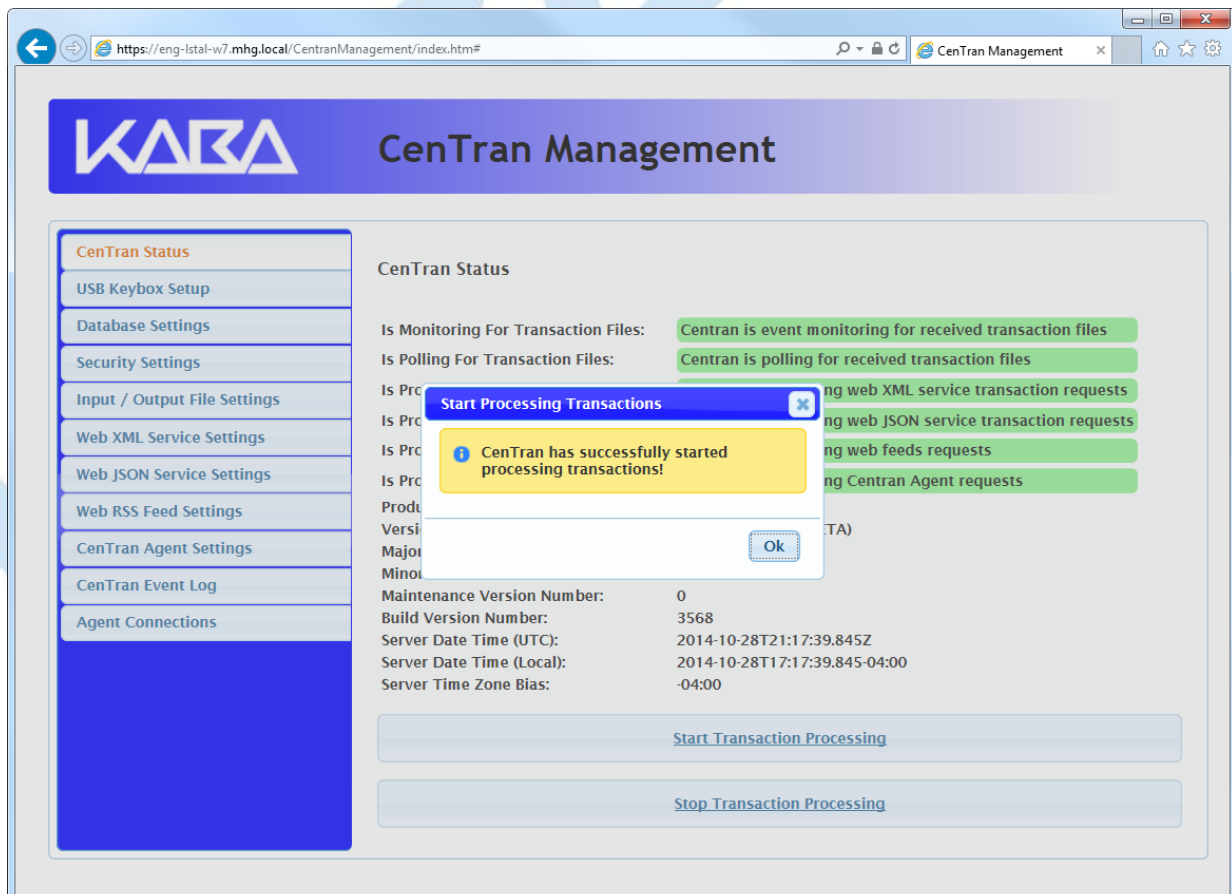
Start Transaction Processing

CenTran 5 Getting Started Guide

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **CenTran Status** tab on the left side:
You should see the following in your web browser:

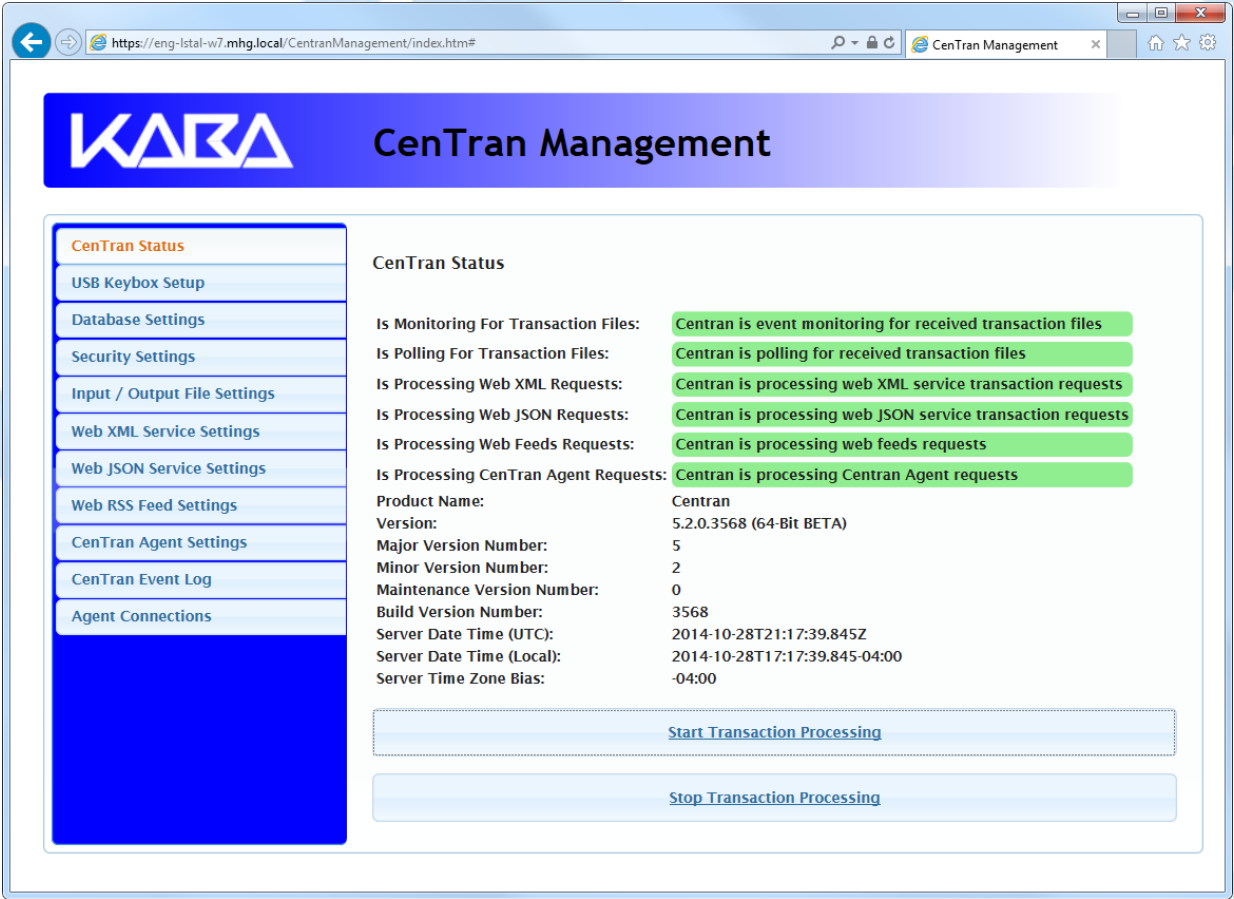


Click on the **Start Transaction Processing** button. You should see the following message dialog displayed:



Click on the message dialog **OK** button.

You should see the following in your web browser:



View Web Service XML Settings

CenTran 5 Getting Started Guide

The web service settings are configured in the **system.serviceModel** section of the CenTran service configuration file. The resultant web service based on the settings can be viewed while the CenTran service is processing transactions.

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Web XML Service Settings** tab on the left side:

You should see the following in your web browser:

The screenshot shows a web browser window with the URL `https://eng-1stai-w7.mhg.local/CenTranManagement/index.htm#`. The page title is "CenTran Management" and features the KABA logo. On the left is a navigation menu with the following items: CenTran Status, USB Keybox Setup, Database Settings, Security Settings, Input / Output File Settings, **Web XML Service Settings** (highlighted in orange), Web JSON Service Settings, Web RSS Feed Settings, CenTran Agent Settings, CenTran Event Log, and Agent Connections. The main content area is titled "Web XML Service Settings" and contains a sub-section "Addresses" with a table of settings.

Name:	Value
Endpoint Name:	NetNamedPipeBinding_ICenTran
Endpoint Address:	net.pipe://localhost/CenTranService
Endpoint Binding:	NetNamedPipeBinding
Endpoint Contract:	ICenTran
Contract Configuration:	CenTran.ICenTran
Operation:	SayHello
	Version
	HandleOptions
	LockDispatch
	LockReassign
	LockUnassign
	LockClose
	LockNamesData
	LockSerialNumbersData
	LockUpdate
	LockRename
	LockDelete
	LockInitSAKeyAuditDownload
	LockReadSAKeyAuditDownload
	LockQuery
	LockQueryCount
	LogNamesData

© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

View Web Service JSON Settings

CenTran 5 Getting Started Guide

The web service settings are configured in the **system.serviceModel** section of the CenTran service configuration file. The resultant web service based on the settings can be viewed while the CenTran service is processing transactions.

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Web JSON Service Settings** tab on the left side:

You should see the following in your web browser:

The screenshot shows a web browser window with the URL <https://eng-1stai-w7.mhg.local/CenTranManagement/index.htm#>. The page title is "CenTran Management" and features the KARA logo. On the left is a navigation menu with the following items: CenTran Status, USB Keybox Setup, Database Settings, Security Settings, Input / Output File Settings, Web XML Service Settings, **Web JSON Service Settings** (highlighted in orange), Web RSS Feed Settings, CenTran Agent Settings, CenTran Event Log, and Agent Connections. The main content area is titled "Web JSON Service Settings" and contains a sub-section "Addresses" with a table of settings.

Name:	Value
Endpoint Name:	WebHttpBinding_ICenTranJSON
Endpoint Address:	https://localhost/CenTranServiceJSON/rest/
Endpoint Binding:	WebHttpBinding
Endpoint Contract:	ICenTranJSON
Contract Configuration:	CenTran.ICenTranJSON
Operation:	SayHello
	Version
	HandleOptions
	LockDispatch
	LockReassign
	LockUnassign
	LockClose
	LockNamesData
	LockSerialNumbersData
	LockUpdate
	LockRename
	LockDelete
	LockInitSAKeyAuditDownload
	LockReadSAKeyAuditDownload
	LockQuery
	LockQueryCount
	LogNamesData

© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

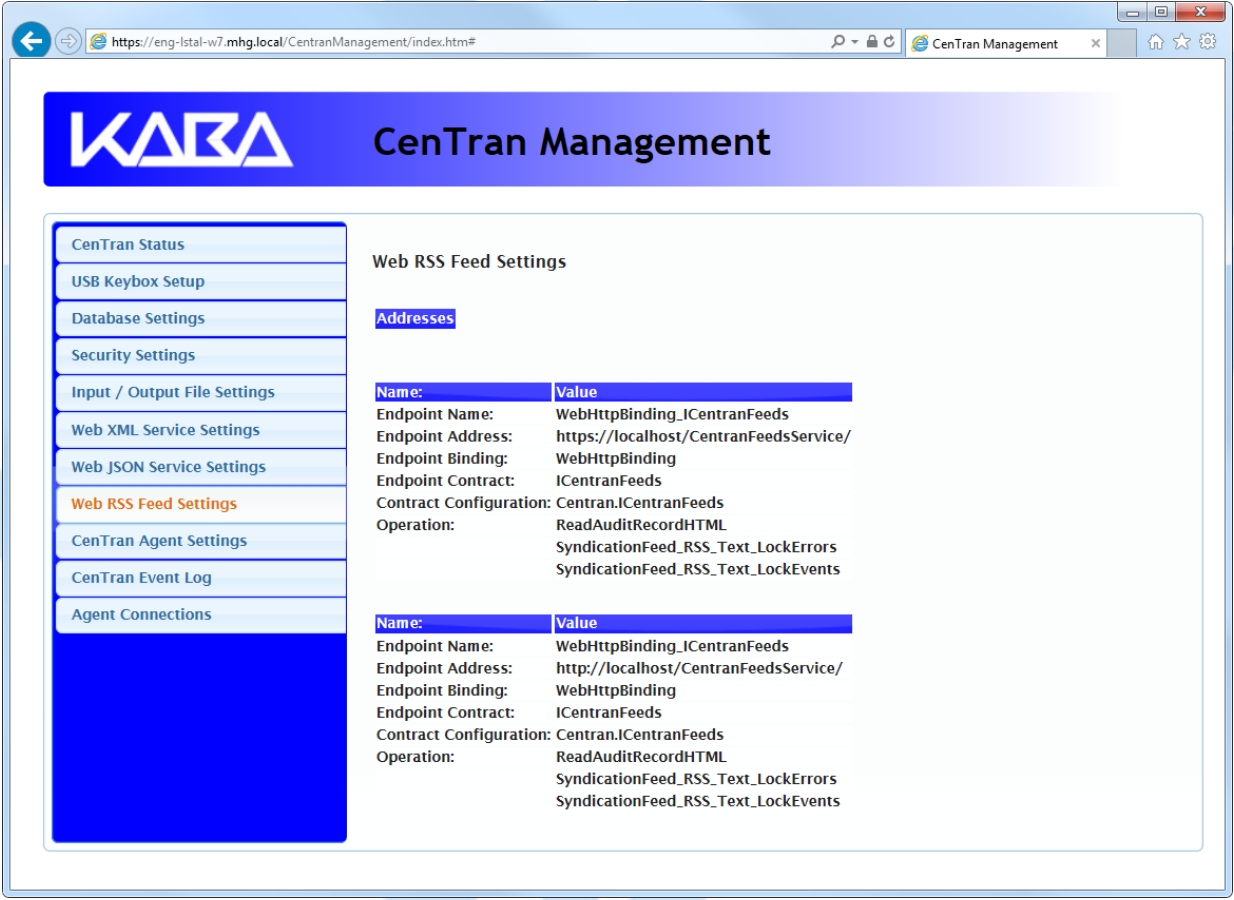
View Web RSS Feed Settings

CenTran 5 Getting Started Guide

The web rss feed settings are configured in the **system.serviceModel** section of the CenTran service configuration file. The resultant web rss feeds based on the settings can be viewed while the CenTran service is processing transactions.

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Web RSS Feed Settings** tab on the left side:

You should see the following in your web browser:



The screenshot shows the CenTran Management web interface. The left sidebar contains a menu with the following items: CenTran Status, USB Keybox Setup, Database Settings, Security Settings, Input / Output File Settings, Web XML Service Settings, Web JSON Service Settings, **Web RSS Feed Settings** (highlighted), CenTran Agent Settings, CenTran Event Log, and Agent Connections. The main content area is titled "Web RSS Feed Settings" and contains a sub-section "Addresses" with two tables of configuration data.

Name:	Value
Endpoint Name:	WebHttpBinding_ICentranFeeds
Endpoint Address:	https://localhost/CentranFeedsService/
Endpoint Binding:	WebHttpBinding
Endpoint Contract:	ICentranFeeds
Contract Configuration:	Centran.ICentranFeeds
Operation:	ReadAuditRecordHTML SyndicationFeed_RSS_Text_LockErrors SyndicationFeed_RSS_Text_LockEvents

Name:	Value
Endpoint Name:	WebHttpBinding_ICentranFeeds
Endpoint Address:	http://localhost/CentranFeedsService/
Endpoint Binding:	WebHttpBinding
Endpoint Contract:	ICentranFeeds
Contract Configuration:	Centran.ICentranFeeds
Operation:	ReadAuditRecordHTML SyndicationFeed_RSS_Text_LockErrors SyndicationFeed_RSS_Text_LockEvents

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

View CenTran Agent Settings

CenTran 5 Getting Started Guide

The CenTran Agent settings are configured in the **sytem.serviceModel** section of the CenTran service configuration file. The resultant web service based on the settings can be viewed while the CenTran service is processing transactions.

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **CenTran Agent Settings** tab on the left side:

You should see the following in your web browser:

CenTran Management

CenTran Agent Settings

Addresses

Name:	Value
Endpoint Name:	WSHttpBinding_ICentranAgent
Endpoint Address:	https://localhost/CenTranAgentService/soap/
Endpoint Binding:	WSHttpBinding
Endpoint Contract:	ICentranAgent
Contract Configuration:	Centran.ICentranAgent
Operation:	Version
	LockRemoteStatus
	LockRemoteDownloadAudits
	LockRemoteEvaluateEvent

Name:	Value
Endpoint Name:	WSHttpBinding_ICentranAgent
Endpoint Address:	http://localhost/CenTranAgentService/soap/
Endpoint Binding:	WSHttpBinding
Endpoint Contract:	ICentranAgent
Contract Configuration:	Centran.ICentranAgent
Operation:	Version
	LockRemoteStatus
	LockRemoteDownloadAudits
	LockRemoteEvaluateEvent

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

View Event Log

CentTran 5 Getting Started Guide

You will need to have already logged onto the CentTran Management interface in your web browser. Click on the **CentTran Event Log** tab on the left side:

You should see the following in your web browser:

The screenshot shows a web browser window with the URL `https://eng-1stai-w7.mhg.local/CenTranManagement/index.htm#`. The page title is "CentTran Management". On the left is a navigation menu with the following items: CentTran Status, USB Keybox Setup, Database Settings, Security Settings, Input / Output File Settings, Web XML Service Settings, Web JSON Service Settings, Web RSS Feed Settings, CentTran Agent Settings, **CentTran Event Log** (highlighted), and Agent Connections. The main content area is titled "CentTran Event Log" and includes a "Refresh" button. Below the title is a table with the following data:

Row ID	Time	Lock	Description
22222	2014-10-28 17:20:55 (DST)		Centran Event - Accepted Agent Persistent Connection: LockSerialNumber:1000116 IP: 10.108.6.103
22221	2014-10-28 17:20:55 (DST)		Centran Event - Accepted Agent Persistent Connection: LockSerialNumber:1158563 IP: 10.108.6.104
22220	2014-10-28 17:20:54 (DST)		Centran Event - Accepted Agent Persistent Connection: KeyBoxSerialNumber:01E164991400008B IP: 10.108.6.103
22219	2014-10-28 17:20:54 (DST)		Centran Event - Started Processing
22218	2014-10-28 17:20:41 (DST)		Centran Event - Stopped Processing
22217	2014-10-28 17:20:10 (DST)		Centran Event - Stopped Processing
22216	2014-10-28 17:17:40 (DST)		Centran Event - Accepted Agent Persistent Connection: KeyBoxSerialNumber:01E164991400008B IP: 10.108.6.103
22215	2014-10-28 17:17:40 (DST)		Centran Event - Accepted Agent Persistent Connection: LockSerialNumber:1158563 IP: 192.168.56.1

The CentTran Management interface loads event log audits 100 at a time. To load additional audits for viewing, scroll to the bottom of the current audits. Additional audits will be loaded automatically, and the scroll position will be moved up.

The CentTran event log is limited in size based on the settings you made in the CentTran service configuration file. Once the event log reaches the limit you set, it will delete the oldest audits to remain within the limit when new audits are added. This occurs based off of the granularity you set in the configuration file. The event log will be allowed to grow slightly larger than the set limit based off of the granularity size used to regulate how often the check is made.

Additional information is available in the CentTran event log registered with the operating system. Service start and stop events are recorded there. Additionally, if internal errors occur within CentTran, the description of the error is recorded there also. This can be accessed by opening the administrative tools section of the control panel for your computer. Under that is an item labeled **Event Viewer**. Open the **Event Viewer**, and you will see a CentTran event log under the application and services event logs section.

Also, additional information is available in the Windows Communication Foundation (WCF) diagnostic output set up from the CentTran configuration file. The default settings from the CentTran configuration file creates a diagnostic output file for Windows Communication Foundation (WCF) events, named **WcfServiceTrace.svclog**. This file will be created within the application directory the CentTran service is installed to. This file can be viewed using the Microsoft Service Trace Viewer (SvcTraceViewer.exe). Double clicking on the file will automatically open the file under the Microsoft Service Trace Viewer.

The Microsoft Service Trace Viewer is available as a free download within the Windows Platform SDK.

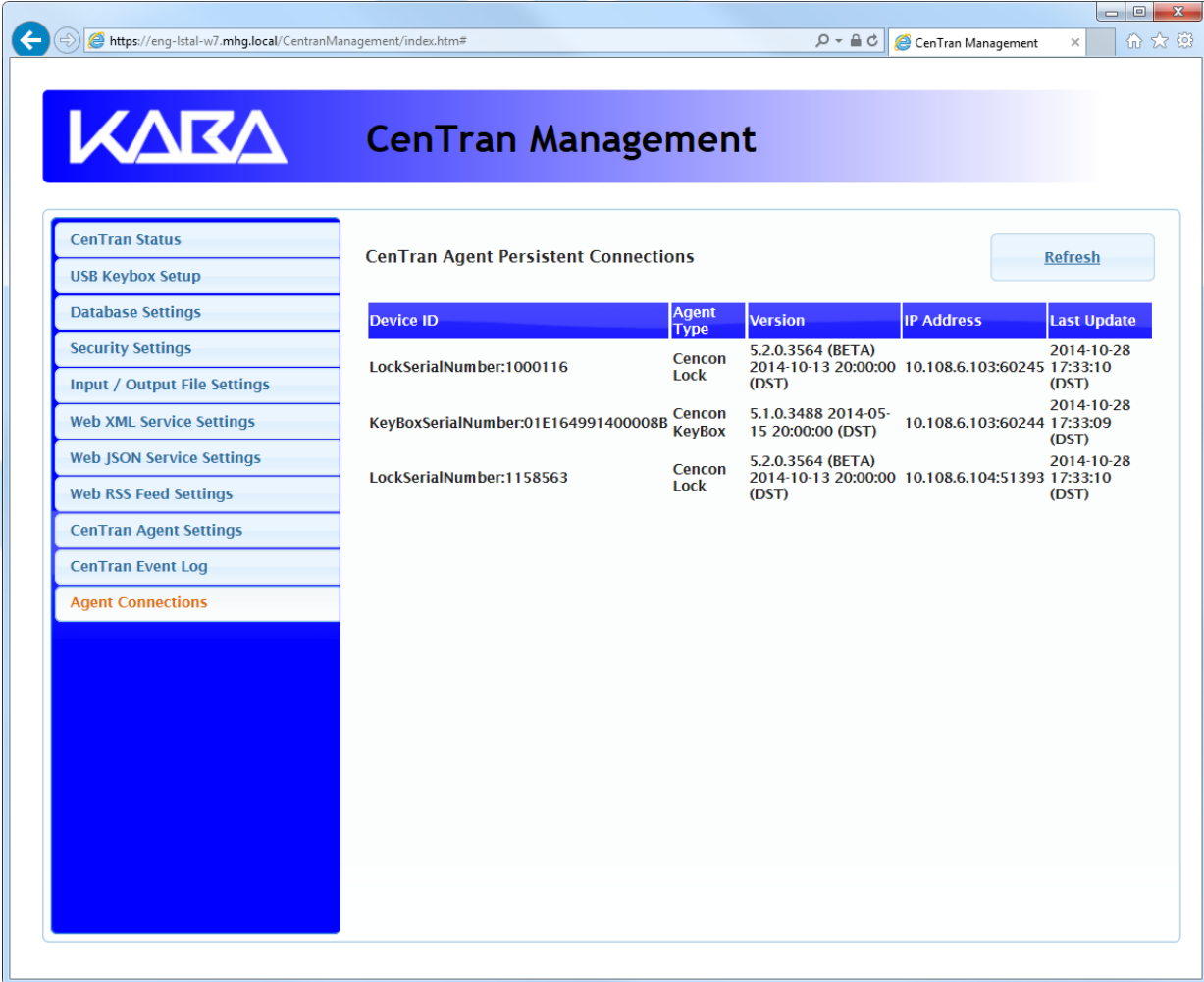
View CenTran Agent Persistent Connections

CenTran 5 Getting Started Guide

CenTran maintains persistent network connections with CenTran Agent installations configured to connect with your current CenTran installation. These connections can be displayed.

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **Agent Connections** tab on the left side:

You should see a similar list to the following in your web browser:



The screenshot shows a web browser window with the URL <https://eng-1stai-w7.mhg.local/CenTranManagement/index.htm#>. The page title is "CenTran Management" and features the KABA logo. On the left is a navigation menu with the following items: CenTran Status, USB Keybox Setup, Database Settings, Security Settings, Input / Output File Settings, Web XML Service Settings, Web JSON Service Settings, Web RSS Feed Settings, CenTran Agent Settings, CenTran Event Log, and Agent Connections (which is highlighted in orange). The main content area is titled "CenTran Agent Persistent Connections" and includes a "Refresh" button. Below the title is a table with the following data:

Device ID	Agent Type	Version	IP Address	Last Update
LockSerialNumber:1000116	Cencon Lock	5.2.0.3564 (BETA) 2014-10-13 20:00:00 (DST)	10.108.6.103:60245	2014-10-28 17:33:10 (DST)
KeyBoxSerialNumber:01E164991400008B	Cencon KeyBox	5.1.0.3488 2014-05-15 20:00:00 (DST)	10.108.6.103:60244	2014-10-28 17:33:09 (DST)
LockSerialNumber:1158563	Cencon Lock	5.2.0.3564 (BETA) 2014-10-13 20:00:00 (DST)	10.108.6.104:51393	2014-10-28 17:33:10 (DST)

You can refresh the display of current CenTran Agent persistent connections by clicking on the **Refresh** button.

Stop Transaction Processing

CenTran 5 Getting Started Guide

You will need to have already logged onto the CenTran Management interface in your web browser. Click on the **CenTran Status** tab on the left side:

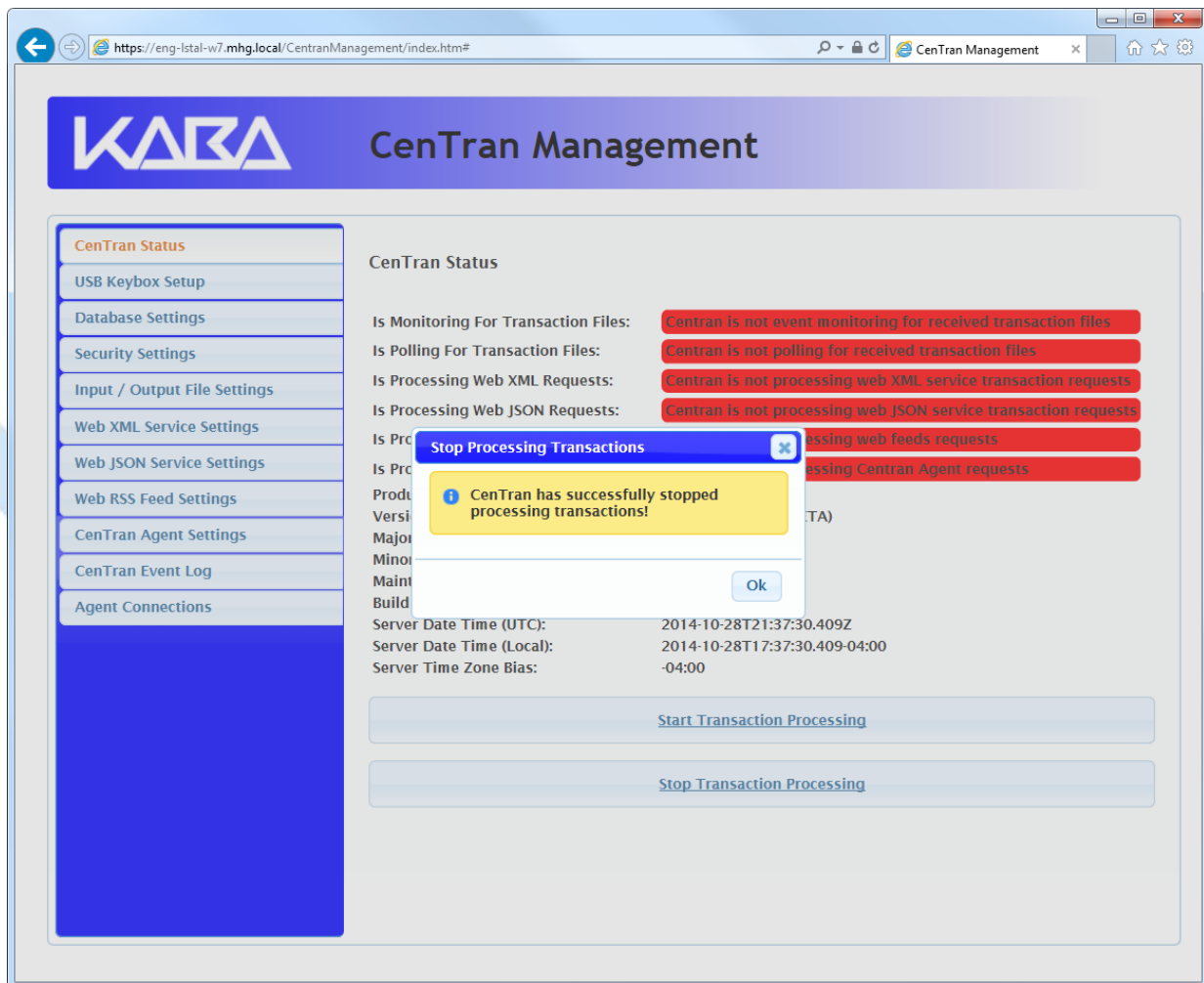
You should see the following in your web browser:

The screenshot shows a web browser window with the URL <https://eng-lstai-w7.mhg.local/CenTranManagement/index.htm#>. The page title is "CenTran Management" and features the KARA logo. On the left is a navigation menu with the following items: **CenTran Status** (highlighted), USB Keybox Setup, Database Settings, Security Settings, Input / Output File Settings, Web XML Service Settings, Web JSON Service Settings, Web RSS Feed Settings, CenTran Agent Settings, CenTran Event Log, and Agent Connections. The main content area is titled "CenTran Status" and displays the following information:

Is Monitoring For Transaction Files:	Centran is event monitoring for received transaction files
Is Polling For Transaction Files:	Centran is polling for received transaction files
Is Processing Web XML Requests:	Centran is processing web XML service transaction requests
Is Processing Web JSON Requests:	Centran is processing web JSON service transaction requests
Is Processing Web Feeds Requests:	Centran is processing web feeds requests
Is Processing CenTran Agent Requests:	Centran is processing CenTran Agent requests
Product Name:	Centran
Version:	5.2.0.3568 (64-Bit BETA)
Major Version Number:	5
Minor Version Number:	2
Maintenance Version Number:	0
Build Version Number:	3568
Server Date Time (UTC):	2014-10-28T21:17:39.845Z
Server Date Time (Local):	2014-10-28T17:17:39.845-04:00
Server Time Zone Bias:	-04:00

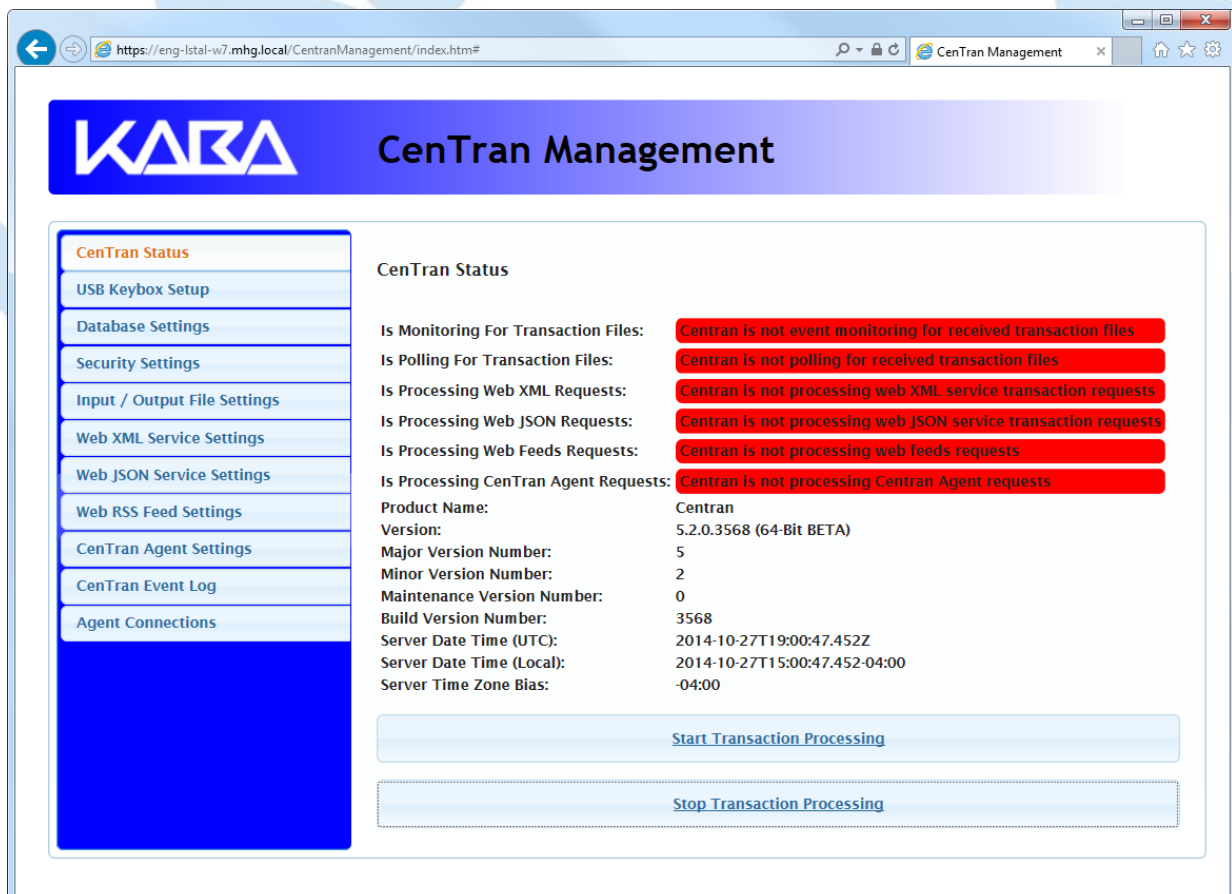
At the bottom of the main content area are two buttons: [Start Transaction Processing](#) and [Stop Transaction Processing](#).

Click on the **Stop Transaction Processing** button. You should see the following message dialog displayed:



Click on the message dialog **OK** button.

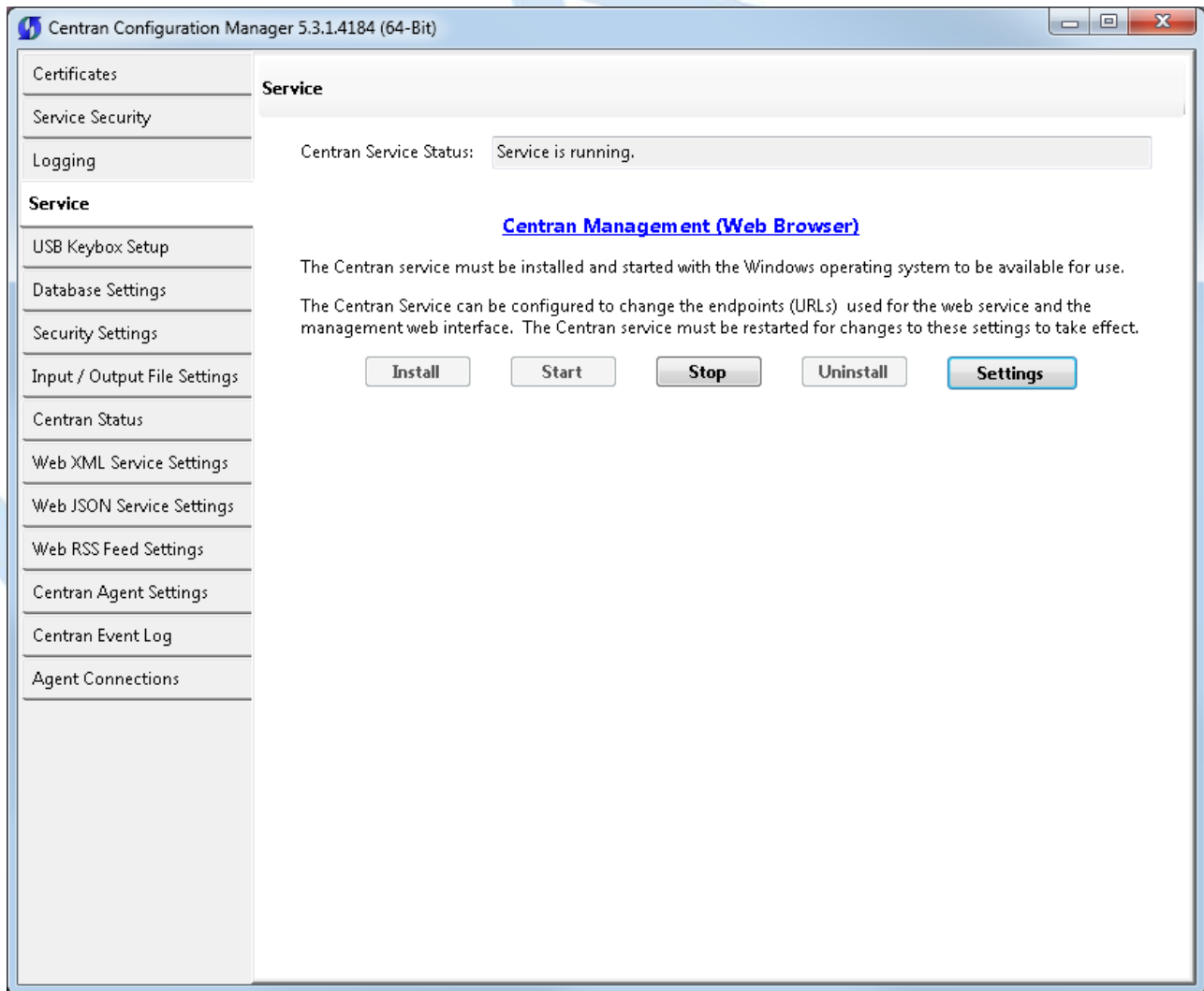
You should see the following in your web browser:



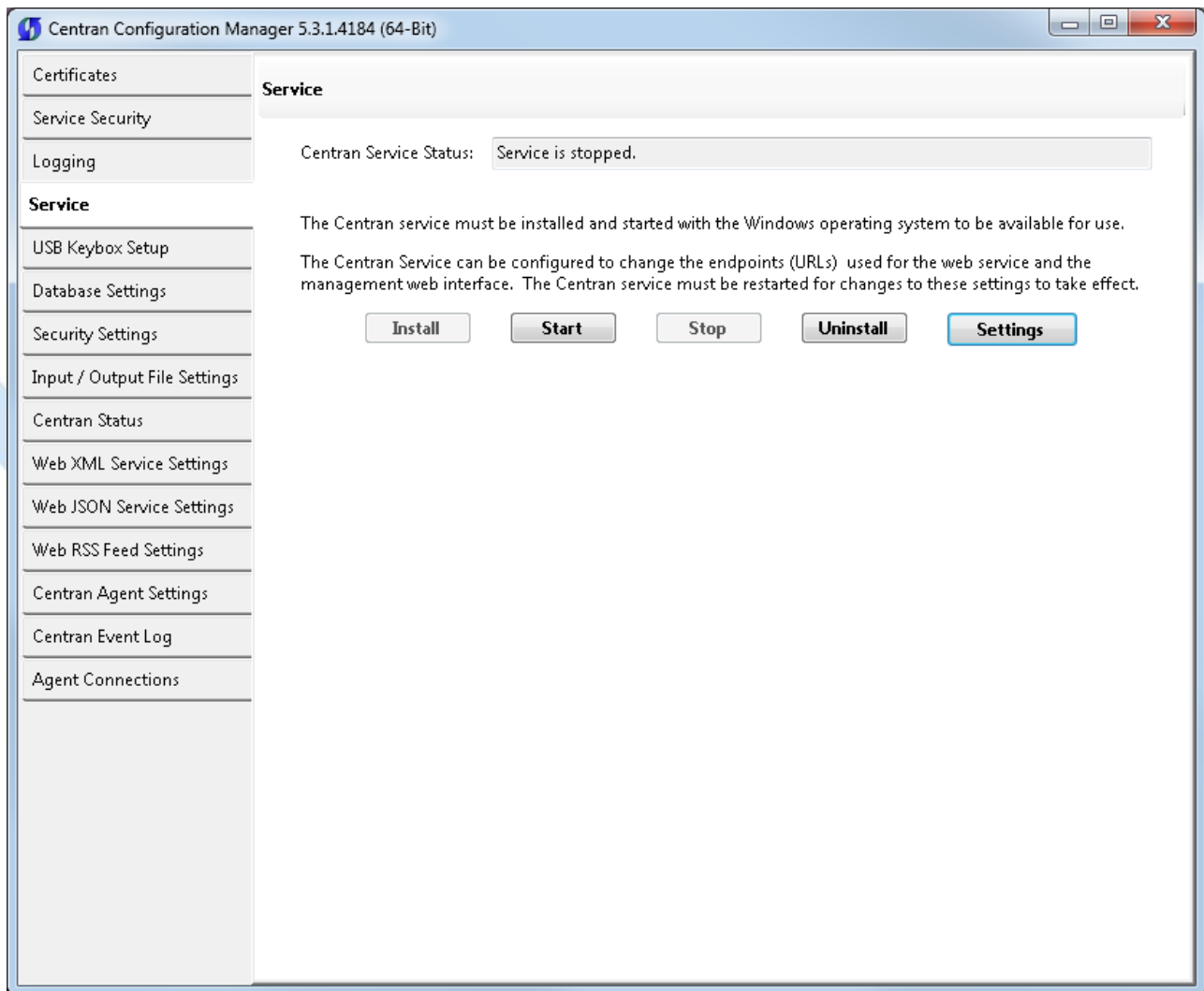
Stop / Uninstall the CenTran Service

CenTran 5 Getting Started Guide

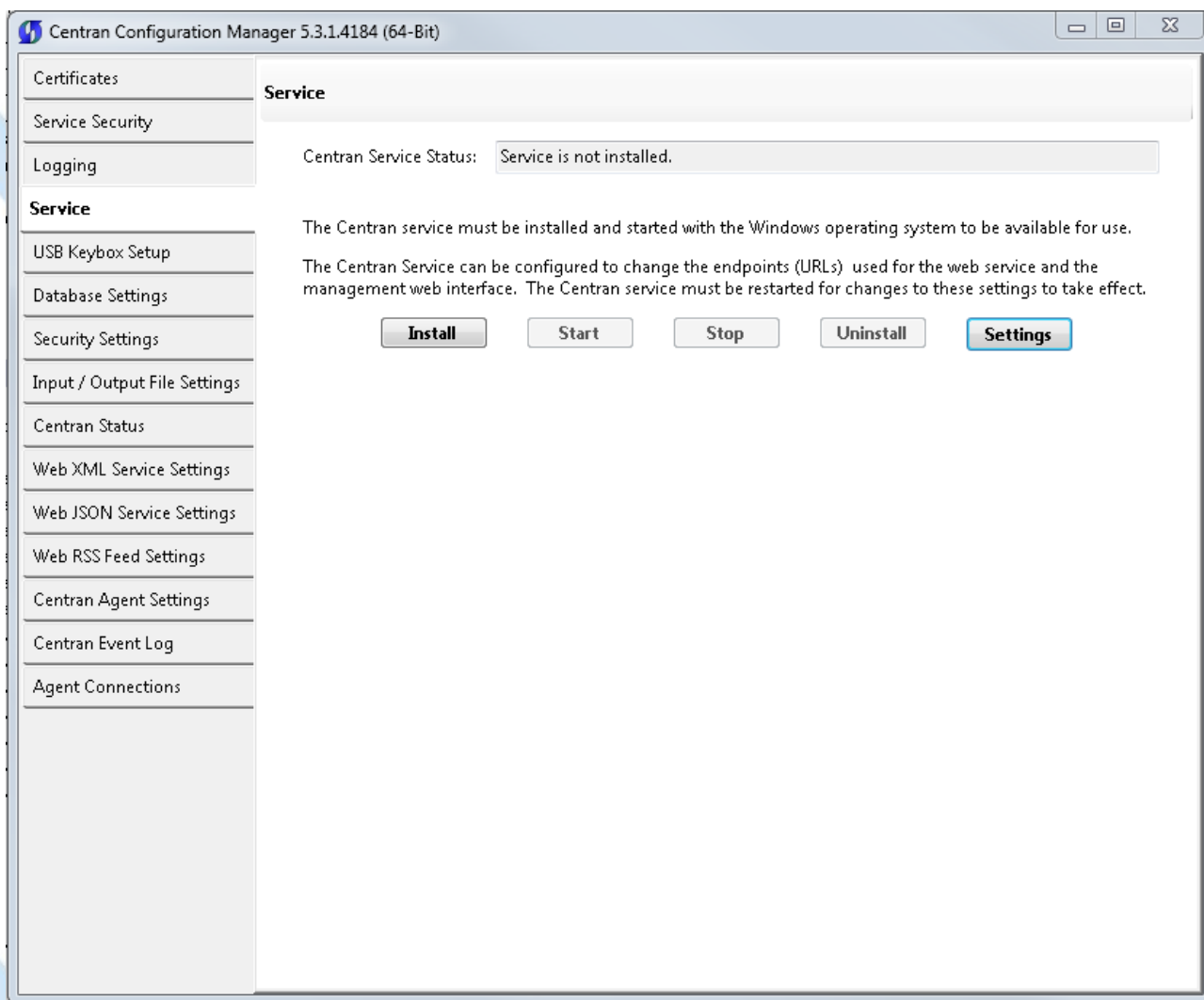
To stop and uninstall the CenTran service, select **CenTran Configuration Manager** from the CenTran entry under the Windows Start menu. You should see the following application:



Select the **Stop** button to stop the CenTran service with the operating system.



Select the **Uninstall** button to uninstall the CenTran service from the operating system.



© 1996-2017 domakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Appendix A - Beta Expiration

CenTran 5 Getting Started Guide

The beta versions of CenTran, the ATM Agents and the Keybox Agents will be assigned an initial expiration date of 180 days after the date of creation by dormakaba.

When CenTran or an agent is within 60 days of its expiration date entries will be posted to the database audit log documenting the situation. CenTran and the agents will continue to function.

When CenTran expires an entry will be posted to the database audit log identifying the event. An expired CenTran will not process transaction requests but will return an error condition to the transaction requestor. An entry will be posted to the database audit log documenting the transaction that failed due to an expired CenTran.

In a future Beta release the customer will be provided with the ability to reset the expiration date, and the date on which the warnings begin, for CenTran and the Agents with help from dormakaba Technical Support.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide

Appendix B - Troubleshooting: Check Certificates

CenTran Version 5 Getting Started Guide

The following items can be checked for CenTran Certificates:

- **CenTran Configuration File:**

The CenTran configuration file section for **behaviors >> serviceBehaviors >> serviceCertificate**. has the entries for what certificate is going to be used by CenTran. See [serviceCertificate of serviceCredentials](#) for a detailed description of these values.

The certificate can be identified by name or by thumbprint. By default it is set up by the CenTran Configuration Manager by thumbprint.

- **CenTran Configuration Manager:**

Open the CenTran Configuration Manager.

Check the **Self Signed Certificates** tab.

The **CenTran Web Service Server Certificate** will show a certificate name. This name must exactly match how the web browser is being used to access CenTran, or the certificate will not match.

- **Certificate Source:**

The certificate can be self signed, or from a certificate authority. If the certificate for the CenTran web service is from a network certificate authority, any clients will automatically trust the CenTran certificate.

If the certificate is self signed, then to establish a chain of trust, that certificate or certificate authority must be installed manually with client systems.

If the certificate is self signed and created on Windows Server 2003, the level and size of the encryption of the certificates do not match the requirement for SSL. To do SSL off of Windows Server 2003, you will need to generate proper certificates from a system running Windows 7 or higher, or get certificates from a network certificate authority.

- **Exporting CenTran Certificate:**

From the start menu, select **Accessories** and right click on **Command Prompt**. Select **Run as administrator**.

The command prompt should have the title **Administrator: Command Prompt**.

Type **mmc** at the administrator command prompt.

You should see a window that says **Console1 - [Console Root]**

Click **File >> Add / Remove Snap In....** A dialog labeled **Add or Remove Snap-ins** should be displayed.

Select **Certificates** and click **Add**. Select **Computer account** and then **Local Computer** from the dialogs that are displayed. Click **Finished**.

Click **OK** in the **Add or Remove Snap-ins** dialog.

Under **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and expand **Certificates**.

Select the certificate matching the Certificate Authority used to generate the self signed certificate used for CenTran. Right click on the certificate and select **All Tasks >> Export....**

The Certificate Export Wizard is displayed. Export the certificate without the private key. Use the default settings to export the certificate to a .CER file.

- **Client System Self Signed Certificate Install:**

Open up a console with the Certificates snap in as administrator as described above, on the client computer system that is going to be accessing the CenTran web service.

Under **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and expand **Certificates**.

Right click on **Certificates** and select **All Tasks >> Import....**

Import the certificate .CER file you exported from the CenTran server.

Appendix C - Troubleshooting: Check Run Time Error

CenTran Version 5 Getting Started Guide

The following places can be checked to determine the nature of a run time error from a transaction with CenTran:

- **CenTran Configuration Manager:**

Open the CenTran Configuration Manager.

Check if the CenTran service is installed and running under the **Service** tab. If the service is not installed and running, go to the Getting Started Guide to set up CenTran.

Check if the CenTran service is processing transactions under the **CenTran Status** tab. If CenTran is properly set up but processing has stopped, attempt stopping and restarting the service.

Check the **CenTran Event Log** for indications of the nature of the error.

- **System Event Log:**

Open **Control Panel >> Administrative Tools**.

Select **Event Viewer**, right click and select **Run as administrator**.

Look for the section labeled **Summary of Administrative Events**. Expand the category that called **Error**. Look for an entry with a **Source** labeled **CenTran Service**, and double click it.

Examine the errors list there. If CenTran has had internal exceptions, the details should be listed as entries here.

- **Windows Communications Foundation (WCF) Trace Log:**

Open the CenTran install directory. Look for a file named **WcfServiceTrace.svclog**. Double click on this file to open it using the Microsoft Service Trace Viewer.

See [Service Trace Viewer Tool \(SvcTraceViewer.exe\)](#) on the Microsoft web site for details. This tool is available with the Microsoft SDK install.

Examine the trace for errors. This will let you know if CenTran received a web service request and what processing occurred. If the web service request was not received, then a browser or network configuration issue is blocking the requests.

© 1996-2017 dormakaba

Document Number 2101.0513 Rev. G 08/17 CenTran® 5 Getting Started Guide