

# Installing SecurTrac on a Domino 14 Server that runs using a non-admin user ID

Important information and tips for running SecurTrac on Domino 14 server that runs using a non-admin user ID. Applicable to Windows Platform only.

Extracomm Inc.

1/26/2024

**extracomm**

## Table of Contents

Installing SecurTrac on a Domino 14 Server that runs using a non-admin user ID.....	1
Introduction: .....	1
Enable running Domino using a non-admin user ID in Domino 14 – Windows platform.....	1
What are the SecurTrac pre-requisites for installation on Domino 14?.....	2
How is SecurTrac impacted by the new default Windows service security settings in Domino 14 on Windows Server platform? .....	2
Domino server notes.ini location: Another fundamental change in Domino 14 that may have an impact on SecurTrac.....	2
SecurTrac installation scenario considerations for Domino 14 – Windows platform. ....	3
Install SecurTrac on Domino 14 running as a non-admin user ID:.....	3
Upgrading SecurTrac on Domino 14 running as a non-admin user ID: .....	3
Manually granting security permissions for SecurTrac on Domino 14 Windows platform:.....	4
Configuring Security permissions using the Windows GUI:.....	5
Configuring Security permissions using command line parameters:.....	6
Troubleshooting SecurTrac problems on Domino 14 – Windows platform: .....	7

# **Installing SecurTrac on a Domino 14 Server that runs using a non-admin user ID.**

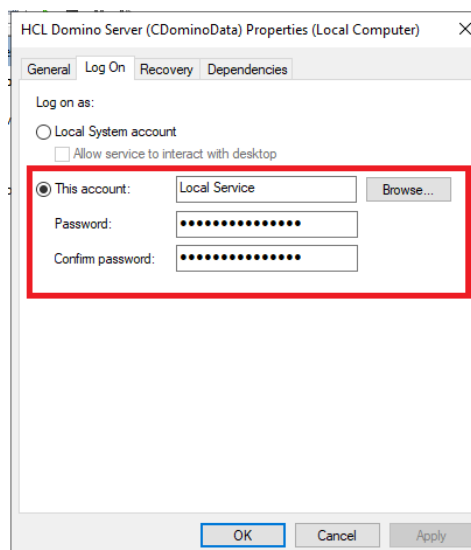
## **Introduction:**

This document is intended for Extracomm SecurTrac customers who are planning upgrades and implementations of HCL Domino 14, most notably on the Windows Server platform. HCL has made fundamental changes that are considered default settings related to how an HCL Domino 14 server runs on a Windows Server. SecurTrac customers are encouraged to read this document in its entirety prior to using SecurTrac on Domino 14. It is also very important to understand how SecurTrac has been impacted and what steps need to be taken to ensure continued smooth operation of SecurTrac when installed on Domino 14.

## **Enable running Domino using a non-admin user ID in Domino 14 – Windows platform.**

HCL Software has made some important changes as it relates to how Domino 14 operates on the Windows Server Platform. As part of the "ongoing work to continuously improve security for Domino", HCL has updated the Windows installer to configure Domino to run using a non-admin user ID by default. Most notably, starting in Domino 14, the Domino Windows service will now use "NT Authority\Local Service" non-admin user ID instead of using a local System account, which was considered the standard Windows service configuration for Domino prior to Domino 14. Use of the default non-admin user ID "NT Authority\LocalService", is not mandatory and there is the option of changing the Domino Windows service to start using any valid Windows non-admin user ID instead.

### **Domino 14 – Windows Service Default Configuration:**



## **What are the SecurTrac pre-requisites for installation on Domino 14?**

SecurTrac version 2.6.2 is the minimum requirement for running SecurTrac on Domino 14. This includes both the Windows & Linux platform. If you are running an earlier version of SecurTrac, you will need to upgrade to SecurTrac 2.6.2. after upgrading to Domino 14. Upgrades are included with Extracomm Maintenance Plus plans. If your company does not currently have an active maintenance plan for SecurTrac, consult your Extracomm Reseller or your Extracomm Sales Channel Manager for more information in order to renew the SecurTrac Maintenance Plan and receive upgrade entitlement.

## **How is SecurTrac impacted by the new default Windows service security settings in Domino 14 on Windows Server platform?**

The fundamental change that has been introduced in Domino 14 Windows platform, where Domino is now configured to run by default with a non-admin user ID can impact existing installations of SecurTrac, where Domino prior to being upgraded to Domino 14, had been configured to run using a Local System account instead.

Windows Security permissions assigned to the SecurTrac data Folder and its file contents, in addition to the SecurTrac sctwork Folder may no longer have the required permissions needed. As a result, normal operation of SecurTrac could be impacted.

## **Domino server notes.ini location: Another fundamental change in Domino 14 that may have an impact on SecurTrac.**

Another notable change introduced in Domino 14 – Windows platform, is that the Domino server notes.ini is now located in the Domino Data folder instead of the Domino program folder. In order for SecurTrac to be able to monitor the Domino server notes.ini, during the SecurTrac 2.6.2 installation on Domino 14, the SecurTrac installer will attempt to detect the notes.ini location. During the SecurTrac 2.6.2 installation process, be sure to validate that the location of the Domino server notes.ini has been correctly detected. If needed, it is possible to manually specify the folder location of the Domino server notes.ini during the SecurTrac 2.6.2. installation process. Failure to specify the correct location of the Domino server notes.ini during the SecurTrac 2.6.2 installation process, may result in SecurTrac not being able to monitor Domino server notes.ini changes.

## SecurTrac installation scenario considerations for Domino 14 – Windows platform.

### Install SecurTrac on Domino 14 running as a non-admin user ID:

In this installation scenario, it is assumed that SecurTrac is being installed on the designated Domino server for the first time and that there is no previous existence of SecurTrac on the Domino server. The SecurTrac 2.6.2 installer will automatically set folder/file permissions needed for SecurTrac to run normally when Domino 14 is configured to run using the default **Local Service** non-admin user ID. However, if Domino 14 is configured to run using a different non-admin user ID, other than the default **Local Service** ID, granting permission to the SecurTrac related folders will need to be done manually. Please refer to section in this document titled “Manually granting security permissions for SecurTrac on Domino 14 Windows platform” for specific instructions. Failure to adjust security permissions as needed may result in SecurTrac not functioning normally and as a result Domino server activity that would normally be logged by SecurTrac could potentially not be detected and/or logged by SecurTrac.

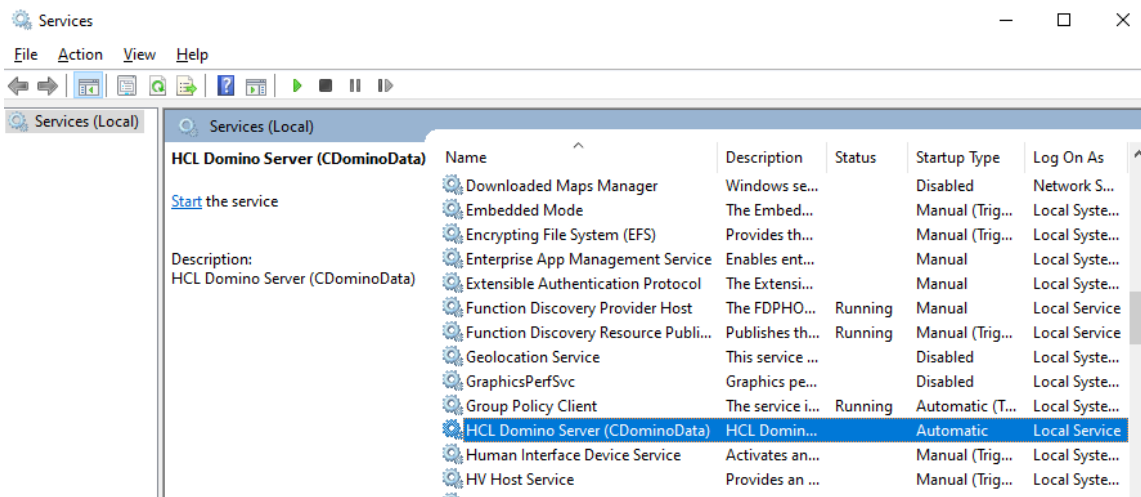
### Upgrading SecurTrac on Domino 14 running as a non-admin user ID:

In this installation scenario, it is assumed that a version of SecurTrac prior to SecurTrac 2.6.2 is already installed on the particular Domino server that has just been upgraded to Domino 14 . The SecurTrac 2.6.2 installer will automatically set folder/file permissions needed for SecurTrac to run normally when Domino 14 is configured to run using the default **Local Service** non-admin user ID. However, if Domino 14 is configured to run using a different non-admin user ID, other than the default **Local Service** ID, granting permission to the SecurTrac related directories will need to be done manually. Please refer to section in this document titled “Manually granting security permissions for SecurTrac on Domino 14 Windows platform” for specific instructions. Failure to adjust security permissions as needed may result in SecurTrac not functioning normally and as a result Domino server activity that would normally be logged by SecurTrac could potentially not be detected and/or logged by SecurTrac.

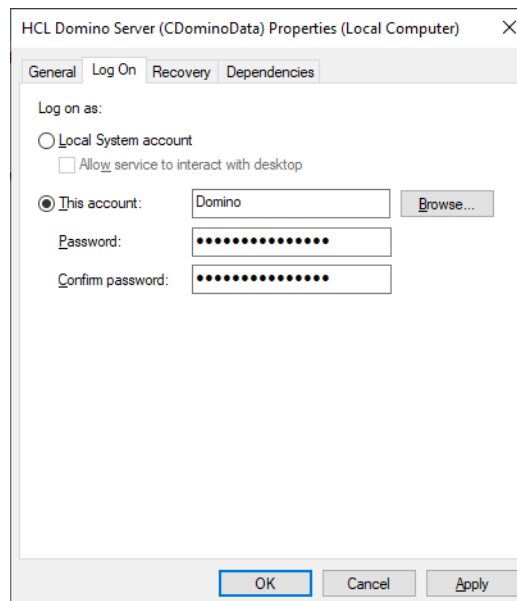
## Manually granting security permissions for SecurTrac on Domino 14 Windows platform:

- 1) To begin the process, launch the Windows Services applet (Services.msc) and locate the service entry for the HCL Domino Server and then view its properties.

### Windows Services List:



### HCL Domino Server – Services Properties



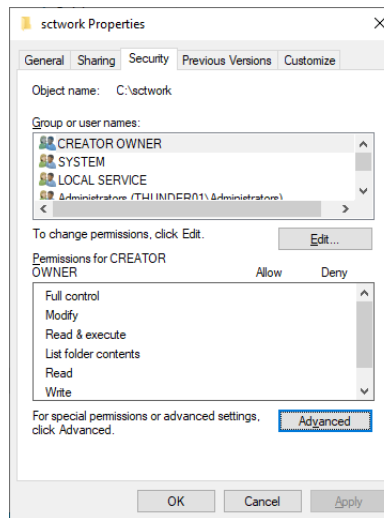
- 2) From the Log On tab, take note of the non-admin user ID that has been specified to start the HCL Domino Server service with. In this case, "Domino" is the user ID that has been specified in place of the default "Local Service" ID that would normally have been configured in a default Domino installation.

- 3) Configuring the folder properties can be accomplished using the GUI of Windows and can also be accomplished using command line parameters. Both methods are described in this document.

## Configuring Security permissions using the Windows GUI:

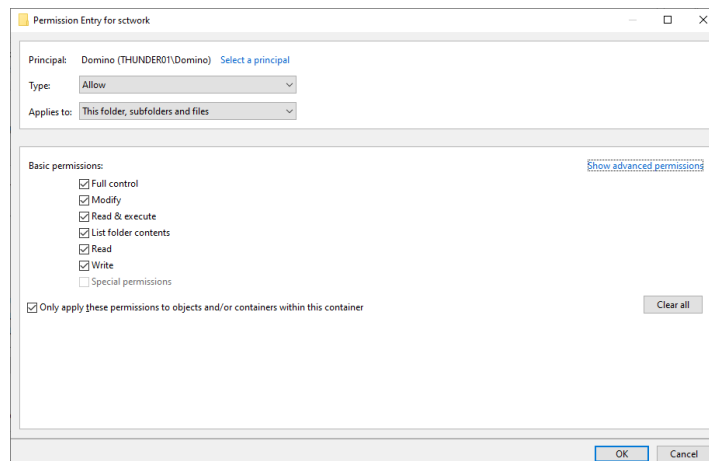
- 1) To configure the security settings using the GUI, next, proceed to open Windows Explorer on the Windows server where Domino is installed and locate the SecurTrac “sctwork” folder, which defaults to C:\sctwork. To identify the location of the sctwork folder on your server, verify the notes.ini parameter SCTWorkFolder. Once the folder location has been identified, in Windows Explorer, view its properties, and then select the **Security** tab and select the **Advanced** button.

### sctwork Folder – Security properties



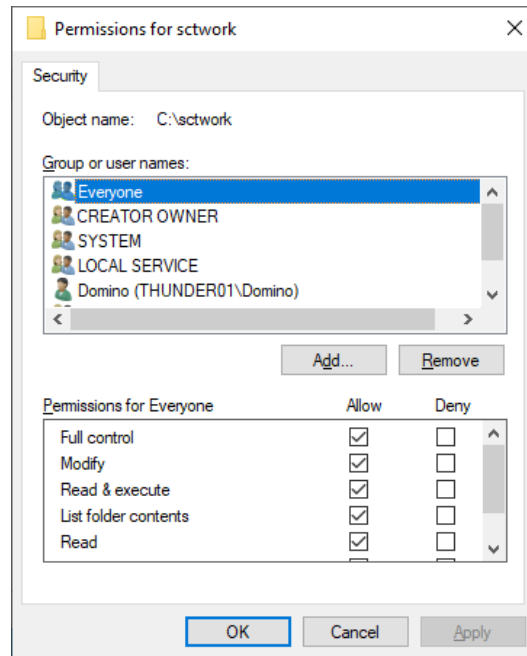
- 2) From the advanced permissions screen, choose **Select a principal** and specify the user ID name identified from the HCL Domino services properties page. In this example, the user ID was identified as “Domino”.
- 3) Grant the appropriate user ID e.g. “Domino” **Full Control** and select “**Only apply these permissions to objects and/or containers within this container**”. Click **OK** and **Apply**.

### sctwork Folder – Advanced Security properties



- 4) While back on the sctwork properties screen, verify if the group “Everyone” exists and if it does, select it and remove its access and then select **Apply** and **OK**.

### **sctwork Folder – Security properties**



- 5) Now, with all folder & file permissions correctly set, when the Domino server is now started, SecurTrac 2.6.2 will resume functioning normally.

### **Configuring Security permissions using command line parameters:**

- 1) Open a Command prompt using elevated Admin privileges and type the following command to set the security permissions to the SecurTrac sctwork folder for the designated non-admin user ID used to start the Domino Windows service as was identified in Step 1 on Page 5.

\*\*\* Grant Domino non-admin user ID full control of sctwork folder and remove access for the Everyone group \*\*\* If the sctwork folder is in a different location, update the command line parameter accordingly.

```
icacls "c:\sctwork" /grant Domino:(OI)(CI)(F)
```

```
icacls "c:\sctwork" /remove:g Everyone /t /c /q
```

- 2) Now, with all folder & file permissions correctly set, when the Domino server is now started, SecurTrac 2.6.2 will resume functioning normally.



## Troubleshooting SecurTrac problems on Domino 14 – Windows platform:

If you suspect that SecurTrac 2.6.2 is not functioning normally on Domino 14 since using "NT Authority\Local Service" or another non-admin user ID to start the HCL Domino service, go ahead and verify that folder/file permissions for the sctwork folder are correctly assigned to include access for the "NT Authority\Local Service" or the other designated non-admin user ID. If you encounter any problems, reach out to Extracomm Technical Support for assistance.



Extracomm Inc.

1730 McPherson Court Unit 6

Pickering, Ontario

Canada, L1W 3E6

Tel: 905-709-8602

Fax: 905-709-8604

<http://www.extracomm.com>

*Product names, logos, brands, and other trademarks featured or referred to within this document are the property of their respective trademark holders.*