everbridge
redsky

Enhanced Onsite Notification (EON) Windows Deployment Guide

An Everbridge Product

September 2025

RedSky Technologies, Inc.
2025
Printed in the USA.

©2025 by RedSky Technologies, Inc., All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of RedSky Technologies, Inc., except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

MyE911®, E911 Anywhere®, and Horizon Mobility® are registered trademarks of RedSky Technologies, Inc.

Introduction **4**
About Us 4
Scope 4
Requirements 5
Creating the Modified Transform File **6**
Component Table 7
CreateFolder Table 8
Directory Table 9
FeatureComponents Table 10
Sample Properties File 11
File Table 12
Media Table 14
MsiFileHash Table 15
Running a Validation Test 16
Generate Transform 18
Deploy Using Windows Group Policy **19**
Deploying to Network-Connected Computers 20
Deploying to Remote Computers 24
Troubleshooting **29**
Checking Group Policy 29
Reviewing Policy Reports 29
Forcing Group Policy Updates 29
Verifying EON® Installer Configuration 29

Introduction

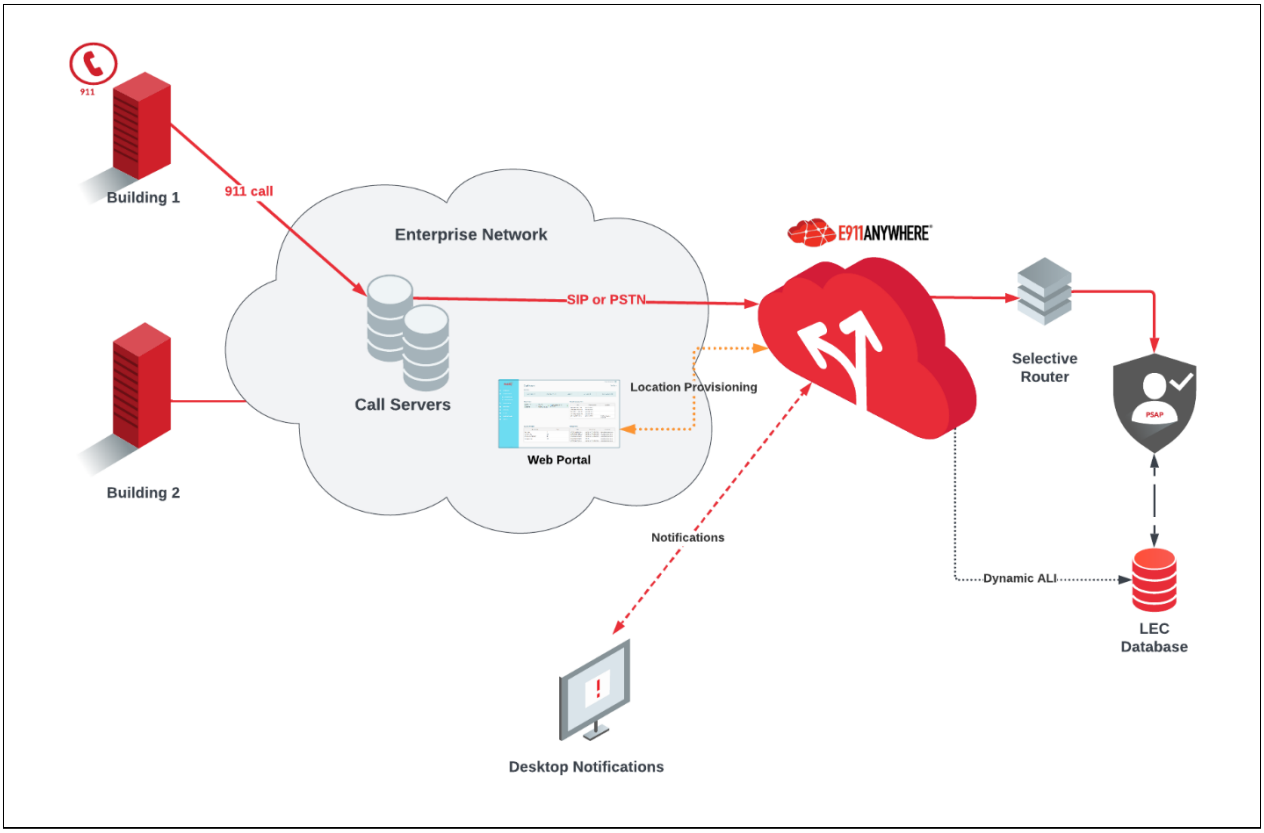
About Us

RedSky Technologies is the leading provider of on-premise and cloud-based E911 solutions. In 1999, we developed and patented the first automated software application to manage 911 location data. As technology has evolved, we have kept pace with emerging voice technology to meet the requirements of modern enterprises. Our E911 enterprise-class software is used by 50 of the Fortune 500 companies. Using state-of-the-art software development languages and frameworks, our solutions are designed to run in the most secure enterprise, government and virtual environments.

Scope

This guide is intended to provide the steps needed to deploy EON Client 4.x to Windows computers using **Group Policy** in **Active Directory**.

EON is a feature in E911 Anywhere® that detects emergency calls. When an emergency call is placed, EON sends designated individuals screen-pop notifications with the complete location record of the caller.



Requirements

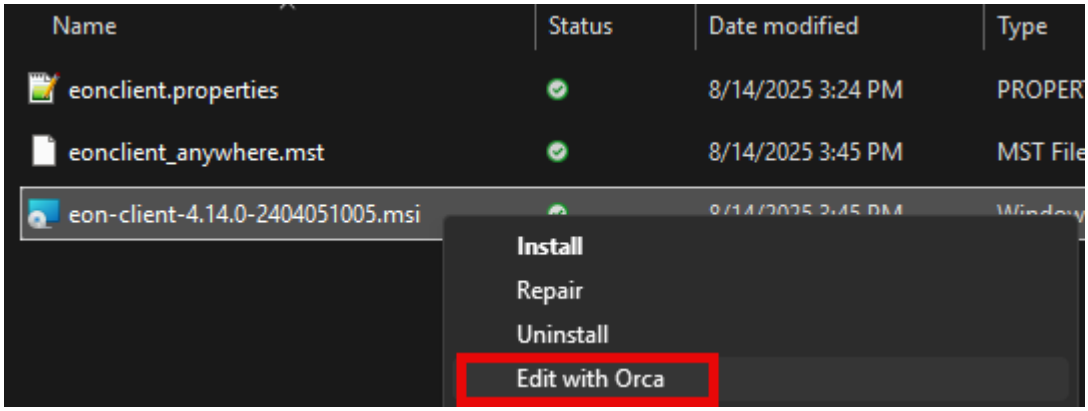
The following items are needed to deploy EON:

1. Latest **EON Client 4.x installation file**.
2. Modified **eonclient.properties file** (See Sample Properties File).
3. Database table editor for creating and editing Windows Installer packages and merge modules.
    - Orca.exe is used in the following procedure.
4. **Active Directory** implemented.

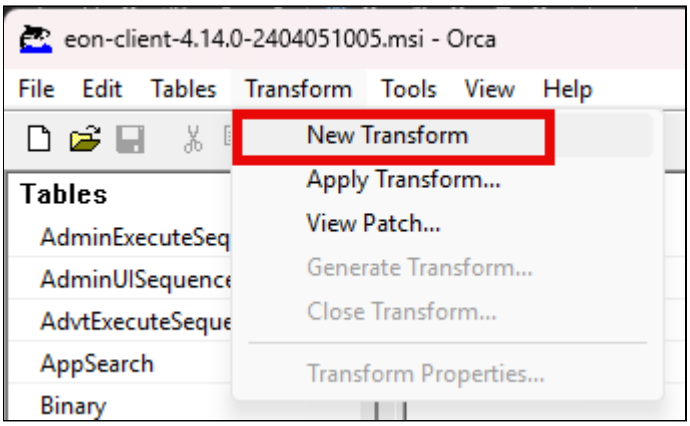
Creating the Modified Transform File

To create the Modified MST Transform File:

1. Open the MSI file with Orca by right-clicking on the file and selecting **Edit with Orca**.



2. Create a new transform file by selecting **Transform** from the menu bar, and then **New transform**.



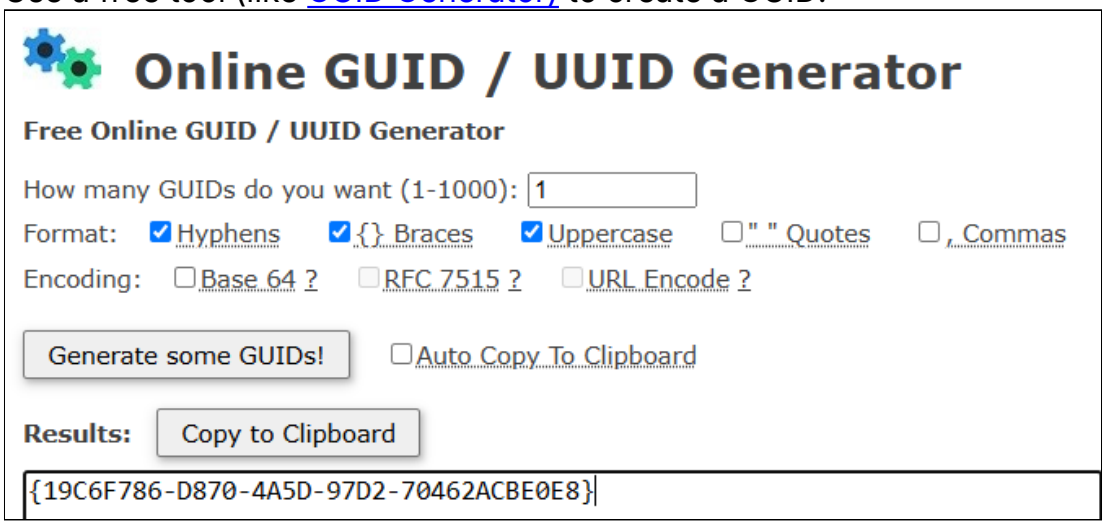
The following tables must be modified:

- Component
- CreateFolder
- Directory
- FeatureComponents
- File
- Media
- MSIFileHash

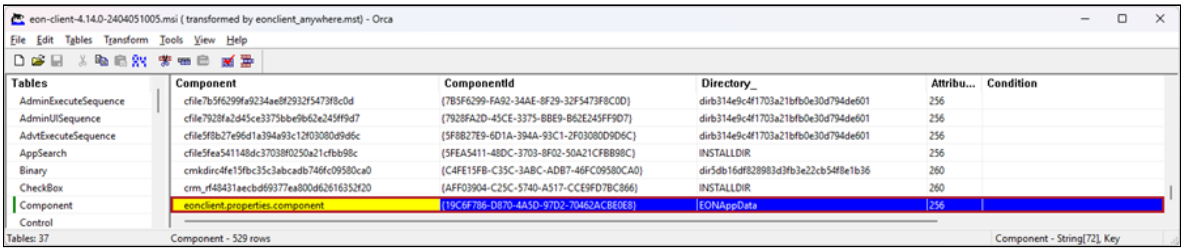
Component Table

To modify the **Component** table:

1. Generate a **Global Unique Identifier (GUID)** with upper case letters, curly braces {}, and hyphens.
   a. Use a free tool (like GUID Generator) to create a GUID.



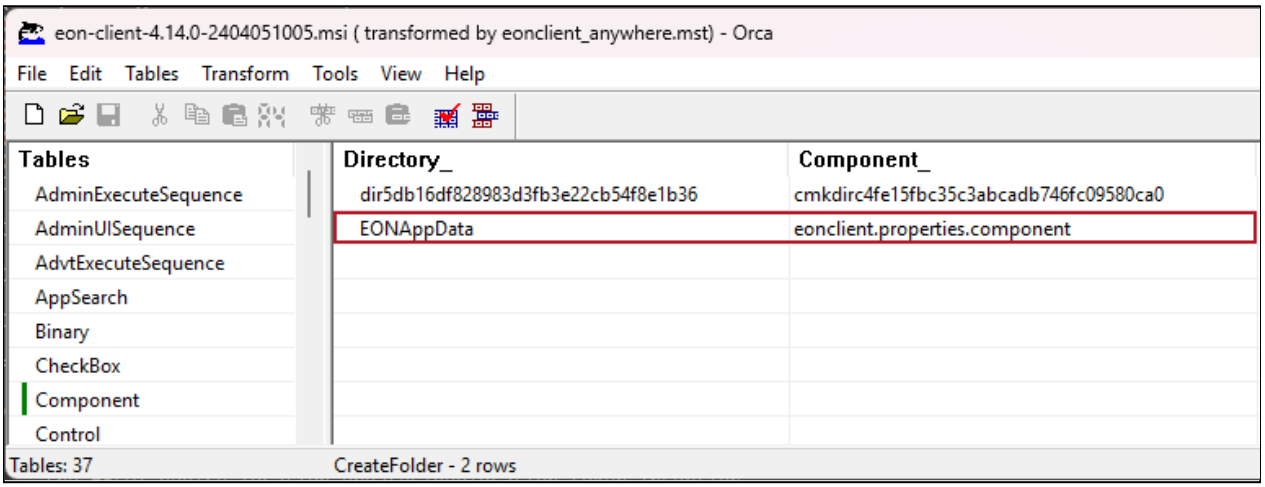
   b. Copy the generated GUID.
2. In Orca, select the **Component** table in the left-hand column.
3. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
   a. **Component** - Enter the name you will use to reference the new component. This must be unique, and it is a key field.
      - Example: eonclient.properties.component
   b. **ComponentId**: This is the GUID created above.
   c. **Directory_**: EONAppData
      - We will need to create the directory where the **eonclient.properties** file will be installed in.
      - This references a key in the **Directory** table. This will be the directory the component is installed in. The **Directory Key** should reference the app directory.
   d. **Attributes**: 256
      - Mark this as a 64-bit component.
4. No other information is needed. Click **OK**.



CreateFolder Table

To modify the **CreateFolder** table:

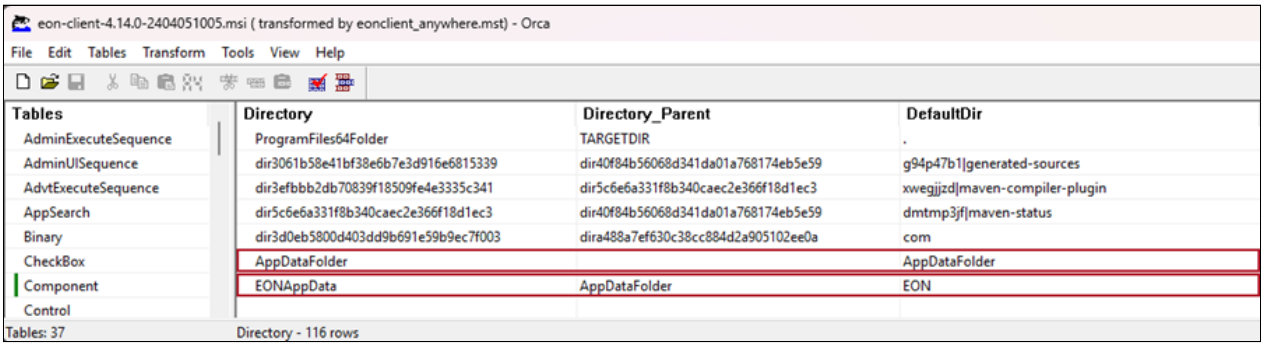
1. Select the **CreateFolder** table in the left-hand column.
2. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
    - **Directory_**: EONAppData
        - This should match the **Directory_** value in Step 3 of Component Table.
    - **Component_**: Name of the **Component** created in Step 3 of Component Table.
        - Example: eonclient.properties.component



Directory Table

To modify the **Directory** table:

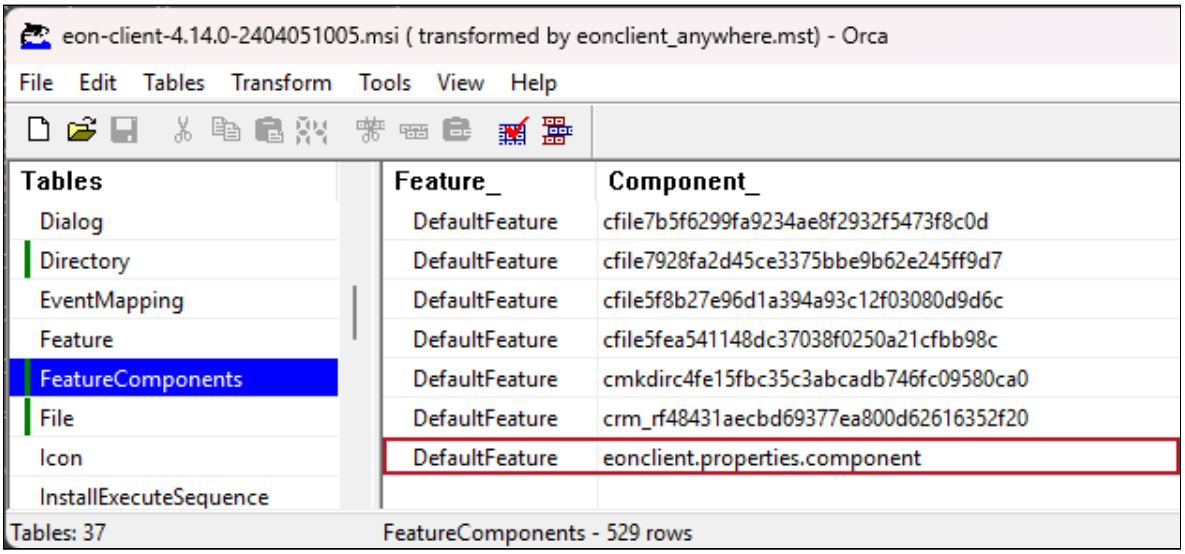
1. Select the **Directory** table in the left-hand column
2. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
    - **Directory**: AppDataFolder
    - **Directory_Parent**: <leave blank>
    - **DefaultDir**: DefaultDir
3. Create a second entry in the table by right-clicking in the right-side pane and selecting **Add Row**. Fill in the dialog box with the following information:
    - **Directory**: EONAppData
    - **Directory_Parent**: AppDataFolder
    - **DefaultDir**: EON



FeatureComponents Table

To modify the **FeatureComponents** table:

1. Select the **FeatureComponent** table in the left-hand column
2. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
    - **Feature_**: DefaultFeature
        - An existing feature in the MSI.
    - **Component_**: Name of the Component created in Step 3 of Component Table.
        - Example: eonclient.properties.component
3. Click **OK**.



Sample Properties File

Copy and paste the below text into Notepad and save the file as "eonclient.properties" in the same folder as the EON® installer:

```
#
#Thu Aug 14 15:13:10 CDT 2025
usingCertificates=false
needsUpdate=false
debug=false
encryptedCertPassword=
proxyUsername=
receiveNonEmergencyCallData=false
proxyPassword=
primaryServer=https\://anywhere.e911cloud.com
useProxy=false
proxyHost=
backupServer=http\://
proxyPort=0
password=
proxyDomain=
sirenMuted=false
sirenVolume=1.0
certificateLocation=
useSystemProxy=true
username=
skippedUpdate=null
```

IMPORTANT: The **eonclient.properties** file must be saved as a **.properties** file type.

Modify the **primaryServer** values to the E911 Anywhere® URL used in your environment. For example:

- primaryServer=https\://anywhere.redskytech.com
- primaryServer=https\://wxc.e911cloud.com
- primaryServer=https\://horizon.e911cloud.com

File Table

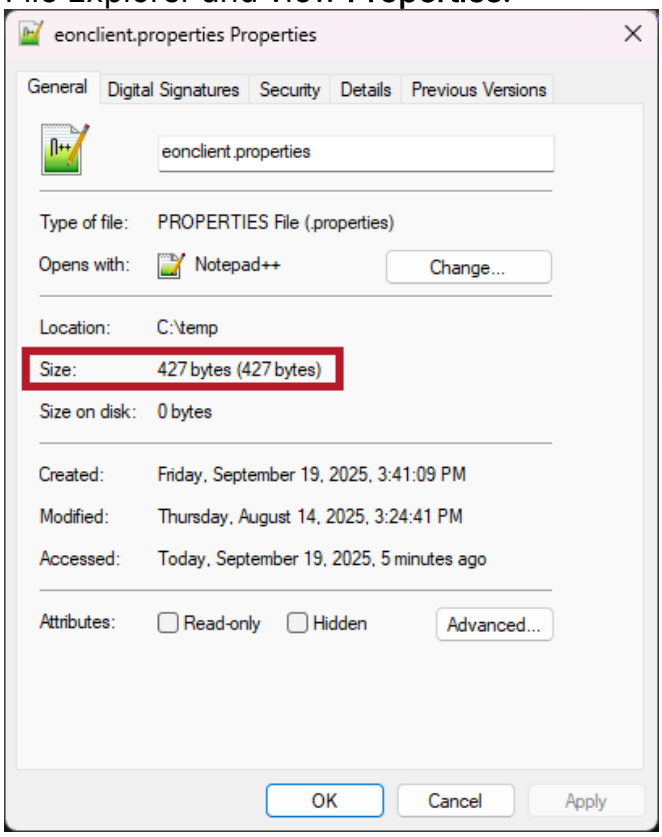
This is where we associate the new component with the **eonclient.properties** file created in Sample Properties File. To do this:

1. Select the **File** table in the left-hand column.
2. Click on the **Sequence** column to sort table in ascending order.
3. Find the largest Sequence number. The new row will have the next Sequence number.
4. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
    - **File**: eonclient.properties
        - This field should match the eonclient.properties file name created from Sample Properties File.
    - **Component_**: This is the Component created in created in Step 3 of Component Table.
        - Example: eonclient.properties.component
    - **FileName**: File identifier
        - E.g., EONCLI~1.PRO|eonclient.properties
        - If the file name does not follow 8.3 short name notation, you will need to enter both the short file name and the long file name separated by vertical bar (|). To find the short file name, open a command prompt, change directory to the location of the eonclient.properties file and run the following command:
            - dir /x

```
C:\>cd C:\temp

C:\temp>dir /x
 Volume in drive C is OS
 Volume Serial Number is 9660-49EE

 Directory of C:\temp

09/19/2025  03:41 PM    <DIR>          .
08/14/2025  03:24 PM               427 EONCLI~1.PRO eonclient.properties
               1 File(s)            427 bytes
               1 Dir(s)  36,254,248,960 bytes free
```

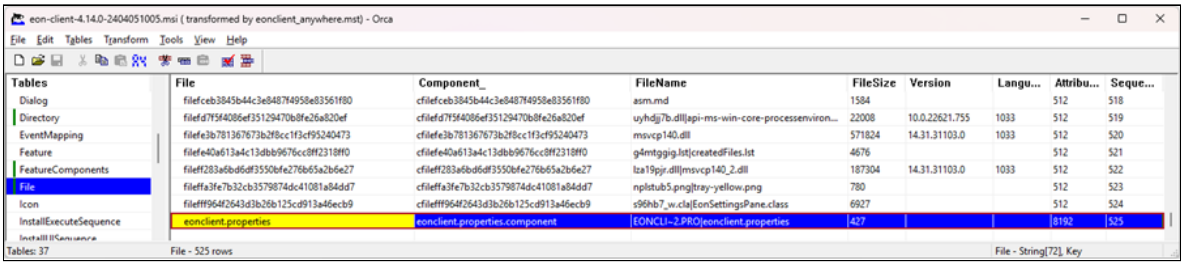
    - **FileSize**: The size of the eonclient.properties file in bytes.

- To determine file size, right click on the **eonclient.properties** file in File Explorer and view **Properties**.



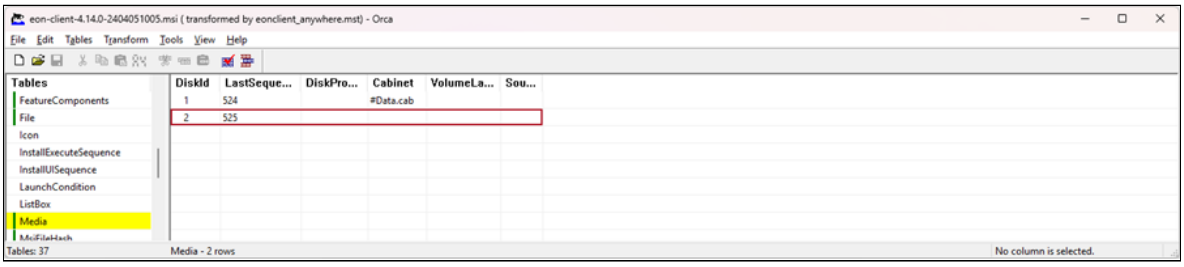
- **Version:** (leave blank)
- **Language:** (leave blank)
- **Attributes:** 8192
- **Sequence:** The next Sequence number in the table.
  - Example: If the last sequence number was 524, enter 525.

5. Click **OK.**



Media Table

1. Select the **Media** table in the left-hand column.
2. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
    - **DiskId**: The next sequential number in the **DiskID** column.
    - **LastSequence**: The Sequence number added in the **File** table.
        - Eg. 525
3. Click **OK**.

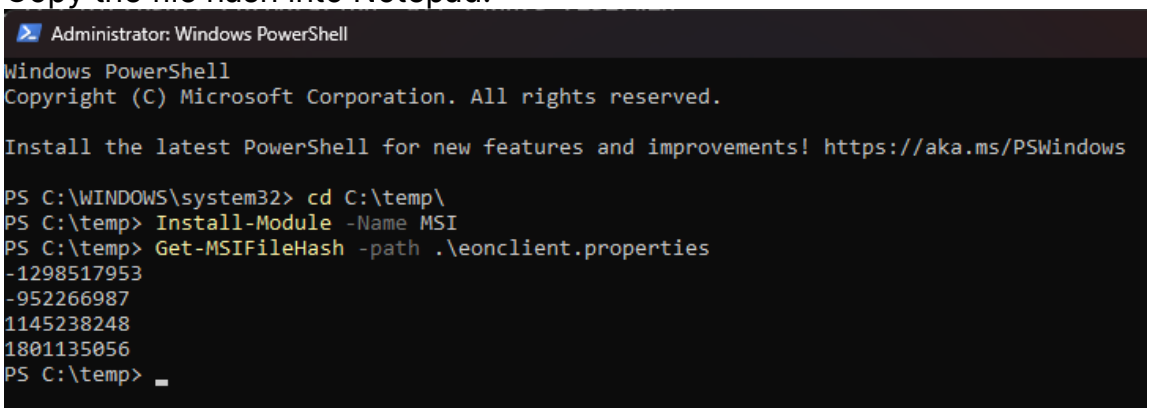


MsiFileHash Table

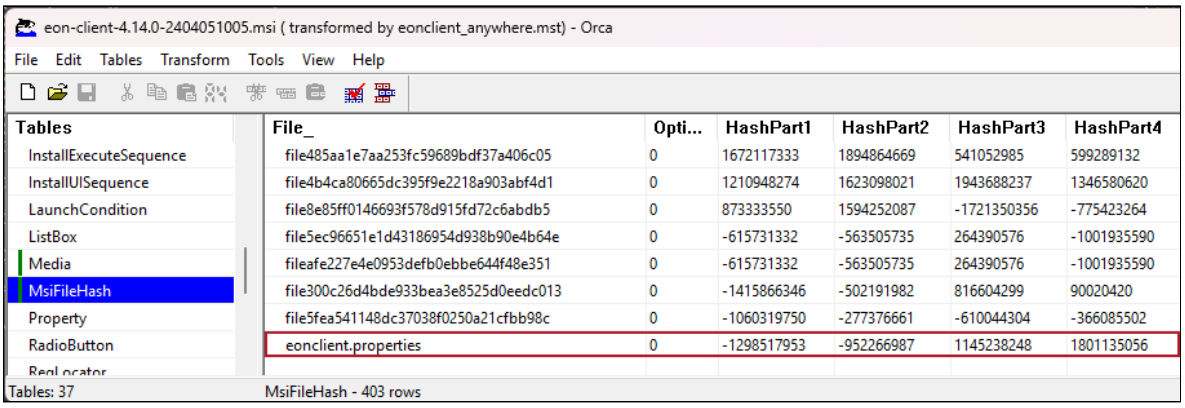
To modify the **MsiFileHash** table:

1. Open an elevated PowerShell window and change directory to the location of the **eonclient.properties file**.
2. Enter the following commands:
   a.
   ```
   Install-Module -Name MSI
   ```
   - Enter "A" to install the untrusted module if prompted.

   b.
   ```
   Get-MSIFileHash -path .\eonclient.properties
   ```
3. Copy the file hash into Notepad.



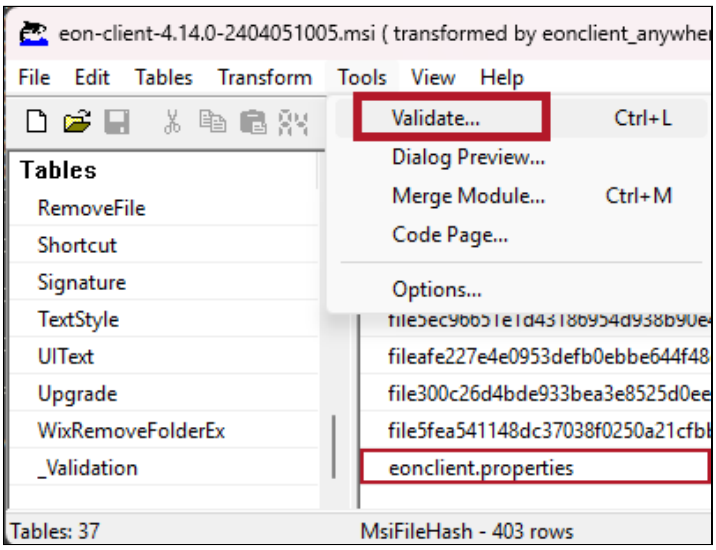
4. In Orca, select the **MsiFileHash** table in the left-hand column.
5. Right-click in the right-side pane and select **Add Row**. Fill in the dialog box with the following information:
   - **File_**: eonclient.properties
   - **Options**: 0
   - **HashPart1 - HashPart4**: Enter the hash numbers returned by the PowerShell command.
6. Click **OK**.



Running a Validation Test

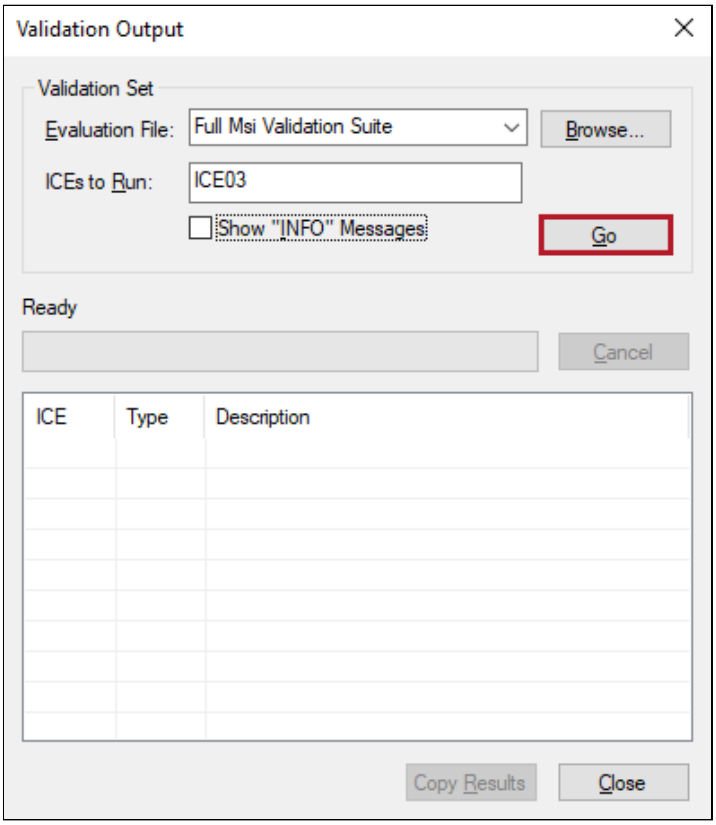
Run a validation test to ensure there are no syntax errors. To do this:

1. Select **Tools** from the menu bar and then **Validate**.



2. The **Validation Output** window will open. Fill in the following information:
   - **Evaluation File**: Full Msi Validation Suite
   - **ICEs to Run**: ICE03
   - **Show "INFO" Messages**: Uncheck the box

3. Click **Go**.

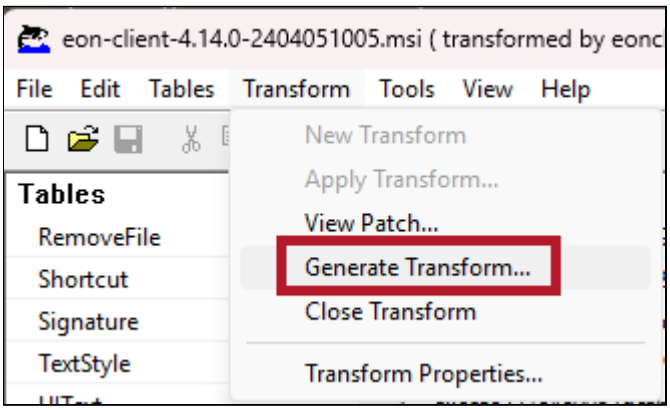


4. Review the results to ensure there are no errors. Correct any errors before proceeding.
5. Close **Validation Output** window.

Generate Transform

To generate the Transform file:

1. Select **Transform** from the menu bar and then **Generate Transform**.



2. Browse to the folder to save the file in and provide a name for the transform file.
3. Exit the Orca editor.

Deploy Using Windows Group Policy

Windows Group Policy can be used to distribute the EON® client using the following methods. The methods differ when computers are always joined to the enterprise network or when a remote user must initiate a virtual private network (VPN) connection to the enterprise network on-demand.

For computers that are connected to the enterprise network upon startup, see Deploying to Network-Connected Computers.

For remote computers that connect to the enterprise network through a separate VPN client, see Deploying to Remote Computers.

Deploying to Network-Connected Computers

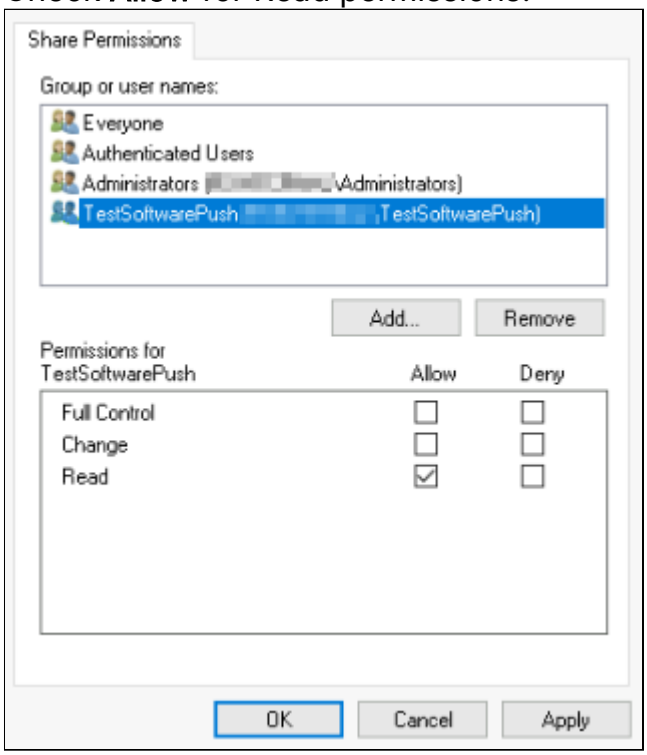
Use the following steps to install EON® on computers that are connected to the enterprise network upon startup.

Creating a Distribution Point

To ceate a distribution point:

1. Log on to the domain controller as an administrator.
2. Create a shared network folder that will contain the **EON® Installer package** (.msi file), **transform file** (.mst file), and **eonclient.properties** files to be deployed.
3. Set permissions on the shared folder to allow access to the distribution package.
    a. Right-click folder and select **Properties**.
    b. Click the **Sharing** tab.
    c. Click **Advanced Sharing**.
    d. Select the **Share this folder** checkbox.
    e. Provide a **Share name** and click **Permissions**.
    f. Add and Select only the group(s) of computers/users EON® will be installed for.

- Check **Allow** for Read permissions.



g. Click **OK** to save all changes.
   - Note the **Network Path** of the folder in the **Sharing** tab.

h. Click **OK** to close the folder properties.

4. Copy the EON® **installer package**, **transform file**, and **eonclient.properties** file to the newly created distribution point.

Creating a Group Policy Object

To create a Group Policy Object (GPO):

1. Start the **Group Policy Management snap-in**.
   a. Click **Start**.
   b. Point to **Windows Administrative Tools**.
   c. Click **Group Policy Management**.
2. In the console tree, navigate to your domain, and expand the options below the domain.
3. Right-click on **Group Policy Objects**, and then click **New**.
   - **Source Start GPO** can be left to (none).
4. Type a name for this new policy (e.g. RedSky Software), and then click **OK**.

Assign Security Group Filters to the GPO

To assign Security Group Filters to the GPO:

1. In the **Group Policy Management** window, expand the **Group Policy Objects** folder in the left pane.
2. Click on the newly-created group policy object in the **Group Policy Objects** folder
3. Optionally, in the **Scope** tab, under **Security Filtering**, click **Authenticated Users**, and then click **Remove**.
    - **Note**: You must remove the default permission granted to all authenticated users and computers to restrict the GPO to only the groups you specify.
4. Click **Add**.
5. In the **Select User, Computer, or Group** dialog box, type the name of the group whose members are to apply the GPO, and then click **OK**.
    - If you do not know the name, you can click **Advanced** to browse the list of groups available in the domain.
6. In the **Group Policy Management snap-in**, navigate to the Site/Domain/OU that you want to apply the GPO to, right-click on the folder from the left-side pane and select **Link an existing GPO**.

Assigning a Package

To assign a package:

1. Right-click on the newly-created GPO, then click **Edit**.
2. Navigate to **Computer Configuration** > **Policies** and expand **Software Settings**.
3. Right-click on **Software Installation** and select **Properties**.
4. In the **General** tab, click on **Advanced** under the **New packages** section.
5. Click **OK**.
6. Right-click **Software installation**, point to **New**, and then click **Package**.
7. In the **Open** dialog box, type the full **Universal Naming Convention** (UNC) path of the shared installer package (e.g. \\file server\share\filename.msi). See Step 3g of Creating a Distribution Point.
    - **Important**: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared installer package.
8. Select the file and click **Open**.
9. Under the **Deployment** tab, click **Assigned**.
10. Under the **Modifications** tab, Click **Add**.
11. In the **Open** dialog box, type the full UNC path of the shared transform file (e.g. \\file server\share\filename.mst). See Step 3g of Creating a Distribution Point.
    - **Important**: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared transform file.
12. Select the file and click **Open**.
13. Click **OK**.

14. The package is listed in the right-pane of the **Group Policy Management Editor** window.
15. Close the **Group Policy Management Editor**.
16. Close the **Group Policy Management** snap-in.
17. After the group policies have replicated between domain controllers, when the client computer starts, the managed software package is automatically installed.

> **NOTE:** Multiple reboots may be required.

Deploying to Remote Computers

Use the following steps to install EON® for remote computers that connect to the enterprise network through a separate VPN client.

Creating a Batch File to Deploy EON®

The following steps will copy the EON® installation file and batch file to target computers and will execute the batch script to locally install EON®.

1. Open a new Notepad file.
2. Paste the following text into the blank file:

```
IF EXIST "C:\Program Files\EON\EON.exe" (
    GOTO :eof
) ELSE (
    msiexec.exe /i "C:\Temp\<EON Installation File>" /qn TRANSFORMS="C:
\Temp\<EON Transform File>"
)

:eof

END && EXIT
```

   Example batch:

```
IF EXIST "C:\Program Files\EON\EON.exe" (
    GOTO :eof
) ELSE (
    msiexec.exe /i "C:\Temp\eon-client-4.14.0-2404051005.msi" /qn
TRANSFORMS="C:\Temp\eonclient_anywhere.mst"
)

:eof

END && EXIT
```

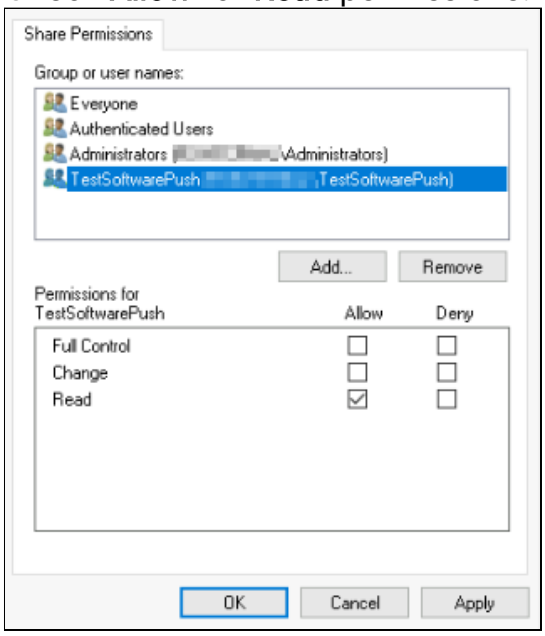
   - **Note**: The batch file looks to see if EON® has been installed on the workstation. If the EON® executable file is present, the installation command is skipped. If EON® has not already been installed, the installation command will be run.
3. Save the Notepad file as **EON.bat**.

Creating a Distribution Point

To create a distribution point:

1. Log on to the domain controller as an administrator.

2. Create a shared network folder that will contain the **EON® Installer package** (.msi file), **transform file** (.mst), **batch file** (.bat file), and **eonclient.properties file** to be deployed.
3. Set permissions on the share to allow access to the distribution package:
    a. Right-click folder and select **Properties**.
    b. Click on **Sharing** tab.
    c. Click on **Advanced Sharing**.
    d. Select the **Share this folder** checkbox.
    e. Provide a **Share name** and click **Permissions**.
    f. **Add** and **Select** only the group(s) of computers/users EON® will be installed for.
        - Check **Allow** for **Read** permissions.



    g. Click **OK** to save all changes.
        - Note the **Network Path** of the folder in the **Sharing** tab.
    h. Click **Close** to close the folder properties.
4. Copy the **EON® installer package**, **transform file**, **batch file**, and **eonclient.properties** file to the newly-created distribution point.

Creating a Group Policy Object

To create a **Group Policy Object** (GPO):

1. Start the **Group Policy Management snap-in**.
    a. Click **Start**.
    b. Point to **Windows Administrative Tools**.
    c. Click **Group Policy Management**.
2. In the console tree, navigate to your domain, and expand the options below the domain.
3. Right-click on **Group Policy Objects**, and then click **New**.

- **Source Start GPO** can be left to (none).

4. Type a name for this new policy (e.g. "RedSky Software"), and then press **Enter**.

Assigning Security Group Filters to the GPO

To assign **Security Group Filters** to the GPO:

1. In the **Group Policy Management** window, expand the **Group Policy Objects** folder in the left pane.
2. Click on the newly-created GPO in the **Group Policy Objects** folder.
3. (Optional) In the **Details** pane, under **Security Filtering**, click **Authenticated Users**, and then click **Remove**.
   - **Note**: You must remove the default permission granted to all authenticated users and computers to restrict the GPO to only the groups you specify.
4. Click **Add**.
5. In the **Select User, Computer, or Group** dialog box, type the name of the group whose members are to apply the GPO, and then click **OK**.
   - If you do not know the name, you can click **Advanced** to browse the list of groups available in the domain.
6. In the **Group Policy Management** window, navigate to the Site/Domain/OU that you want to apply the GPO to, right-click on the folder from the left-side pane and select **Link an existing GPO**.

Configure Group Policy Preferences

To configure the Group Policy Preferences:

1. Right-click on the newly-created GPO, and then click **Edit**.
2. Navigate to **Computer Configuration** > **Preferences** and expand **Windows Settings**.
3. Right-click on **Files**, point to **New**, and then click **File**.
4. In the **Open** dialog box, select the following:
   a. **Action**: Update
   b. **Source file(s)**: Type the full **Universal Naming Convention** (UNC) path of the shared installer package.
      - **Important**: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared installer package (e.g. \\file server\share\ eon-client-4.14.0-2404051005.msi). See Step 3g of Creating a Distribution Point.
   c. **Destination File**: C:\Temp\<EON installation file>
5. Click **OK**.
6. Right-click **Files**, point to **New**, and then click **File**.
7. In the **Open** dialog box, select the following:

   a. **Action**: Update
   b. **Source file(s)**: Type the full Universal Naming Convention (UNC) path of the generated transform file.
      - **Important**: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared transform file (e.g. \\file server\share\eonclient_anywhere.mst). See Step 3g of Creating a Distribution Point.
   c. **Destination File**: C:\Temp\<EON transform file>
8. Click **OK**.
9. Right-click **Files**, point to **New**, and then click **File**.
10. In the **Open** dialog box, select the following:
   a. **Action**: Update
   b. **Source file(s)**: Type the full Universal Naming Convention (UNC) path of the batch file created in Creating a Batch File to Deploy EON®.
      - **Important**: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared batch file (e.g. \\file server\share\EON.bat). See Step 3g of Creating a Distribution Point.
   c. **Destination File**: C:\Temp\EON.bat
11. Right-click **Files**, point to **New**, and then click **File**.
12. In the **Open** dialog box, select the following:
   a. **Action**: Update
   b. **Source file(s)**: Type the full Universal Naming Convention (UNC) path of the modified eonclient.properties file.
      - **Important**: Do not use the **Browse** button to access the location. Make sure that you use the UNC path of the shared **eonclient.properties file** (e.g. \\file server\share\eonclient.properties). See Step 3g of Creating a Distribution Point.
   c. **Destination File**: C:\Temp\eonclient.properties
13. Click **OK**.

Configuring Startup Script to Locally Run Batch File

To configure the startup script to locally run the batch file:

1. In the **Group Policy Management Editor** Window, navigate to: **Computer Configuration** > **Policies** > **Windows Settings** > **Scripts**.
2. In the main window, right-click on **Startup** and select **Properties**.
3. Click **Add**.
4. Enter **Script Name**: C:\Temp\EON.bat.
5. Click **OK** to exit **Add a Script** window.
6. Click **OK** to exit **Startup Properties** window.
7. Close the **Group Policy Management Editor**.
8. Close the **Group Policy Management snap-in**.

9. After the group policies have replicated between domain controllers, when the client computer starts, the managed software package is automatically installed.

> **NOTE:** Multiple reboots may be required.

Verification

To ensure a correct deployment, make sure to:

- Verify that EON® is installed on target computers.
- Verify the optional parameters are configured for EON® by opening the application or verifying the contents of the **eonclient.properties** file in the **%APPDATA%\EON** directory.

Troubleshooting

This section provides commands and tips to diagnose and resolve issues with Group Policy settings and EON® installation.

Checking Group Policy

Run the following command in Command Prompt or PowerShell (must be opened as Administrator):

```
gpresult.exe /SCOPE <USER or COMPUTER> /Z
```

- **/SCOPE** - Displays the applied Group Policy Objects (GPOs) for the user or computer based on the scope you specify.
- **/Z** - Shows in-depth information of the applied GPOs, allowing you to see them in greater detail.

Reviewing Policy Reports

Run the following command to generate a report of applied GPO settings:

```
rsop.msc
```

- Provides administrators with a clear report of which GPOs are applied to users and computers.
- Useful for verifying whether a specific GPO has been applied successfully.

Forcing Group Policy Updates

Use the following command to refresh and apply new policy settings:

```
gpupdate /force
```

- Forces an immediate update of Group Policy Objects.
- New policies are normally applied at startup or when a user logs in.
- A reboot or logging off/on may be required to apply changes fully.

Verifying EON® Installer Configuration

Ensure that the modified **eonclient.properties** file is in the same directory as the **EON® installer** and the **modified transform file**.