MyE911 4.x Windows Deployment Guide

Version 1.3

July 9, 2021

RedSky Technologies, Inc.
333 North Michigan Avenue, Suite 1600
Chicago, IL 60601
www.redskye911.com

Revision History

Date	Version	Revision	Made By
1/27/2020	1.0	Initial Draft	Jen Wilhelm
1/29/2020	1.1	Copyedit	Chelsea Bumpus
1/22/2021	1.2	Added steps for users connecting through VPN client	Dennis Penaranda
7/9/2021	1.3	Added section for Deploying MyE911 using SCCM	Dennis Penaranda

Table of Contents

1. 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.

2. Scope

Overview

This guide is intended to provide the steps to push an installation or upgrade to RedSky's MyE911 PC Client for Windows. Organization Administrators should refer to this guide for questions about creating distribution points, group policy objects, assigning group filters to the GPO and verifying the update.

Point of Contact

To submit recommendations for comments and changes to this manual or the E911 Manager® application, please contact us at:

RedSky Technologies, Inc.
333 North Michigan Avenue, Suite 1600
Chicago, IL 60601
Toll Free: 866-778-2435
Email: support@redskytech.com

3. MyE911 Installer Options

The MyE911 client provides the capability of being able to install silently. In this mode, the user can set the following parameters on the installer command line during an interactive installation. These parameters can be used in conjunction with a centralized deployment system to install MyE911 remotely.

3.1 Parameters supported by the MyE911 Installer

Parameter	Value	Description	Default Value
API	text	Cirrus cloud host (default to https if protocol is absent)	
FREQ	number	How often to scan for network changes	10
LLDP	boolean (true or false)	Enable / Disable LLDP Support. Default is false.	false
LLDP_TIMEOUT	number	For how long to wait on LLDP packets	30
OVERRIDE_PROPERTIES	boolean (true or false)	Properties provided with installer should override existing properties stored at properties file (useful on client updates). Default is false.	false

Values should be specified in lower case values and surrounded by quotes. API is required for new installs. The API will be the domain name of the server the MyE911 Client communicates with.

The OVERRIDE_PROPERTIES parameter is used when you perform an upgrade. By default, if the MyE911 client has been previously installed, the installer will ignore any parameter changes from a pushed update. If you need to update the API value, you will also need to include this parameter and set to true.

3.2 Using the Windows Installer

Using the built-in Windows Installer functionality, the MyE911 Client can be installed unattended. The Windows Installer is launched by using the msiexec application. Must be an administrator to install MyE911 using the command line.

The format for the msiexec command is as follows:

```
C:\>msiexec.exe /i "C:\path-to-file\redsky-mye911-versionnum.msi" /qn
MY_PROP="myValue"
```

The /qn switch means to not display the installer User Interface during installation.

MY_PROP is one of the 5 properties list in section 3.1

3.2.1 New Installation Examples

```
C:\>msiexec.exe /i "C:\path-to-file\redsky-mye911-versionnum.msi" /qn
API="anywhere.e911cloud.com"
```

```
(with LLDP functionality)
```

```
C:\>msiexec.exe /i "C:\path-to-file\redsky-mye911-versionnum.msi" /qn
API="anywhere.e911cloud.com" LLDP=true
```

3.2.2 Update Examples

```
C:\>msiexec.exe /i "C:\path-to-file\redsky-mye911-versionnum.msi" /qn
```

```
C:\>msiexec.exe /i "C:\path-to-file\redsky-mye911-versionnum.msi" /qn
OVERRIDE_PROPERTIES=true FREQ=5
```

4. Using Windows Group Policy

Group Policy can be used to distribute the MyE911 application using the following methods. The methods differ when computers are always joined to the enterprise network or when a remote user must initiate a VPN connection to the enterprise network on-demand.

For computers that are connected to the enterprise network upon startup, follow steps 4.1.1 – 4.1.5:

For remote computers that connect to the enterprise network through a separate VPN client, follow steps 4.2.1 – 4.2.6:

4.1.1 Create a Transform File to Modify Installer Properties

*****Use the following steps to install MyE911 for computers that are connected to the enterprise network upon startup*****

Orca.exe is a database table editor for creating and editing Windows Installer packages and merge modules.

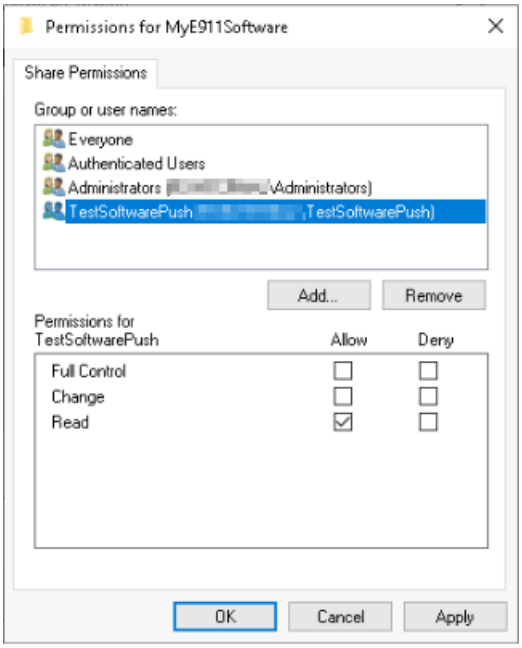
This tool is only available in the Windows SDK Components for Windows Installer Developers. It is provided as an Orca.msi file. After installing the Windows SDK Components for Windows Installer Developers, double click Orca.msi to install the Orca.exe file.

1. Open the MyE911 installer file within Orca.exe
2. Click on Transform > New Transform
3. Click on the '**Property**' Table in the left-hand column
4. Modify desired parameters listed in Section 3.1
    a. Add Row for API to enter URL for Cirrus cloud host
        i. Example URL: anywhere.e911cloud.com
5. Click on Transform > Generate Transform
6. Enter name for transform file and click Save
7. Exit Orca.exe

4.1.2 Create a Distribution Point

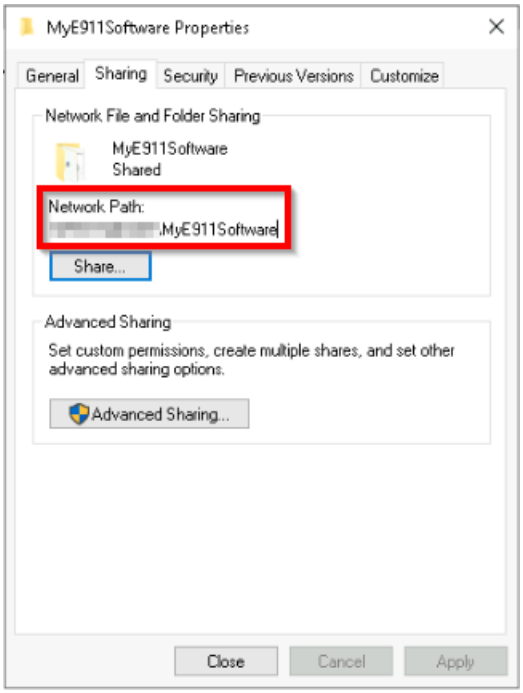
1. Log onto the domain controller as an administrator
2. Create a shared network folder that will contain the MyE911 Installer package (.msi file) and transform file (.mst file) to be deployed
3. Set permissions on the shared folder to allow access to the distribution package
    a. Right-click folder and select 'Properties'
    b. Click on 'Sharing' tab
    c. Click on 'Advanced Sharing'
    d. Click 'Share this folder' checkbox
    e. Provide a Share name and click ‘Permissions’
    f. Add and Select only the group(s) of computers/users MyE911 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 MyE911 installer package and transform file to the newly created distribution point

4.1.3 Create a Group Policy Object

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
   a. Source Start GPO can be left to (none)
4. Type a name for this new policy (e.g. Redsky Software), and then click OK

4.1.4 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. (Optional) In the Scope tab, under Security Filtering, click Authenticated Users, and then click Remove
   a. 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
    a. 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

4.1.5 Assign a package

1. Right-click on the newly created Group Policy Object, and 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. See step 4.1.2.g (e.g. \\file server\share\filename.msi)
    a. 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 Universal Naming Convention (UNC) path of the transform file. See step 4.1.2.g (e.g. \\file server\share\filename.mst).
    a. Important!! **Do not** use the Browse button to access the location. Make sure that you use the UNC path of the 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

4.2.1 Create a Batch File to Deploy MyE911

*****Use the following steps to install MyE911 for remote computers that connect to the enterprise network through a separate VPN client *****

The following steps will copy the MyE911 installation file and batch file to target computers and will execute the batch script to locally install MyE911.

1. Open a new notepad file
2. Paste the following text into the blank file, substituting the appropriate values for:
    a. E911 Anywhere URL
    b. MyE911 Version
    c. PC Network Monitor

```
IF EXIST "C:\Program Files\Redsky\MyE911\<PC Network Monitor>" (
        GOTO :eof
) ELSE (
        msiexec.exe /i "C:\Temp\<MyE911 Version>" /qn API="<E911 Anywhere URL>" LLDP=true
)

:eof

END && EXIT
```

Example Batch File:

```
IF EXIST "C:\Program Files\Redsky\MyE911\pc-network-monitor-4.7.18577.17525.jar" (
        GOTO :eof
) ELSE (
        msiexec.exe /i "C:\Temp\redsky-mye911-4.7.0-2011110942.msi" /qn
API="anywhere.e911cloud.com" LLDP=true
)

:eof

END && EXIT
```

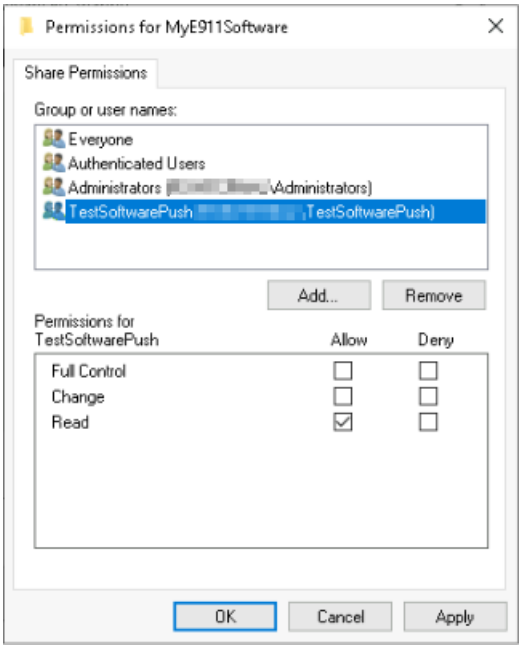
- **Note:** Batch file looks to see if the PC network monitor tool has been installed on the workstation. If PC network monitor is present, the installation command is skipped. If PC network monitor is not present, the installation command will be run.

3. Save notepad file as 'MyE911.bat'

4.2.2 Create a Distribution Point

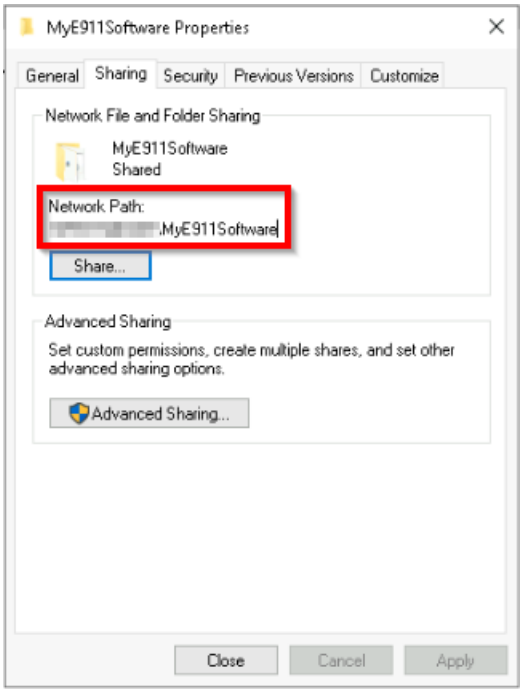
1. Log onto the domain controller as an administrator
2. Create a shared network folder that will contain the MyE911 Installer package (.msi file) and batch file (.bat file) to be deployed
3. Set permissions on the share to allow access to the distribution package
    a. Right-click folder and select 'Properties'
    b. Click on 'Sharing' tab
    c. Click on 'Advanced Sharing'
    d. Click 'Share this folder' checkbox
    e. Provide a Share name and click ‘Permissions’
    f. Add and Select only the group(s) of computers/users MyE911 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 MyE911 installer package and batch file to the newly created distribution point

4.2.3 Create a Group Policy Object

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
   a. Source Start GPO can be left to (none)
4. Type a name for this new policy (e.g. Redsky Software), and then press Enter

4.2.4 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. (Optional) In the details pane, under Security Filtering, click Authenticated Users, and then click Remove.
   a. 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.

    a. 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

4.2.5 Configure Group Policy Preferences

1. Right-click on the newly created Group Policy Object, and then click Edit
2. Navigate to: Computer Configuration > Preferences and expand Windows Settings
3. Right-click '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
        i. Important!! **Do not** use the Browse button to access the location. Make sure that you use the UNC path of the shared installer package. See step 4.2.2.g (e.g. \\file server\share\filename.msi)
    c. Destination File: **C:\Temp\<MyE911 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 batch file created in step 4.2.1
        i. Important!! **Do not** use the Browse button to access the location. Make sure that you use the UNC path of the shared installer package. See step 4.2.2.g (e.g. \\file server\share\MyE911.bat)
    c. Destination File: **C:\Temp\MyE911.bat**
8. Click OK

4.2.6 Configure Startup Script to Locally Run 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\MyE911.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

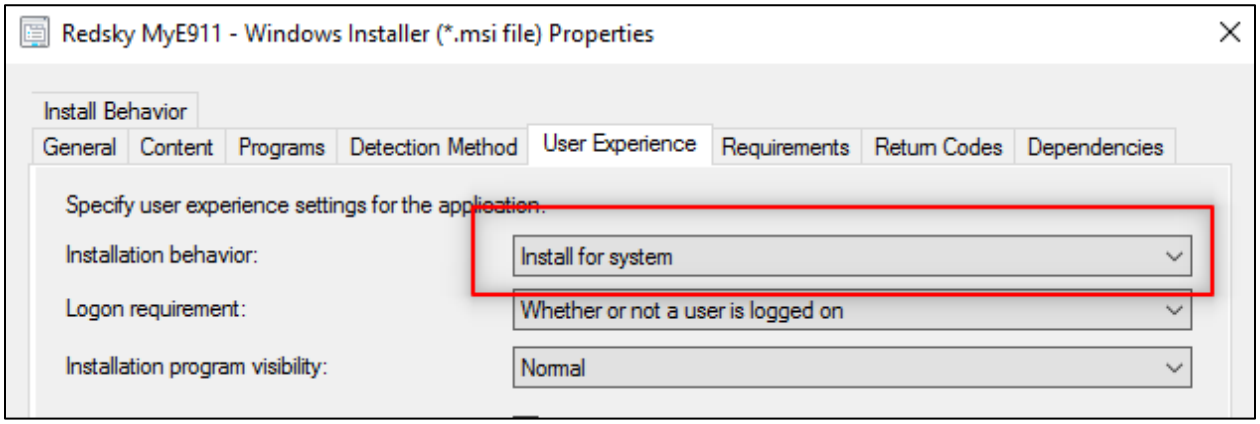
5. Using Microsoft System Center Configuration Manager (SCCM)

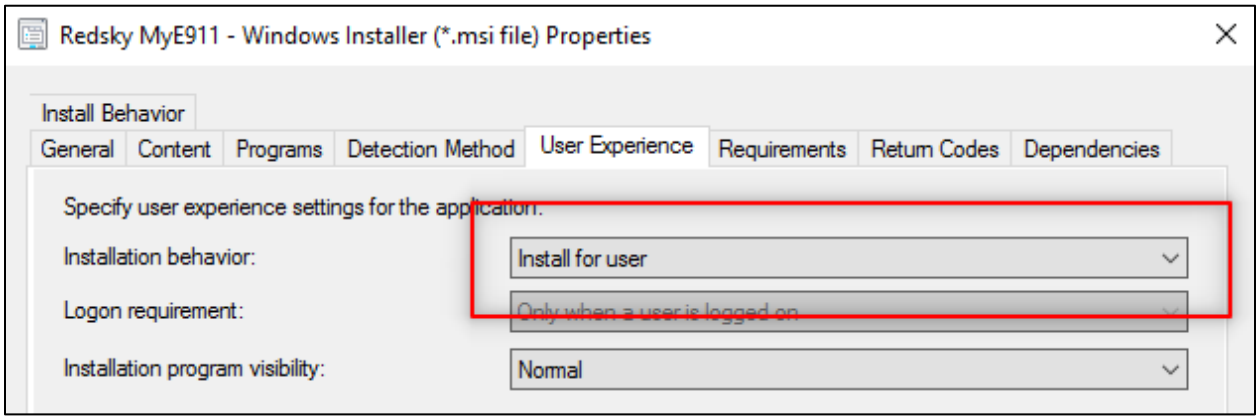
The MyE911 MSI installer package creates a single properties file, *redsky-nm.properties*, for the account used to run the installation program. This file is created in the following directory: %AppData%\Redsky.

If the **Installation behavior** in SCCM is set to "Install for system", the *redsky-nm.properties* file will not be located in the correct directory when a user logs onto the machine. MyE911 users will need to re-enter the MyE911 parameters (see Section 3.1) manually instead of having the options configured at the time of the installation.

Workarounds (use one of the following methods):

1. Change the SCCM **Installation behavior** from "Install for system" to "Install for user".





   This workaround is suitable when each windows device is used by one person and users have Admin permissions to install applications.

2. Create and copy the *redsky-nm.properties* file to a user's "%AppData%\Redsky" directory before the MyE911 installation.

The *redsky-nm.properties* file should include the desired custom parameters listed in Section 3.1. When the *redsky-nm.properties* file is copied to the %AppData% directory ahead of the install, no additional msiexec command line parameters need to be specified.

Sample *redsky-nm.properties* file with server URL configured and LLDP enabled:

```
#
#Mon Jul 05 15:00:00 CDT 2021
api=https\://anywhere.e911cloud.com
lldp=true
```

Within the *redsky-nm.properties* file, the "secret=" and "token=" lines will automatically be generated for the user once the application starts.

The same modified .properties file can be copied to each specific user directory.

6. Verification

1. Verify that MyE911 is installed on target computers
2. Verify the optional parameters are configured for MyE911 by Right-clicking on the MyE911 icon in the systray and selecting 'Settings'

7. Troubleshooting

1. gpresult.exe /SCOPE <USER or COMPUTER> /Z
    a. /SCOPE will display the applied group policy objects for the user or computer based on what you specify
    b. /Z Specifies that the super-verbose information should be displayed. This will allow you to see in greater detail the applied group policies
    c. cmd prompt/Powershell need to be opened as an Administrator
2. rsop.msc
    a. Provides administrators a report on what group policy settings are getting applied to users and computers
    b. Useful to see if the specific GPO has been applied to machines/users
3. Gpupdate /force
    a. This will force an update of the group policy objects. New policies are applied when the computer starts and when the user logs on
    b. Rebooting or logging off/logging should suffice to apply a group policy, but multiple reboots may be required