AddSecure Device Manager

User Manual

Table of Contents

Introduction

AddSecure Device Manager is the tool used to work with many of the AddSecure products. This document describes how to work in AddSecure Device Manager.

The Device Manager is reached at the following URL:
https://devicemanager.addsecure.com/

The following products can be managed by Device Manager:

- Edge RT7020 Enterprise
- Edge VS53xx
- Edge DS2320

Shortly after a new Edge VS or DS subscription has been ordered the new subscription is available in Device Manager, where terminal settings and status can be viewed/edited. Edge RT7020, however, involves a manual process within AddSecure before the new subscription is available in Device Manager.

Edge RT7020 Enterprise

Workflow

1. Ordering a subscription
   After an Edge RT7020 subscription has been ordered via the AddSecure e-com portal, the order will then be handled by the AddSecure Support team, and finally a new configuration will be available in Device Manager.
2. Setup terminal configuration
   The terminal configuration, like inputs or serial ports, are set up in Device Manager.
3. Programming of the Terminal
   After a new (or factory defaulted) terminal has been installed and powered on, a programming operation must be done via Device Manager.
   Select the configuration in the Configurations list and press “Program”. The Validation code for the terminal must be entered during the initial programming of the device. The Validation code is printed on the label of the terminal, and it consists of six alphanumeric characters.
4. Commissioning of an ARC
   To start the Alarm communication the Commissioning process must be done via Device Manger. Select the configuration you want to be Commissioned in the Configurations list and press the “Commission” button. This needs to be done only once.
   An Edge RT7020 is ready to be used after it is Commissioned.
5. Reconfiguration
   After any configuration change in Device Manager a new “Program” operation must be performed to transfer the new terminal settings to the terminal. A subsequent Commissioning process is not necessary in this case.

Terminal status

To get the latest status from an Edge RT7020 Enterprise, you can press the get status button. GET STATUS

Terminal settings

To view or change any of the terminal settings, select the desired configuration from the Configurations list, then click Edit under the Alarm Transmitter Service.

VPN Services

VPN services are available for the Edge RT7020 as an add-on feature. VPN settings are available via the Edit icon under Service “Edge VPN Remote Access” or “Edge VPN Site-to-site access”.

VPNs are connected or disconnected under the VPN tab on the upper part of the page, where each VPN can be connected or disconnected.

Edge VS and Edge DS Families

This chapter describes the workflow for Edge VS and Edge DS terminals.

Workflow

1. Ordering a subscription
   When a subscription is ordered through the e-com portal, it will be handled automatically by AddSecure. The new subscription will be available in the Device Manager right when this process is finished.
2. Automated user creation
   If the person ordering the subscription does not already have an account for Device Manager, one will be created for them. A welcome email will be sent to the user, with instructions on how to log in.
3. Terminal configuration
   Configuring the terminal, like modifying its inputs, panel type or serial interface, is done in the Device Manager.
4. Activating the terminal
   When the new (or factory defaulted) terminal has been installed and powered on, an activation operation must be done via the Device Manager.
   Select the desired configuration from the Configurations list and press the "Activate" button.
   The TAC code for the terminal must be entered during the activation process. The TAC is printed on the label of the terminal, and consists of eight alphanumerical characters.
   When the activation is completed, the terminal will receive the latest firmware automatically, and it will be ready for use right after. Note also that the Alarm Receiving Center must have completed the registration process on their end before you can carry out a proper end-to-end test.
5. ARC registration schema – dependent on type of service
   A Registration schema must be sent to the ARC by pressing the “Send Reg. Schema” button under the Alarm Receiving Center information box.

   The ARC registration schema will include various details needed by the ARC to create the new account in their systems. AddSecure Device Manager provides text fields that will be part of the Registration Schema.

   a. Subscription related details
      Some information can be changed or added via the edit icon under "Information Details"
   b. ARC related information
      Information can also be changed or added via the edit icon under "Alarm Receiving Centers"

Make sure any additional information related to ARC Registration schema, as well as the configuration, is completed before pressing the “Send Reg. Schema” button.

6. Adding ARC details – dependent on type of service
   Under the ARC section the details of the receiver has to be entered.
   Destination IP Address and account number are mandatory fields to fill in.
   Depending on the application, also the phone number of the ARC can be inserted here. ERS stands for Emergency Response Service, and we call this number the "ERS phone number".
   Please note that to configure the terminal to use the ERS phone number, instead of the number coming from the panel, you will have to change the setting under Edit-> Panel Connectivity-> Application-> General-> Voice call Number Override Type.
   Further, regardless if the number dialed by the terminal is defined by the ERS number or the panel, the number must have a country code prefix for the SIP service to function properly.

Terminal settings

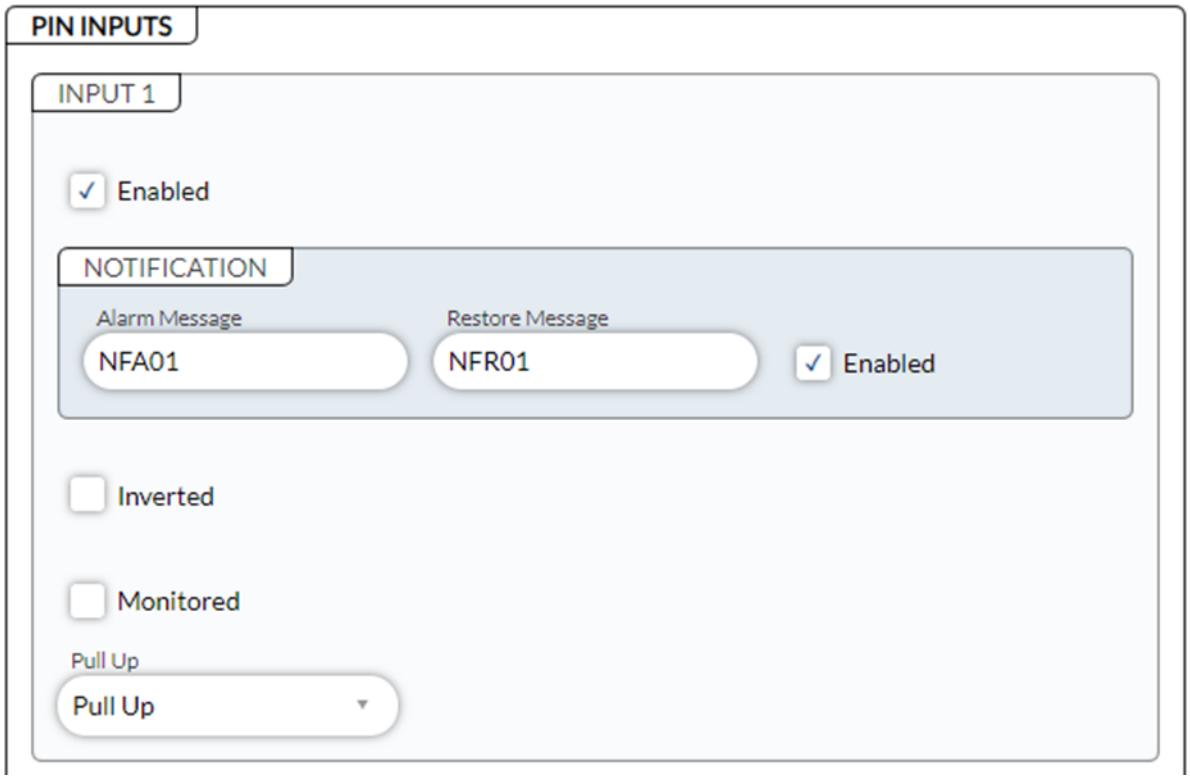
All settings are available after clicking the “Edit” button on the subscription page. The different settings are divided into separate sections that can either be expanded or collapsed so that they are easily readable, independent of screen resolution.
Several settings are read only since they must remain in a known or default state for the AddSecure Connect platform to route and function properly. If you wish to change settings that have read only access, please contact AddSecure technical support for assistance.

The terminals use SIA event codes when sending alarms and notifications. If/when applicable notifications are to be modified, then the following syntax must be used:

- SIA event code is proceeded with an “N” (for new)
- Optional: Area code. Proceeded with “ri” (0000-9999). If Area code is used, then it is inserted between the “N” and the SIA code.
- Optional: Zone number. 000-999. This should be inserted after the SIA event code.
- If additional text is to be used, then the character “^” must encapsulate the text.

Example without an Area code: NBA01^Burglary Alarm^
Example including an Area code: Nri1234BA01^Burglary Alarm^

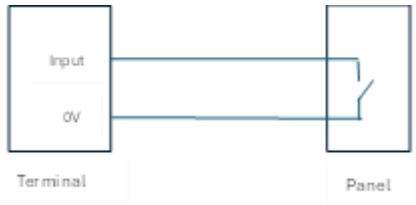
Pin Inputs



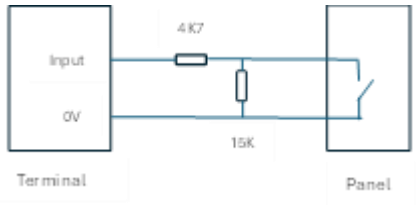
Pull configuration:

1. Pullup
   This is the “standard” configuration.
   If the relay at the panel is open then the terminal treats this as the Alarm condition. So it sends the configured ‘alarm’ message.
   When the relay is closed, the configured ‘restore’ message is sent.
   So in non-inverted mode, the output at the panel should be in closed state (NC) when in normal condition.

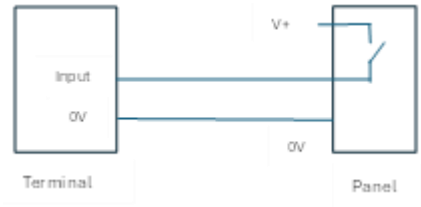
   The terminal provides a reference voltage (3,3V) via an internal pullup resistor.
   a. Unmonitored option
      The alarm panel shorts the **input** to 0V, via a relay output or a transistor output.



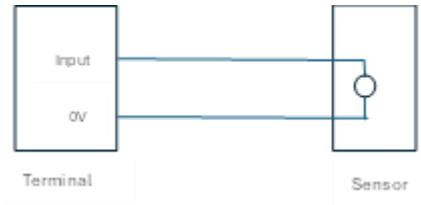
   b. Monitored option
      Additional resistors are wired in-line, near to the panel, to detect tampering of the cable.



2. Pulldown
   This configuration is used with signals powered by the alarm panel.
   The terminal provides the 0V reference via a pulldown resistor.
   The powered output may also be connected to auxiliary equipment, such as a siren, and the input would indicate when such equipment is activated.



3. None
   This configuration is used with sensors that provide an analogue voltage.
   The terminal provides a high impedance (no pull resistor) at its input.
   In the case of a temperature sensor, the measured input voltage would indicate a temperature reading.



Inverted checkbox:

If ticked, the input is interpreted by the terminal in the opposite manner than described above. Example: Ref 1a of this section.
If Inverted is ticked, the terminal sends the configured 'alarm' message when the relay is closed and the configured 'restore' message when the relay is opened.

Monitored checkbox:

If ticked, and resistors are wired in correctly, then the input detects tamper (short circuit and break of line) as well as alarm and normal states.

Minimum required settings per application type

Depending on what application the terminal is set up for, there are a few mandatory settings that need to be applied.

Elevator:

- **Panel Type** must be defined. You will find this setting under *Panel Connectivity->Panel Group*.

Intercom:

- For the SIP service to work, all numbers dialed by the terminal must have a country code prefix. If the numbers that have been entered in the intercom panel do not have country code prefixes, it must be added using the setting under *Panel Connectivity->Intercom-> Add Call Prefix*. Note that only number digits can be entered in this section.
  Depending on format of the numbers stored in the panel, stripping the leading zero off the number might be neccessary. This is done using the feature *Panel Connectivity->Intercom-> Strip Call Prefix.*
  Note that stripping the call prefix happens before adding the call prefix.
  Example:
  The number stored in the intercom panel is 0102345678.
  Adding the prefix 0046, gives the number 00460102345678
  Adding the prefix 0046 and removing the prefix 0, gives the number 0046102345678

Intruder:

- If pin inputs are used, they must be defined. You will find these settings under *Panel Connectivity->Pin Inputs.*
- If the dial capture interface is going to be used, it will be on by default. But you can verify it by viewing the Enabled checkbox under *Panel Connectivity->Dial Capture.* You do not have to specify the panel type since the terminal will auto detect the correct protocol to use when the panel type is supported.
- If Relay outputs are to be used, they must be defined.
  Input follower means the relay will change state whenever a certain input is triggered.
  Input Alarm Ack means that the relay will be used to signal that an input alarm message has been successfully delivered.
  Trouble Reporting means that the relay will be used to signal if an input alarm message has *not* been successfully delivered.

For all applications:

- Verify your Ethernet settings. You will find the settings under *IP Paths->Ethernet.* The default setting is to utilize the DHCP client.

Terminal status

To ask a Edge VS or DS terminal for its latest status, press the get status button. 

Organizations, Users and Privileges

A user account is needed to access the Device Manager application. Each user belongs to an organization. AddSecure will create the organization and the first user account if it does not exist at the time when a subscription is ordered. The first user will get the “Administrator” user privilege. Users in the same organization can all work with the subscriptions/terminals owned by the organization, or terminals shared to the organization. See chapter about shares.

User privileges

Each user in Device Manager has a defined user privilege setting. The user privilege decides what a user can see and do within the Device Manager. The table below lists and describes the different user privileges.

	Admin	Admin Read Only	Local Admin	Installer	Installer Read Only
User Management	✓	✓	✓ limited		
Activate Terminals	✓		✓	✓	✓
Program Terminals	✓		✓	✓	
See Terminals	✓	✓	✓	✓	✓
Edit terminals	✓		✓	✓	
Create Folders	✓				
Share to other organization	✓				

Administrator

An Administrator can do everything within Device Manager, like manage users, shares, folders, and any setting on the installations.

Administrator Read Only

A user with Administrator Read Only access can see everything but not change anything within Device Manager, i.e. no configuration or user can be changed, no folders can be created.

Local Administrator

A user with Local Administrator access is an administrator in a folder shared to the user.

Installer

An installer can access and work with terminals that has been shared to them. The share can be a specific configuration, or it can be a folder. The installer can edit, activate, and program terminals. Note that a new Installer user does not have any shares by default, and thus cannot access anything until a share has been created. If the Installer needs access to all configurations, a share of “All Configurations” can be created.

Installer Read Only

In Installer Read only can se same things as an Installer, but has no rights to change anything.

User management

Users with User Management rights will see an “Organization” menu under the hamburger icon in the upper right corner of the page header. All the users are listed here, including the user privileges, creation date, their shares, last login date, and activation status. New users can be created here as well, by pressing the “+” sign.

When a new user account has been created, a welcome email is automatically sent to the new user. The recipient needs to activate the account via the link in the email, and then set a new password via the “Forgot your password?” link on the Device Manager login page. The “Forgot your password” process includes an One-time-code (OTC) that is sent to the user via email.

Shares

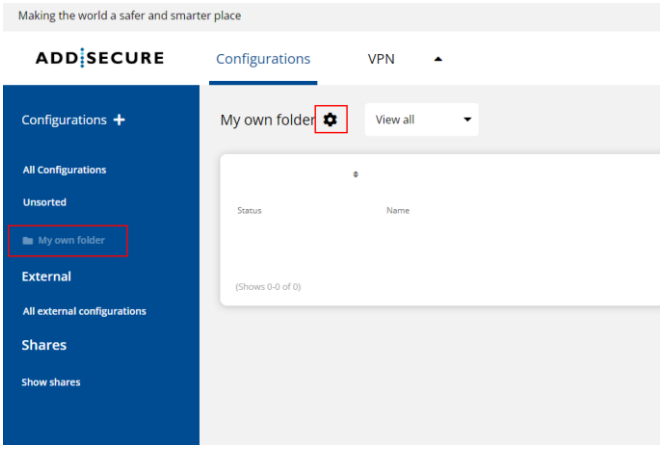
AddSecure Device Manager uses a sharing concept for both users and organizations. Within an organization, shares must be given to all users except “Administrators” and “Administrators read” to create configurations, or folder, visible for the user.

User shares

For a user with installer user rights a share must be created to allow the user to access configurations within Device Manager. Shares can be created at the configuration or the folder level. To allow an installer to access everything, simply share the “All configuration” folder.

Share a folder

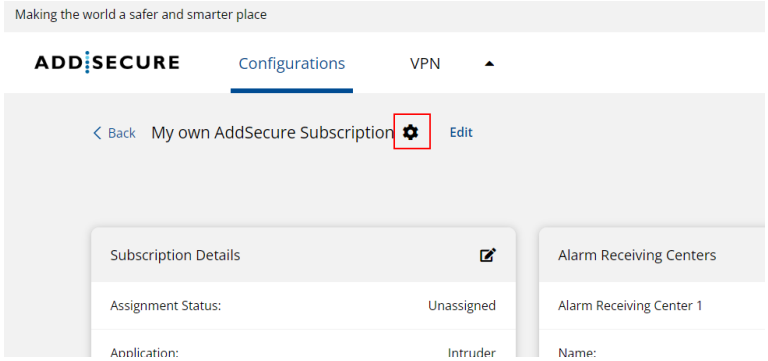
To share a folder, select the folder, then select the item “Share to users” under the cogwheel icon:



Select the user to whom the folder shall be shared and press OK.

Share a configuration

To share an individual configuration, select the configuration in the configuration list. In the next view (see below), select the item “Share configuration” under the cogwheel icon:



Select the user to whom the configuration shall be shared and press OK.

Organization shares

Shares between organizations allow one organization to access and work with subscriptions/terminals that are owned by another organization. A share must be created by the organization owning the folder or configuration to be shared. When creating a share, the item to be shared is selected, followed by selecting the “Share to other organization” item under the cogwheel icon. The following details must be configured to create the share:

- Company ID
  A six-digit identification number of the receiving organization. This must be provided by an Administrator user in the receiving organization, and is found under the Organizations page in Device Manager, next to the Organization name.
- Privileges
  The share can be a read only share, which means that the receiving organization cannot edit or change the shared items.
  “Read and write” allows the receiving organization to also modify the shared item.
- Time limit
  A date can be configured after which the share shall no longer be valid. The share will still exist after this date, but it will no longer have any effect.
  If no date is set then no end date exists for the share.