



Process Monitor Agent

Administrator Manual

Software Version 1.0.0



EducateIT GmbH

Steinenbergstrasse 7, 4532 Feldbrunnen, Switzerland

Phone: +41 32 355 39 00

E-Mail: info@educateit.ch

Web: <http://www.educateit.ch/>

Process Monitor Agent – Administrator Manual

Copyright: ©2016 by EducateIT GmbH

EducateIT GmbH
Steinenbergstrasse 7
CH-4532 Feldbrunnen
Switzerland

Phone: +41 32 355 39 00
E-Mail: info@educateit.ch
Web: <http://www.educateit.ch/>

Illustrations and Text: TE

Layout and Design: [TE](#)

Last Modification: 2016-01-12 12:39

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by and means, electronic, mechanical, photocopying, recording, or otherwise, without the prior consent of the EducateIT GmbH. The EducateIT GmbH assumes no responsibility for errors or omissions, or for damages that may result from the use of information (especially including example configurations and listings) contained herein.

Table of Contents

Table of Contents	3
Preface	5
Features	5
See Also	5
Configuration	7
apiOnlyLocal	7
apiPort	7
apiSecrets.....	7
Deployment	11
Create Secrets in Stock	11
Create a Custom Setup	11
Setup a Production Log File	11
Testing the Installation	12

Preface

The *Process Monitor Agent* is a lightweight service to provide process information for the *Process Monitor Collector* with a very low *CPU* and network impact. Using the *Process Monitor Agent* is the recommended way to provide process information. The agent uses a very simple configuration and can be easily deployed on many systems. While idle, the service has almost no impact on the system – it just listens on a network port for incoming connections from a collector service.

Features

- Simple configuration.
- Very low *CPU* and network impact.
- While idle almost no impact on the host system.
- Encrypted SSL connection and strong authentication.

See Also

The service is using the *Configuration B* system for the configuration. To understand all aspects of the configuration, it is recommended to read the document “*Configuration B - Administrator Manual*”.

The service also uses the *EducateIT Service Framework* and the *EducateIT Log System*. Both systems provide several features which are explained in their own manuals: “*Service Framework – Administrator Manual*” and “*Log System – Administrator Manual*”.

You should get all these documents along with this manual. If not, please request them from us.

Configuration

The configuration of this application is based on “*Configuration B*” and is supporting all features of this system. The configuration is stored in the file “`configuration.xml`” which is placed in the program directory beside the executable, but can also be placed in any of the searched directories to be more OS compliant. Read the “*Configuration B*” manual, section “Files and Locations” for details.

Illustration 1 on page 8 shows the structure of the application configuration. The following sections describe each value of the configuration in detail.

API?

API is a shortcut for Application Program Interface. In the context of the process monitor agent, this is the interface where the collector can access the agent and retrieve the current running processes.

apiOnlyLocal

This optional value controls if the *API* is accessible from external computers. In a production environment this value should be set to No.

If you set this value to Yes, the *API* is only accessible via *localhost*. This means only applications running in the same host as the service can access the *API*. If you set this value to No, the *API* is accessible from outside.

If you omit this value, it is set to Yes, which prevents access from outside. This is only useful for testing, where you can install all systems on the same computer and prevent any access from outside.

apiPort

This optional value changes the port where the service listens for *API* access. Valid values are numbers between 1 and 65535. Depending on the operating system, port numbers below 1024 are only possible if the service is running with administrator privileges.

If you omit this value the port 17697 is used for *API* access.

If you are unsure, omit this value and use the default port.

apiSecrets

This list controls which systems can access the agent using the *API*. You generate secret pairs using the *EducatelT Secret Gen-*

Module	Application
Value	apiOnlyLocal Optional Boolean
Default	Yes
Value	apiPort Optional Integer
Constraints	- Minimum value: 1 - Maximum value: 65535
Default	17697
List	apiSecrets
Definition	List Entry Definition authorizedNetworks Optional String key String label String secret Password
Value	
Constraints	Must not be empty.
Value	
Constraints	Must not be empty.
Value	
Constraints	Must not be empty.

Illustration 1 The Application module for the application.

```
<List name="apiSecrets">
  <ListEntry>
    <Value name="label">Collector Production 1</Value>
    <Value name="key">fMATR;8Gq_pPai/7P827;ripX1ymYBx3Es;KZ;B.!X+oJsdv3PYVIV-fupuJf}~</Value>
    <Value name="secret">cx(5:K5(9siRU?+I:)6#5oK{Sc)GwiiSt/1/lwVY*k#H{Kx4g@I2qv0GRJxA08{2 0e8ouJWNLXHo3fA
fos4Zix3VGvm*qZxtGNhiVFwtgTXc*iGkIpQf+dZ4Bs0Z3T85tzSQw9AK8s8n9DL7nTpDZA===</Value>
    <Value name="authorizedNetworks">10.0.0.0/16 127.0.0.1/24</Value>
  </ListEntry>
  <ListEntry>
    <Value name="label">Collector Test A</Value>
    <Value name="key">?1.RAf"|#:ZQj:Z621-W_BjdoKh6KmF{35EU=_Q{N|qyaliRd+vU/-X97l!Q6,A9</Value>
    <Value name="secret">_k:([%pW3IY@D_/vE$WvuT*w^FKT,t!:({/mQUf,%hEo1efkB@/JM07_C8tMiX9V dbcE2xi+XtUSz6o
E+7XpF6FWnnNqM4fAQ07BT*PLizr7RhyEMTgAxBbvX/DLogL0zkV1DQjyjkIh7K1TXrw==</Value>
  </ListEntry>
</List>
```

Listing 1 An example how the secret list can look like. This is only an example, these entries are not valid.

erator. The client is the software which would like to access the process list, which is the process monitor collector in this context. The server is the process monitor agent service.

You should generate a own secret pair for each collector which would like to access the process list.

There is also the possibility to limit the access using the `authorized networks` value. If you know a client is always connecting from the IP range `10.0.0.0/24`, you can limit the access further by specify this network in the `authorizedNetworks` value.

See [Listing 1 on page 8](#) how this list could look like.

apiSecrets » label

This is a label which is used for the client in log files. The label helps to easily know which secret was used to access the *API*.

apiSecrets » key

This is the key for the API secret pair. Copy this value from the generated secret pair using the *EducateIT Password Encoder*.

apiSecrets » secret

This is the server secret generated with the *EducateIT Password Encoder*. It is unpractical to generate a client secret from the server secret. Nevertheless you should limit the access to the configuration as good as possible.

apiSecrets » authorizedNetworks

This value can contain a whitespace separated list of networks from where this secret can be used.

Deployment

If you deploy the agent in large enterprise networks, there are a few things to consider.

Create Secrets in Stock

You can create one single configuration with a list of secrets which is deployed with all agents in the network. For later changes you should always add a number of additional secrets to the configuration. Keep the additional secret pairs in a password manager for later use.

If you ever extend the system with additional collector services, you can use from these secrets in your stock and there is no need to update the configuration of all deployed agents.

Create a Custom Setup

The default setup is not suitable for a large deployment, but it is not difficult to create a own. Like almost all our software, it is working based on a simple file installation. Therefore if you create a test installation with a correct configuration file, you can just copy the application directory with all files to another system and it will work.

You can also adjust the service settings to your needs and just export the registry entries for the service. If you copy the files from the application directory and install the registry entries for the service, the deployment is already done.

There are no other dependencies and no additional registry entries required.

Setup a Production Log File

The generated log file is very helpful to locate issues with the system. Therefore you should always setup a log file, but make sure you filter all trace messages from the log.

See [for an example configuration for a production environment](#). It will write only information, error and warning messages to the log and create a new log every month.

Make sure you create the directory for the log file in your setup process on the deployment.

```
<Module name="Log">
  <List name="FileWriter">
    <ListEntry>
      <Value name="LogFilePath">C:\LogFiles\PMAgent.log</Value>
      <Value name="LevelFilter">Warning</Value>
      <Value name="Rotation">Monthly</Value>
    </ListEntry>
  </List>
</Module>
```

Listing 2 The log configuration for a production environment.

Testing the Installation

After installation on all systems in your network you can easily test for the services using a network scanner. Just test for the configured port and you will get a list of systems where the agent is correctly installed and running.

The following example uses one of the most popular network scanner nmap to scan for the running agents. Make sure you network operator is informed about the scan in advance.

```
nmap -p 17697 --open 10.0.0.0/16
```




EducateIT GmbH
Steinenbergstrasse 7, 4532 Feldbrunnen, Switzerland
Phone: +41 32 355 39 00
E-Mail: info@educateit.ch
Web: <http://www.educateit.ch/>