Pro-face Connect 11.0

Release Notes

PFCNT-RN_00
12/2023

Pro-face™

by Schneider Electric

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Pro-face brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

Document Scope

This document contains important information about the Pro-face Connect 11.0. Read the complete document and the Pro-face Connect Quick Start Guide, before you use the product or products that are described herein.

Validity Note

The information in this release notes document is applicable only for Pro-face Connect compatible products.

This document has been updated for the release of Pro-face Connect 11.0.

Restrictions about this product are available at https://www.pro-face.com/trans/en/manual/1072.html

Related Documents

Title of documentation	Reference number
Pro-face Connect Quick Start Guide	PFCNT-QSG (Eng)
	PFCNT-QSG (Jap)

You can download the manuals related to this product, such as the software manual, from our support site at https://www.pro-face.com/trans/en/manual/1085.html

Trademark

Schneider Electric has made every effort to supply trademark information about company names, products, and services mentioned in this manual.

GP-Pro EX, BLUE, and GP-Viewer EX are registered trademarks or trademarks of Schneider Electric.

GateManager, LinkManager, and SiteManager, are registered trademarks of Secomea A/S.

Microsoft, Windows, Windows Server, Internet Explorer, Windows Media, Excel, Visio, DirectX, Visual Basic, Visual C++, and Visual Studio are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Product Information

Pro-face Connect allows technicians and programmers to remotely monitor, diagnose, control, and program devices.

System Requirements

Pro-face Connect LinkManager can be installed on a personal computer with the following system requirements:

- Windows 10 or 11, 64-bit edition and with Administrator privileges
- Internet browser — Google Chrome, any recent version of Mozilla Firefox or Microsoft Edge can also be used.

Installation Instructions

Launch the Pro-face Connect and follow the instructions. For more details, refer Pro-face Connect Quick Start Guide.

GateManager 8250 Server

New Features and Enhancements

- RD-6391: Show last-login on **Group > Accounts** tab.

  A **last login** column has been added to the **Group > Accounts** table.

- RD-6399: Simplify handling of option toggles through **gm** command.

  Certain advanced settings can now be enabled and disabled through the **gm** command line tool.

  Use **gm options** to see these settings and **gm enable/disable** to edit them.

  Use **gm help** to view all commands of the **gm** line tool.

- RD-6428: Improve user feedback on when auto-disable is enabled.

  When an account is set to auto-disable at a given date and time, the user is now informed (through an "Expires" message at the top menu bar in the GateManager and LinkManager portals). Also, if user logs into a disabled account (with proper credentials), the user is now informed that the login failed because the account is disabled.

  Related to this, if an administrator account (which is set to auto-disable at a given date and time) creates or modifies another account, that other account will automatically be set to auto-disable at the same time as the administrator account (unless it is already set to auto-disable at an earlier date or time).

- RD-6429: Use free ClamAV for scanning public and shared files.

  GateManager now has built-in support for installing and running the free ClamAV malware detection software when uploading and downloading files to and from the server. The feature is enabled via the new Miscellaneous > "Enable ClamAV virus scanner" setting. Using this feature may impact server performance and reliability, so please read the associated online help before enabling the feature. notably, 3 GB RAM is required by the ClamAV software.

- RD-6433: Stop offering deprecated elliptic curves on web server.

  Some of the elliptic curves for key exchange previously offered by GM's web server have been deprecated (RFC 8422). These are no longer offered. All contemporary browsers support at least one of the remaining (stronger) curves offered, so this should not affect interoperability.

- RD-6434: Enhance information available via CRM API.

  The creation date for accounts, appliances, and agents is now available through CRM API version 1.9.

- RD-6435: Manage advanced groups via CRM API.

  The CRM API now has support for managing advanced groups, as well as a new /all/ request type which returns a flat array of all objects of a given type (rather than a tree structure).

Mitigated Anomalies

- RD-6134: SME 6322 is not recognized in Domain Content summary.

  The v6322 SME product was not listed correctly in domain content summary. This has been fixed.

- RD-6369: Insufficient verification of new WS certificate and private key.

  In some rare cases, GM failed to recognize a broken web server x509 certificate or private key, and would install it on the server, causing it to become unresponsive. This has been fixed.

- RD-6372: GM firmware update script reports "server timed out" for all errors.

  GateManager uses cURL to connect to the firmware portal, but if connection failed, all error were logged as a "server timeout" in the firmware update log. This has been fixed by logging the failing cURL process' exit code which indicates the actual failure (run "man curl" for details).

- RD-6375: Audit log from SiteManager is not stored correctly.

    GateManager 10.1 changed the way some events (like Remote Attach) are stored in the audit log, but the printing of these entries were not updated accordingly, so some information was missing in the **Audit** tab. This has been fixed.

- RD-6377: GTA buttons are shown for offline appliances and agents.

    Since GateManager 10.0, **Go To Appliance** and **Connect** buttons are shown also for offline appliances and agents, but that should only happen when **Request for Access** is enabled. This has been fixed.

- RD-6379: AD script does not work for domain names with periods '.'

    When automatically creating GateManager accounts on first SSO login, the target domain can now be specified using a domain token prefixed by a @-character.

- RD-6396: In-browser GTA fails for devices accessed via Advanced Groups.

    Starting the in-browser VNC viewer failed to connect if the device agent is accessible to the user through an Advanced Group. This has been fixed.

- RD-6398: Some GM settings block various CRM API requests.

    Certain CRM API requests would fail in some rather obscure situations. This has been fixed.

- RD-6412: Obsolete javascript and css files do not get deleted on upgrade.

    Old .js and .css files did not get deleted when upgrading GateManager. This has been fixed.

- RD-6422: Extra new line is added to scripts on each save.

    When editing scripts or templates through the related Files menus, a blank line was added to the end of the script on each save. This has been fixed.

- RD-6439: Joined objects cannot be (un)joining to an advanced group.

    It was not possible to join or unjoin objects to a group if those objects were joined to the current account. This has been fixed.

SiteManager and SiteManager Embedded

New Features and Enhancements

- RD-6368: Add device search to UPLINK interface.

  The Search function on the GateManager→ **Agents** page now searches for devices on both UPLINK and DEV networks.

- RD-6384: New JTM2M APN for nextm2m.

  JTM2M has been added to the list of APNs to automatically try for SIM cards from NextM2M / Jersey Things (MCC/MNC 234/50).

Mitigated Anomalies

- RD-6312: DEV ports may be blocked by BPDU protection of external switch.

  When multiple DEV ports in separation mode are connected to the same external switch, the switch may block the ports due to BPDU protection.

  This happens because all DEV ports use the same MAC address, so the switch might think that a loop exists and block the ports.

  This has been fixed by using unique MAC addresses on DEV ports that are in separation mode. Note that this was actually fixed in release 10.1, but was by mistake not included in the 10.1 release notes.

- RD-6381: Connection to GM port 11444 via proxy does not work.

  In release 10.1, support was added for also trying to reach GateManager on port 11444 through web proxy (configured or auto-detected) - RD-6212.

  However, this did not work as intended, so the connection would not actually get established if ports 80 and 443 were blocked on the GateManager. This has now been fixed.

- RD-6382: Proxy authentication using "Digest" method does not work.

  Applies to: LinkManager and SiteManager Embedded 6110 for Windows.

  Connections to GateManager through a proxy that required (or offered) Digest authentication would fail to get established. This has been fixed.

- RD-6389: SiteManager Fix button leads to incorrect menu.

  Since SiteManager release 10.1, if the Setup Assistant showed a "Need Reboot" warning, the associated "**Fix**" button navigated to the wrong subpage. This has been fixed.

- RD-6401: The following security vulnerability has been addressed in this release:

  SiteManager Embedded: CWE-416: Use After Free.

  For more information please refer to https://cwe.mitre.org/data/definitions/416.html

LinkManager Windows Client

Mitigated Anomalies

RD-6382: Proxy authentication using "Digest" method does not work.

Applies to: LinkManager and SiteManager Embedded 6110 for Windows.

Connections to GateManager through a proxy that required (or offered) Digest authentication would fail to get established. This has been fixed.

PFCNT-RN_00