

CIRRUS SAP CLOUD COMPUTING: PREREQUISITES TO ACCESS THE MANAGEMENT INTERFACE

Version e-x-1-0
Date August 2009
Status approved

Cirrus Services AG
Hodlerstrasse 16
CH-3011 Bern
T +41 58 455 04 40
F +41 58 455 04 41
www.cirrus-group.com

Proprietary Notice

© 2009 Cirrus Group. All rights reserved.

This document is private and confidential. Without written confirmation by Cirrus the content may not be disclosed to any other legal entity or third party. The right to copy or reproduce this document - or part of it - is denied.

Cirrus disclaims confirmation or promise of completeness and correctness of the information herein stated. Cirrus can not be made responsible for damage caused on actions based on the information stated in this document.

This document contains no supplementary assurance that exceeds the contractual agreement.

Cirrus Services AG
Hodlerstrasse 16
CH-3011 Bern

Phone: +41(0)58 455 0 400
Fax: +41(0)58 455 0 401

<http://www.cirrus-group.com>

Index

- 1 CLIENT-SIDE PRODUCTS AND ENVIRONMENTS..... 4
 - 1.1 Overview of Client-Side Support 4
 - 1.2 Platform and Browser Requirements..... 4

1 CLIENT-SIDE PRODUCTS AND ENVIRONMENTS

1.1 Overview of Client-Side Support

The following sections provide information about Web client environment requirements for both the PPM Center standard interface and the PPM Workbench as well as support for optional, third-party, client-based products.

1.2 Platform and Browser Requirements

Client requirements include the following:

Operating system

- Microsoft® Windows® XP Professional SP1
- Microsoft Windows XP Professional SP2 (both 32- and 64-bit)
- Microsoft Vista Business Edition (both 32- and 64-bit)
- Microsoft Vista Enterprise Edition (both 32- and 64-bit)

Hardware

- 1.0 GHz (or faster) processor
- RAM
 - At least 512 MB
 - For PPM Workbench, at least 1 GB

Adobe Acrobat Reader 5.0 (or later)

Browser

- Mozilla Firefox 2.0.x
- Microsoft Internet Explorer 6.0 SP2
The following security settings must be enabled for the zone in which PPM Center is run:
 - Run ActiveX controls and plug-ins
 - Script ActiveX controls marked safe for scripting
 - Access these settings using **Tools > Internet Options > Security Tab**.
 - HP recommends using the default settings for the Internet zone.

- Microsoft Internet Explorer 7.0

The ActiveX security settings required for Microsoft Internet Explorer 6.0 SP2 are not required for Microsoft Internet Explorer version 7.0 provided the following setting is enabled:

- Enable native XMLHTTP support

Access this setting using **Tools > Internet Options > Advanced Tab > Security (Section)**.