Ivanti Policy Secure Supported Platforms Guide

9.1R17

Build - 8885

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

Protected by patents, see https://www.ivanti.com/patents.

Contents

Introduction

This document describes the client environments and IT infrastructure that are compatible with this release.

In this document, **Qualified** terminology indicates that the item was systematically tested by QA for this release.

Revision History

Table lists the revision history for this document.

Revision	Description
December 2022	Ivanti Policy Secure Release 9.1R17
July 2022	Ivanti Policy Secure Release 9.1R16
April 2022	Ivanti Policy Secure Release 9.1R15
January 2022	Ivanti Policy Secure Release 9.1R14
December 2021	Ivanti Policy Secure Release 9.1R13.1 updates
October 2021	Ivanti Policy Secure Release 9.1R13 updates
August 2021	Ivanti Policy Secure Release 9.1R12 updates
February 2021	Ivanti Policy Secure Release 9.1R11 updates
December 2020	Ivanti Policy Secure Release 9.1R10 updates
October 2020	Ivanti Policy Secure Release 9.1R9 updates
July 2020	Ivanti Policy Secure Release 9.1R8 updates
June, 2020	Ivanti Policy Secure Release 9.1R7 updates
April 6, 2020	Ivanti Policy Secure Release 9.1R5 updates
September 2019	Ivanti Policy Secure Release 9.1R3.1 updates
September 2019	Ivanti Policy Secure Release 9.1R3 updates
July 2019	Ivanti Policy Secure Release 9.1R2 updates
May 2019	Added Juniper switch model as qualified for Policy Enforcement using SNMP (ACL based)
April 2019	Ivanti Policy Secure Release Notes 9.1R1 updates

Hardware

You can install and use Release software on the following platforms.

- PSA300
- PSA3000
- PSA5000
- PSA7000f
- PSA7000c
- Virtual Appliances (PSA-V) on ESXi, OpenStack KVM and Hyper-V, Microsoft Azure, Amazon Web Services (AWS).

Administrator Web User Interface

Table lists qualified platforms for the administrator user interface.

Operating System	Browsers
Windows	
Windows 11, 22H2 (22621) Enterprise 32-bit and 64-bit	Firefox Google Chrome Microsoft Edge
Windows 11, 21H2 (22000) Enterprise 32-bit and 64-bit	Firefox Google Chrome Microsoft Edge
Windows 10, 21H2 (19044) Enterprise 32-bit and 64-bit	Firefox Google Chrome Microsoft Edge
Windows 10, 21H1 (19043) Windows 10, 20H2 (19042) Windows 8.1 Enterprise, 64-bit	Firefox Google Chrome Microsoft Edge
Mac	
Mac OSX 12.6 (Monterey) Mac OSX 11.6 (Big Sur)	Safari Google Chrome

Ivanti Secure Access Client Software

For a list of supported platforms for the Ivanti Secure Access Client, refer to *Ivanti Secure Access Client Supported Guide*.

Pulse Secure Client is referred as Ivanti Secure Access Client. The release numbering is updated to 22.RX. Complete UX rebranding and the UI upgrade is implemented. There is also an option to switch between the Classic UI and New-UI to maintain user experience. The Pulse Secure client icon is replaced by Ivanti Secure Access Client icon  . For more information refer KB45301.

Third-Party Wireless LAN Controller

lists platform requirements for third-party wireless LAN Controller.

Platform	Environment
Cisco	
	Cisco WLC - Model 2500 8.5.135.0 Cisco 2500 WLC [version 8.0.140.0] AIR-CAP702I [version is 15.2(4) JB6] Cisco catalyst 3850 [Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 03.07.00E] AIR-CAP702I (version is 15.3(3) JNB)
Aruba	
	Aruba 650 WLC [Aruba OS 6.1.3.6], AP-105 [ArubaOS Version 6.1.3.6] Aruba 3400 WLC [Aruba OS 6.4.4.6], AP-205 [ArubaOS Version 6.4.2.4] Aruba Instant Access Point 205 AP-205 [6.4.2.3-4.1.1.3]
Ruckus	
	Zone Director 1200 Series WLC [9.9.0.0.216] Virtual SmartZone – High Scale [3.2.0.0.790] Access Points (Zone flex R500 & Zone flex R310)
Cisco Meraki	Model: MR 42 Firmware version: MR 25.13
Huawei	V200R011C10SPC500
Juniper Mist	AP Model: AP41 Version: 0.5.17122

Third-Party 802.1X Supplicants

The following table lists platform requirements for third-party 802.1X supplicants.

Platform	Environment
Windows	
	Windows 11, 22H2 (22621) Windows 11, 21H2 (22000) Windows 10, 21H2 (19044)
	Windows 10, 21H1 (19043) Windows 10, 20H2 (19042) Windows 10, 2004 Windows 8.1 Enterprise, 64-bit
Mac	
	Mac OSX 12.6 (Monterey) Mac OSX 11.6 (Big Sur)
Google Android	
	Android 12.0
Apple iOS	
	iOS 16.0.3

Agentless Access (Browsers)

The following table lists desktop platform requirements for the agentless access using browsers.

Operating System	Browsers/Java
Windows	
Windows 11, 22H2 (22621)	Firefox Google Chrome Microsoft Edge
Windows 11, 21H2 (22000)	Google Chrome Microsoft Edge Firefox
Windows 10, 21H2 (19044)	Google Chrome Microsoft Edge Firefox
Windows 10, 21H1 (19043) Windows 10, 20H2 (19042)	Google Chrome Microsoft Edge Firefox ESR
Mac	
Mac OSX 12.6 (Monterey) Mac OSX 11.6 (Big Sur)	Safari Google Chrome
Linux	
Ubuntu 20.04, 22.04	Firefox ESR Oracle JRE 8

Table lists requirements for the smart mobile devices that can gain agentless access to the network using the Web browsers indicated.

Device/Operating System	Browsers/Java
Apple 13.1.2	Safari
Google Android 9.0	Android native browser

Host Checker

Table lists the HC support on different platforms.

Operating System	Browsers/Security Products
Windows	
Windows 11, 22H2 (22621)	Google Chrome Microsoft Edge Firefox
Windows 11, 21H2 (22000)	Google Chrome Microsoft Edge Firefox
Windows 10, 21H2 (19044)	Google Chrome Microsoft Edge Firefox
Windows 10, 21H1 (19043) Windows 10, 20H2 (19042)	Firefox ESR Google Chrome Microsoft Edge
Windows 8.1 Update/ Professional / Enterprise, 64-bit	Google Chrome Firefox
Mac OSX	
Mac OS 12.4 (Monterey) Mac OSX 11.6 (Big Sur)	Safari, Google Chrome

Note: Ubuntu 20.04 and 22.04 works with ISAC.

Platform Support for Device Onboarding

Table lists platform requirements for device onboarding features that are qualified with this release.

Operating System/Feature	Certificate	Wifi
iOS 16.0.3	Q	Q
*Android 12.0	Q	Q
Windows 10/11	Q	Q
Mac OS X 12.6	Q	Q

Enterprise onboarding is not working on Android devices. See the *Release Notes* for more details.

Platform Support for AAA

Table lists platform requirements for third-party AAA servers that are compatible with this release.

From 9.1R15 onwards, support for Siteminder, LDAP Novell eDirectory, LDAP iPlanet AAA servers are deprecated. Ensure you remove all configurations related to these servers before upgrading to 9.1R15. Upgrade may fail if all configurations are not removed. For more information refer KB45044.

Third-Party AAA Server	Qualified
Active Directory	Windows Server 2019
LDAP using Active Directory	Windows Server 2019
LDAP (other standards-compliant servers)	OpenLDAP 2.3.27
RADIUS	Steel-Belted Radius (SBR) 6.1 RSA Authentication Manager 6.1 Defender 5.2 Windows IAS 2008
ACE	RSA Authentication Manager 7.1 SP4 RSA Authentication Manager 6.1 RSA Authentication Manager 5.2
Certificate	Windows Server 2019
SQL	Oracle 11g Express Edition
MSSQL	SQL Server 2019
MYSQL	MYSQL 8.0
*SAML 2.0,1.1	Okta, Ping One, ADFS, ICS, Azure AD

MDM Solutions

Table lists the requirements for integration with mobile device management (MDM) vendors.

MDM Solutions

The following **MDM Vendors** table lists the requirements for integration with mobile device management (MDM) vendors:

Solution	Supported Version
VMWare Workspace One(formerly Airwatch)	
VMWare Workspace One(formerly Airwatch) Cloud Intelligent Hub Application	22.4.0.6 (2204) 22.06.0.11; Android version 12 iOS version 15.5
Ivanti (formerly MobileIron)	
Endpoint Manager Mobile (formerly MobileIron Core)	Core 11.5.0.0 Build 11
Mobile work application on endpoint	11.7.1.0.8R(662) Android OS: 13, Model: Pixel 5 12.11.71a iOS: 16, iPhone 12 pro
Neurons for MDM (formerly MobileIron Cloud)	MI cloud server version : Cloud 87
Mobileiron go version	85.2.0.6 Android OS: 13, Model: Pixel 5 85.1.0a(85.1.0.11 64-bit) iOS: 16, iPhone 12 pro
Microsoft Intune	
Cloud service	Release version 2106
Pulse Workspace	
Cloud service	1.8.0-1628

802.1X Authenticators in Layer 2 Network Access Control Deployments

Table lists the 802.1X authenticators that have been qualified with this release. 802.1X authenticators are Layer 2 Ethernet switches. In addition to the qualified platforms, other 802.1X standards-compliant Ethernet switches are compatible.

Platforms	Hardware Models	OS Version
EX Series	EX 8200 EX 6200 EX 4500 EX 4200	Junos OS 15.1R4, 17.0
Cisco Series	Cisco 2960 Cisco 3850 Cisco 3750 Cisco WLC 2500 Series Meraki MR 42	15.2(6) E2 16.9.1 12.2(55) SE11 8.5.135.0 MR 25.13
Huawei	Huawei S5720	5.170
HP Procurve	2920 series	WB.15.12.0015
Aruba	Aruba3400	6.4.4.6
Ruckus	Zone Director SmartZone	9.9.0.0 build 216 3.5.1.0.296
SRX Series	SRX 650 SRX VM	Junos 12.3X48-D30.7 Junos 15.1X49-D140.2

Endpoint Security Assessment Plug-in (ESAP) Compatibility

The default version for ESAP is 4.0.5.

Infranet Enforcers in Layer 3 Resource Policy Deployments

Table lists Infranet Enforcers that have been qualified with this release. Infranet Enforcers are enforcement points in Layer 3 resource policy deployments. In addition to the qualified platforms, other Screen OS, SRX Series, and EX Series models are compatible, provided the firewall or switch model and software version supports integration with Ivanti Policy Secure.

Platform	Hardware Models	Software Versions
Checkpoint Firewall	Virtual Appliance	R81.10
Palo Alto Network	Virtual Appliance	10.1.3
SRX Series	SRX 220 SRX 650	Junos OS 19.X Junos OS 15.X
FortiGate Firewall		V6.0.4 Build 0231

Admission/Identity Control

Table lists the IDP devices that are supported.

Hardware Models	Software Versions
Fortinet Fortigate Firewall	Fortinet Firewall: V6.4.1 Build 1637 Fortinet Firewall: v6.0.4 build0231 (GA) Fortinet Firewall: v6.0.2 build0163 (GA) Fortinet Firewall v5.6.2, build1486 (GA) Fortinet Firewall: v5.4.2, build1100 (GA)
Forti Authenticator	v6.0.0, build0010 (GA) v 5.5.0, build0366(GA) v5.2.1, build0161 (GA) v4.00-build0019-20151007-patch00
Forti Analyzer	v6.0.4-build0292 190109 (GA) v6.0.2-build0205 180813 (GA) v5.4.2-build1151 161213 (GA) v5.6.2-build1151 161213 (GA)
Palo Alto Networks Firewall	10.1.3
Juniper SDSN Solution	Junos SRX 15.1X49-D140.2 Junos Space 18.3
Nozomi Network SCADAguardian Device	20.0.2-04240901_A6A9C
Check Point	R81.10
McAfee ePO	5.10.0
IBM QRadar	7.3.2

TACACS+

Table lists the switch models that are supported.

Hardware Models	Software Versions
Juniper Switch – Model EX 2200-48t-4g	15.1R4.6
F5 Load Balancer Build: 2,0.291	11.5.4
Arista Switch – Model DCS-7010T-48-R , Hardware version: 12.03	4.22.1FX-CLI
Cisco Switch - Model WS-C3650-24TS	16.06.05
Cisco Switch - Model WS-C3850-24T	16.9.1
Cisco Switch - Model WS-C2960X-24PD-L	15.2(6)E2
HP Procurve Switch - 2920 series	WB.16.02.0014
Cisco WLC - Model- 2500	8.5.135.0

HTTP Attribute Server

Table lists the switch models that are supported.

Hardware Models	Software Versions
Nozomi Networks	20.0.2-04240901_A6A9C
McAfee ePO	5.10.0

Behavioral Analytics

Table lists the switch models that are supported.

Hardware Models	Software Versions
Cisco 3850	03.06.08E
Cisco 2960	15.2(6)E1

IF-MAP Compatibility

Table lists the IF-MAP clients that are supported.

IF-MAP Client	Qualified Version
Ivanti Connect Secure	9.1R9 and later
Ivanti Policy Secure	9.1R9 and later

Policy Enforcement Using SNMP

Table lists the switches which are qualified for Policy Enforcement using SNMP.

Platform	Hardware Models	Software Version
VLAN/ACL Based		
Cisco	2960 Series 3750 Series	15.0.(2)EX5 12.2(55)ES8
HP	2920 Series	A3600-24
HP 3Com	A3600-24 Series	Version 5.20.99, Release 2108P01
Dell	N3024	6.3.3.10
Juniper	EX4200	15.1R4.6
Alcatel-Lucent Enterprise	OS6450-24	6.7.2.191.R04 GA
Arista	12.03	4.22.1FX-CLI
Huawei	S5720	5.170 (S5720 V200R011C10SPC500)

Profiling using Network Infrastructure Device collector

Table lists the devices which are qualified for device profiling using Network Infrastructure Device Collector.

Platform	Hardware Models	Software Version
Cisco	2960 Series	15.2(2) E3
HP	2920 Series	WB.15.12.0015
Juniper	EX 2200 Series	12.3R12.4
Foundry	FESX424 Series	07.2.02
Nortel	2526T Series	4.0.0.000
D-Link	DES-3226S	4.01-B21
Cisco WLC	2500 WLC	7.6.130.0
Aruba WLC	3400 WLC	6.4.2.4
Ruckus WLC	1200 WLC	9.9.0.0.216
Trapeze WLC		
FortiGate	100D	
Palo Alto Networks Firewall	PA 3000	OS 9.1.7/OS 9.1.7 (VM)
Huawei	S5720	
Viptela	NA	vEdge-1000 VM Viptela OS 18.4.4

Agentless Host Checker with Profiler

Table lists qualified Windows platforms and Security Products for Agentless Host checking with Profiler.

Operating System	Security Products (Antivirus / Firewall / Antispyware)
Windows 11/64-bit	Kaspersky Endpoint Security for Window McAfee Endpoint Security (10.x) McAfee Total Protection (14.x) McAfee Total Protection (16.x) Microsoft Security Essentials (2.x) Microsoft Security Essentials (4.x) Sophos Endpoint Protection (10.8.x) Sophos Home (2.x) Symantec Endpoint Protection (14.0.x) Symantec Endpoint Protection (14.2.x) Trend Micro Maximum Security (15.x) Windows Defender (4.x)
Windows 8/64-bit	
Windows 10/64-bit	

General Notes

For policy reasons, security issues are not normally mentioned in release notes. To find more information about our security advisories, please see our security advisory page.

Documentation

Ivanti documentation is available at https://www.ivanti.com/support/product-documentation.

Technical Support

When you need additional information or assistance, you can contact Ivanti Global Support Center:

- https://support.pulsesecure.net
- support@pulsesecure.net

Call us at 1- 844-751-7629 (toll-free USA)

For more technical support resources, browse the support website https://support.pulsesecure.net