# Ivanti Policy Secure Supported Platforms Guide

9.1R18.1

**Build - 9527**

**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.

Copyright © 2023, Ivanti. All rights reserved.

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.

Page 4 of 27

# Revision History

Table lists the revision history for this document.

| Revision | Description |
| --- | --- |
| July 2023 | Ivanti Policy Secure Release 9.1R18.1 |
| April 2023 | Ivanti Policy Secure Release 9.1R18 |
| 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/Java |
|---|---|
| Windows | |
| Windows 11, 22H2 (22621) | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 11, 22H2 (22612) Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 10, 22H2 (19045) Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 10, 21H2 (19044)<br>Windows 11, 21H2 (22000)<br>Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Mac | |
| MAC OSX 13.4.1 (Ventura) | Safari 16.6<br>Chrome 114 |
| MAC OSX 12.6.8 (Montery) | Safari 16.6<br>Chrome 114 |
| Mac OSX 11.5 (Montery-M1/Intel) | Safari 16.6<br>Chrome 114 |

## 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<br>Cisco 2500 WLC [version 8.0.140.0]<br>AIR-CAP702I [version is 15.2(4) JB6]<br>Cisco catalyst 3850 [Cisco IOS Software, IOS-XE Software,<br>Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 03.07.00E]<br>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]<br>Aruba 3400 WLC [Aruba OS 6.4.4.6], AP-205 [ArubaOS Version 6.4.2.4]<br>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]<br>Virtual SmartZone – High Scale [3.2.0.0.790]<br>Access Points (Zone flex R500 & Zone flex R310) |
| **Cisco Meraki** | Model: MR 42<br>Firmware version: MR 25.13 |
| **Huawei** | V200R011C10SPC500 |
| **Juniper Mist** | AP Model: AP41<br>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)<br>Windows 11, 22H2 (22612)<br>Windows 11, 21H2 (22000)<br>Windows 10, 22H2 (19045)<br>Windows 10, 21H2 (19044)<br>Windows 10, 20H2 (19042) |
| **Mac** | |
| | MAC OSX 13.4.1 (Ventura)<br>MAC OSX 12.6.8 (Montery)<br>Mac OSX 11.5 (Montery- M1/Intel) |
| **Google Android** | Android 13.0 |
| **Apple iOS** | iOS 16.5.1 |

# 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 102.13<br>Chrome 114<br>Edge 114 |
| Windows 11, 22H2 (22612) Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 10, 22H2 (19045) Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 10, 21H2 (19044)<br>Windows 11, 21H2 (22000)<br>Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Mac | |
| MAC OSX 13.4.1 (Ventura) | Safari 16.6<br>Chrome 114 |
| MAC OSX 12.6.8 (Montery) | Safari 16.6<br>Chrome 114 |
| Mac OSX 11.5 (Montery-M1/Intel) | Safari 16.6<br>Chrome 114 |

# Host Checker

Table lists the HC support on different platforms.

| Operating System | Browsers/Java |
|---|---|
| Windows | |
| Windows 11, 22H2 (22621) | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 11, 22H2 (22612) Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 10, 22H2 (19045) Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Windows 10, 21H2 (19044)<br>Windows 11, 21H2 (22000)<br>Enterprise 64-bit | Firefox 102.13<br>Chrome 114<br>Edge 114 |
| Mac | |
| MAC OSX 13.4.1 (Ventura) | Safari 16.6<br>Chrome 114 |
| MAC OSX 12.6.8 (Montery) | Safari 16.6<br>Chrome 114 |
| Mac OSX 11.5 (Montery-M1/Intel) | Safari 16.6<br>Chrome 114 |

**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 16.5.1 | Q | Q |
| *Android 13.0 | Q | Q |
| Windows 10/11 | Q | Q |
| Mac OS X 13.4.1 | 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.

ℹ️ 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 Radius Server 3.0.26 |
| ACE | RSA Server 8.7 |
| Certificate | Windows Server 2019 |
| SQL | Oracle 11g Express Edition |
| MSSQL | SQL Server 2019 |
| MYSQL | MYSQL 8.0 |
| *SAML 2.0,1.1 | PingFederate 6.4.1.1 |

# 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<br>Intelligent Hub Application | 22.4.0.6 (2204)<br>22.06.0.11;<br>Android version 12<br>iOS version 15.5 |
| **Ivanti (formerly MobileIron)** | |
| Endpoint Manager Mobile (formerly MobileIron Core) | Core 11.8.0.0 Build 29 |
| Mobile@work application on endpoint | 11.10.0.0.71R; Android OS:13 Model: Pixel 512.11.101a; iOS: 16, iPhone12pro |
| Neurons for MDM (formerly MobileIron Cloud) | MI cloud server version : Cloud 91 |
| Ivanti Go (formerly Mobileiron go version) | 89.1.0.4(20084); Android OS: 13, Model: Pixel 589.0.0a; 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<br>EX 6200<br>EX 4500<br>EX 4200 | Junos OS 15.1R4, 17.0 |
| Cisco Series | Cisco 2960<br>Cisco 3850<br>Cisco 3750<br>Cisco WLC 2500 Series<br>Meraki MR 42 | 15.2(6) E2<br>16.9.1<br>12.2(55) SE11<br>8.5.135.0<br>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<br>SmartZone | 9.9.0.0 build 216<br>3.5.1.0.296 |
| SRX Series | SRX 650<br>SRX VM | Junos 12.3X48-D30.7<br>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<br>Fortinet Firewall: v6.0.4 build0231 (GA)<br>Fortinet Firewall: v6.0.2 build0163 (GA)<br>Fortinet Firewall v5.6.2, build1486 (GA)<br>Fortinet Firewall: v5.4.2, build1100 (GA) |
| Forti Authenticator | v6.0.0, build0010 (GA)<br>v 5.5.0, build0366(GA)<br>v5.2.1, build0161 (GA)<br>v4.00-build0019-20151007-patch00 |
| Forti Analyzer | v6.0.4-build0292 190109 (GA)<br>v6.0.2-build0205 180813 (GA)<br>v5.4.2-build1151 161213 (GA)<br>v5.6.2-build1151 161213 (GA) |
| Palo Alto Networks Firewall | 10.1.3 |
| Juniper SDSN Solution | Junos SRX 15.1X49-D140.2<br>Junos 19.R4 |
| 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 | 9.1R17 and later |
| Ivanti Policy Secure | 9.1R17 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<br>3750 Series | 15.0.(2)EX5<br>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<br>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 Total Protection (16.x) |
| Windows 10/64-bit | |
| | Windows Defender (4.x) |

## 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://forums.ivanti.com/s/contactsupport

- support@ivanti.com

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

For more technical support resources, browse the support website
https://forums.ivanti.com/s/contactsupport