思科身份服务引擎网络组件兼容性，版本 2.7

Revised: 2022 年 3 月 29 日

概述

注释 此产品的文档集力求使用无偏见语言。在本文档集中，无偏见定义为不暗示基于年龄、残障、性别、种族身份、族群身份、性取向、社会经济地位和交叉性的歧视的语言。由于产品软件的用户界面中使用的硬编码语言，基于RFP文档使用的语言或引用的第三方产品使用的语言，文档中可能存在例外情况。

Cisco ISE 支持 RADIUS、其关联的 RFC 标准和 TACACS+ 等协议标准。有关详细信息，请参阅 ISE 社区资源。

Cisco ISE 支持与实施通用 RADIUS 行为的任何 Cisco 或非 Cisco RADIUS 客户端网络接入设备 (NAD) 进行交互操作，以便执行基于标准的身份验证。

Cisco ISE 可与遵守标准协议的第三方 TACACS+ 客户端设备完全互操作。TACACS+ 功能支持取决于设备具体实施情况。

经验证的网络访问设备

RADIUS

Cisco ISE 可与遵守标准协议的第三方 RADIUS 设备完全互操作。RADIUS 功能支持取决于设备具体实施情况。

某些高级使用案例（例如涉及安全状态评估、分析和网络身份验证的场景）并不总是适用非Cisco设备，或者提供的功能可能受限。我们建议您验证所有网络设备及其软件的硬件功能或特定软件版本中的漏洞。

如果网络设备既不支持动态 URL 重定向，也不支持静态 URL 重定向，则Cisco ISE 提供身份验证 VLAN 配置，用于模拟 URL 重定向。有关详细信息，请参阅 《Cisco 身份服务引擎管理员指南》的“安全有线访问”一章中的“Cisco ISE 中第三方网络设备支持”部分。

TACACS+

Cisco ISE 可与遵守标准协议的第三方 TACACS+ 客户端设备完全互操作。TACACS+ 功能支持取决于设备具体实施情况。

有关在网络交换机上启用 Cisco ISE 特定功能的信息，请参阅 《Cisco 身份服务引擎管理员指南》的“支持 Cisco ISE 功能所需的交换机和无线局域网控制器配置”一章。

ISE 社区资源

ISE 是否支持我的网络接入设备？

有关第三方 NAD 配置文件的信息，请参阅 《ISE 第三方 NAD 配置文件和配置》。

有关如何为 Nexus 设备配置 TACACS+ 的信息，请参阅 《Cisco ISE 设备管理说明性部署指南》。

注释

- 有些交换机型号和 IOS 版本可能已达到寿命终止日期，并且可能互操作性不受 Cisco TAC 支持。
- 您必须为 Cisco ISE 分析服务使用最新版本的 NetFlow。如果使用 NetFlow 5 版本，则只能在接入层的主 NAD 上使用。

对于无线局域网控制器，请注意以下事项：

- MAC 身份验证旁路 (MAB) 支持使用 RADIUS 查找执行 MAC 过滤。
- 对 MAC 过滤的会话 ID 和 COA 的支持提供类似于 MAB 的功能。
- WLC 8.0 及更高版本支持基于 DNS 的 ACL 功能。并非所有无线接入点都支持基于 DNS 的 ACL。有关详细信息，请参阅 《*Cisco* 无线接入点版本说明》。

有关使用Cisco ISE 验证的设备的信息，请参阅 《Cisco 身份服务引擎验证的网络设备功能》。

以下标记用于标记设备支持：

- √ ：完全支持
- X：不支持
- ! ：有限的支持，部分可能不受支持

各项特性支持的功能如下：

表 *1:* 特性和功能

特性	功能
AAA	802.1X、MAB、VLAN 分配、dACL
分析	RADIUS CoA 和分析探测
自带设备	RADIUS CoA、URL 重定向和 SessionID
访客	RADIUS CoA、本地网络身份验证、URL 重定向和 SessionID
访客原始 URL	RADIUS CoA、本地网络身份验证、URL 重定向和 SessionID
状态	RADIUS CoA、URL 重定向和 SessionID
MDM	RADIUS CoA、URL 重定向和 SessionID
TrustSec	SGT 分类

经验证的 Cisco 接入交换机

表 *2:* 经验证的 *Cisco* 接入交换机

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
IE2000 IE3000	Cisco IOS 15.2（2）E4 Cisco IOS 15.2（4）EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0（2）EB	√	√	√	√	*X*	√	√	√
IE4000 IE5000	Cisco IOS 15.2（2）E5 Cisco IOS 15.2（4）E2 Cisco IOS 15.2（4）EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	Cisco IOS 15.2（2）E5 Cisco IOS 15.2（4）E2	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
CGS 2520	Cisco IOS 15.2（3）E3	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2（3）E3	√	√	√	√	*X*	√	√	√
Catalyst 1000	Cisco IOS 15.2（7）E3	√	√	√	√	√	√	√	—
	Cisco IOS 15.2（7）E3	√	√	√	√	√	√	√	—

设备	经验证的操作系统[1] 最低操作系统 [3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec [2]
Catalyst 2960 LAN Base	Cisco IOS 15.0（2）SE11	√	√	√	√	*X*	√	√	*X*
	Cisco IOS v12.2（55）SE5[4]	√	√	√	!	*X*	!	!	*X*
Catalyst 2960-C Catalyst 3560-C	Cisco IOS 15.2（2）E4	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）EX3	√	√	√	√	√	√	√	√
Catalyst 2960-L	Cisco IOS 15.2（6.1.27）E2	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.2（6）E2	√	√	√	√	√	√	√	*X*
Catalyst 2960-Plus Catalyst 2960-SF	Cisco IOS 15.2（2）E4	√	√	√	√	√	√	√	√
	Cisco IOS 15.0（2）SE7	√	√	√	√	√	√	√	*X*
Catalyst 2960-S	Cisco IOS 15.2（2）E6 Cisco IOS 15.2（2）E9 Cisco IOS 15.0.2SE10a Cisco IOS 15.0（2）SE11	√ √ √	√ √ √	√ √ √	√ √ √	√ √ √	√ √ √	√ √ √	√ *X* *X*
	Cisco IOS 12.2.（55）SE5	√	√	√	√	√	√	√	*X*

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
Catalyst 2960 – XR Catalyst 2960 – X	Cisco IOS 15.2（2）E6 Cisco IOS 15.2（2）E5 Cisco IOS 15.2（4）E2 Cisco IOS 15.2.6E1（ED） Cisco IOS 15.2（2）E9 Cisco IOS 15.2（7）E0a	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
Catalyst 2960-CX Catalyst 3560-CX	Cisco IOS 15.2（3）E1	√	√	√	√	√	√	√	√
	Cisco IOS 15.2（3）E	√	√	√	√	√	√	√	√
Catalyst 3560-G Catalyst 3750-G Cat 3750-E	Cisco IOS 15.2（2）E6 Cisco IOS 12.2（55）SE5 Cisco IOS 12.2（55）SE10 Cisco IOS 12.2（55）SE11 Cisco IOS 15.0（2）SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）SE5	√	√	√	√	√	√	√	√
Catalyst 3560V2 Catalyst 3750V2	Cisco IOS 12.2（55）SE10	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）SE5	√	√	√	√	√	√	√	√

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
Catalyst 3560-E	Cisco IOS 15.0（2）SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）SE5	√	√	√	√	√	√	√	√
Catalyst 3560-X	Cisco IOS 15.2（2）E5 Cisco IOS 15.2（2）E6 Cisco IOS 15.2（4）E9	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）SE5	√	√	√	√	√	√	√	√
Catalyst 3650 Catalyst 3650-X	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√
Catalyst 3750-E	Cisco IOS 15.2（2）E6 Cisco IOS 15.0（2）SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）SE5	√	√	√	√	√	√	√	√
Catalyst 3750-X	Cisco IOS 15.2（2）E6 Cisco IOS 15.2（2）E5 Cisco IOS 15.2（4）E2	√	√	√	√	√	√	√	√
	Cisco IOS 12.2（55）SE5	√	√	√	√	√	√	√	√

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
Catalyst 3850	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS XE 3.6.7E Cisco IOS XE 3.6.9E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√
Catalyst 4500-X	Cisco IOS XE 3.6.6 E Cisco IOS 15.2（2）E5 Cisco IOS 15.2（4）E2 Cisco IOS 15.2（6）E	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	X	√	√	√
Catalyst 4500 管理引擎 7-E、7L-E	Cisco IOS XE 3.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	X	√	√	√
Catalyst 4500 管理引擎 6-E、6L-E	Cisco IOS 15.2（2）E4	√	√	√	√	X	√	√	√
	Cisco IOS 15.2(2)E	√	√	√	√	X	√	√	√
Catalyst 4500 管理引擎 8-E	Cisco IOS XE 3.6.4 Cisco IOS XE 3.6.8E Cisco IOS 15.2（6）E Cisco IOS 3.11.0E ED	√	√	√	√	X	√	√	√
	Cisco IOS XE 3.3.2 XO	√	√	√	√	X	√	√	√
Catalyst 5760	Cisco IOS XE 3.7.4	√	√	√	√	X	√	√	√
	-	-	-	-	-	-	-	-	-

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
Catalyst 6500-E（管理引擎 32）	Cisco IOS 12.2（33）SXJ10	√	√	√	√	X	√	√	√
	Cisco IOS 12.2（33）SXI6	√	√	√	√	X	√	√	√
Catalyst 6500-E（管理引擎 720）	Cisco IOS 15.1（2）SY7	√	√	√	√	X	√	√	√
	Cisco IOS v12.2（33）SXI6	√	√	√	√	X	√	√	√
Catalyst 6500-E (VS-S2T-10G)	Cisco IOS 152-1. SY1a	√	√	√	√	X	√	√	√
	Cisco IOS 15.0（1）SY1	√	√	√	√	X	√	√	√
Catalyst 6807-XL Catalyst 6880-X (VS-S2T-10G)	Cisco IOS 152-1. SY1a	√	√	√	√	X	√	√	√
	Cisco IOS 15.0（1）SY1	√	√	√	√	X	√	√	√
Catalyst 6500-E（管理引擎 32）	Cisco IOS 12.2（33）SXJ10	√	√	√	√	X	√	√	√
	Cisco IOS 12.2（33）SXI6	√	√	√	√	X	√	√	√
Catalyst 6848ia	Cisco IOS 152-1. SY1a	√	√	√	√	X	√	√	√
	Cisco IOS 15.1(2) SY+	√	√	√	√	X	√	√	√
Catalyst 9200	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9200-H	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
Catalyst 9200-L	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9300	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS 16.9.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9300H Catalyst 9300L Catalyst 9300S Catalyst 9300 24H	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
Catalyst 9400 Catalyst 9400 LC Catalyst 9400 PoE	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS XE 16.9.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√

设备	经验证的操作系统[1] 最低操作系统[3]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec[2]
Catalyst 9500	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS XE 16.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9500H	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
Catalyst 9600 Catalyst 9600 LC	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
Meraki MS 平台	最新版本	![5]	√	√	![6]	*X*	√	![7]	*X*
	最新版本	!	√	√	!	*X*	√	!	*X*

[1] 经验证的操作系统为经过兼容性和稳定性测试的版本。
[2] 有关 Cisco TrustSec 功能支持的完整列表，请参阅 《Cisco TrustSec 产品公告》。
[3] 最低操作系统为推出功能的版本。
[4] 由于CSCsx97093，IOS 12.x版本不完全支持安全评估和访客流量。对此的解决方法是，在Cisco ISE中配置URL重定向时，请将值分配给“ coa-skip-logical-profile。”
[5] Meraki 交换机不支持 dACL。
[6] Meraki 交换机不支持本地 Web 身份验证。
[7] 仅支持 Meraki MDM。不支持第三方 MDM。

Cisco ISE 支持 Cisco Catalyst 交换机的 SNMP CoA。Cisco Catalyst 交换机的 SNMP CoA 支持以下功能：

- 状态
- 自带设备
- 访客

有关设备传感器支持的 Catalyst 平台的信息，请参阅 https://communities.cisco.com/docs/DOC-72932。

经验证的第三方接入交换机

表 *3:* 经验证的第三方接入交换机

设备	经验证的操作系统[8] 最低操作系统 [10]	AAA	分析	自带设备	访客	终端安全评估	MDM	TrustSec [9]
Avaya ERS 2526T	4.4	√	!	*X*	*X*	*X*	*X*	*X*
	4.4	√	!	*X*	*X*	*X*	*X*	*X*
Brocade ICX 6610	8.0.20	√	√	√	√	√	*X*	*X*
	8.0.20	√	√	√	√	√	*X*	*X*
Extreme X440-48p	ExtremeXOS 15.5	√	*X*	√	√	√	*X*	*X*
	ExtremeXOS 15.5	√	*X*	√	√	√	*X*	*X*
HP H3C HP Procurve	5.20.99	√	√	√	√	√	*X*	*X*
	5.20.99	√	√	√	√	√	*X*	*X*
HP ProCurve 2900	WB.15.18.0007	√	√	√	√	√	*X*	*X*
	WB.15.18.0007	√	√	√	√	√	*X*	*X*
Juniper EX3300	12.3R11.2	√	√	√	√	√	*X*	*X*
	12.3R11.2	√	√	√	√	√	*X*	*X*

[8] 经验证的操作系统为经过兼容性和稳定性测试的版本。
[9] 有关 Cisco TrustSec 功能支持的完整列表，请参阅 《Cisco TrustSec 产品公告》。
[10] 最低操作系统为推出功能的版本。

有关第三方设备支持的详细信息，请参阅 https://communities.cisco.com/docs/DOC-64547

经验证的 Cisco 无线局域网控制器

表 *4:* 经验证的 ***Cisco*** 无线局域网控制器

设备	经验证的操作系统[11]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec [12]
WLC 2100	AireOS 7.0.252.0	!	√	*X*	!	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0（最低）	!	√	*X*	!	*X*	*X*	*X*	*X*
WLC 2504	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√

设备	经验证的操作系统[11]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec [12]
WLC 3504	AirOS 8.5.105.0	√	√	√	√	√	√	√	未验证
WLC 4400	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最低）	!	√	X	!	X	X	X	X
WLC 2500	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 7.2.103.0（最低）	!	√	√	√	X	√	√	X
WLC 5508	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.3.114.x	√	√	√	√	X	√	√	√
	AireOS 8.3.140.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 7.0.116.0（最低）	!	√	X	!	X	X	X	√
WLC 5520	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 8.5.1.x	√	√	√	√	√	√	√	√
	AireOS 8.6.1.x	√	√	√	√	√	√	√	√
	AirOS 8.6.101.0（ED）	√	√	√	√	√	√	√	√
	AireOS 8.1.122.0（最低）	√	√	√	√	X	√	√	√

设备	经验证的操作系统[11]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec [12]
WLC 7500	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.2.154.x	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√
	AireOS 7.2.103.0（最低）	!	√	X	X	X	X	X	X
WLC 8510	AireOS 8.0.135.0	√	√	√	√	X	√	√	X
	AireOS 7.4.121.0（最低）	√	√	X	X	X	X	√	X
WLC 8540	AireOS 8.1.131.0	√	√	√	√	X	√	√	X
	AireOS 8.1.122.0（最低）	√	√	√	√	X	√	√	X
Catalyst 9800-CL	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-L	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-40	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-80	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√

设备	经验证的操作系统[11]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec [12]
Catalyst 9300 上的 Catalyst 9800	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
vWLC	AireOS 8.0.135.0	√	√	√	√	X	√	√	X
	AireOS 7.4.121.0（最低）	√	√	√	√	X	√	√	X
WiSM1 6500	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最低）	!	√	X	!	X	X	X	X
WiSM2 6500	AireOS 8.0.135.0	√	√	√	√	X	√	√	√
	AireOS 7.2.103.0（最低）	!	√	√	√	X	√	√	√
WLC 5760	IOS XE 3.6.4	√	√	√	√	√	√	√	√
	IOS XE 3.3（最低）	√	√	√	√	X	√	√	√
适用于 ISR（ISR2 ISM、SRE700 和 SRE900）的 WLC	AireOS 7.0.116.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最低）	!	√	X	!	X	X	X	X
Meraki MR 平台	公共测试版	√	√	√	√	√	√	√	X
	最新版本（最低）	√	√	√	√	√	√	√	X
Catalyst 接入点-9117AX 上的 Cisco 嵌入式无线控制器	IOS XE 16.12.1	√	√	√	√	√	√	√	X
	IOS XE 16.12.1 IOS XE 17.1.1	√	√	√	√	√	√	√	X

设备	经验证的操作系统[11]	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec [12]
Catalyst 接入点-9115 上的 Cisco 嵌入式无线控制器	IOS XE 16.12.1 IOS XE 17.1.1	√	√	√	√	√	√	√	*X*
	IOS XE 16.12.1	√	√	√	√	√	√	√	*X*

[11] 经验证的操作系统为经过兼容性和稳定性测试的版本。
[12] 有关 Cisco TrustSec 功能支持的完整列表，请参阅 《Cisco TrustSec 产品公告》。

有关受支持操作系统的完整列表，请参阅 《Cisco 无线解决方案软件兼容性列表》 。

注释 由于 CSCvi10594，AireOS 版本 8.1 及更高版本中的 IPv6 RADIUS CoA 失败。对此，您可以使用 IPv4 RADIUS 或将 Cisco 无线局域网控制器降级到 AireOS 8.0 版。

注释 Cisco 无线局域网控制器 (WLC) 和无线服务模块 (WiSM) 不支持可下载的 ACL (dACL)，但支持命名 ACL。自主 AP 部署不支持终端安全状况评估。通过 802.1X 身份验证的 WLAN（自 WLC 7.0.116.0 开始）和通过 MAB 身份验证的 WLAN（自 WLC 7.2.110.0 开始）支持分析服务。集中身份验证配置部署（自 WLC 7.2.110.0 开始）支持 FlexConnect（以前称为“混合远程边缘无线接入点 (HREAP) 模式）。有关 FlexConnect 支持的更多信息，请参阅适用的无线控制器平台的版本说明。

支持的 Cisco 接入点

表 *5:* 支持的 *Cisco* 接入点

Cisco 接入点	最低 Cisco Mobility Express 版本	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec
Cisco Aironet 1540 系列	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1560 系列	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*

Cisco 接入点	最低 Cisco Mobility Express 版本	AAA	分析	自带设备	访客	访客原始 URL	终端安全评估	MDM	TrustSec
Cisco Aironet 1815i	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 1815m	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 1815w	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 2800 系列	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 3800 系列	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X

经验证的第三方无线局域网控制器

表 *6:* 经验证的第三方无线局域网控制器

设备	经验证的操作系统[13] / 最低操作系统 [15]	AAA	分析	自带设备	访客	终端安全评估	MDM	TrustSec [14]
Aruba 3200[16]	6.4	√	√	√	√	√	X	X
Aruba 3200XM	6.4	√	√	√	√	√	X	X
Aruba 650	6.4	√	√	√	√	√	X	X
Aruba 7000	6.4.1.0	√	√	√	√	√	X	X
Aruba IAP	6.4.1.0	√	√	√	√	√	X	X
Motorola RFS 4000	5.5	√	√	√	√	√	X	X
	5.5	√	√	√	√	√	X	X

设备	经验证的操作系统[13] 最低操作系统 [15]	AAA	分析	自带设备	访客	终端安全评估	MDM	TrustSec [14]
HP 830	35073P5	√	√	√	√	√	X	X
	35073P5	√	√	√	√	√	X	X
Ruckus ZD1200	9.9.0.0	√	√	√	√	√	X	X
	9.9.0.0	√	√	√	√	√	X	X

13 经验证的操作系统为经过兼容性和稳定性测试的版本。
14 有关 Cisco TrustSec 功能支持的完整列表，请参阅 《Cisco TrustSec 产品公告》。
15 最低操作系统为推出功能的版本。
16 Aruba 3200 支持 ISE 2.2 补丁 2 及更高版本。

有关第三方设备支持的详细信息，请参阅 https://communities.cisco.com/docs/DOC-64547

经过验证的 Cisco 路由器

表 7: 经过验证的 *Cisco* 路由器

设备	经验证的操作系统[17] 最低操作系统 [18]	AAA	分析	自带设备	访客	终端安全评估	MDM	TrustSec [19]
ISR 88x、89x 系列	IOS 15.3.2T(ED)	√	X	X	X	X	X	X
	IOS 15.2(2)T	√	X	X	X	X	X	X
ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X	IOS XE 17.1.1 IOS XE 17.2.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√
ISR 19x、29x、39x 系列	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
	IOS 15.2(2)T	√	!	X	!	X	X	√
CE 9331	IOS XE 17.1.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√
CGR 2010	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
	IOS 15.3.2T(ED)	√	!	X	!	X	X	√

设备	经验证的操作系统[17] 最低操作系统 [18]	AAA	分析	自带设备	访客	终端安全评估	MDM	TrustSec [19]
4451-XSM-X L2/L3 Ethermodule	IOS XE 3.11	√	√	√	√	√	√	√
	IOS XE 3.11	√	√	√	√	√	√	√

17 经验证的操作系统为经过兼容性和稳定性测试的版本。
18 最低操作系统为推出功能的版本。
19 有关 Cisco TrustSec 功能支持的完整列表，请参阅 《Cisco TrustSec 产品公告》。

经验证的 Cisco 远程访问

表 *8:* 经验证的 *Cisco* 远程访问

设备	经验证的操作系统[20] 最低操作系统 [22]	AAA	分析	自带设备	访客	终端安全评估	MDM	TrustSec [21]
ASA 5500、ASA 5500-X（仅限远程访问）	ASA 9.2.1	不适用	不适用	√	不适用	√	*X*	√
	ASA 9.1.5	不适用	不适用	*X*	NA	*X*	*X*	*X*
Meraki MX 平台	最新版本	√	√	√	√	√	√	*X*
	最新版本	√	√	√	√	√	√	*X*

20 经验证的操作系统为经过兼容性和稳定性测试的版本。
21 有关 Cisco TrustSec 功能支持的完整列表，请参阅 《Cisco TrustSec 产品公告》。
22 最低操作系统为推出功能的版本。

RADIUS 代理服务的 AAA 属性

关于 RADIUS 代理服务，在 RADIUS 通信中必须包含以下身份验证、授权和记帐 (AAA) 属性：

- Calling-Station-ID (IP 或 MAC_ADDRESS)
- RADIUS :: NAS_IP_Address
- RADIUS :: NAS_Identifier

第三方 VPN 集中器的 AAA 属性

为了使 VPN 集中器与 Cisco ISE 相集成，在 RADIUS 通信中必须包含以下身份验证、授权和记帐 (AAA) 属性：

- Calling-Station-ID（按 MAC 或 IP 地址跟踪单个客户端）
- 用户名（按登录名跟踪远程客户端）

- NAS 端口类型（有助于确定连接类型为 VPN）
- RADIUS 记帐开始（触发会话的正式开始）
- RADIUS 记帐停止（触发会话的正式结束并发布 ISE 许可证）
- RADIUS 记帐 IP 地址更改临时更新（例如，SSL VPN 连接从基于 Web 的过渡到全隧道客户端）

注释 对于 VPN 设备，RADIUS 记帐消息必须将 Framed-IP-Address 属性设置为 VPN 客户端的 IP 地址池以在受信任网络上跟踪端点。

经验证的外部身份源

表 *9:* 经验证的外部身份源

外部身份来源	操作系统/版本
Active Directory [2324]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [25]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [26]	Windows Server 2019
LDAP 服务器	
SunONE LDAP 目录服务器	版本 5.2
OpenLDAP 目录服务器	2.4.23 版
任何 LDAP v3 兼容服务器	任何符合 LDAP v3 的版本
令牌服务器	
RSA ACE/Server	6.x 系列
RSA Authentication Manager	7.x 和 8.x 系列
兼容 RADIUS RFC 2865 的任何令牌服务器	符合 RFC 2865 标准的任何版本
安全断言标记语言 (SAML) 单点登录 (SSO)	
Microsoft Azure	最新

外部身份来源	操作系统/版本
Oracle Access Manager (OAM)	版本 11.1.2.2.0
Oracle Identity Federation (OIF)	版本 11.1.1.2.0
PingFederate 服务器	版本 6.10.0.4
PingOne云	最新
安全身份验证	8.1.1
任何符合 SAMLv2 的身份提供程序	符合 SAMLv2 的任何身份提供程序版本
开放式数据库连接 (ODBC) 身份源	
Microsoft SQL Server	Microsoft SQL Server 2012
Oracle	企业版版本12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
社交登录（用于访客用户帐户）	
Facebook	最新

[23] Cisco ISE OCSP 功能仅适用于 Microsoft Windows Active Directory 2008和更高版本。

[24] 在 Cisco ISE 上最多只能添加 200 个域控制器。如果超出此限制，您将收到错误：

```
错误创建 <DC FQDN> 时出错 - DC 数超出允许的最大值 200
```

[25] Cisco

ISE 支持 Microsoft Windows Active Directory 2012 R2 中的所有旧功能，但不支持 Microsoft Windows Active Directory 2012 R2 中的新功能，例如保护用户组。

[26] Cisco ISE 2.6补丁4及更高版本支持Microsoft Windows Active Directory 2019中的所有旧功能。

获取详细信息，请参阅 《*Cisco* 身份识别服务引擎管理员指南》 。

已验证的 MDM 服务器

经验证的 MDM 服务器包括来自以下供应商的产品：

- Absolute
- VMware AirWatch
- Citrix XenMobile

- Globo
- Good Technology
- IBM MaaS360
- JAMF Software
- Meraki SM/EMM
- MobileIron
- SAP Afaria
- SOTI
- Symantec
- Tangoe
- Microsoft Intune - 用于移动设备
- Microsoft SCCM - 用于桌面设备

管理员门户支持的浏览器

- Mozilla Firefox 88 及更低版本
- Mozilla Firefox ESR 60.9 及更低版本
- Google Chrome 90 及更低版本
- Microsoft Internet Explorer 11.x

支持的硬件

Cisco ISE 版本 2.7 可以安装在以下平台上：

表 *10:* 支持的平台

硬件平台	配置
Cisco SNS-3515-K9（小型）	有关设备硬件规格，请参阅 《*Cisco* 安全网络服务器硬件安装指南》 。
Cisco SNS-3595-K9（大型）	
Cisco SNS-3615-K9（小）	
Cisco SNS-3655-K9（中）	
Cisco SNS-3695-K9（大）	

安装完成后，您可以在上述表格中列出的平台上使用指定组件角色，如管理、监控或 pxGrid 配置 Cisco ISE。除这些角色外，Cisco ISE 还包含策略服务中的其他类型的角色，如分析服务、会话服务、以威胁为中心的 NAC 服务、TrustSec SXP 服务、TACACS+ 设备管理服务和被动身份服务。

注意

- Cisco ISE 3.1 不支持 Cisco 安全网络服务器（SNS）3515 设备。
- Cisco ISE 版本 2.4 及更高版本不支持 Cisco SNS 3400 系列设备。
- VM 设备配置均不支持少于 16 GB 的内存分配。如果出现 Cisco ISE 行为问题，所有用户都需要在使用 Cisco 技术支持中心新建案例之前，将分配的内存更改为至少 16 GB。
- 旧版访问控制服务器 (ACS) 和网络访问控制 (NAC) 设备（包括 Cisco ISE 3300 系列）不支持 Cisco ISE 版本 2.0 和更高版本。

经验证的虚拟环境

Cisco ISE 支持以下虚拟环境平台：

- VMware ESXi 5.x（5.1 U2及更高版本支持RHEL 7），6.x

注释 如果要在 ESXi 5.x 服务器上安装或升级 Cisco ISE，请将 VMware 硬件版本更新至 9 或更高版本来支持 RHEL 7 作为访客操作系统。RHEL 7 支持与 VMware 硬件版本 9 及更高版本配合使用。

-
- QEMU 1.5.3-160 上的 KVM
- Microsoft Windows Server 2012 R2 及更高版本上的 Microsoft Hyper-V

注意 VMware 快照用于保存 VM 在给定时间点的状态，因此 Cisco ISE 不支持使用 VMware 快照备份 ISE 数据。在多节点 Cisco ISE 部署中，所有节点中的数据都与当前数据库信息保持同步。恢复快照可能会导致数据库复制和同步问题。建议您使用 Cisco ISE 中包含的备份功能来存档和恢复数据。

使用 VMware 快照备份 ISE 数据将导致停止 Cisco ISE 服务。需要重启才能激活 ISE 节点。

经验证的 Cisco 全数字化网络架构中心版本

表 *11:* 经验证的 *Cisco* 全数字化网络架构中心版本

经验证的 Cisco DNA 中心版本	经验证的 Cisco ISE 版本
1.2.12.0	Cisco ISE 2.7
1.3.0.0	Cisco ISE 2.7

经验证的 **Cisco DNA** 中心版本	经验证的 **Cisco ISE** 版本
1.3.0.6	Cisco ISE 3.0
1.3.1.0	Cisco ISE 2.4 补丁 9、补丁 11 Cisco ISE 2.6 补丁 2 Cisco ISE 2.7
1.3.1.4	Cisco ISE 2.4 补丁 12 Cisco ISE 2.6 补丁 6 Cisco ISE 2.7 补丁 2 Cisco ISE 3.0
1.3.2.0	Cisco ISE 2.4 补丁 10、补丁 11 Cisco ISE 2.7
1.3.3.0	Cisco ISE 2.7 补丁 1 Cisco ISE 3.0
1.3.3.4	Cisco ISE 2.6 补丁 6
1.3.3.5	Cisco ISE 2.4 补丁 13 Cisco ISE 2.7 补丁 2
2.1.1.0	Cisco ISE 2.4 补丁 12 Cisco ISE 2.6 补丁6、补丁 7 Cisco ISE 2.7 补丁1、补丁2 Cisco ISE 3.0
2.1.1.1	Cisco ISE 3.0
2.1.2.0	Cisco ISE 2.4 补丁12、补丁13 Cisco ISE 2.6 补丁6、补丁8 Cisco ISE 2.7 补丁1、补丁3 Cisco ISE 3.0
2.1.2.4	Cisco ISE 3.0 补丁 1
2.1.2.5	Cisco ISE 3.0 补丁 1、补丁 2
2.1.2.6	Cisco ISE 2.4 补丁 14 Cisco ISE 2.7 补丁 4

经验证的 Cisco DNA 中心版本	经验证的 Cisco ISE 版本
2.2.1.0	Cisco ISE 2.4 补丁13、补丁14 Cisco ISE 2.6 补丁 7、补丁 8、补丁 9 Cisco ISE 2.7 补丁 2 Cisco ISE 3.0 补丁 1、补丁 3
2.2.2.0	Cisco ISE 2.4 补丁 14 Cisco ISE 2.6 补丁 8、补丁 9 Cisco ISE 2.7 补丁 2、补丁 3、补丁 4 Cisco ISE 3.0 补丁 1

有关 Cisco ISE 与 Cisco 全数字化网络架构中心（Cisco DNA 中心）的兼容性的详细信息，请参阅 Cisco SD-Access 兼容性列表。

经验证的 Cisco Mobility Services Engine 版本

Cisco ISE 与 Cisco Mobility Services Engine（MSE）相集成，版本 8.0.110.0 以提供位置服务（也称为“情景感知服务”）。此服务允许您跟踪无线设备的位置。

有关如何集成 Cisco ISE 与 Cisco MSE 的信息，请参阅以下内容：

- Mobility Services Engine (MSE) 和身份服务引擎 (ISE) 2.0 的基于位置的授权
- *Cisco* 身份服务引擎管理员指南

经验证的 Cisco Prime 基础设施版本

Cisco Prime 基础设施版本 3.6 或更高版本可与 Cisco ISE 2.6 或更高版本集成，以利用 Cisco ISE 的监控和报告功能。

经验证的 Cisco Stealthwatch 版本

Cisco ISE 2.7 已通过 Cisco Stealthwatch 版本 7.0 验证。

经过验证的 Cisco WAN 服务管理员版本

支持威胁中心的 NAC

Cisco ISE 已使用以下适配器进行验证：

- Sourcefire FireAMP
- 感知威胁分析 (CTA) 适配器
- Rapid7 Nexpose

- Tenable 安全中心
- Qualys（ TC-NAC 流目前仅支持 Qualys 企业版）

经过验证的客户端机器操作系统、请求者和代理

此处列出了支持的客户机操作系统、浏览器及支持每种客户机类型的代理版本。对于所有设备，还必须在 Web 浏览器中启用 Cookies。Cisco AnyConnect-ISE 终端安全评估支持图表位于：https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

Cisco ISE 版本 2.3 及更高版本仅支持 Cisco AnyConnect 和 Cisco 临时代理。

所有标准 802.1X 请求者均可与 Cisco ISE 版本 2.4 和更高标准和高级功能搭配使用，只要它们支持 Cisco ISE 支持的标准身份验证协议即可。对于用于无线部署的 VLAN 变更授权功能，请求者必须支持对 VLAN 变更进行 IP 地址刷新。

终端安全评估和自带设备（BYOD）流程受 Cisco ISE UI 中列出的操作系统通用可用性版本（基于最新终端安全评估更新）的支持。终端安全评估和BYOD流程也可在 Cisco ISE UI 中列出的测试版 macOS 版本中使用。例如，如果在 Cisco ISE UI 中列出了 **macOS 12 Beta**（**全部**），则安全评估和自带设备流量可能适用于 macOS 12 Beta 终端。尽力提供支持，因为测试版操作系统版本通常会在初始版本和通用版本之间进行重大更改。

请注意，当您将操作系统（OS）更新为新版本时，您可能会遇到对 Posture Feed Server 中更新的操作系统版本的支持和复制延迟（几小时或一天）的情况。

Google Android

由于 Android 实施在特定设备上开放访问的性质，Cisco ISE 可能不支持某些 Android 操作系统版本和设备组合。

以下 Google Android 版本已通过 Cisco ISE 验证：

- Google Android 10.x
- Google Android 9.x
- Google Android 8.x
- Google Android 7.x

以下 Android 设备已通过 Cisco ISE 验证。有关在Cisco ISE中支持BYOD流程的设备列表，请参阅验证的网络访问设备部分。，第 2 页

表 *12:* 经验证的 *Android* 设备

设备型号	**Android 版本**
Google Pixel 3	10
OnePlus 6	10
Samsung S9	9
Google Nexus 6P	8.1
华为 Mate Pro 10	8

在启动请求方调配向导（SPW）之前，请确保在 Android 9.x 和 10.x 设备上启用了位置服务。

Android 不再使用公用名（CN）。主机名必须在 subjectAltName（SAN）扩展名中，否则信任会失败。 如果您使用的是自签名证书，请从门户的 SAN 下拉列表中选择域名或 IP 地址选项（在 **管理 > 系统 > 证书 > 系统证书**）下重新生成 Cisco ISE 自签名证书。

如果您使用的是 Android 9.x，则必须更新 Cisco ISE 中的终端安全评估源以获取 Android 9 的 NSA。

Apple iOS

尽管 Apple iOS 设备对于 Cisco ISE 或 802.1x 使用受保护的扩展身份验证协议 (PEAP)，但公共证书包括 iOS 设备需要验证的 CRL 分布点，不过如果没有网络访问，则无法执行验证。点击 iOS 设备中的“确认/接受”(confirm/accept) 可验证网络。

以下Apple iOS版本已通过Cisco ISE验证：

- Apple iOS 13.x
- Apple iOS 12.x
- Apple iOS 11.x

以下 iPhone / iPad 设备已通过 Cisco ISE 验证。有关在 Cisco ISE 中支持BYOD流程的设备列表，请参阅部分。

表 *13:* 经验证的 *iPhone/iPad* 设备

设备型号	**iOS 版本**
iPhone X	iOS 13
iPhone 8	iOS 12.3
iPhone 7	iOS 13.2
iPhone 6	iOS 12.6
iPhone 5s	iOS 12，iOS 10.3
iPad	iPad OS 13.1

注释

- 如果您使用的是Apple iOS 12.2或更高版本，则必须手动安装下载的证书/配置文件。要执行此操作，请在Apple iOS设备中选择 **设置**（**Settings**）**>常规**（**General**）**>配置文件**（**Profile**），然后点击**安装**（**Install**）。
- 如果您使用的是Apple iOS 12.2或更高版本，则RSA密钥大小必须为2048位或更高。否则，您可能会在安装 BYOD 配置文件时看到错误。
- 如果您使用的是 Apple iOS 13或更高版本，请通过添加<FQDN>在DNS字段中。
- 如果您使用的是 Apple iOS 13或更高版本，请确保选择 **SHA-256** （或更高版本）作为签名算法。

Apple macOS

表 14: Apple macOS

客户机操作系统	**AnyConnect**
Apple macOS 11	4.9.04043 或更高版本
Apple macOS 10.15	4.8.01090 或更高版本
Apple macOS 10.14	4.8.01090 或更高版本
Apple macOS 10.13	4.8.01090 或更高版本

Cisco ISE 可以与早期版本的 AnyConnect 4.x 配合使用。但是，只有较新的 AnyConnect 版本支持较新的功能。

注释 对于 Apple macOS 11，您必须使用 Cisco AnyConnect 4.9.04043 或更高版本以及 MAC OSX 合规性模块 4.3.1466.4353 或更高版本。

如果您使用的是 Apple macOS 11，您可能会在安装 Cisco 网络设置助手时看到手动安装配置文件的提示。在这种情况下，您必须执行以下操作：

1. 导航至下载文件夹。
2. 双击 cisco802dot1xconfiguration.mobileconfig 文件。
3. 选择 **系统 > 首选项**。
4. 点击 **配置文件**。
5. 安装配置文件。
6. 在 Cisco 网络设置助手中显示的提示符中点击 **确定** 继续安装。

注释 适用于 MAC OSX 版本 3.1.0.1 的请求方调配向导捆绑包适用于所有 Cisco ISE 版本。已使用 Cisco ISE 2.4 补丁 12、Cisco ISE 2.6 补丁 8、Cisco ISE 2.7 补丁 3 和 Cisco ISE 3.0 补丁 2 进行了验证。

有关 Cisco ISE 终端安全评估代理支持的 Windows 和 MAC OSX 防恶意软件、补丁管理、磁盘加密和防火墙产品的信息，请参阅 Cisco AnyConnect-ISE 终端安全评估支持图表。

注释

- 所有浏览器均已将报告的 Apple macOS 版本限制为 10.15.7，并提高了用户隐私。
- 在调配期间，我们将无法识别 Apple macOS 11 终端。当客户端运行 Apple macOS 11 时，这会导致安全评估和 BYOD 流中的 CP 策略匹配出现问题。对此的解决方法是，将 Apple macOS 11 的终端安全评估和自带设备流程作为映射 CP 策略作为 macOS 全部。
- 在分类期间，我们将无法识别 Apple macOS 11 终端。这会导致客户端运行 Apple macOS 11 时分析策略匹配出现问题。

Microsoft Windows

表 *15: Microsoft Windows*

客户机操作系统	请求者 (802.1X)	Cisco 临时代理	AnyConnect 如果安装了 AnyConnect 网络访问管理器（NAM），NAM 优先于 Windows 本机请求方作为 802.1X 请求方，并且它不支持自带设备流程。[27]
Microsoft Windows 10			

客户机操作系统	请求者 (802.1X)	Cisco 临时代理	AnyConnect 如果安装了 AnyConnect 网络访问管理器（NAM），NAM 优先于 Windows 本机请求方作为 802.1X 请求方，并且它不支持自带设备流程。[27]
• Windows 21H1 Windows 20H2 • Windows 20H1 • Windows 19H2 • Windows 19H1 • Windows 10 企业版 • Windows 10 企业版 N • Windows 10 企业版 E • Windows 10 企业版 LTSB • Windows 10 企业版 N LTSB • Windows 10 专业版 • Windows 10 专业版 N • Windows 10 专业版 E • Windows 10 教育版 • Windows 10 家庭版 • Windows 10 家庭版 中文版 • Windows 10.0 SLP（单语言包）	• Microsoft Windows 10 802.1X 客户端 • AnyConnect 网络访问管理器	4.5 或更高版本	4.8.01090 或更高版本

[27] 您必须完全禁用 NAM 或在特定接口上禁用 NAM。有关详细信息，请参阅《Cisco AnyConnect 安全移动客户端管理员指南》。

要在 Firefox 70 中为自带设备、访客和客户端调配门户启用无线重定向，请执行以下操作：

Google Chromebook

Google Chromebook 是受管设备，不支持终端安全评估服务。获取详细信息，请参阅 《*Cisco* 身份识别服务引擎管理员指南》 。

表 *16: Google Chromebook*

客户机操作系统	Web 浏览器	Cisco ISE
Google Chromebook	Google Chrome 版本 49 或更高版本	Cisco ISE 2.4 补丁 8 Cisco ISE 2.6 补丁 1

Cisco ISE BYOD 或访客门户可能无法在 Chrome 操作系统 73 中启动，即使 URL 已成功重定向。要在 Chrome 操作系统 73 中启动门户，请执行以下步骤：

1. 通过填充“主题备用名称”(Subject Alternative Name) 字段，从 ISE GUI 生成新的自签证书。必须填充 DNS 和 IP 地址。
2. 导出证书并将其复制到最终客户端（Chrome 手册）。
3. 选择 **设置 > 高级 > 隐私和安全 > 管理证书 > 颁发机构**。
4. 导入证书。
5. 打开 Chrome 浏览器，然后尝试重定向门户。

在 Chromebook 76 及更高版本中，如果您使用用于 EAP 的内部 CA 配置 EAP-TLS 设置，请将包含 SAN 字段的 CA 证书链上传到 Google 管理控制台 **设备管理 > 网络 > 证书**。CA 链上传后，Cisco ISE 生成的具有 SAN 字段的证书会映射到 **Chromebook Authorities** 部分，以将您的 Cisco ISE 证书视为受信任证书。

如果您使用的是第三方 CA，则无需将 CA 链导入到 Google 管理控制台。选择 **设置 > 高级 > 隐私和安全 > 管理证书 > 服务器证书颁发机构**，然后从下拉列表中选择 **使用任何默认证书颁发机构** 。

其他操作系统

表 *17:* 其他操作系统

客户机操作系统	Web 浏览器 [28]	请求者 (802.1X)
Red Hat Enterprise Linux (RHEL)	• Google Chrome • Mozilla Firefox	未经广泛测试 [29]

[28] Google Chrome 不支持 32 位 Linux 系统。
[29] Cisco 未对 802.1X 支持进行广泛的测试，但只要 802.1X 请求者符合 IEEE 802.1X 标准，即受支持。

“发起方”(Sponsor)、“访客”(Guest) 和“我的设备”(My Devices) 门户的经验证操作系统和浏览器

这些 Cisco ISE 门户支持以下操作系统和浏览器组合。这些门户要求您在 Web 浏览器中启用 Cookies。

表 *18:* 经验证的操作系统和浏览器

支持的操作系统[30]	浏览器版本
Google Android[31] 10.x，9.x，8.x，7.x	• 本机浏览器 • Mozilla Firefox • Google Chrome
Apple iOS 13.x，12.x，11.x	• Safari
Apple macOS 11、10.15、10.14、10.13	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10	• Microsoft IE 11.x • Mozilla Firefox • Google Chrome

[30] 最近正式发布的两款浏览器版本适用于Microsoft Windows之外的所有操作系统；有关支持的Internet Explorer版本，请参阅表格 14。

[31] 由于 Android 实施在特定设备上开放访问的性质，Cisco ISE 可能不支持某些 Android 操作系统版本和设备组合。

注册和证书调配的经验证的设备

对于自带设备功能，需要Cisco无线局域网控制器(WLC)7.2或更高版本的支持。有关任何已知问题或警告，请参阅 《Cisco身份服务引擎发行说明》 。

注释 要获取Cisco支持的最新客户端操作系统版本，请检查终端安全评估更新信息（“管理”（**Administration**）>“系统”（**System**）>“设置”（**Settings**）>“终端安全评估”（**Posture**）>“更新”（**Updates**））然后点击“立即更新”（**Update Now**）。

表 *19:* 自带设备注册和证书调配 - 经验证的的设备和操作系统

设备	操作系统	单 SSID	双 SSID（“打开”(open) >“PEAP”(无证书)或“打开”(open) >“TLS”）	注册方法
Apple iDevice	Apple iOS 13.x，12.x，11.x Apple iPad OS 13.x	支持	是[32]	Apple 配置文件配置（本地）
Google Android	10.x，9.x，8.x，7.x	是[33]	支持	Cisco 网络设置助理
Barnes & Noble Nook (Android) HD/HD+已安装Google Play Store[34]	-	-	-	-
Windows	Windows 10 EAP TEAP需要Microsoft Windows 10版本2004（操作系统19041.1）及更高版本。	在配置连接的无线属性[35]	支持	2.2.1.53 或更高版本
Windows	Mobile 8、Mobile RT、Surface 8 和 Surface RT	否	否	-
Apple macOS	Apple macOS 11、10.15、10.14、10.13	是	是	2.2.1.43 或更高版本

[32] 调配后连接到安全 SSID。

[33] 如果使用Android 6.0或更高版本，则无法使用Cisco请求方调配向导（SPW）修改系统创建的SSID。当SPW提示您忘记网络时，您必须选择此选项并按“后退”按钮以继续调配流程。

[34] 2.1.0 时，可以使用 Barnes & Noble Nook (Android)。

[35] （“安全”(Security) >“身份验证方法”(Auth Method) >“设置”(Settings) >“验证服务器证书”(Validate Server Certificate)）时，请取消选中有效的服务器证书选项。如果选中此选项，请确保选择正确的根证书。

支持的协议标准，RFC 和 IETF 草案

Cisco ISE 符合以下协议标准，征求意见稿（RFC）和 IETF 草案：

- **支持的 IEEE 标准**
  - IEEE802.1X-Std-2001
  - IEEE802.1X-Std-2004
- **支持的 IETF RFC**

- RFC2138 - RADIUS
- RFC2139 - RADIUS 记账
- RFC2246 - TLSv1.0
- RFC2284 - EAP
- RFC2548 - Microsoft 供应商特定的 RADIUS 属性
- RFC2716 - EAP TLS
- RFC2759 - Microsoft PPP CHAP扩展，版本2
- RFC2865 - RADIUS
- RFC2866 - RADIUS 记账
- RFC2867 - 适用于隧道协议支持的 RADIUS 记帐修改
- RFC2868 - 用于隧道协议支持的 RADIUS 属性
- RFC2869 - RADIUS 扩展
- RFC3579 - RADIUS 的 EAP 支持
- RFC3580 - IEEE 802.1X RADIUS 准则
- RFC3748 - EAP - 已过时 RFC2284
- RFC4017 - 无线 LAN 的 EAP 方法要求
- RFC4851 - EAP - FAST
- RFC5176 - 到 RADIUS 的动态授权许可扩展
- RFC5216 - EAP - TLS 身份验证协议

部分支持以下 RFC：

- RFC2548 - Microsoft 供应商特定的 RADIUS 属性
- RFC2882 - 网络接入服务器要求：扩展 RADIUS 做法
- RFC7030 - 安全传输注册 (EST)（作为自带设备流程的一部分支持
- RFC7170 - 隧道可扩展身份验证协议 (TEAP) 版本 1

- **支持的 IETF 草稿**
  - IETF 草稿 - 使用 EAP-FAST 进行动态调配
  - IETF 草案 - EAP-TTLSv1.0
  - IETF 草案 - PEAP 版本 0
  - IETF 草案 - PEAP 版本 1

- IETF 草案 - PEAP 版本 2

经验证的 OpenSSL 版本

Cisco ISE 已使用 OpenSSL 1.0.2.x (CiscoSSL 6.0) 进行验证。

支持的密码套件

Cisco ISE 支持 TLS 版本 1.0、1.1 和 1.2。

Cisco ISE 支持 RSA 和 ECDSA 服务器证书。支持以下椭圆曲线：

- secp256r1
- secp384r1
- secp521r1

下表列出了支持的密码套件：

密码套件	当 Cisco ISE 配置为 EAP 服务器时 当 Cisco ISE 配置为 RADIUS DTLS 服务器时	当 Cisco ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL 时 当 Cisco ISE 配置为安全系统日志客户端或安全 LDAP 客户端时 当 Cisco ISE 配置为 CoA 的 RADIUS DTLS 客户端时
TLS 1.0 支持	当允许 TLS 1.0 时 （DTLS 服务器仅支持 DTLS 1.2） 默认情况下，在Cisco ISE 2.3 及更高版本中，“允许 TLS 1.0”选项(Allow TLS 1.0) 选项处于禁用状态。当禁用此选项时，基于 TLS 的 EAP 身份验证方法（EAP-TLS、EAP-FAST/TLS）和 802.1X 请求方不支持 TLS 1.0。如果要在 TLS 1.0 中使用基于 TLS 的 EAP 身份验证方法，请选中**安全设置 (Security Settings)**窗口中的“允许 TLS 1.0”(Allow TLS 1.0) 复选框。要查看此窗口，请依次选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > 安全设置 (Security Settings)**。	当允许 TLS 1.0 时 （DTLS 客户端仅支持 DTLS 1.2）

TLS 1.1 支持	当允许 TLS 1.1 时 默认情况下，在Cisco ISE 2.3 及更高版本中，“允许 TLS 1.1”选项(Allow TLS 1.1) 选项处于禁用状态。当禁用此选项时，基于TLS 的 EAP 身份验证方法（EAP-TLS、EAP-FAST/TLS）和 802.1X 请求方不支持 TLS 1.1。如果要在 TLS 1.1 中使用基于 TLS 的 EAP 身份验证方法，请选中“安全设置”(Security Settings) 窗口（管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > 安全设置 (Security Settings)）中的“允许 TLS 1.1”(Allow TLS 1.1) 复选框。	当允许 TLS 1.1 时
ECC DSA 密码		
ECDHE-ECDSA-AES256-GCM-SHA384	是	是
ECDHE-ECDSA-AES128-GCM-SHA256	是	是
ECDHE-ECDSA-AES256-SHA384	是	是
ECDHE-ECDSA-AES128-SHA256	是	是
ECDHE-ECDSA-AES256-SHA	当允许 SHA-1 时	当允许 SHA-1 时
ECDHE-ECDSA-AES128-SHA	当允许 SHA-1 时	当允许 SHA-1 时
ECC RSA 密码		
ECDHE-RSA-AES256-GCM-SHA384	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES128-GCM-SHA256	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES256-SHA384	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES128-SHA256	当允许 ECDHE-RSA 时	当允许 ECDHE-RSA 时
ECDHE-RSA-AES256-SHA	当允许 ECDHE-RSA/SHA-1 时	当允许 ECDHE-RSA/SHA-1 时
ECDHE-RSA-AES128-SHA	当允许 ECDHE-RSA/SHA-1 时	当允许 ECDHE-RSA/SHA-1 时
DHE RSA 密码		
DHE-RSA-AES256-SHA256	不支持	支持
DHE-RSA-AES128-SHA256	不支持	支持
DHE-RSA-AES256-SHA	否	当允许 SHA-1 时

DHE-RSA-AES128-SHA	否	当允许 SHA-1 时
RSA 密码		
AES256-SHA256	是	是
AES128-SHA256	是	是
AES256-SHA	当允许 SHA-1 时	当允许 SHA-1 时
AES128-SHA	当允许 SHA-1 时	当允许 SHA-1 时
3DES 密码		
DES-CBC3-SHA	当允许 3DES / SHA-1 时	当启用 3DES/DSS 和 SHA-1 时
DSS 密码		
DHE-DSS-AES256-SHA	否	当启用 3DES/DSS 和 SHA-1 时
DHE-DSS-AES128-SHA	否	当启用 3DES/DSS 和 SHA-1 时
EDH-DSS-DES-CBC3-SHA	否	当启用 3DES/DSS 和 SHA-1 时
弱 RC4 密码		
RC4-SHA	当“允许的协议”（Allowed Protocols）页面中启用“允许弱密码”（Allow weak ciphers）选项且允许 SHA-1 时	否
RC4-MD5	当“允许的协议”（Allowed Protocols）页面中启用“允许弱密码”（Allow weak ciphers）选项时	否
仅 EAP-FAST 匿名调配： ADH-AES-128-SHA	支持	不支持
对等证书限制		
验证 KeyUsage	对于以下密码，客户端证书应具有 KeyUsage=密钥协议和 ExtendedKeyUsage=客户端身份验证： • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

验证 ExtendedKeyUsage	对于以下密码，客户端证书应具有 KeyUsage=密钥加密和 ExtendedKeyUsage=客户端加密： • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	服务器证书应具有 ExtendedKeyUsage=服务器身份验证

CA 与 Cisco ISE 互操作的要求

在 CA 服务器中使用 Cisco ISE 时，请确保满足以下要求：

- 密钥大小应为 1024、2048 或更高。在 CA 服务器中，密钥大小使用证书模板定义。您可以使用请求方配置文件在 Cisco ISE 上定义密钥大小。
- 密钥使用应允许在扩展中应用签名和加密。
- 通过 SCEP 协议使用 GetCACapabilities 时，应支持加密算法和请求散列。建议使用 RSA 和 SHA1。
- 支持在线证书状态协议 (OCSP)。虽然这在自带设备 (BYOD) 中并不会直接使用，但是可以使用能充当 OCSP 服务器的 CA 来撤销证书。

注释 对于代理 SCEP，Cisco ISE 不支持企业 Java Beans 证书颁发机构 (EJBCA)。Cisco ISE 支持使用 EJBCA 进行 PEAP、EAP-TLS 等标准 EAP 身份验证。

- 如果您使用企业 PKI 为 Apple iOS 设备颁发证书，请务必在 SCEP 模板中配置密钥用法并启用**密钥加密 (Key Encipherment)** 选项。

如果您使用 Microsoft CA，请在证书模板中编辑“密钥用法扩展”(Key Usage Extension)。在**加密 (Encryption)** 区域中，点击**只在密钥加密时允许密钥交换（密钥加密）(Allow Key Exchange only with Key Encryption (Key encipherment))** 单选按钮，并选中**允许对用户数据加密 (Allow encryption of user data)** 复选框。

- Cisco ISE 支持为信任证书和终端证书使用 RSASSA-PSS 算法，以进行 EAP-TLS 身份验证。查看证书时，签名算法以 1.2.840.113549.1.1.10 形式列出，而非算法名称。

注释 如果您对自带设备流量使用 Cisco ISE 内部 CA，则不应使用 RSASSA-PSS 算法（由外部 CA 签名）对管理员证书签名。Cisco ISE 内部 CA 无法验证使用此算法签名的管理员证书，请求将会失败。

基于证书的身份验证对客户端证书的要求

要在 Cisco ISE 上进行基于证书的身份验证，客户端证书应满足以下要求：

表 *20: RSA* 和 *ECC* 的客户端证书要求

RSA		
支持的密钥大小	1024、2048 和 4096 位	
支持的安全散列算法 (SHA)	SHA-1 和 SHA-2（包括 SHA-256）	
ECC [3637]		
支持的曲线类型	P-192、P-256、P-384 和 P-521	
支持的安全散列算法 (SHA)	SHA-256	
客户端计算机操作系统和支持的曲线类型		
Windows	8 及更高版本	P-256、P-384 和 P-521
Android	4.4 及更高版本 **注释** Android 6.0 需要 2016 年 5 月的补丁以支持 ECC 证书。	所有曲线类型（Android v6.0 除外，它不支持 P-192 曲线类型）。

[36] Windows 7 和 Apple iOS 无法在本地支持用于 EAP-TLS 身份验证的 ECC。
[37] 此 Cisco ISE 版本不支持在 Mac OS X 设备上使用 ECC 证书。

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
CiscoSystems(USA)Pte.Ltd.
Singapore

欧洲总部
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。