Performance and Scalability Guide for Cisco Identity Services Engine

Revised: July 4, 2024

Overview

This document lists the sizing guidelines for Cisco Identity Services Engine (Cisco ISE).

Cisco ISE Node Terminology

A Cisco ISE node can provide various services based on the persona that it assumes. The menu options that are available through the Admin portal are dependent on the role and personas that a Cisco ISE node assumes.

Table 1: Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, configurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service nodes in a network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage the network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports.
pxGrid node	You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes (like sharing tags and policy objects between Cisco ISE and third party vendors) and for other information exchanges.

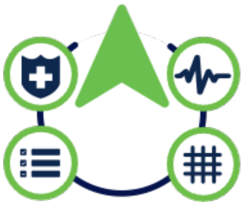
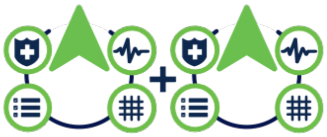
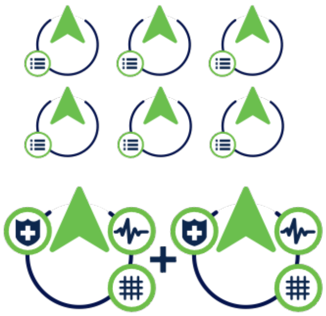
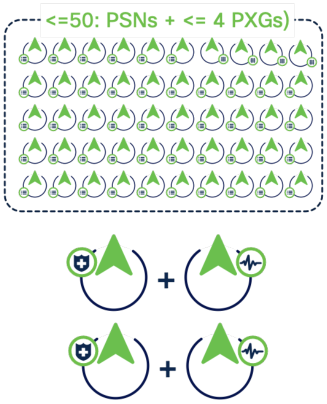
Different Types of Cisco ISE Deployment

A deployment is one or more Cisco ISE nodes connected together in a cluster (distributed system).

A deployment that has a single Cisco ISE node is called a standalone deployment. This node runs all the personas. Standalone deployment is not recommended for production because it does not provide redundancy.

A deployment that has more than one Cisco ISE node is called a distributed deployment. To support failover and to improve performance, you can set up a deployment with multiple Cisco ISE nodes in a distributed fashion. In a Cisco ISE distributed deployment, administration and monitoring activities are centralized, and processing is distributed across the Policy Service nodes. Depending on your performance needs, you can scale your deployment. The following table describes the different types of Cisco ISE deployment.

Table 2: Types of Cisco ISE Deployments

Evaluation	Small Deployment	Medium Deployment	Large Deployment
 - All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM instance. - Not recommended for production.	 - All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM instances. - Two-node deployment. One node as primary and the other node as secondary for redundancy. - An additional node can be added (which is optional) to a small deployment as a PSN, pxGrid, or Health Check node. The additional node can be a combination of any of the following personas: Dedicated PSN pxGrid node Health Check node **Note** Adding an extra node with a PSN, pxGrid, or Health Check persona does not alter the existing scale limits of the small deployment. We recommend that you use the additional node only for load sharing purposes.	 - PAN + MnT + pxGrid running on the same node. - One node as primary and the other node as secondary for redundancy. - PSNs on dedicated nodes. - Nodes can be appliances or equivalent VMs. - Supports up to 6 PSNs (for Cisco ISE 3.0 and above). You can also enable pxGrid persona on any of the PSN or add dedicated pxGrid nodes (maximum up to 2) to the deployment. - Maximum 8 nodes (2 x PAN/MnT/pxGrid + 6 x PSN Or 2 x PAN/MnT + 4 x PSN + 2 x pxGrid/SXP)	 - PAN (2), MnT (2), pxGrid, and PSNs on dedicated nodes. - Nodes can be appliances or equivalent VMs. - Supports up to 4 pxGrid nodes. - Supports up to 50 PSNs - Maximum 58 nodes (2 x PAN + 2 x MnT + 50 x PSN + 4 x pxGrid)

Sizing Guidelines for ISE Deployment

You can choose the right ISE deployment based on the maximum scale numbers for active endpoints offered by specific deployment type, maximum scale numbers for active endpoints supported by individual PSN nodes and other relevant factors that are described in the below sections.

Every endpoint with unique MAC address is considered as one active session and the concurrent active sessions support is applicable for all types of sessions including Dot1x, Mab, Guest, BYOD, and Posture.

The maximum number of active sessions in the below table are derived based on tests under following conditions:

ISE deployments are formed in single datacenter deployed in same region, low latency (less than 5 ms) between the ISE internode communications, dot1xauthentications and accounting events generated by endpoints in the range of 2 to 4 repetitions per day, and majority of the sessions are RADIUS protocols authenticating with local ID providers.

ISE Deployment Scale

Table 3: Maximum Concurrent Active Sessions for Deployments with Different ISE Appliances Acting as PAN, MnT, PAN/MnT

Deployment	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Large	500,000	Unsupported	Unsupported	500,000	750,000	2,000,000	2,000,000
Medium	20,000	12,500	75,000	25,000	150,000	50,000	150,000
Small	20,000	12,500	25,000	25,000	50,000	50,000	50,000

Policy Service Node Scale

Table 4: Maximum Concurrent Active Sessions for Different ISE Appliances Acting as PSNs

PSN Type	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795*
Dedicated PSN (Cisco ISE node has only PSN persona)	40,000	25,000	50,000	50,000	100,000	100,000	100,000
Shared PSN (Cisco ISE node has multiple personas)	20,000	12,500	25,000	25,000	50,000	50,000	50,000

*Cisco SNS 3795 is equipped with more RAM and better Disk Read/Write performance. It is best suited for dedicated PAN, dedicated MNT, or PAN/MNT personas and provides no added value when deployed as a dedicated PSN.

Note

- SNS 3595 is supported in Cisco ISE Release 3.2 and earlier versions.
- SNS 3515 is supported in Cisco ISE Release 3.0 and previous versions. The number of maximum concurrent active endpoints supported by a dedicated PSN is 7,500 and a shared PSN is 5,000.

Considerations for Choosing a Deployment

- You can choose small deployment for up to 50,000 concurrent active sessions and medium deployment for up to 150,000 concurrent active sessions.
- Large deployment is required for more than 150,000 concurrent concurrent active sessions. You must register MnT nodes as Dedicated MnT nodes in Large deployment.
- We recommend that you deploy PSNs closer to workload and Identity Providers (such as AD, LDAP) for performance sensitive loads.
- We recommend that you group PSNs for similar workload (for example, RADIUS Dot1x, Guest/BYOD, TACACS+) and distribute traffic through load balancer.
- For better performance, it is recommended to configure Calling-Station-ID (MAC) based stickiness in the load balancer.
- It is recommended to configure the PSNs in Node-groups if you are using the services that need URL redirect (for example, posture services, guest services, MDM, and so on).
- It is recommended to have multiple datacenters and group PSNs per datacenter. You can implement RADIUS (Primary/Secondary/Tertiary) failover on NAS devices. For example, if the primary datacenter (DC-A) fails, 50 percent NADs can failover to secondary datacenter (DC-B) and remaining NADs can failover to tertiary datacenter (DC-C).
- It is recommended to implement N+1 or N+2 redundancy within a PSN group.
- It is highly recommended to purge guest and inactive endpoints at regular intervals to avoid latency in ISE operations.
- The maximum concurrent active session values given above for each deployment are applicable for connected devices that are generating dot1x authentications up to 4 times a day.
- In case of deployments where endpoints generate repeated authentication and accounting events, more number of PSNs are required in PSN group to help in handling heavy traffic scenarios like simultaneous login events from huge number of users, Wi-Fi users roaming from one location to another, and so on.
- PSN node variations include TACACS+ PSN (T+PSN), TC-NAC PSN (TCNPSN), Guest PSN (GPSN), Cisco TrustSec PSN (CTSPSN), Security Group eXchange Protocol PSN (SXPSN), and PassiveID PSN (PIDPSN). For better performance, it is recommended to reserve TACACS+, RADIUS, Guest/BYOD workloads to dedicated PSN groups within a deployment.
- It is recommended to assign separate Cisco TrustSec PSNs (CTSPSNs) to handle TrustSec functions for TrustSec deployments to avoid overloading of RADIUS PSNs while pushing policies.
- For large scale NAC environments with huge number of Device Administration tasks (for example, heavy usage of scripts or Network management Systems), we recommend that you split the deployments and use a separate deployment for Device Administration (TACACS+).

RADIUS Authentication Rates

The following table shows the authentication rates for RADIUS protocols when a Cisco ISE node acts as a single dedicated PSN in a deployment.

Table 5: RADIUS Transactions per Second (TPS) for a Dedicated PSN Node

Authentication Method	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3755/3695/3795
PAP with internal user database	900	1100	1300
PAP with Active Directory	250	250	300
PAP with LDAP Directory	300	300	350
PEAP (MSCHAPv2) with internal user database	150	150	200
PEAP (MSCHAPv2) with Active Directory	150	150	175
PEAP (GTC) with internal user database	150	150	250
PEAP (GTC) with Active Directory	100	150	175
EAP-FAST (MSCHAPv2) with internal user database	350	400	500
EAP-FAST (MSCHAPv2) with Active Directory	200	250	300
EAP-FAST (GTC) with internal user database	350	400	450
EAP-FAST (GTC) with Active Directory	200	200	300
EAP-FAST (GTC) with LDAP Directory	200	300	300
EAP-TLS with internal user database	150	150	200
EAP-TLS with Active Directory	150	150	200
EAP-TLS with LDAP Directory	150	200	200
EAP TEAP with internal user database	100	100	200
MAB with internal user database	500	900	1000
MAB with LDAP Directory	400	500	600
EAP-TTLS PAP with Microsoft Entra ID	30	30	50
EAP-TLS with Microsoft Entra ID	40	40	50

Note

- EAP-TLS authentication rates for Microsoft Entra ID are applicable for Cisco ISE Release 3.2 Patch 3 and above and Cisco ISE Release 3.3 and above releases.
- EAP-TTLS PAP authentication rates for Microsoft Entra ID are applicable for Cisco ISE Release 3.3 and above releases.

TACACS+ Authentication Rates

The following table shows the authentication rates for TACACS+ protocol when a Cisco ISE node acts as a single dedicated PSN in a deployment.

Table 6: TACACS+ Transactions per Second (TPS) for a Dedicated PSN Node

Scenario	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3755/3695/3795
TACACS+ Function: PAP	2500	3000	3200
TACACS+ Function: CHAP	2500	3000	3500
TACACS+ Function: Enable	1000	1000	1100
TACACS+ Function: Session Authorization	2500	3000	3500
TACACS+ Function: Command Authorization	2500	2500	3500
TACACS+ Function: Accounting	3000	7000	9000

Scenario-Specific Authentication Rates

The following table shows the transactions per second (TPS) when Cisco ISE node is acting as a single dedicated PSN in a deployment for different scenarios.

The authentication values provided below may have + or - 5 percent deviation in production environment.

Table 7: Scenario-Based Authentications Per Second For a Dedicated PSN

Scenario	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3
Posture authentication	50	50	
Guest Hotspot authentication	75	100	
Guest Sponsored authentication	50	75	
BYOD Onboarding single SSID	10	10	
BYOD Onboarding dual SSID	10	15	
MDM	150	200	
Internal CA certificate issuance	50	50	

Scenario	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3755
New endpoints profiled per second/profile updates per second	200	250	
Maximum PassiveID sessions processed per second	1000	1000	
Sessions published per second to 200 pxGrid subscribers	300	400	

Table 8: Time Taken to Perform Various Operations in Seconds

Scenario	Cisco SNS 3615/3715	Cisco SNS 3595	Cisco SNS 3655/3755/3695/3795
Time taken to push 300 TrustSec policies to 254 NADs	50	50	50
Time taken for 5000 TrustSec policies to download 2GB data via REST API	50	50	50
Time taken to connect SXP to SXPSN	10	5	5
Time taken for 200 pxGrid subscribers bulk download with 20,000 sessions	50	50	50
Time taken for ERS Endpoints Bulk API for 1000 endpoints	15	10	10
Time taken for ERS Guest Bulk API for 1000 endpoints	15	10	10
Time taken for ERS: Trustsec Bulk API for 1000 endpoints	200	200	100
Time taken for pxGrid ANC APIs to quarantine or unquarantine 10,000 endpoints (with 100 requests per second)	120	120	120

Cisco ISE Deployment Scale Limits

Table 9: Deployment Scale Limits

Attribute	Maximum Limit
Maximum pxGrid nodes in Large or Dedicated deployment	4
Maximum pxGrid subscribers per pxGrid node	200
Dedicated PSN with SXP service enabled	8 nodes, or 4 pairs
Maximum ISE SXP peers per PSN with SXP service enabled	200
Maximum network device entries*	100,000 (unicast addresses)

Attribute	**Maximum Limit**
Maximum network device groups (NDG)	10,000
Maximum Active Directory forests (Join Points)	50
Maximum Active Directory controllers (WMI query)	100
Maximum internal users	300,000
Maximum internal guests**	1,000,000
Maximum user certificates	1,000,000
Maximum server certificates	1,000
Maximum trusted certificates	1,000
Maximum concurrent active endpoints	2,000,000
Maximum policy sets	200
Maximum authorization rules***	1000 (3,200 authorization profiles)
Maximum attribute-value (AV) pairs	64
Maximum user identity groups	1,000
Maximum endpoint identity groups	1,000
TrustSec Security Group Tags (SGTs) TrustSec Security Group ACLs (SGACLs) TrustSec IP-SGT Static Bindings (over SSH)	10,000 1,000 10,000
Maximum concurrent REST API connections	ERS API: 100 OpenAPI: 150
Maximum PassiveID sessions for Large deployment	3695/3795 PAN, MnT: 2,000,000 3595 PAN, MnT: 500,000 3655 PAN, MnT: 500,000 3755 PAN, MNT: 750,000
Maximum network latency between primary PAN and any other Cisco ISE node including the secondary PAN, MnT, and PSNs	300 milliseconds
Maximum PassiveID sessions providers	
Maximum AD Domain Controllers Maximum REST API Providers Maximum Syslog Providers	100 50 70
MnT API Performance	

Attribute	Maximum Limit
MnT API (https://<MnTIP>/admin/API/mnt/AuthStatus/MACAddress/<MACValue>/432000/500/All) requests per second in Medium deployment	3655/3755: 10 3695/3795: 200
MnT API (https://<MnTIP>/admin/API/mnt/AuthStatus/MACAddress/<MACValue>/432000/500/All) requests per second for Large deployment	3655/3755: 100 3695/3795: 400
Time taken by MnT API (https://<MnTIP>/admin/API/mnt/Session/ActiveList) to download 200,000 endpoints in Medium and Large deployments	40 seconds

*Up to 300,000 NADs are supported. You must provide the network address and subnet in the **Administration > Network Resources > Network Devices** page.

**Having more than 500,000 guest users might create latency in user authentication.

***It is not recommended to have more than 600 authorization rules in a single policy set. Increasing the number of conditions per authorization rule might impact the performance.

Cisco ISE SXP Scaling

Table 10: SXP Scaling for Different Deployments

Deployment Type	Platform	Max PSNs	Max ISE SXP Bindings	Max ISE SXP Listener Peers
Standalone (all personas on same node) 2 nodes redundant	3595	0	20,000	30
	3615	0	12,500	30
	3655/3715	0	25,000	40
	3695/3755/3795	0	50,000	50
Unified PAN+MnT on same node and dedicated PSNs	3595 as PAN and MnT	6	20,000	200
	3655 as PAN and MnT	6	25,000	200
	3695 as PAN and MnT	6	50,000	200
	3715 as PAN and MnT	6	75,000	200
	3755/3795 as PAN and MnT	6	150,000	200

Deployment Type	Platform	Max PSNs	Max ISE SXP Bindings	Max ISE SXP Listener Peers
Dedicated (all personas on dedicated nodes)	3595 as PAN and MnT	50	350,000 (1 pair) 500,000 (2 pairs)	200 (1 pair) 400 (2 pairs)
	3655 as PAN and MnT	50	350,000 (1 pair) 500,000 (2 pairs)	200 (1 pair) 400 (2 pairs)
	3695/3755/3795 as PAN and Large MnT	50	350,000 (1 pair) 700,000 (2 pairs) 1,050,000 (3 pairs) 1,400,000 (4 pairs)	200 (1 pair) 400 (2 pairs) 600 (3 pairs) 800 (4 pairs)

Cisco ISE pxGrid Direct Scaling

This section specifies the time taken for Cisco ISE and pxGrid Direct server integration for different scales of endpoints and also the points to note during the endpoints synchronization.

Table 11: Cisco ISE pxGrid Direct Scaling

Scenario	Time (in minutes)
Time taken to download 250,000 endpoints from CMDB server to PAN	60
Time taken to replicate 250,000 endpoints to all the PSNs	60
Time taken to download 2,000,000 endpoints from CMDB server	420
Time taken to replicate 2,000,000 endpoints to all the PSNs	480

Note

- The above values are applicable only when the network latency between ISE and CMDB is less than 50 milliseconds.
- The above data is applicable for endpoints having around 10 attributes each.
- You might see Slow Replication alarms due to synchronization of endpoints across all the PSNs while downloading or replicating the data.
- It is recommended to schedule synchronization in batches (250,000 to 500,000 endpoints) to reduce the impact on incoming authentication rates.
- The resynchronization time for 100 endpoints is 1 second.

Configuration Best Practices

This section lists the best practices recommended while configuring the network devices and Cisco ISE for better performance.

Some of the factors that affect authentications are:

- Network adapter disconnecting or reconnecting and leading to new authentication process
- Network switches configured with very less session time
- Network switches configured with frequent accounting interim updates
- Power outages
- Automated scripts requiring mass reboot of systems

Each of above event results in new authentication (Access-Request), accounting-interim update, or accounting stops.

Table 12: Configuration Best Practices for Cisco ISE

Attribute	Recommendation
Profiling probes	If you are not using the profiling feature, turn off all the profiling probes.
Endpoint Attribute filter	This filter is disabled by default. We recommend that you enable this filter.
MnT suppression	Ensure that the **Suppress Repeated Passed and Failed Clients** option in the **RADIUS Settings** page is enabled. This option is enabled by default.
EAP-FAST reconnect and session resume	Enable this option in the **Policy** > **Results** > **Allowed Protocols** > **Allow EAP-FAST** page. This helps client devices to reduce the load on Cisco ISE for EAP. In case of BYOD flow where remote management of client device is not possible, this feature has minimal impact.

DNS caching	If Remote Logging Targets (**Administration** > **System** > **Logging** > **Remote Logging Targets**) are used with FQDN, DNS caching must be enabled. Set **Time To Live** value as 180 by using the following command in the command line interface:
	`configure terminal`
	`  service cache enable hosts ttl 180`

Table 13: Configuration Best Practices for Network Devices

Attribute	Recommendation
RADIUS timeout	Recommended range is from 5 to 10 seconds. This range will help the endpoints to boot without causing the DHCP requests to expire and will also avoid latency between Cisco ISE and network devices.

Attribute	Recommendation
RADIUS interim accounting	This option must be disabled or set to more than 24 hours for wireless and wired devices. This limits the interim accounts from the network devices when there is no significant change in the network. This also limits the incoming data to Cisco ISE, thereby reducing the RADIUS accounting updates and logs and allowing PSNs to effectively process the new incoming authentication requests. If the ratio of authentication to accounting interim updates is more than 1:5, we strongly recommended that you check the network connectivity and the network device configuration for accounting updates. You must update the configuration to reduce the frequent interim updates from the network access devices. If you have enabled automated turning off for the network devices in large scale, we recommend that you do this operation in batches. In addition, ensure that each batch does not include more than 500 devices. Otherwise, this operation might cause delay in incoming authentications.
Client exclusion	This configuration is applicable for wireless IOS devices. Set the value to 60 seconds.
Session timeout	Recommended value is more than 24 hours for both wired and wireless devices, unless your security policy dictates that you must perform authentication more frequently.
Inactivity timeout	Set the value to 300 seconds or more. This helps reduce the number of reauthentication requests.
RADIUS device sensor	If profiling is required, use the device sensor instead of other probes. While using the device sensor, other probes can be disabled for wireless devices.
RADIUS Dead Timer	Recommended range is from 10 to 15 minutes. This ensures that the RADIUS server marked down is not used for the specified interval.
Guest Anchoring	If WLAN is anchored, RADIUS accounting must be disabled in the WLAN settings on the anchor controller.
Polling interval for SNMP	We recommend that you set the **SNMP Polling Interval** value (**Administration** > **Network Resources** > **Network Devices** > **Add** > **SNMP Settings**) to 8 hours or higher to reduce performance impact due to large number of SNMP events. Setting a lower value might create large profiling events and impact system performance.

Cisco ISE Hardware Appliances

Cisco SNS hardware appliances support the Unified Extensible Firmware Interface (UEFI) secure boot feature. This feature ensures that only a Cisco-signed Cisco ISE image can be installed on the Cisco SNS hardware appliances, and prevents the installation of any unsigned operating system even with physical access to the device.

Table 14: Specifications for Cisco SNS 3500/3600 Series Hardware Appliances

Specifications	Cisco SNS 3615	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3695
Processor	Intel Xeon 2.10 GHz 4110	Intel Xeon 2.60 GHz E5-2640	Intel Xeon 2.10 GHz 4116	Intel Xeon 2.10 GHz 4116

Specifications	Cisco SNS 3615	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3695
Cores per Processor	8 Cores and 16 Threads	8 Cores and 16 Threads	12 Cores and 24 Threads	12 Cores and 24 Threads
Memory	32 GB (2x16 GB)	64 GB (4x16 GB)	96 GB (6x16 GB)	256 GB (8x32 GB)
Hard Disk	1 x 600-GB 6 Gb SAS 10K RPM	4 x 600-GB 6 Gb SAS 10K RPM	4 x 600-GB 6 Gb SAS 10K RPM	8 x 600-GB 6 Gb SAS 10K RPM
Hardware RAID	—	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller
Network Interfaces	2 X 10 Gbase-T 4 x 1 GBase-T	6 x 1 GBase-T	2 X 10 Gbase-T 4 x 1 GBase-T	2 X 10 Gbase-T 4 x 1 GBase-T
Power Supplies	1 x 770W	2 x 770W	2 x 770W	2 x 770W

Table 15: Specifications for Cisco SNS 3700 Series Hardware Appliances

Specifications	Cisco SNS 3715	Cisco SNS 3755	Cisco SNS 3795
Processor	Intel Xeon 2.1 GHz 4310	Intel Xeon 2.3 GHz 4316	Intel Xeon 2.3 GHz 4316
Cores per processor	12 Cores and 24 Threads	20 Cores and 40 Threads	20 Cores and 40 Threads
Memory	32 GB 2 x 16GB	96 GB 6 x 16GB	256 GB 8 x 32GB
Hard disk	1 60012G SAS 10K RPM SFF HDD Or 800 GB 2.5in Enterprise Performance 12G SAS SSD (3x endurance)	4 60012G SAS 10K RPM SFF HDD Or 800 GB 2.5in Enterprise Performance 12G SAS SSD (3x endurance)	8 60012G SAS 10K RPM SFF HDD Or 800 GB 2.5in Enterprise Performance 12G SAS SSD (3x endurance)
Hardware RAID	Level 0	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller
Network interface	2 x 10Gbase-T 4 x 10GE SFP	2 x 10Gbase-T 4 x 10GE SFP	2 x 10Gbase-T 4 x 10GE SFP
Power supplies	1 x 1050W	2 x 1050W	2 x 1050W
TPM chip	Yes	Yes	Yes

Note

- Cisco ISE Release 3.1 Patch 6 and later and Cisco ISE Release 3.2 Patch 2 and later versions support Cisco SNS 3700 series appliances.
- You cannot add additional hardware resources like memory, processor, or hard disk to a Cisco SNS hardware appliance.
- Mixing SAS/SATA hard drives and SAS/SATA SSDs is not supported. You must use either SAS/SATA hard drives or SAS/SATA SSDs.
- SSD offers improved performance in disk read/write operations and other Cisco ISE operations like boot, installation (up to 10% improvement), and upgrade database intensive tasks like backup and reports generation (up to 20% improvement). Note that the PSN performance for RADIUS and TACACS+ operations will remain the same as described in preceding sections.
- Additional power supplies can be ordered separately for SNS 3615 and SNS 3715. For component part numbers, see the Cisco Secure Network Server Data Sheet.

Cisco ISE Virtual Machine and Cloud Platforms

Cisco ISE can be installed on VMware servers, KVM hypervisors, Hyper-V, and Nutanix AHV. To achieve performance and scalability comparable to Cisco ISE hardware appliances, virtual machines must be allocated system resources equivalent to the Cisco SNS 3500 or 3600 series appliances as described in table below.

It is recommended that you reserve CPU and memory resources that match the resource allocation. Failure to do so may significantly impact Cisco ISE performance and stability.

For a VM deployment, the number of cores is twice the number of cores in a physical appliance due to hyperthreading. For example, in case of a small network deployment, allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU cores or 16 threads.

Deploy dedicated VM resources and do not share or oversubscribe resources across multiple guest VMs.

Cisco ISE is now available from the cloud, enabling you to scale your Cisco ISE deployments quickly and easily to meet changing business needs.

Cisco ISE is available as an Infrastructure as Code solution, helping you to rapidly deploy network accesses and control services anywhere.

Extend the Cisco ISE policies in your home network to new remote deployments securely through Amazon Web Services (AWS), Azure Cloud Services, or Oracle Cloud Infrastructure (OCI). AWS supports Cisco ISE Release 3.1 and later releases.

OCI and Azure Cloud support is available from Cisco ISE Release 3.2 and later releases.

See Deploy Cisco ISE Natively on Cloud Platforms and respective cloud documentations for resource specifications of supported instances.

Table below describes matrix of VM specification, cloud instances to their equivalent Cisco SNS appliances.

Table 16: Specifications for Cisco ISE VM and Cloud Instances

Models	Cisco SNS 3615	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3695	Cisco SNS 3715	Cisco SNS 3755	Cisco SNS 3795
VM Specification	16vCPU 32 GB	16vCPU 64 GB	24vCPU 96 GB	24vCPU 256 GB	24vCPU 32GB	40vCPU 96GB	40vCPU 256GB
AWS	c5.4xlarge*	m5.4xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge	c5.9xlarge* m5.8xlarge	—	m5.16xlarge
Azure	Standard_F16s_v2*	Standard_D16s_v4	Standard_F32s_v2* Standard_D32s_v4	Standard_D64s_v4	Standard_F32s_v2* Standard_D32s_v4	—	Standard_D64s_v4
OCI	Optimized3.Flex* (8 OCPU** and 32 GB)	Standard3.Flex (8 OCPU and 64 GB)	Optimized3.Flex (16 OCPU and 64 GB)* Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 256 GB)	Optimized3.Flex (16 OCPU and 64 GB)* Standard3.Flex (16 OCPU and 128 GB)	—	Standard3.Flex (32 OCPU and 256 GB)

*This instance is compute-optimized and provides better performance compared to the general purpose instances.

**In OCI, you choose CPU in terms of Oracle CPU (OCPU). Each OCPU provides CPU capacity equal to one physical core of an Intel Xeon processor with hyper-threading enabled. Each OCPU equals two hardware execution threads known as vCPUs.

Note There is no equivalent cloud profile for Cisco SNS 3755. We recommend that you use the cloud instances that are specified for Cisco SNS 3795.

Extra Small Form Factor for Cisco ISE VM and Cloud Instances

Extra Small VM specification, 8 vCPU and 32 GB is available only on VMware servers such as KVM hypervisors, Hyper-V and Nutanix AHV and Cloud instances.

This specification is not available on SNS appliances.

The Extra Small form factor support is available from Cisco ISE Release 3.2 onwards.

Extra Small form factor ISE VM supports 12000 endpoints.

Only dedicated PSN persona is supported. Extra Small form factor node is not supported for large deployments and must not be deployed.

Extra Small form factor ISE VM performance for RADIUS and TACACS+ authentication is around 40 percent of that of Cisco SNS 3615.

For example, if the RADIUS authentication rate of Cisco SNS 3615 for PEAP-MSCHAP2 with internal user database is 150, this value will be 60 (40% of 150) for the Extra Small form factor ISE VM.

Table 17: Extra Small Form Factor for Cisco ISE VM and Cloud Instances

Virtual Machines	Specifications
VM	8 vCPU 32GB
AWS	m5.2xlarge
Azure	Standard_D8s_v4
OCI	Standard3.Flex (4 OCPU and 32 GB)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.