Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA98114

Role: Access Point

Wi-Fi Agile Multiband™ (continued)

Fast Transition OTA on WPA2-Personal

Wi-Fi CERTIFIED 6™

4 antenna support
A-MPDU with A-MSDU
DL MU-MIMO
DL OFDMA
iTWT
LDPC Rx
LDPC Tx
MCS 8-9 Rx
MCS 8-9 Tx
MCS 10-11 Rx
MCS 10-11 Tx
Operating Mode
SU beamformer
UL OFDMA

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ ac

Extended 5 GHz Channel Support
A-MPDU with A-MSDU
DL MU-MIMO
LDPC Rx
LDPC Tx
MCS 8-9 Rx
Short Guard Interval
STBC
SU beamformer

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n

Short Guard Interval
STBC

Wi-Fi Enhanced Open™ 2020-02

República Federativa do Brasil
Agência Nacional de Telecomunicações

ANATEL

Certificado de Homologação

(Intransferível)

Nº **04129-19-01086**

Validade: **Indeterminada**

Emissão: **13/06/2019**

Requerente:
CISCO DO BRASIL LTDA.
DAS NAÇÕES UNIDAS Nº12901 25 ANDAR
BROOKLIN PAULISTA
04578000 SÃO PAULO SP

Fabricante:
CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE SAN JOSE
ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC 17058/19, emitido pelo **Associação NCC Certificações do Brasil.** Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:
Transceptor de Radiação Restrita - II

Modelo - Nome Comercial (s):
Cisco Catalyst 9115AX Series Access Points - (C9115AXI-Z) /Cisco Catalyst 9115AX Series Access Points - (C9115AXE-Z)

Características técnicas básicas:

Potência Máxima de Saída (W)	Tecnologias	Faixa de Frequências Tx (MHz)	Designação de Emissões	Tipo de Modulação
0,0025	SEQÜÊNCIA DIRETA	2.400,0 a 2.483,5	700KF7D	GFSK
0,5763	SEQÜÊNCIA DIRETA	2.400,0 a 2.483,5	8M03X9D	DBPSK/DQPSK/CCK
0,7409	OFDM	2.400,0 a 2.483,5	16M3X9D	BPSK/QPSK/16-64QAM
0,9605	OFDM	2.400,0 a 2.483,5	17M5X9D	BPSK/QPSK/16-64QAM
0,9506	OFDM	2.400,0 a 2.483,5	18M9X9D	BPSK/QPSK/16-64-256-1024QAM
0,1186	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64QAM
0,1208	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64QAM
0,1169	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64QAM
0,1052	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64QAM
0,0964	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64QAM
0,1469	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64-256-1024QAM
0,0443	OFDM	5.150,0 a 5.350,0	-	BPSK/QPSK/16-64-256-1024QAM
0,1786	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64QAM
0,0664	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64QAM
0,1072	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64QAM
0,1216	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64QAM
0,0906	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64QAM
0,0332	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64-256-1024QAM
0,0536	OFDM	5.470,0 a 5.725,0	-	BPSK/QPSK/16-64-256-1024QAM
0,9042	OFDM	5.725,0 a 5.850,0	16M3X9D	BPSK/QPSK/16-64QAM

Potência Máxima de Saída (W)	Tecnologias	Faixa de Frequências Tx (MHz)	Designação de Emissões	Tipo de Modulação
0,718	OFDM	5.725,0 a 5.850,0	17M6X9D	BPSK/QPSK/16-64QAM
0,9908	OFDM	5.725,0 a 5.850,0	36M3X9D	BPSK/QPSK/16-64QAM
0,8461	OFDM	5.725,0 a 5.850,0	76M0X9D	BPSK/QPSK/16-64QAM
0,787	OFDM	5.725,0 a 5.850,0	76M6X9D	BPSK/QPSK/16-64-256-1024QAM

Ensaio de SAR não aplicável.

Na instalação do produto, devem ser observadas as condições de uso conforme estabelecido no Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Davison Gonzaga da Silva
Gerente de Certificação e Numeração

República Federativa do Brasil
Agência Nacional de Telecomunicações

ANATEL

Certificado de Homologação

(Intransferível)

Nº **00648-19-01086**

Validade: **Indeterminada**

Emissão: **05/05/2020**

Requerente:
CNPJ: 00.028.666/0001-58
CISCO DO BRASIL LTDA.

Fabricante:

CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE
Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC 16675/19, emitido pelo **Associação NCC Certificações do Brasil.** Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:
Equipamento de Rede de Dados - III

Modelo - Nome Comercial (s):
Cisco Catalyst 9200 Series - (C9200L-24T-4G-E) /Cisco Catalyst 9200 Series - (C9200L-24P-4G-E) /Cisco Catalyst 9200 Series - (C9200L-48T-4G-E) /Cisco Catalyst 9200 Series - (C9200L-48P-4G-E) /Cisco Catalyst 9200 Series - (C9200L-24T-4X-E) /Cisco Catalyst 9200 Series - (C9200L-24P-4X-E) /Cisco Catalyst 9200 Series - (C9200L-48T-4X-E) /Cisco Catalyst 9200 Series - (C9200L-48P-4X-E) /Cisco Catalyst 9200 Series - (C9200-24T-X) /Cisco Catalyst 9200 Series - (C9200-24P-X) /Cisco Catalyst 9200 Series - (C9200-48T-X) /Cisco Catalyst 9200 Series - (C9200-48P-X) /Cisco Catalyst 9200 Series - (C9200L-24PXG-4X-X) /Cisco Catalyst 9200 Series - (C9200L-24PXG-2Y-X) /Cisco Catalyst 9200 Series - (C9200L-48PXG-4X-X) /Cisco Catalyst 9200 Series - (C9200L-48PXG-2Y-X) /Cisco Catalyst 9200 Series - (C9200-48PXG) /Cisco Catalyst 9200 Series - (C9200-24PXG) /Cisco Catalyst 9200 Series - (C9200-24PB) /Cisco Catalyst 9200 Series - (C9200-48PB)

Características técnicas básicas:

Equipamento de rede de dados com características de comutador (switch) para aplicações em redes Ethernet.

Observações

:mais módulos de interface e protocolos de sinalização passíveis de homologação, especificados em documentos técnicos do produto, não :ão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.

Este certificado substitui o de mesmo número emitido em 19/08/2019

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Davison Gonzaga da Silva
Gerente de Certificação e Numeração

República Federativa do Brasil
Agência Nacional de Telecomunicações

ANATEL

32

Certificado de Homologação

(Intransferível)

Nº **04632-21-01086**

Validade: **Indeterminada**

Emissão: **17/05/2021**

Requerente:
CNPJ: 00.028.666/0001-58
CISCO DO BRASIL LTDA.

Fabricante:

CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE
Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC 19396/21, emitido pelo **Associação NCC Certificações do Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:
Estação Terminal de Acesso - I

Modelo - Nome Comercial (s):
P-LTEA-LA

Características técnicas básicas:

Faixa de Frequências Tx (MHz)	Potência Máxima de Saída (W)	Designação de Emissões	Tecnologia	Tipo de Modulação
824,0 a 849,0	0,166	5M00G7W	WCDMA/HSDPA/HSUPA	QPSK/16QAM
898,5 a 901,0	0,163	5M00G7W	WCDMA/HSDPA/HSUPA	QPSK/16QAM
907,5 a 915,0	0,163	5M00G7W	WCDMA/HSDPA/HSUPA	QPSK/16QAM
1.749,9 a 1.784,9	0,163	5M00G7W	WCDMA/HSDPA/HSUPA	QPSK/16QAM
1.920,0 a 1.980,0	0,16	5M00G7W	WCDMA/HSDPA/HSUPA	QPSK/16QAM
703,0 a 748,0	0,205	3M00G7W/5M00G7W/10M0G7W	LTE	QPSK/16QAM
703,0 a 748,0	0,205	15M0G7W/20M0G7W	LTE	QPSK/16QAM
824,0 a 849,0	0,207	1M40G7W/3M00G7W	LTE	QPSK/16QAM
824,0 a 849,0	0,207	5M00G7W/10M0G7W	LTE	QPSK/16QAM
898,5 a 901,0	0,203	1M40G7W/3M00G7W/5M00G7W	LTE	QPSK/16QAM
907,5 a 915,0	0,203	1M40G7W/3M00G7W/5M00G7W	LTE	QPSK/16QAM
1.710,0 a 1.785,0	0,203	1M40G7W/3M00G7W/5M00G7W	LTE	QPSK/16QAM
1.710,0 a 1.785,0	0,203	10M0G7W/15M0G7W/20M0G7W	LTE	QPSK/16QAM
1.885,0 a 1.895,0	0,191	5M00G7W/10M0G7W	LTE	QPSK/16QAM
1.920,0 a 1.980,0	0,19	5M00G7W/10M0G7W	LTE	QPSK/16QAM
1.920,0 a 1.980,0	0,19	15M0G7W/20M0G7W	LTE	QPSK/16QAM
2.500,0 a 2.570,0	0,15	5M00G7W/10M0G7W	LTE	QPSK/16QAM
2.500,0 a 2.570,0	0,15	15M0G7W/20M0G7W	LTE	QPSK/16QAM
2.570,0 a 2.620,0	0,149	5M00G7W/10M0G7W	LTE	QPSK/16QAM
2.570,0 a 2.620,0	0,149	15M0G7W/20M0G7W	LTE	QPSK/16QAM

Antenas 4G: O equipamento pode ou não ser comercializado com antena externa.
A antena que pode ser comercializada é a de modelo LTE-ANTM-D com ganho de 3,7dBi.
O equipamento implementa o protocolo IPV6.
Ensaio de SAR não aplicável: o equipamento é um produto não acabado cuja a integração em outros equipamentos requer nova avaliação.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Davison Gonzaga da Silva
Gerente de Certificação e Numeração

Cisco Collaboration Flex Plan 3.0

Contents

Cisco Collaboration Flex Plan 3.0

With the release of Flex 3.0, the Cisco® Collaboration Flex Plan is evolving to accelerate and incentivize the move to Flex, simplify quoting and ordering, and improve collaboration by bundling Webex® Meetings and Ca

K ovements to the Cisco Collaboration Flex Plan:

- ew! Webex Suite Enterprise Agreement and Named User
- Single tier Active User (AU) Buying Model – Meetings only
- The Cisco Enterprise Agreement (EA) is simplified by consolidating three tiers into a single tier.
- Hard bundle better-together Meeting + Calling. Customers benefit when buying them together.

Buying models

Three buying models are available: Enterprise Agreement, Active User, and Named User. You can choose different buying models for Meetings and Calling, but you may not have more than one buying model for either solution at any point. During your subscription, you also have the flexibility to change your buying model from:

- Named User to Active User or Enterprise Agreement, or
- Active User to Enterprise Agreement

An Enterprise Agreement (EA) covers all Knowledge Workers (KW) in an organization and allows for 20 percent growth with additional value-added benefits to cover organizational needs. A minimum of 250 KWs are required.

Active User (AU) is a usage-based subscription for meetings that allows customers to purchase meetings entitlements according to adoption and closely track the return on investment. A minimum of 40 Active Users is required.

Named User (NU) is a per-user subscription that enables customers to provide Webex Meetings or Calling services for individuals, teams, or departments and add additional entitlements as adoption grows. Entitlements can be purchased per user with no minimum. No growth is included.

Named User Calling Value Tiers

Professional – the full-featured tier for employees and contractors who use multiple communication devices as part of their job duties. This tier includes voicemail.

Enhanced – the feature rich tier optimized for task-based workers who use a single device without the need to voicemail.

A – the entry level tier for a dial-tone and basic calling capabilities on basic devices.

ment models

You will choose a software deployment model for each of your users. Customers can choose to mix deployment models to fit their needs and deploy cloud Meetings and Calling on-premises, hosted by a partner, and/or via a cloud (either Cisco Unified Communications Manager [UCM] Cloud and/or Webex Calling). Note that when you choose an on-premises or partner-hosted deployment, you will also receive the cloud service Webex app. You have the flexibility to transition from on-premises or partner-hosted to a cloud deployment and

vice versa. The deployment model you choose for a user determines their software entitlement. Table 1 shows which deployment models are available for Meetings and Calling.

Table 1. Availability of Meetings and Calling by deployment model

	Cloud	On-premises	Partner hosted
Meetings	X		
Calling	X	X	X

Meetings features and benefits

When you choose Cisco Collaboration Flex Plan Meetings, you receive entitlements to a bundle of features. Table 2 describes the included features and the availability of each feature to users with the EA, NU and AU buying models. Table 3 describes the add-on features that can be purchased on top of your subscription and the availability of each add-on feature based on the designated buying model.

Table 2. Included features and buying model availability

Included feature	Benefit	Buying model available		
		EA	NU	AU
Advanced Meetings	The following video and web conferencing solutions are included: Webex Meetings with a capacity of 1000 attendees per session Webex Training with a capacity of 1000 attendees per session Webex Events with a capacity of 1000 attendees per session Webex Support with a capacity of 5 attendees per session Webex Meetings suite includes Webex Meetings, Webex Training, Webex Events, and Webex Support in a single bundle. A Branded microsite included See supported languages. For Named User, customers can choose either the entire Webex Meetings suite or a-la-carte combination of Webex Meetings, Webex Training, Webex Events, and Webex Support. You cannot select this option in combination with Webex Events 3000.	X	X	X
Webex meetings	Host or join Webex Meetings natively from the Webex App with common meeting experiences and controls, no matter how participants join. Note: Calendar service must be enabled.	X	X	X

Included feature	Benefit	Buying model available		
		EA	NU	AU
Pro Pack for Control Hub	With Pro Pack for Control Hub, administrators can provision, manage, and analyze the entire Webex experience. Pro Pack delivers additional levels of security controls, compliance management, and business insights to meet the needs of customers who are looking for advanced capabilities.	X	X	X
Cisco Webex Conferencing Audio (voice over IP [VoIP])	Each knowledge worker has unlimited access to VoIP. Cisco Webex VoIP capabilities may not be available to participants in certain countries. Refer to the "Important Information Regarding Audio Services" section of the Cisco Webex Audio Offering data sheet for more details.	X	X	X
Cisco Webex Conferencing Audio (toll dial-in audio) Or Cisco Cloud Connected Audio Service Provider User	Each knowledge worker has unlimited access to global toll call-in services. Local toll call-in number(s) are provided for participants in covered countries to join a Cisco Webex meeting. Refer to the Cisco Webex Audio Offering data sheet (Table 2) for a list of covered countries. Or, Under the Cloud Connected Audio Service Provider (CCA SP User) Audio option, a service provider partner peers with Cisco and provides the transport and access (phone numbers) to a customer, while Cisco provides audio bridging. The service provider partner also provides lifecycle support; that is, day-0, day-1, and day-2 support.	X	X	X
Enhanced messaging in the Webex App	Get secure, all-in-one team collaboration from Webex. Webex is an app for continuous teamwork. Move work forward in secure work spaces where everyone can contribute anytime with messaging, file sharing, white boarding, video meetings, calling, and more.	X	X	X
Webex Assistant	Webex Assistant interacts with you to help with note taking, action items, reminders, closed captioning, and more, all controlled by voice command.	X	X	X
Polling/Q&A (Slido)	Slido is an audience engagement platform with expanded polling/Q&A technology now integrated with Webex.	X	X	X
Cloud device registration	The cloud device registration provides the ability to register Cisco video devices purchased upfront as well as Hardware as a Service to the Webex cloud, with no need for on-premises infrastructure.	X		X
Cisco TelePresence Management Suite	Cisco TelePresence® Management Suite provides complete control, management, and scheduling capabilities of telepresence conferencing and media services infrastructure and endpoints. It includes a base software license, 250 system management licenses, and API integration licenses.	X	X	X
Webex Hybrid Services	Integrate your existing IT assets with Webex to provide a single, integrated experience. Hybrid Services include Call Service, Calendar Service, Directory Service, Video	X	X	X

Included feature	Benefit	Buying model available		
		EA	NU	AU
	Mesh, and Data Security Service.			

Included feature	Benefit	Buying model available		
		EA	NU	AU
Webex Edge Audio	Webex Edge Audio is suitable for customers that have a cloud meetings solution coupled with an on-premises calling solution. It provides an on-net path (VoIP) for participants to join meetings from their existing IP phones with no change in behavior or training required. Edge Audio supports all Cisco Unified Communications solutions, providing high-quality audio (wideband codec) and cost savings by bypassing PSTN.	X	X	X

Table 3 shows the add-on features by buying model that are available for purchase.

Table 3. Add-on features buying model availability

Add-on feature	Benefit	Buying model available		
		EA	NU	AU
Webex Suite	The Webex Suite can be purchased under Flex 3.0 to bring the full power of the Webex platform with Cloud Calling, Meetings, Messaging, Polling and Events to your organization's users. Webex Suite is a cloud only option. For more information on Webex Suite, please visit the Webex Suite Ordering Guide.	X	X	
Webex Messaging 1 TB file storage	Gain additional file storage beyond the pooled 20 GB of file storage per knowledge worker in the standard offer. Extra storage is purchased in unitary increments.	X	X	X
Cloud device registration*	The cloud device registration provides the ability to register Cisco video devices purchased upfront as well as Hardware as a Service to the Webex cloud, with no need for on-premises infrastructure.	Included	X	Included
Cisco TelePresence Room*	TelePresence Room and Expressway™ Room enable call control for room-based immersive and multipurpose Cisco TelePresence system endpoints.		X	
Real-time translation	Real-time translation for Webex Meetings is the ability to translate English in over 100+ languages natively within Webex.	X	X	
Expert on Demand	Expert on Demand provides the ability for experts to remotely join a Webex meeting through their supported RealWear Headset.*	X	X	X
Network-based Recording Storage (NBR)	Additional Webex Meetings Network-Based Recording (NBR) storage is available in 500-GB and in 100-GB increments. This is incremental to the included 1 GB per-user NBR storage entitled with EA and NU. And 5 GB per-Active-User NBR storage entitled with AU.	X	X	X

Add-on feature	Benefit	Buying model available		
		EA	NU	AU
Telehealth Meeting Broker	Host Telehealth meetings and access Electronic Medical Records (EMR) while leveraging Epic's APIs. Available in 2 varieties: Standard and Enhanced.	X	X	X
The following audio add-ons are available only for Cisco Webex Conferencing Audio (not Cloud Connected Audio)				
Cisco Webex Conferencing Audio (Bridge Country Callback Audio)*	Each knowledge worker has unlimited access to global toll call-in plus bridge country callback services. Local toll call-in number(s) are provided for participants to join a Webex meeting. Bridge Country Callback Audio allows participants in the bridge country to join a Webex meeting by having the meeting call them at the number they specify once they've joined over the web. Bridge Country Callback Audio is available only to participants in certain countries. Refer to the "Important Information Regarding Audio Services" section of the Cisco Webex Audio Offering data sheet for a list of covered countries.	X	X	X
Cisco Webex Conferencing Audio (Bridge Country Callback + Toll-Free Audio) for the U.S. and Canada*	Each knowledge worker has unlimited access to global toll call-in plus bridge country callback and bridge country toll free services. Local toll call-in number(s) are provided for participants to join a Webex meeting. Bridge Country Callback Audio allows participants in the bridge country to join a Webex meeting by having the meeting call them at the number they specify once they've joined over the web. Bridge Country Toll Free Audio provides participants toll free call-in numbers to join the Webex meeting. Bridge Country Callback + Toll Free Audio is available only to participants in the United States and Canada. Refer to the "Important Information Regarding Audio Services" section of the Cisco Webex Audio Offering data sheet for a list of covered countries.	X	X	X
Cisco Webex Conferencing Audio (global callback audio)*	Each knowledge worker has unlimited access to global toll call-in plus global callback. Local toll call-in numbers are provided for participants joining a Webex meeting. Global Callback Audio allows participants in covered countries to join a Webex meeting by having the meeting call them at the number they specify once they've joined over the web. Refer to Cisco Webex Audio Offering data sheet (Table 3) for a list of covered countries.	X	X	X

Add-on feature	Benefit	Buying model available		
		EA	NU	AU
Webex Audio (per minute)	The following Webex Audio services are available for purchase on a per-minute basis: • Bridge country toll-free call-in:* Toll-free call-in number(s) are provided for participants in the bridge country to join a Webex meeting. • Bridge country callback:* Allows participants in the bridge country to join a Webex meeting by having the meeting call them at the number they specify once they've joined over the web. • Global toll-free call-in: Toll-free call-in numbers are provided for participants in covered countries to join a Webex meeting. Refer to the Webex Audio data sheet for a list of covered countries. • Global premium toll call-in: Local toll call-in numbers are provided for participants in covered countries to join a Webex meeting. Refer to the Webex Audio data sheet for a list of covered countries. • Global callback: Allows participants in covered countries to join a Webex meeting by having the meeting call them at the number they specify once they've joined over the web. Refer to the Cisco Webex Audio data sheet for a list of covered countries. *Per-minute bridge country audio services are available only to participants in certain countries. Refer to the "Important Information Regarding Audio Services" section of the Cisco Webex Audio Offering data sheet for more details. Each of these services can be included in or excluded from the order and subsequent site provisioning. All included services will be made available to all site knowledge workers by default, and knowledge worker-level entitlements can be selectively modified using site administration tools. You will be required to choose one of the following billing models with your order: Uncommitted billing – Invoiced monthly in arrears, based on actual usage over the billing period. Per-use fees are subject to change. The subscriber will be charged at the applicable rate in effect at the time the service is used. Committed billing – Invoiced monthly in advance for the duration of the audio service subscription term, based on a monthly committed dollar amount (minimum of $226 per month). Usage in excess of committed amounts is invoiced monthly in arrears at the discounted rate. Committed amounts that are not used by the subscriber during the month may not be carried forward into the next month.	X	X	X

Add-on feature	Benefit	Buying model available		
		EA	NU	AU
Webex Edge Connect	Webex Edge Connect is suitable for customers who have a cloud meetings solution coupled with an on-premises calling solution. It provides a dedicated, managed, Quality-of-Service (QoS)-enabled IP link from the customer's premises to the Webex Cloud through direct peering, leading to better and faster Webex meetings powered by the Cisco Webex Backbone. The direct connection provides enhanced meeting quality with consistent network performance and added security. It is recommended that customers that deploy Webex Edge Audio purchase Webex Edge Connect to experience premium meeting quality and significant cost savings by combining audio and Internet bandwidth.	X	X	X

Webex Calling features and benefits

When you choose Cisco Collaboration Flex Plan Calling, you receive entitlements to a bundle of calling features. Figure 1 highlights the device support for the Named User buying model. Table 4 describes the included features and the availability of each feature to users with the EA and NU buying model, as well as the availability of each feature to users with a cloud, on-premises, or partner-hosted deployment model. Table 5 describes the add-on features that can be purchased on top of your subscription and the availability of each add-on feature based on the designated buying model as well as the availability of each feature to users with a cloud, on-premises, or partner-hosted deployment model. Table 6 highlights the Named User value tiers.

Figure 1
Named User device support

Table 4. Included features, buying model, and deployment model availability

Included feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
[illegible]alling	Webex Calling is the latest Cloud Calling offering that delivers proven enterprise-class Cisco hosted calling functionality. Webex Calling for SP is a cloud calling offer targeting service providers that delivers a proven enterprise-class cloud PBX. Both Webex Calling and Webex Calling for SP provide an enterprise license delivering a full-featured, robust offer targeted to an organization's knowledge workers. It includes unified communications (Webex Calling) and mobility (desktop and mobile clients with support for multiple devices). Webex Calling (formerly Cisco Spark Call) includes a cloud-based phone system and the ability to connect other Cisco call control capabilities and services through Webex Hybrid Services. It encompasses all the devices to make calls.	X	X	X		
Cisco Calling Plan	The Cisco Calling Plan is a new offer that provides Cisco public switched telephone network (PSTN) connectivity to Webex Calling customers. Partners can now order outbound calling plans for their customers directly from Cisco on Cisco Commerce Workplace (CCW). Partners and customers can also order outbound calling plans and telephone numbers directly from Cisco on Webex Control Hub. Cisco Calling Plans are managed natively from Webex Control Hub and are billed from Cisco (through partners). With Cisco Calling Plans, partners and customers can benefit from a single vendor for cloud calling services and support, and centralized trials and provisioning.	X	X	X		

Included feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
Cisco Unified Communications Manager Cloud (UCM Cloud) Calling	Cisco Unified Communications Manager (UCM) Cloud delivers proven enterprise-grade unified communications and collaboration as a service, with the features and benefits of Cisco IP phones, mobile devices, and desktop clients, delivered from the Cisco Webex cloud. Cisco UCM Cloud offers voice, video, messaging, presence, emergency, mobility, team collaboration, and soft client solutions enabled by Cisco Unified Communications Manager, Cisco Unity® Connection, Cisco Emergency Responder 911, Cisco Expressway, and Cisco Jabber® bundled into a cloud consumption model.	X	X	X		
Enhanced messaging in Cisco Webex App	Secure, all-in-one team collaboration from Webex. Webex is an app for continuous teamwork. Move work forward in secure workspaces where everyone can contribute anytime with messaging, file sharing, white boarding, video meetings, calling, and more.	X	X	X	X	X
Cloud device registration	The cloud device registration provides the ability to register Cisco video devices purchased upfront as well as Hardware as a Service to the Webex cloud, with no need for on-premises infrastructure.	X		X	X	X
TelePresence Room*	TelePresence Room and Expressway® Room enable call control for room-based immersive and multipurpose Cisco TelePresence system endpoints.	X		X	X	X
Webex Hybrid Services	Integrate your existing IT assets with Webex to provide a single, integrated experience. Webex Hybrid Services include Call Service, Calendar Service, Directory Service, Video Mesh, and Data Security Service. These services are not available for Webex Calling for SP.	X	X	X	X	
Cisco Unified Communications Manager	Cisco Unified Communications Manager provides an enterprise-class IP telephony call-processing system. In addition to traditional telephony features, it provides advanced capabilities such as video.	X	X		X	X

Included feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
Cisco Expressway Series (Expressway-C and Expressway-E)	Cisco Expressway Series works as part of the Cisco Unified Communications Manager product family to provide access for mobile, desktop, and fixed clients. The application provides advanced multimodal firewall traversal and access services for secure voice, video, instant messaging and presence, directory, and visual voicemail outside your enterprise firewall without the need for a VPN. It includes. • Base software license • Expressway-E license • Series feature license • Desk phone and room registration licenses	X	X	X	X	X
Cisco Unity Connection	Access your Cisco Unity Connection voice messages the way you prefer—whether from an IP phone, a mobile phone, a web browser, an email client, or a desktop client such as Cisco Jabber.	X	X		X	X
Soft clients	Cisco Jabber® clients: • Cisco Jabber for Windows (softphone, video, instant messaging, presence) • Cisco Jabber for Mac (softphone, video, instant messaging, presence) • Cisco Jabber for Android (softphone, video, instant messaging) • Cisco Jabber for iOS (softphone, video, instant messaging) • Cisco Jabber SDK (software development kit for web) • Cisco Virtualization Experience Media Edition (VXME) • Cisco Jabber Guest	X	X		X	X
Cisco Emergency Responder 911	Cisco Emergency Responder enhances the existing emergency 9-1-1 functionality offered by Cisco Unified Communications Manager. It helps assure that Cisco Unified Communications Manager will send emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes. Cisco Emergency Responder exports Automatic Location Information (ALI) data in formats defined by the National Emergency Number Association (NENA), an industry standards body in the United States. These data formats may not be suitable for use outside the United States and Canada; manual modification of the exported files may be	X	X	X	X	X

Included feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
	required.					
Cisco Unified Survivable Remote Site Telephony (SRST)	Cisco Unified SRST provides cost-effective solutions for supporting redundant call control in remote branch offices and the homes of teleworkers.	X	X	X	X	X
Cisco Unified Communications Manager Session Management Edition (SME)	Cisco Unified Communications Manager SME helps enterprises create a centralized architecture to more easily and efficiently manage and evolve their networks as collaboration needs change. With SME, enterprises can: • Simplify. Reduce complexity by aggregating third-party PBXs, and ease migration to an all-IP environment. • Extend. Deploy collaboration applications at the network core and extend them to users, even those on third-party PBXs.	X			X	X
Pro Pack for Control Hub[1]	With Pro Pack for Control Hub, administrators can provision, manage, and analyze the entire Webex experience. Pro Pack delivers additional levels of security controls, compliance management, and business insights to meet the needs of customers who are looking for advanced capabilities.	X	X	X	X	X

[1] Not applicable for Webex Calling

Table 5. Add-on features, buying model, and deployment model availability for purchase.

Add-on feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
Webex Suite	The Webex Suite can be purchased under Flex 3.0 to bring the full power of the Webex platform with Cloud Calling, Meetings, Messaging and Events to your organization's users. Webex Suite is a cloud only option. For more information on Webex Suite, please visit the Webex Suite Ordering Guide.	X	X	X		
Webex Setup Assist	Webex Setup Assist is a Cisco-provided migration and implementation service assistance for partners to include on all cloud calling opportunities. This is available as a purchasable option for Webex Calling and UCM Cloud Calling.	X	X	X		
Cisco UCM Cloud Direct Connect (UCM Cloud Only)	Cisco UCM Cloud Direct Connect is a set of services that allows customers to connect direct to the Cisco UCM Cloud in the Cisco Webex Cloud. Virtual Connect (SD-WAN or VPN) enables customers to securely extend their private network virtually over the Internet to the Cisco UCM Cloud without the need to own and support the remote infrastructure and dedicated circuits. The supported options are SD-WAN (Meraki or Viptela) or VPN. The customer is responsible for the corresponding premises equipment and Cisco SD-WAN licenses. In both cases Cisco hosts, manages, and assures redundant customer dedicated routers (VPN router or SD-WAN vEdge) with Internet access in the Cisco UCM Cloud data center region(s) where service is required. The customer is responsible for the corresponding premises equipment and Cisco SD-WAN licenses. Fiber Connect enables customers to securely connect their private network via their point-to-point fiber circuit directly to the Cisco UCM Cloud. Cisco provides the customer the ability to securely terminate redundant fiber connections in the Cisco UCM Cloud data center region(s) where service is required. The customer is responsible for the fiber circuit and the corresponding premises equipment. MPLS Connect enables customers to securely connect their private network via their MPLS connection directly to the Cisco UCM Cloud. Cisco provides the customer the ability to securely terminate redundant MPLS	X	X	X		

Add-on feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
	connections in the Cisco UCM Cloud data center region(s) where service is required. The customer is responsible for the MPLS circuit and the corresponding premises equipment.					
Cisco Unified Attendant Console (UCM Cloud only)	Cisco Unified Attendant Console (UAC) High Availability bundle and additional Advanced licenses are available as part of the Collaboration Flex Plan. Cisco UAC Advanced with UCM Cloud is a high availability deployment to protect your system from down time. Cisco UAC Advanced offers a power queuing engine that helps manage several calls from many sources. The robust directory can handle up to 100,000 contacts and synchronize directly with Active Directory.	X	X	X		
Cisco Unified Attendant Console (CUAC)	Cisco Unified Attendant Console (CUAC) Standard and Advanced are available as part of the Collaboration Flex Plan. CUAC Advanced comes with optional high availability to protect your system from down time. CUAC Standard offers enhanced features such a modern user interface and searchable speed dials. It includes busy lamp field and Cisco Jabber presence. CUAC Advanced offers a powerful queuing engine that helps users manage several calls from many sources. The robust directory can handle up to 100,000 contacts and synchronize directly with Active Directory.	X	X		X	X
Additional MRA registration capacity (UCM Cloud Only)	Get additional device registration capacity for secure mobile and remote access for mobile, desktop, and fixed clients. The capacity provides advanced multimodal firewall traversal and access services for secure voice, video, instant messaging and presence, directory, and visual voicemail outside your enterprise firewall without the need for a VPN.	X	X	X		
UCM Cloud Enterprise Service (UCM Cloud Only)	Cisco UCM Cloud Enterprise Service is a set of expert cloud lifecycle services designed to accelerate the realization of the value of the Cloud and provide an optimized experience by providing extensive monitoring and management services.	X	X	X		
Cisco Unified Communications Manager Express (CME)	Cisco Unified Communications Manager Express (Unified CME) enables powerful unified communications for distributed enterprise branch-office and retail environments. As a licensed feature set of Cisco IOS® XE Software, it is easy to configure and can be	X	X	X	X	X

Add-on feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
	tailored to the needs of an individual site. It is feature-rich and can be combined with other services on the Cisco router platforms to provide an all-in-one branch-office solution that saves valuable real estate.					
Cisco Unified Border Element (CUBE)	CUBE has a wide range of capabilities that may be used to secure, monitor, and maintain business-critical connections and to ensure compliance with industry standards. Collectively, CUBE features provide exceptional flexibility when architecting highly available enterprise communications networks that save money and offer richer voice and video collaboration experiences to users.	X	X	X	X	X
SpeechView Standard	Cisco SpeechView converts voice messages to text and delivers the text version of the voice message to the user's email inbox. The original audio version of each voice message remains within Cisco Unity Connection and is available to the user anywhere, anytime. Standard is an AI-based service, without human intervention.	X	X	X	X	X
Cisco Unified Communications Manager Session Management Edition (SME)	Cisco Unified Communications Manager SME helps enterprises create a centralized architecture to more easily and efficiently manage and evolve their networks as collaboration needs change. With SME, enterprises can: • Simplify. Reduce complexity by aggregating third-party PBXs, and ease migration to an all-IP environment. • Extend. Deploy collaboration applications at the network core and extend them to users, even those on third-party PBXs.	Included	X	X	X	X
nnected UC	A set of services in Webex cloud that provide admin workflows with enhanced business and operational insights to improve admin productivity. For customers who: • Would like to leverage benefits of Webex cloud, but desire to keep critical calling workload on-premises • Desire a single global view to manage on-premises UC, along with any Webex cloud, or hybrid services they already use • Desire efficient, cloud based managed services (delivered by partner) for an on-premises UCM deployment	X	X		X	

Add-on feature	Benefit	Buying model		Deployment model available		
		EA	NU	Cloud	On-premises	Partner hosted
Unity Connection with Speech Connect	Access your Cisco Unity® Connection voice messages the way you prefer—whether from an IP phone, a mobile phone, a web browser, an email client, or a desktop client such as Cisco Jabber. Speech Connect is a speech-enabled automated attendant that is included as part of Cisco Unity Connection. It let the customer use voice commands (they say the name of the person they want to call) instead of dialing a number.	X	X	X	X	X
Common Area add-on	Get add-on licenses for common-area phones not associated with knowledge workers. A common area (Places) phone option is also available for Webex Calling, offering analog phone type functionality with a minimal set of additional feature capabilities.	X		X	X	X
Access add-on	Add-on licenses for Access phone not associated with a knowledge workers.	X		X	X	X
Enterprise to MPP firmware migration	Migrate certain phone models from "enterprise" firmware to MPP firmware. This option is available only for Webex Calling.	X	X	X		

Table 6. Named User value tiers

	Professional	Enhanced	Access	Deployments		
				Prem/HCS	UCMC	WxC
SRST	Included	Included	Included	Available	Available	N/A
CER	300%	Included	Included	Available	Available	N/A
Pro Pack	Included	Included	N/A	Available	Available	Available
Mobile Remote Access[1]	Included	Included	N/A	Available	Available	N/A
Webex Messaging (Managed)[1]	Included	Included	N/A	Available for purchase	Available for purchase	Available for purchase
Unity Connection (Enhanced) [SA]	Included	Optional purchase	Optional purchase	Available for purchase	Available for purchase	N/A
SpeechConnect [SA]	Included	Included with Unity Connection	Included with Unity Connection	Available	Available	N/A
Session Manager	Optional purchase	Optional purchase	Optional purchase	Available for purchase	Available	N/A

	Professional	Enhanced	Access	Deployments		
				Prem/HCS	UCMC	WxC
Expressway Base	Included	Included	N/A	Available	Available	N/A
way RMS	Optional purchase	Optional purchase	Optional purchase	Available for purchase	Available for purchase	N/A
Premises device registration	Optional purchase	Optional purchase	Optional purchase	Available for purchase	Available for purchase	N/A
Cloud device registration	Optional purchase	Optional purchase	Optional purchase	Available for purchase	Available for purchase	Available for purchase
Cloud Connected UC	Optional $0	Optional $0	Optional $0	Available (on-premises only)	N/A	N/A
SpeechView – Std [SA]	Optional purchase	Optional purchase	Optional purchase	Available for purchase	Available for purchase	N/A
CUBE (phase 1) (local gateway)	Included	Included	N/A	N/A	N/A	Available for purchase
Enterprise to MPP firmware migration	Optional $0	Optional $0	N/A	N/A	N/A	Available

[1] Entitlement as % of KW

[SA] Stand Alone Add-On

[1] Feature only, no separate entitlement

Table 7. Platform and messaging add-ons

Add-on feature	Benefits
Webex messaging add-on	Secure, all-in-one team collaboration from Webex. Webex is an app for continuous teamwork. Move work forward in secure work spaces where everyone can contribute anytime with messaging, file sharing, white boarding, video meetings, calling, and more.
Cisco Jabber option	Cisco Jabber instant messaging can be opted in addition to Webex Messaging at no cost and at equal license count as Webex Messaging. This is intended to aid customer migration from Jabber to Cisco Webex App.
Webex Messaging 1 TB file storage	Get additional file storage in addition to the pooled 24 GB of file storage per knowledge worker or 20 GB of file storage per named user in the standard offer. Purchased in unitary increments.
d Security	The Extended Security Pack bundle includes full-functionality Cisco CloudLock® for data loss prevention and anti-malware scanning for all Webex files. This add-on provides collaboration administrators agility and the ability to securely deploy Webex in their enterprises by addressing all InfoSec concerns in a tightly integrated solution without the procurement and deployment hurdles of buying multiple products.

[1] Extended Security Pack requires a purchase with Calling and/or Meetings.

Technical support and customer success services

Cisco offers support services covering the areas of problem resolution, customer success and adoption, and designated support management in three service tiers: Basic, Enhanced, and Premium. Basic support is included at no additional cost for the duration of your subscription. For more information about the available technical support services, contact your partner or Cisco sales agent.

On-premises licensing and software delivery

On-premises licenses are delivered to you via your Smart Account. The partner is responsible for entering your Smart Account information at the time your order is placed.

The on-premises software and license Product Authorization Keys (PAKs) are available through the links provided in the eDelivery email that will be sent to the email address(es) provided on the order. Instructions will be included on how to register the PAKs and install the license.bin file.

Ordering information

To place an order, contact your certified Cisco partner or Cisco sales agent. If you need help finding a partner in your area, use the Partner Locator tool. Your partner or Cisco sales agent can also assist with any modifications to your subscription after your initial order is placed.

Entry-level Webex service

If you elect not to renew your subscription, your Webex account will be converted to an entry-level cloud service. The free cloud service has fewer features and differing usage limits than the paid cloud service. Cisco may at any time change those features and limits at our discretion and without notice. Cisco may also deactivate or delete your free account and any related data if you exceed the 5-GB storage limit per user.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® financing makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

Appendix

Collaboration Flex Plan 3.0 Ordering Guide

For information on how to order, see our Flex Plan 3.0 Ordering Guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
the Netherlands

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

Printed in USA

C78-744220-00 09/21

Cisco Identity Services Engine Installation Guide, Release 3.1

CONTENTS

CHAPTER 1

Network Deployments in Cisco ISE

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco ISE Network Architecture

Cisco ISE architecture includes the following components:

- Nodes and persona types
  - Cisco ISE node—A Cisco ISE node can assume any or all of the following personas: Administration, Policy Service, Monitoring, or pxGrid
- Network resources
- Endpoints

The policy information point represents the point at which external information is communicated to the Policy Service persona. For example, external information could be a Lightweight Directory Access Protocol (LDAP) attribute.

Cisco ISE Deployment Terminology

This guide uses the following terms when discussing Cisco ISE deployment scenarios:

Term	Definition
Service	A specific feature that a persona provides such as network access, profiling, posture, security group access, monitoring, and troubleshooting.
Node	An individual physical or virtual Cisco ISE appliance.
Node Type	The Cisco ISE node can assume any of the following personas: Administration, Policy Service, Monitoring.
Persona	Determines the services provided by a node. A Cisco ISE node can assume any or all of the following personas: . The menu options that are available through the administrative user interface depend on the role and personas that a node assumes.
Role	Determines if a node is a standalone, primary, or secondary node and applies only to Administration and Monitoring nodes.

Node Types and Personas in Distributed Deployments

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment can assume the Administration, Policy Service, pxGrid, and Monitoring personas. In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration nodes for high availability
- A pair of Monitoring nodes for automatic failover
- One or more Policy Service nodes for session failover
- One or more pxGrid nodes for pxGrid services

Administration Node

A Cisco ISE node with the Administration persona allows you to perform all administrative operations on Cisco ISE. It handles all system-related configurations that are related to functionality such as authentication, authorization, and accounting. In a distributed deployment, you can have a maximum of two nodes running the Administration persona. The Administration persona can take on the standalone, primary, or secondary role.

Policy Service Node

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. You can have more than one node assume this persona. Typically, there would be more than one Policy Service node in a distributed deployment. All Policy Service nodes that reside in the same high-speed Local Area Network (LAN) or behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset any URL-redirected sessions.

At least one node in your distributed setup should assume the Policy Service persona.

Monitoring Node

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 a network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports. Cisco ISE allows you to have a maximum of two nodes with this persona, and they can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring nodes collect log messages. In case the primary Monitoring node goes down, the secondary Monitoring node automatically becomes the primary Monitoring node.

At least one node in your distributed setup should assume the Monitoring persona. We recommend that you do not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. We recommend that the Monitoring node be dedicated solely to monitoring for optimum performance.

pxGrid Node

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as ISE Eco system 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. Cisco pxGrid also allows third party systems to invoke adaptive network control actions (EPS) to quarantine users/devices in response to a network or security event. The TrustSec information like tag definition, value, and description can be passed from Cisco ISE via TrustSec topic to other networks. The endpoint profiles with Fully Qualified Names (FQNs) can be passed from Cisco ISE to other networks through a endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

You can publish and subscribe to SXP bindings (IP-SGT mappings) through pxGrid. For more information about SXP bindings, see Source Group Tag Protocol section in *Cisco Identity Services Engine Administrator Guide*.

In a high-availability configuration, Cisco pxGrid servers replicate information between the nodes through the PAN. When the PAN goes down, pxGrid server stops handling the client registration and subscription. You need to manually promote the PAN for the pxGrid server to become active.

Standalone and Distributed ISE Deployments

A deployment that has a single Cisco ISE node is called a *standalone deployment*. This node runs the Administration, Policy Service, and Monitoring personas.

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. A Cisco ISE node can assume any of the following personas: Administration, Policy Service, and Monitoring.

Distributed Deployment Scenarios

- Small Network Deployments
- Medium-Sized Network Deployments
- Large Network Deployments

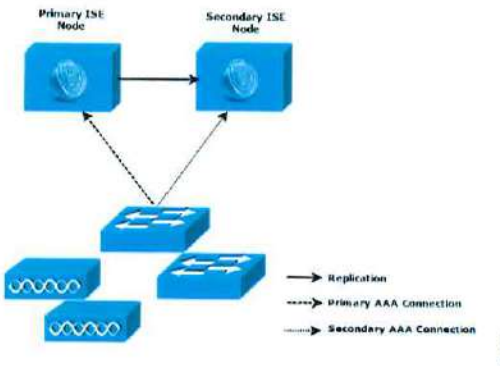
Small Network Deployments

The smallest Cisco ISE deployment consists of two Cisco ISE nodes with one Cisco ISE node functioning as the primary appliance in a small network.

The primary node provides all the configuration, authentication, and policy capabilities that are required for this network model, and the secondary Cisco ISE node functions in a backup role. The secondary node supports the primary node and maintains a functioning network whenever connectivity is lost between the primary node and network appliances, network resources, or RADIUS.

Centralized authentication, authorization, and accounting (AAA) operations between clients and the primary Cisco ISE node are performed using the RADIUS protocol. Cisco ISE synchronizes or replicates all of the content that resides on the primary Cisco ISE node with the secondary Cisco ISE node. Thus, your secondary node is current with the state of your primary node. In a small network deployment, this type of configuration model allows you to configure both your primary and secondary nodes on all RADIUS clients by using this type of deployment or a similar approach.

Figure 1: Small Network Deployment



As the number of devices, network resources, users, and AAA clients increases in your network environment, you should change your deployment configuration from the basic small model and use more of a split or distributed deployment model.

Split Deployments

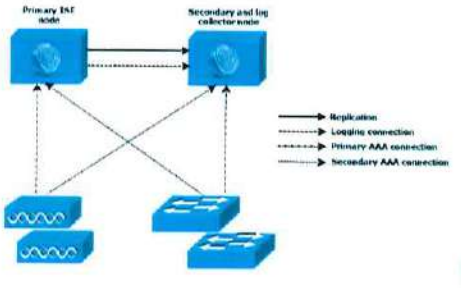
In split Cisco ISE deployments, you continue to maintain primary and secondary nodes as described in a small Cisco ISE deployment. However, the AAA load is split between the two Cisco ISE nodes to optimize the AAA workflow. Each Cisco ISE appliance (primary or secondary) needs to be able to handle the full workload if there are any problems with AAA connectivity. Neither the primary node nor the secondary nodes handles all AAA requests during normal network operations because this workload is distributed between the two nodes.

The ability to split the load in this way directly reduces the stress on each Cisco ISE node in the system. In addition, splitting the load provides better loading while the functional status of the secondary node is maintained during the course of normal network operations.

In split Cisco ISE deployments, each node can perform its own specific operations, such as network admission or device administration, and still perform all the AAA functions in the event of a failure. If you have two Cisco ISE nodes that process authentication requests and collect accounting data from AAA clients, we recommend that you set up one of the Cisco ISE nodes to act as a log collector.

In addition, the split Cisco ISE deployment design provides an advantage because it allows for growth.

Figure 2: Split Network Deployment



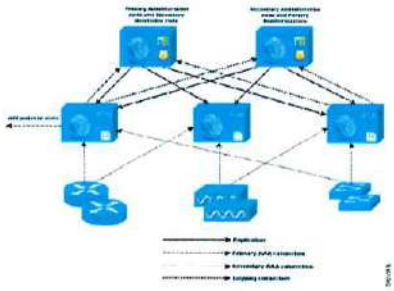
Medium-Sized Network Deployments

As small networks grow, you can keep pace and manage network growth by adding Cisco ISE nodes to create a medium-sized network. In medium-sized network deployments, you can dedicate the new nodes for all AAA functions, and use the original nodes for configuration and logging functions.

Note In a medium-sized network deployment, you cannot enable the Policy Service persona on a node that runs the Administration persona, Monitoring persona, or both. You need dedicated policy service node(s).

As the amount of log traffic increases in a network, you can choose to dedicate one or two of the secondary Cisco ISE nodes for log collection in your network.

Figure 3: Medium-Sized Network Deployment



Large Network Deployments

Centralized Logging

We recommend that you use centralized logging for large Cisco ISE networks. To use centralized logging, you must first set up a dedicated logging server that serves as a Monitoring persona (for monitoring and logging) to handle the potentially high syslog traffic that a large, busy network can generate.

Because syslog messages are generated for outbound log traffic, any RFC 3164-compliant syslog appliance can serve as the collector for outbound logging traffic. A dedicated logging server enables you to use the reports and alert features that are available in Cisco ISE to support all the Cisco ISE nodes.

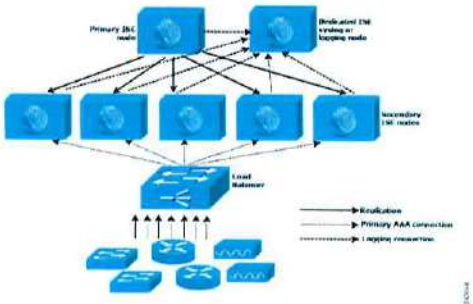
You can also consider having the appliances send logs to both a Monitoring persona on the Cisco ISE node and a generic syslog server. Adding a generic syslog server provides a redundant backup if the Monitoring persona on the Cisco ISE node goes down.

Load Balancers

In large centralized networks, you should use a load balancer, which simplifies the deployment of AAA clients. Using a load balancer requires only a single entry for the AAA servers, and the load balancer optimizes the routing of AAA requests to the available servers.

However, having only a single load balancer introduces the potential for having a single point of failure. To avoid this potential issue, deploy two load balancers to ensure a measure of redundancy and failover. This configuration requires you to set up two AAA server entries in each AAA client, and this configuration remains consistent throughout the network.

Figure 4: Large Network Deployment

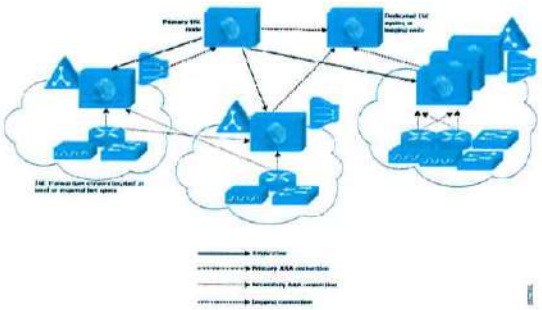


Dispersed Network Deployments

Dispersed Cisco ISE network deployments are most useful for organizations that have a main campus with regional, national, or satellite locations elsewhere. The main campus is where the primary network resides, is connected to additional LANs, ranges in size from small to large, and supports appliances and users in different geographical regions and locations.

Large remote sites can have their own AAA infrastructure for optimal AAA performance. A centralized management model helps maintain a consistent, synchronized AAA policy. A centralized configuration model uses a primary Cisco ISE node with secondary Cisco ISE nodes. We still recommend that you use a separate Monitoring persona on the Cisco ISE node, but each remote location should retain its own unique network requirements.

Figure 5: Dispersed Deployment



Considerations for Planning a Network with Several Remote Sites

- Verify if a central or external database is used, such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). Each remote site should have a synchronized instance of the external database that is available for Cisco ISE to access for optimizing AAA performance.
- The location of AAA clients is important. You should locate the Cisco ISE nodes as close as possible to the AAA clients to reduce network latency effects and the potential for loss of access that is caused by WAN failures.
- Cisco ISE has console access for some functions such as backup. Consider using a terminal at each site, which allows for direct, secure console access that bypasses network access to each node.
- If small, remote sites are in close proximity and have reliable WAN connectivity to other sites, consider using a Cisco ISE node as a backup for the local site to provide redundancy.
- Domain Name System (DNS) should be properly configured on all Cisco ISE nodes to ensure access to the external databases.

Maximum Supported Sessions for Each Deployment Model

The following tables list the maximum supported sessions for each deployment model.

Table 1: Maximum Supported Sessions per Deployment Model

Deployment Model	Platform	Maximum Sessions
Standalone (All personas on a single node)	3615	10,000
	3655	25,000
	3695	50,000
	3595	20,000
Basic 2-node deployment (redundant)	3615	10,000
	3655	25,000
	3695	50,000
	3595	20,000
Hybrid-Distributed deployment (Admin and MnT on same appliance; Policy Service on dedicated appliance)	3615 as PAN and MnT	10,000
	3655 as PAN and MnT	25,000
	3695 as PAN and MnT	50,000
	3595 as PAN and MnT	20,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	3595 as PAN and MnT	500,000
	3655 as PAN and MnT	500,000
	3695 as PAN/MnT	2,000,000

Table 2: Maximum Active Sessions per PSN

Scaling per PSN[1]	Max Active Sessions
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3595	40,000

[1] Dedicated Policy nodes (Max sessions gated by Total Deployment size)

Deployment Size and Scaling Recommendations for SNS 3500/3600 Series Appliances

Table 3: Maximum RADIUS Scaling for SNS 3500/3600 Series Appliances

Deployment Model	Platform	Max Number of Dedicated PSNs	Max RADIUS Sessions Per Deployment
Standalone	3595	0	20,000
	3615	0	10,000
	3655	0	25,000
	3695	0	50,000
PAN and MnT on same node and Dedicated PSNs	3595 as PAN and MnT	6	20,000
	3615 as PAN and MnT	6	10,000
	3655 as PAN and MnT	6	25,000
	3695 as PAN and MnT	6	50,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	3595 as PAN and MnT	50	500,000
	3655 as PAN and MnT	50	500,000
	3695 as PAN and MnT	50	2,000,000

Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions

To ensure that Cisco ISE can interoperate with network switches and that functions from Cisco ISE are successful across the network segment, you must configure your network switches with certain required Network Time Protocol (NTP), RADIUS/AAA, IEEE 802.1X, MAC Authentication Bypass (MAB), and other settings.

ISE Community Resource

For information about setting up Cisco ISE with WLC, see Cisco ISE with WLC Setup Video.

CHAPTER 2

Cisco Secured Network Server 3500/3600 Series Appliances and Virtual Machine Requirements

Hardware and Virtual Appliance Requirements

Cisco Identity Services Engine (ISE) can be installed on Cisco SNS hardware or virtual appliances. To achieve performance and scalability comparable to the Cisco ISE hardware appliance, the virtual machine should be allocated system resources equivalent to the Cisco SNS 3500 or 3600 series appliances. This section lists the hardware, software, and virtual machine requirements required to install Cisco ISE.

Note Harden your virtual environment and ensure that all the security updates are up-to-date. Cisco is not liable for any security issues found in hypervisors.

Cisco Secured Network Server 3500 and 3600 Series Appliances

For Cisco Secured Network Server (SNS) hardware appliance specifications, see "Table 1, Product Specifications" in the Cisco Secure Network Server Data Sheet.

For Cisco SNS 3500 series appliances, see Cisco SNS-3500 Series Appliance Hardware Installation Guide.

For Cisco SNS 3600 series appliances, see Cisco SNS-3600 Series Appliance Hardware Installation Guide.

Note Cisco ISE 3.1 does not support Cisco SNS 3515 appliance. For information about the supported hardware platforms for Cisco ISE 3.1, see Supported Hardware.

VMware Virtual Machine Requirements

Cisco ISE supports the following VMware servers and clients:

- VMware version 11 (default) for ESXi 6.*x*
- VMware Version 13 (default) for ESXi 7.*x*

Cisco ISE supports the cold VMware vMotion feature that allows you to migrate virtual machine (VM) instances (running any persona) between hosts. For the VMware vMotion feature to be functional, the following condition must be met:

- Cisco ISE must be shutdown and powered off. Cisco ISE does not allow to stop or pause the database operations during vMotion. This might lead to data corruption issues. Hence, ensure that Cisco ISE is not running and active during the migration.

Note Cisco ISE VM does not support Hot vMotion.

Refer to your VMware documentation for more information on VMotion requirements.

Caution If the Snapshot feature is enabled on the VM, it might corrupt the VM configuration. If this issue occurs, you might have to reimage the VM and disable VM snapshot.

Note Cisco ISE does not support VMware snapshots for backing up ISE data because a VMware snapshot saves the status of a VM at a given point in time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. We recommend that you use the backup functionality included in Cisco ISE for archival and restoration of data. Using VMware snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

Cisco ISE offers the following OVA templates that you can use to install and deploy Cisco ISE on virtual machines (VMs):

- ISE-3.1.0.xxx-virtual-SNS3615-SNS3655-300.ova
- ISE-3.1.0.xxx-virtual-SNS3615-SNS3655-600.ova
- ISE-3.1.0.xxx-virtual-SNS3655-SNS3695-1200.ova
-

The 300 GB OVA templates are sufficient for Cisco ISE nodes that serve as dedicated Policy Service or pxGrid nodes.

The 600 GB and 1.2 TB OVA templates are recommended to meet the minimum requirements for ISE nodes that run the Administration or Monitoring personas. For additional information about disk space requirements, see Disk Space Requirements, on page 22.

If you need to customize the disk size, CPU, or memory allocation, you can manually deploy Cisco ISE using the standard .iso image. However, it is important that you ensure the minimum requirements and resource reservations specified in this document are met. The OVA templates simplify ISE virtual appliance deployment by automatically applying the minimum resources required for each platform.

Table 4: OVA Template Reservations

OVA Template Type	Number of CPUs	CPU Reservation (in MHz)	Memory (in GB)	Memory Reservation (in GB)
Evaluation	4	No reservation.	16	No reservation.
Small	16	16,000	32	32
Medium	24	24,000	96	96
Large	24	24,000	256	256

We strongly recommend that you reserve CPU and memory resources to match the resource allocation. Failure to do so may significantly impact ISE performance and stability.

For information about the product specifications for Cisco SNS appliances, see Cisco Secure Network Server Data Sheet.

The following table lists the VMware virtual machine requirements.

Table 5: VMware Virtual Machine Requirements

Requirement Type	Specifications
CPU	• Evaluation ◦ Clock speed: 2.0 GHz or faster ◦ Number of CPU cores: 4 CPU cores • Production ◦ Clock speed: 2.0 GHz or faster ◦ Number of cores: ▪ SNS 3600 Series Appliances • Small: 16 • Medium: 24 • Large: 24 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3600 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU Cores or 16 Threads

Requirement Type	Specifications
Memory	• Evaluation: 16 GB • Production ◦ Small: 32 GB for SNS 3615 ◦ Medium: 96 GB for SNS 3655 ◦ Large: 256 GB
Hard Disks	• Evaluation: 300 GB • Production 300 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following links: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine for Cisco ISE, use a single virtual disk that meets the storage requirement. If you use more than one virtual disk to meet the disk space requirement, the installer may not recognize all the disk space.
Storage and File System	The storage system for the Cisco ISE virtual appliance requires a minimum write performance of 50 MB per second and a read performance of 300 MB per second. Deploy a storage system that meets these performance criteria and is supported by VMware server. Cisco ISE provides a number of methods to verify if your storage system meets these minimum requirements before, during, and after Cisco ISE installation. See Virtual Machine Resource and Performance Checks, on page 45 for more information. We recommend the VMFS file system because it is most extensively tested, but other file systems, transports, and media can also be deployed provided they meet the above requirements.
Disk Controller	Paravirtual or LSI Logic Parallel For best performance and redundancy, a caching RAID controller is recommended. Controller options such as RAID 10 (also known as 1+0) can offer higher overall write performance and redundancy than RAID 5, for example. Additionally, battery-backed controller cache can significantly improve write operations. **Note** Updating the disk SCSI controller of an ISE VM from another type to VMware Paravirtual may render it not bootable.

Requirement Type	Specifications
NIC	1 NIC interface required (two or more NICs are recommended; six NICs are supported). Cisco ISE supports E1000 and VMXNET3 adapters. **Note** We recommend that you select E1000 to ensure correct adapter order by default. If you choose VMXNET3, you might have to remap the ESXi adapter to synchronize it with the ISE adapter order.
VMware Virtual Hardware Version/Hypervisor	VMware Virtual Machine Hardware Version 11 or higher on ESXi 6.x and 7.x.

Linux KVM Requirements

Table 6: Linux KVM Virtual Machine Requirements

Requirement Type	Minimum Requirements
CPU	• Evaluation ◦ Clock Speed: 2.0 GHz or faster ◦ Number of Cores: 4 CPU cores • Production ◦ Clock Speed: 2.0 GHz or faster ◦ Number of Cores: ▪ SNS 3600 Series Appliances: • Small: 16 • Medium: 24 • Large: 24 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3600 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU Cores or 16 Threads.

Requirement Type	Minimum Requirements
Memory	• Evaluation: 16 GB • Production ◦ Small: 32 GB for SNS 3615 ◦ Medium: 96 GB for SNS 365. ◦ Large: 256 GB
Hard Disks	• Evaluation: 300 GB • Production 300 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following links: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine for Cisco ISE, use a single virtual disk that meets the storage requirement. If you use more than one virtual disk to meet the disk space requirement, the installer may not recognize all the disk space.
KVM Disk Device	Disk bus - virtio, cache mode - none, I/O mode - native Use preallocated RAW storage format.
NIC	1 NIC interface required (two or more NICs are recommended; six NICs are supported). Cisco ISE supports VirtIO drivers. We recommend VirtIO drivers for better performance.
Hypervisor	KVM on QEMU 2.12.0-99

Microsoft Hyper-V Requirements

Table 7: Microsoft Hyper-V Virtual Machine Requirements

Requirement Type	Minimum Requirements
CPU	• **Evaluation** • Clock speed: 2.0 GHz or faster • Number of cores: 4 CPU cores • **Production** • Clock speed: 2.0 GHz or faster • **Number** of Cores: • SNS 3600 Series Appliance: • Small: 16 • Medium: 24 • Large: 24 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3600 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU Cores or 16 Threads.
Memory	• **Evaluation**: 16 GB • **Production** • Small: 32 GB for SNS 3615 • Medium: 96 GB for SNS 3655 • Large: 256 GB

Requirement Type	Minimum Requirements
Hard disks	• **Evaluation**: 300 GB • **Production** 300 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following link: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine for Cisco ISE, use a single virtual disk that meets the storage requirement. If you use more than one **virtual** disk to meet the disk space requirement, the installer may not recognize all the disk space.
NIC	1 NIC interface required (two or more NICs are recommended; six NICs are supported).
Hypervisor	Hyper-V (Microsoft)

Support for Cisco ISE on VMware Cloud on Amazon Web Services and Azure VMware Solution

The process of installing Cisco ISE on VMware Cloud is exactly the same as that of installing Cisco ISE on VMware virtual machine.

- Cisco ISE virtual machine deployed on VMware cloud in Amazon Web Services (AWS): Cisco ISE can be hosted on software-defined data center (SDDC) provided by VMware Cloud on AWS. Ensure that appropriate security group policies are configured on VMware Cloud (under **Networking and Security > Security > Gateway Firewall Settings**) to enable reachability to on-premises deployment, required devices and services.
- Cisco ISE virtual machine deployed on Azure VMware Solution (AVS): AVS runs VMware workloads natively on Microsoft Azure, where Cisco ISE can be hosted as VMware virtual machine.

Virtual Machine Appliance Size Recommendations

Large VM for Monitoring nodes was introduced in Cisco ISE 2.4. Deploying a Monitoring persona on a large VM improves performance in terms of faster response to live log queries and report completion.

Note This form factor is available only as a VM in Release 2.4 and later, and requires a large VM license.

The virtual machine (VM) appliance specifications should be comparable with physical appliances run in a production environment.

Keep the following guidelines in mind when allocating resources for the appliance:

- Failure to allocate the specified resources might result in performance degradation or service failure. We highly recommend that you deploy dedicated VM resources and not share or oversubscribe resources across multiple guest VMs. Deploying Cisco ISE virtual appliances using the OVF templates ensures that adequate resources are assigned to each VM. If you do not use OVF templates, then ensure that you assign the equivalent resource reservations when you manually install Cisco ISE using the ISO image.

  Note If you choose to deploy Cisco ISE manually without the recommended reservations, you must assume the responsibility to closely monitor your appliance's resource utilization and increase resources, as needed, to ensure proper health and functioning of the Cisco ISE deployment.

  Note OVF templates are not applicable for Linux KVM. OVF templates are available only for VMware virtual machines.

- If you are using the OVA templates for installation, check the following settings after the installation is complete:
  - Ensure that you assign the resource reservations that are specified in the VMware Virtual Machine Requirements, on page 14 section in the CPU/Memory **Reservation** field (under the **Virtual Hardware** tab in the **Edit Settings** window) to ensure proper health and functioning of the Cisco ISE deployment.
  - Ensure that the CPU usage in the **CPU Limit** field (under the **Virtual Hardware** tab in the **Edit Settings** window) is set to **Unlimited**. Setting a limit for CPU usage (for example, setting the CPU usage limit as 12000 MHz) will impact the system performance. If limit has been set, you must shutdown the VM client, remove the limit, and the restart the VM client.
  - Ensure that the memory usage in the **Memory Limit** field (under the **Virtual Hardware** tab in the **Edit Settings** window) is set to **Unlimited.** Setting a limit for memory usage (for example, setting the limit as 12000 MB) will impact the system performance.
  - Ensure that the **Shares** option is set as **High** in the **Hard Disk** area (under the **Virtual Hardware** tab in the **Edit Settings** window).

    Admin and MnT nodes rely heavily on disk usage. Using shared disk storage VMware environment might affect the disk performance. You must increase the number of disk shares allocated to a node to increase the performance of the node.
- Policy Service nodes on VMs can be deployed with less disk space than Administration or Monitoring nodes. The minimum disk space for any production Cisco ISE node is 300 GB. See Disk Space Requirements, on page 22 for details on the disk space required for various Cisco ISE nodes and personas.
- VMs can be configured with 1 to 6 NICs. The recommendation is to allow for 2 or more NICs. Additional interfaces can be used to support various services such as profiling, guest services, or RADIUS.

Note RAM and CPU adjustments on VM doesn't require re-image.

Disk Space Requirements

The following table lists the Cisco ISE disk-space allocation recommended for running a virtual machine in a production deployment.

Note You must change the firmware from **BIOS** to EFI in the boot mode of VM settings to boot GPT partition with 2 TB or above.

Table 8: Recommended Disk Space for Virtual Machines

Cisco ISE Persona	Minimum Disk Space for Evaluation	Minimum Disk Space for Production	Recommended Disk Space for Production	Maximum Disk Space
Standalone Cisco ISE	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration only	300 GB	600 GB	600 GB	2.4 TB
Distributed Cisco ISE, Monitoring only	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Policy Service only	300 GB	300 GB	300 GB	2.4 TB
Distributed Cisco ISE, pxGrid only	300 GB	300 GB	300 GB	2.4 TB
Distributed Cisco ISE, Administration and Monitoring (and optionally, pxGrid)	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration, Monitoring, and Policy Service (and optionally, pxGrid)	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB

Note Additional disk space is required to store local debug logs, staging files, and to handle log data during upgrade, when the Primary Administration node temporarily becomes a Monitoring node.

39

Disk Space Guidelines

Keep the following guidelines in mind when deciding the disk space for Cisco ISE:

- Cisco ISE must be installed on a single disk in virtual machine.
- Disk allocation varies based on logging retention requirements. On any node that has the Monitoring persona enabled, 60 percent of the VM disk space is allocated for log storage. A deployment with 25,000 endpoints generates approximately 1 GB of logs per day.

  For example, if you have a Monitoring node with 600-GB VM disk space, 360 GB is allocated for log storage. If 100,000 endpoints connect to this network every day, it generates approximately 4 GB of logs per day. In this case, you can store 76 days of logs in the Monitoring node, after which you must transfer the old data to a repository and purge it from the Monitoring database.

For extra log storage, you can increase the VM disk space. For every 100 GB of disk space that you add, you get 60 GB more for log storage.

If you increase the disk size of your virtual machine after initial installation, then you must perform a fresh installation of Cisco ISE on your virtual machine to properly detect and utilize the full disk allocation.

The following table lists the number of days that RADIUS logs can be retained on your Monitoring node based on the allocated disk space and the number of endpoints that connect to your network. The numbers are based on the following assumptions: Ten or more authentications per day per endpoint with logging suppression enabled.

Table 9: Monitoring Node Log Storage—Retention Period in Days for RADIUS

No. of Endpoints	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

The following table lists the number of days that TACACS+ logs can be retained on your Monitoring node based on the allocated disk space and the number of endpoints that connect to your network. The numbers are based on the following assumptions: The script runs against all NADs, 4 sessions per day, and 5 commands per session.

Table 10: Monitoring Node Log Storage—Retention Period in Days for TACACS+

No. of Endpoints	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

Increasing Disk Size

If you find that context and visibility is slow, or you are running out of room for logs, you need to allocate more disk space.

To plan for additional log storage, for every 100 GB of disk space that you add, 60 GB is available for log storage.

In order for ISE to detect and utilize the new disk allocation, you must deregister the node, update the VM settings, and reinstall ISE. One way to do this is to install ISE on a new larger node, and add that node to the deployment as high availability. After the nodes have synchronized, make the new VM the primary and deregister the original VM.

CHAPTER 3

Install Cisco ISE

Install Cisco ISE Using CIMC

This section lists the high-level installation steps to help you quickly install Cisco ISE:

Before you begin

- Ensure that you have met the Hardware and Virtual Appliance Requirements as specified in this guide.
- (Optional; required only if you are installing Cisco ISE on virtual machines) Ensure that you have created the virtual machine correctly. See the following topics for more information:
  - Configure a VMware Server, on page 47
  - Install Cisco ISE on KVM, on page 58
  - Create a Cisco ISE Virtual Machine on Hyper-V, on page 59
- (Optional; required only if you are installing Cisco ISE on SNS hardware appliances) Ensure that you set up the Cisco Integrated Management Interface (CIMC) configuration utility to manage the appliance and configure BIOS. See the following document for more information:
  - For SNS 3500 series appliances, see Cisco SNS-3500 Series Appliance Hardware Installation Guide.
  - For SNS-3600 series appliances, see Cisco SNS-3600 Series Appliance Hardware Installation Guide.

Step 1 If you are installing Cisco ISE on a:

- Cisco SNS appliance: Install the hardware appliance. Connect to CIMC for server management.
- Virtual Machine: Ensure that your VM is configured correct.

Step 2 Download the Cisco ISE ISO image.

a) Go to http://www.cisco.com/go/ise. You must already have valid Cisco.com login credentials to access this link.

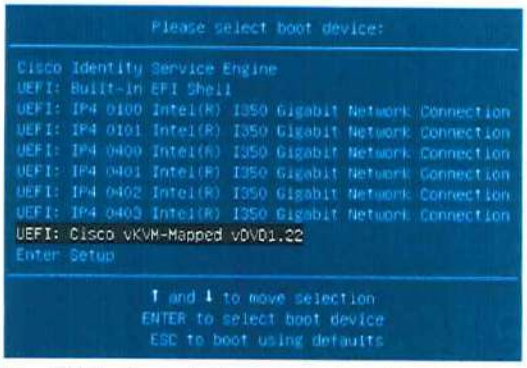
b) Click **Download Software for this Product.**

The Cisco ISE image comes with a 90-day evaluation license already installed, so you can begin testing all Cisco ISE services when the installation and initial configuration is complete.

Step 3 Boot the appliance or the virtual machine.

- Cisco SNS appliance:
  a. Connect to CIMC and log in using the CIMC credentials.
  b. Launch the KVM console.
  c. Choose Virtual Media > Activate Virtual Devices.
  d. Choose Virtual Media > Map CD/DVD and select the ISE ISO image and click Map Device.
  e. Choose Macros > Static Macros > Ctrl-Alt-Del to boot the appliance with the ISE ISO image.
  f. Press F6 to bring up the boot menu. A screen similar to the following one appears:

Figure 8: Boot Device Selection



Note If the SNS appliances are placed in a remote location (for example, data centers), to which you do not have any physical access and need to perform CIMC install from remote servers, it might t[illegible] hours for installation. We recommend that you copy the ISO file on a USB drive and use i[illegible] remote location to speed up the installation process.

- Virtual Machine:

a. Map the CD/DVD to an ISO image. A screen similar to the following one appears. The following message and installation menu are displayed.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 2.0.0.xxx

Available boot options:

Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

Step 4 At the boot prompt, press 1 and Enter to install Cisco ISE using a serial console.

If you want to use a keyboard and monitor, use the arrow key to select the **Cisco ISE Installation (Keyboard/Monitor)** option. The following message appears.

```
Please type 'setup' to configure the appliance
```

Step 5 At the prompt, type **setup** to start the Setup program. See Run the Setup Program on page 37 for details about the Setup program parameters.

Step 6 After you enter the network configuration parameters in the Setup mode, the appliance automatically reboots, and returns to the shell prompt mode.

Step 7 Exit from the shell prompt mode. The appliance comes up.

Step 8 Continue with Verify the Installation Process on page 53.

Run the Setup Program

This section describes the setup process to configure the ISE server.

The setup program launches an interactive command-line interface (CLI) that prompts you for the required parameters. An administrator can use the console or a dumb terminal to configure the initial network settings and provide the initial administrator credentials for the ISE server using the setup program. This setup process is a one-time configuration task.

Note If you are integrating with Active Directory (AD), it is best to use the IP and subnet addresses from a dedicated Site created specifically for ISE. Consult with the staff in your organization responsible for AD and retrieve the relevant IP and subnet addresses for your ISE nodes prior to installation and configuration.

Note It is not recommended to attempt offline installation of Cisco ISE as this can lead to system instability. When you run the Cisco ISE installation script offline, the following error is shown:

Sync with NTP server failed' Incorrect time could render the system unusable until it is re-installed. Retry? Y/N [Y]:

Choose **Yes** to continue with the installation. Choose **No** to retry syncing with the NTP server.

It is recommended to establish network connectivity with both the NTP server and the DNS server while running the installation script.

To run the setup program:

Step 1 Turn on the appliance that is designated for the installation.

The setup prompt appears:

```
Please type 'setup' to configure the appliance
localhost login:
```

Step 2 At the login prompt, enter **setup** and press **Enter**.

The console displays a set of parameters. You must enter the parameter values as described in the table that follows.

Note The eth0 interface of ISE must be statically configured with an IPv6 address if you want to add a Domain Name Server or an NTP Server with an IPv6 address.

Table 11: Cisco ISE Setup Program Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical (A–Z, a–z, 0–9), and the hyphen (-). The first character must be a letter. **Note** We recommend that you use lowercase letters to ensure that certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verifications. You cannot use "localhost" as hostname for a node.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 or Global IPv6 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14/ 2001:420:54ff:4::458:121:119

Prompt	Description	Example
Netmask	Must be a valid IPv4 or IPv6 netmask.	255.255.255.0/ 2001:420:54ff:4::458:121:119/122
Default gateway	Must be a valid IPv4 or Global IPv6 address for the default gateway.	10.12.13.1/ 2001:420:54ff:4::458:1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	example.com
Primary name server	Must be a valid IPv4 or Global IPv6 address for the primary name server.	10.15.20.25 / 2001:420:54ff:4::458:118
Add/Edit another name server	Must be a valid IPv4 or Global IPv6 address for the primary name server.	(Optional) Allows you to configure multiple name servers. To do so, enter y to continue.
Primary NTP server	Must be a valid IPv4 or Global IPv6 address or hostname of a Network Time Protocol (NTP) server. **Note** Ensure that the primary NTP server is reachable.	clock.nist.gov / 10.15.20.25 / 2001:420:54ff:4::458:117
Add/Edit another NTP server	Must be a valid NTP domain.	(Optional) Allows you to configure multiple NTP servers. To do so, enter y to continue.

Prompt	Description	Example
System **Time Zone**	Must be a valid time zone. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or Coordinated Universal Time (UTC) minus 8 hours). **Note** Ensure that the system time and time zone match with the CIMC or Hypervisor Host OS time and time zone. System performance might be affected if there is any mismatch between the time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones. **Note** We recommend that you set all the Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports, logs, and posture agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (*admin*), you must create a new username. The username must be three to eight characters in length and comprise of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password in order to continue because there is no default password. The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note When you create a password for the administrator during installation or after installation in the CLI, do not use the $ character in your password, unless it is the last character of the password. If it is the first or one of the subsequent characters, the password is accepted, but cannot be used to log in to the CLI.

If you inadvertently create such a password, reset your password by logging into the console and using the CLI command, or by getting an ISE CD or ISO file. Instructions for using an ISO file to reset the password are explained in the following document: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

After the setup program is run, the system reboots automatically.

Now, you can log in to Cisco ISE using the username and password that was configured during the setup process.

Verify the Installation Process

To verify that you have correctly completed the installation process:

Step 1 When the system reboots, at the login prompt enter the username you configured during setup, and press **Enter**.

Step 2 Enter a new password.

Step 3 Verify that the application has been installed properly by entering the **show application** command, and press Enter. The console displays:

```
ise/admin# show application
<name>          <Description>
ise             Cisco Identity Services Engine
```

Note The version and date might change for different versions of this release.

Step 4 Check the status of the ISE processes by entering the **show application status ise** command, and press Enter. The console displays:

```
ise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          14890
Database Server                        running          79 PROCESSES
Application Server                     running          19138
Profiler Database                      running          18793
ISE Indexing Engine                    running          20775
AD Connector                           running          22486
M&T Session Database                   running          14195
M&T Log Collector                      running          19234
M&T Log Processor                      running          19207
Certificate Authority Service          running          22247
EST Service                            running          21841
SXP Engine Service                     disabled
Docker Daemon                          running          21140
TC-NAC Service                         disabled
Wifi Setup Helper Container            not running
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
```



```
PassiveID API Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled

ise/admin#
```


CHAPTER 4

Install Cisco ISE with Amazon Web Services

Cisco ISE on Amazon Web Services

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 AWS.

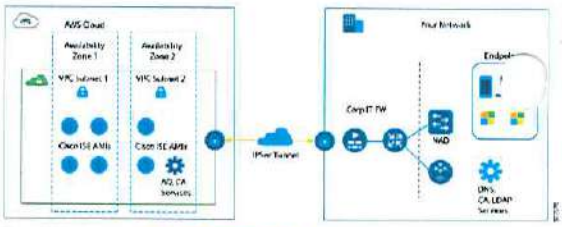
You can install and launch Cisco ISE in Amazon Web Services (AWS) through two methods:

- Launch Cisco ISE Through AWS Marketplace, on page 37
- Launch Cisco ISE With CloudFormation Template , on page 39

Cloud Formation Templates (CFT) are AWS solutions that allow you to easily create and manage cloud deployments. Extend your network into the cloud by creating a Virtual Private Cloud in AWS, and configure a virtual private gateway to enable communication with your organization's network over an IPsec Tunnel.

The following illustration is only an example. You can place common services like CA, AD, DNS, and LDAP on-premise or in AWS, based on the needs of your organization.

Figure 7: Example of a Deployment Connected to AWS Cloud



To use CFTs in AWS, see AWS CloudFormation User Guide.

The following table contains the details of the Cisco ISE instances that are currently available. You must purchase a Cisco ISE VM License to use any of the following instances. See Amazon EC2 On-Demand Pricing for information on EC2 instance pricing for your specific requirements.

Table 12: Cisco ISE Instances

Cisco ISE Instance Type	CPU Core	RAM
c5.4xlarge	16	32
m5.4xlarge	16	64
c5.9xlarge	36	72

Configure Policy Administration nodes (PAN) or Monitoring and Troubleshooting nodes (MnT node) on m5 Cisco ISE instance types. Configure Policy Service nodes (PSN) or Standalone nodes on c5 Cisco ISE instance types.

Table 13: Cisco ISE c5 Instances

Cisco ISE Instance Type	Recommended Persona for Instance Type	Maximum Endpoint Sessions Per Node: Dedicated PSN	Maximum Endpoint Sessions Per Node: All Personas Enabled
c5.4xlarge	Dedicated PSN	40,000	10,000
c5.9xlarge	Dedicated PSN	100,000	25,000

Table 14: Cisco ISE m5 Instances

Cisco ISE Instance Type	Recommended Persona for Instance Type	Maximum Active Sessions Per Deployment
m5.4xlarge	Dedicated PAN or dedicated MnT node	500,000

Prerequisites to Create a Cisco ISE AWS Instance

- You must be familiar with AWS solutions like EC2 instances and EBS volumes, and concepts like Regions, Availability Zones, Security Groups, VPCs, and so on. See the AWS documentation for information on these solutions.

  You must also be familiar with managing AWS service quotas.

- **Virtual Private Cloud (VPC) Configuration in AWS**

  When you configure your AWS VPC, choose one of the following:

  - **VPC With Public and Private Subnets and Hardware VPN Access**: This option allows both online and offline feed updates in Cisco ISE.
  - **VPC With a Private Subnet Only and Hardware VPN Access**: This option allows both online and offline feed updates in Cisco ISE. You must configure an enterprise proxy in Cisco ISE for online feed updates.

  Note You can also choose to configure your VPC without using a VPN.

  See What is AWS Site-to-Site VPN? and VPC with public and private subnets and AWS Site-to-Site VPN access.

- Create security groups, subnets, and key pairs in AWS before you configure a Cisco ISE instance.

  When you create a security group for Cisco ISE, you must create rules for all the ports and protocols for the Cisco ISE services you want to use. See Cisco ISE Ports Reference, on page 105.

- To configure an IPv6 address for the network interface, the subnet must have an IPv6 CIDR pool enabled in AWS.

- The IP address that you enter in the Management Network field when you configure a Cisco ISE instance must not be an IP address that is already added as a Network Interface object in AWS.

- You can configure a static IP as a Private IP in your deployment. However, the static IP must be configured with a DNS-resolvable hostname.

Known Limitations

The following are the known limitations with using Cisco ISE in AWS:

- You can only access and use Cisco ISE on AWS from your enterprise intranet through site-to-site VPN tunnels.
- The public cloud supports Layer 3 features only. Cisco ISE nodes on AWS instances do not support Cisco ISE functions that depend on Layers 1 and 2 capabilities. For example, DHCP SPAN profiler probes and CDP protocol functions through the Cisco ISE CLI are functions that are currently not supported.
- NIC Bonding is not supported.

- Dual NIC is supported with only two NICs—Gigabit Ethernet 0 and Gigabit Ethernet 1. To configure a secondary NIC in your Cisco ISE instance, you must first create a Network Interface object in AWS, and then attach this Network Interface object to your Cisco ISE. After you install and launch Cisco ISE on AWS, through the Cisco ISE CLI, manually configure the IP address of the Network Interface object as the secondary NIC.
- Cisco ISE upgrade workflow is not available in Cisco ISE on AWS. Only fresh installs are supported through the CFTs. However, you can carry out Backup and Restore of configuration data. When you restore the data in a Cisco ISE AWS instance, the data is upgraded to the Cisco ISE Release 3.1 version.
- SSH access to Cisco ISE CLI using password-based authentication is not supported in AWS. You can only access the Cisco ISE CLI through the key-pair generated in AWS and this key-pair must be stored securely.

  If you lose the Private Key (or PEM) file, you will not be able to access the Cisco ISE CLI.

  Any integration that uses a password-based authentication method to access Cisco ISE CLI is not supported. For example, Cisco DNA Center Releases 2.1.2 and earlier.
- You might receive an **Insufficient Virtual Machine Resources** alarm when Cisco ISE is in idle state. You can ignore this alarm as the CPU frequency is maintained lower than the required baseline frequency (2 GHz) for effective power conservation.
- When you run the `show inventory` CLI command through a Cisco ISE instance launched through AWS, the output for the command does not display the instance type of the Cisco ISE on AWS in the output.
- You cannot configure an IPv6 server as an NTP server when launching Cisco ISE through AWS.
- Serial Console monitoring is not supported.
- An initial administrator user account name, "admin", is generated by default. This user account name is used for both SSH and GUI access to Cisco ISE after the installation process is complete.
- You cannot resize an EC2 instance.
- You cannot convert a Cisco ISE Disk EBS Volume as an AMI and then relaunch another EC2 instance with this AMI.
- You cannot take an Amazon EBS snapshot of a Cisco ISE instance and then create another EBS volume with the snapshot.
- You can integrate external identity sources that are located on-premise. However, since traffic is hairpinned, Cisco ISE performance when on-prem identity sources are used, is not at par with Cisco ISE performance when AWS-hosted identity sources or the Cisco ISE internal user database are used.
- The following deployment types are supported, but you must ensure that inter-node latencies are below 200 milliseconds:
  - Hybrid deployments with some Cisco ISE nodes on-premise and some nodes in AWS.
  - Inter-region deployments via VPC peering connections.
- Amazon EC2 user data scripts are not supported.
- In the Cisco ISE CFT that you configure, you define Volume Size in GB. However, AWS creates EBS storage volumes in Gibibyte (GiB). Therefore, when you enter 600 as the Volume Size in the Cisco ISE CFT, AWS creates 600GiB (or 644.25 GB) of EBS volume.

Launch Cisco ISE Through AWS Marketplace

You can only set up standalone nodes through the CFT configurations. To create a Cisco ISE deployment, see Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

You cannot add multiple DNS or NTP servers through the CFT. After you create the Cisco ISE instance, you can add additional DNS or NTP servers through the Cisco ISE CLI. You also cannot configure IPv6 DNS or NTP servers through the CFT. Use the Cisco ISE CLI to configure IPv6 servers.

Before you begin

Create in AWS the security groups and management networks that you wish to include in your Cisco ISE CFT configuration.

Step 1 Log in to the Amazon Management Console at https://console.aws.amazon.com/, and search for `AWS Marketplace Subscriptions`.

Step 2 In the **Manage Subscriptions** window that is displayed, click **Discover Products** in the left menu.

Step 3 Enter `Cisco Identity Services Engine (ISE)` in the search bar.

Step 4 Click the product name, and in the new window displayed, click **Continue to Subscribe**.

Step 5 Click **Continue to Configuration**.

Step 6 In the **Configure this software** area, click **Learn More** and click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system. You can use this template to automate the configuration of other Cisco ISE instances, as required.

You can also click **View Template** in the **Learn More** dialog box to view the CFT the AWS CloudFormation Designer.

Step 7 Choose the required values from the **Software Version** and **AWS Region**.

Step 8 Click **Continue to Launch**.

Step 9 Choose **Launch CloudFormation** from the **Choose Action** drop-down list.

Step 10 Click **Launch**.

Step 11 In the **Create Stack** window, choose **Template Is Ready** and **Amazon S3 URL**.

Step 12 Click **Next**.

Step 13 In the new window, enter a value in the **Stack Name** field.

Step 14 Enter the required details in the following fields in the **Parameters** area:

- **Hostname**: This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.
- **Instance Key Pair**: To access the Cisco ISE instance via SSH, choose the PEM file that you created in AWS for the username "admin". Create a PEM key pair in AWS now if you have not configured one already. For example, `ssh -i mykeypair.pem AdminMyHostname.compute-1.amazonaws.com`.
- **Management Security Group**: Choose the security group from the drop-down list. You must create the security group in AWS before configuring this CFT.
- **Management Network**: Choose the subnet to be used for the Cisco ISE interface. To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets. Create a Subnet in AWS now if you have not configured one already.

- **Management Private IP**: Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IP address.

  After the Cisco ISE instance is created, copy the private IP address from the Instance Summary window. Then, add the IP-hostname mapping to your DNS server before you create a Cisco ISE deployment.
- **Timezone**: Choose a system time zone from the drop-down list.
- **Instance Type**: Choose a Cisco ISE instance type from the drop-down list.
- **EBS Encryption**: Choose **True** from the drop-down list to enable encryption. The default value for this field is **False**
- **Volume Size**: Specify the volume size in GB. The accepted range is 300 GB to 2400 GB. We recommend 600GB for production use. Configure a volume size lesser than 600GB only for evaluation purposes. When you terminate the instance, the volume is also deleted.

  Note AWS creates EBS storage volumes in Gibibyte (GiB). When you enter 600 in the Volume Size field, AWS creates 600GiB (or 644.25 GB) of EBS volume.
- **DNS Domain**: field are ASCII characters, numerals, hyphen (-), and period (.).
- **Name Server**: Enter the IP address of the name server in the correct syntax.
- **NTP Server**: Enter the IP address or hostname of the NTP server in the correct syntax (for example, `time.nist.gov`). Your entry is not verified on submission. If you use the wrong syntax, Cisco ISE services might not come up on launch.

  Note If the IP address or the hostname that you enter here is incorrect, Cisco ISE cannot synchronize with the NTP server. You must SSH to Cisco ISE and use the Cisco ISE CLI to configure the correct NTP server.
- **ERS**: To enable ERS services at Cisco ISE launch, enter `yes`. The default value for this field is No.
- **OpenAPI**: To enable OpenAPI services in Cisco ISE launch, enter `yes`. The default value for this field is No.
- **pxGrid**: To enable pxGrid services at Cisco ISE launch, enter `yes`. The default value for this field is No.
- **pxGrid Cloud**: The default value for this field is No.

  Note This feature is currently not available as there are dependencies on complementary product releases. Do not enable pxGrid Cloud services.
- **Enter Password**: Enter the administrative password that must be used for GUI. The password must be in compliance with the Cisco ISE password policy. The password is displayed in plaintext in the **User Data** area of the Instance settings window in the AWS console. See "User Password Policy" in Chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.
- **Confirm Password**: Retype the administrative password

Step 15 Click **Next** to initiate the instance creation process.

Launch Cisco ISE With CloudFormation Template

You can only set up standalone nodes through the CFT configurations. To create a Cisco ISE deployment, see Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

You cannot add multiple DNS or NTP servers through the CFT. After you create the Cisco ISE instance, you can add additional DNS or NTP servers through the Cisco ISE CLI. You also cannot configure IPv6 DNS or NTP servers through the CFT. Use the Cisco ISE CLI to configure IPv6 servers.

Before you begin

Create in AWS the security groups and management networks that you wish to include in your Cisco ISE CFT configuration.

Step 1 Log in to the Amazon Management Console at `https://console.aws.amazon.com/`, and search for `AWS Marketplace Subscriptions`.

Step 2 In the **Manage Subscriptions** window that is displayed, click **Discover Products** in the left menu.

Step 3 Enter `Cisco Identity Services Engine (ISE)` in the search bar.

Step 4 Click the product name, and in the new window displayed, click **Continue to Subscribe**.

Step 5 Click **Continue to Configuration**.

Step 6 In the **Configure** this software area, click **Learn More** and click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system. You can use this template to automate the configuration of other Cisco ISE instances, as required.

You can also click **View Template** in the **Learn More** dialog box to view the CFT the AWS CloudFormation Designer.

Step 7 In the AWS search bar, search for `cloudformation`.

Step 8 From the **Create Stack** drop-down list, choose **With new resources (standard)**.

Step 9 In the **Create Stack** window, choose **Template Is Ready** and **Upload a Template File**.

Step 10 Click **Choose File** and upload the CFT file that you downloaded in Step 7.

Step 11 Click **Next**.

Step 12 In the new window, enter a value in the **Stack Name** field.

Step 13 Enter the required details in the following fields in the **Parameters** area.

- **Hostname**: This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.
- **Instance Key Pair**: To access the Cisco ISE instance via SSH, choose the PEM file that you created in AWS for the username "admin". Create a PEM key pair in AWS now if you have not configured one already. For example, `ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com`.
- **Management Security Group**: Choose the security group from the drop-down list. You must create the security group in AWS before configuring this CFT.
- **Management Network**: Choose the subnet to be used for the Cisco ISE interface. To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets. Create a Subnet in AWS now if you have not configured one already.
- **Management Private IP**: Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IP address.

After the Cisco ISE instance is created, copy the private IP address from the Instance Summary window. Then, add the IP-hostname mapping to your DNS server before you create a Cisco ISE deployment.

- **Timezone**: Choose a system time zone from the drop-down list.
- **Instance Type**: Choose a Cisco ISE instance type from the drop-down list.
- **EBS Encryption**: Choose **True** from the drop-down list to enable encryption. The default value for this field is False.
- **Volume Size**: Specify the volume size in GB. The accepted range is 300 GB to 2400 GB. We recommend 600GB for production use. Configure a volume size lesser than 600GB only for evaluation purposes. When you terminate the instance, the volume is also deleted.

  Note AWS creates EBS storage volumes in Gibibyte (GiB). When you enter 600 in the Volume Size field, AWS creates 600GiB (or 644.25 GB) of EBS volume.

- **DNS Domain**: field are ASCII characters, numerals, hyphen (-), and period (.).
- **Name Server**: Enter the IP address of the name server in the correct syntax.
- **NTP Server**: Enter the IP address or hostname of the NTP server in the correct syntax (for example, `time.nist.gov`). Your entry is not verified on submission. If you use the wrong syntax, Cisco ISE services might not come up on launch.

  Note If the IP address or the hostname that you enter here is incorrect, Cisco ISE cannot synchronize with the NTP server. You must SSH to Cisco ISE and use the Cisco ISE CLI to configure the correct NTP server.

- **ERS**: To enable ERS services at Cisco ISE launch, enter `yes`. The default value for this field is No.
- **OpenAPI**: To enable OpenAPI services at Cisco ISE launch, enter `yes`. The default value for this field is No.
- **pxGrid**: To enable pxGrid services at Cisco ISE launch, enter `yes`. The default value for this field is No.
- **pxGrid Cloud**. The default value for this field is No.

  Note This feature is currently not available as there are dependencies on complementary product releases. Do not enable pxGrid Cloud services.

- **Enter Password**: Enter the administrative password that must be used for GUI. The password must b[illegible]pliance with the Cisco ISE password policy. The password is displayed in plaintext in the **User Data** area[illegible]stance settings window in the AWS console. See "User Password Policy" in Chapter "Basic Setup" of the [illegible] *ISE Administrator Guide* for your release.
- **Confirm Password**: Retype the administrative password.

Step 14 Click **Next** to initiate the instance creation process.

Post-Installation Notes and Tasks

To check the status of the instance launch, in the left side menu of the AWS console, click Instances. The **Status Check** column for the instance displays Initializing while the instance is being configured. When the instance is ready and available, the column displays **x checks done**.

You can access the Cisco ISE GUI or CLI about 30 minutes after the Cisco ISE EC2 instance is built. You can access the CLI and GUI of Cisco ISE with the IP address that AWS provides for your instance, and log in to the Cisco ISE administration portal or console.

When the Cisco ISE instance is ready and available for use, carry out the following steps:

1. When you create a Key Pair in AWS, it is automatically downloaded to your local system. The key that you download from AWS contains specific permissions that you must update to successfully SSH to the Cisco ISE instance.

   If you use Linux or macOS operating systems, run the following command in your CLI application:

   `sudo chmod 0400 mykeypair.pem`

   If you use Windows operating system:

   a. Right-click the key file in your local system.
   b. Choose **Properties** > **Security** > **Advanced**.
   c. In the **Permissions** tab, assign full control to the appropriate user, and click **Disable Inheritance**.
   d. In the Block Inheritance dialog box, click **Convert inherited permissions into explicit permissions on this object**.
   e. In the **Permissions** tab, choose system and administrator users and click **Remove**.
   f. Click Apply, and then click **OK**.

2. Access the Cisco ISE CLI by running the following command in your CLI application:

   `ssh -i mykeypair.pem admin@Cisco ISE Private IP Address`

3. At the login prompt, enter `admin` as the username.
4. At the system prompt, enter `show application version ise` and press **Enter**.
5. To check the status of the Cisco ISE processes, enter `show application status ise` and press **Enter**.

   If the output displays that Application Server is in running state, Cisco ISE is ready for use.

6. You can then log in to the Cisco ISE GUI.

Then, carry out the post-installation tasks listed in List of Post-Installation Tasks, on page 93.

Compatibility Information for Cisco ISE on AWS

This section details compatibility information that is unique to Cisco ISE on AWS. For general compatibility details for Cisco ISE, see *Cisco Identity Services Engine Network Component Compatibility, Release 3.1*.

Cisco DNA Center Integration Support

You can connect your Cisco ISE to Cisco DNA Center Release 2.2.1 and later releases.

Load Balancer Integration Support

You can integrate AWS-native Network Load Balancer (NLB) with Cisco ISE for load balanci[illegible]IUS traffic. However, the following caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation in NLB.
- Unequal load balancing might occur as NLB only supports source IP affinity and does not support calling station ID-based sticky sessions.
- Traffic might be sent to a Cisco ISE PSN even if the RADIUS service is not active on the node as NLB does not support RADIUS-based health checks.

You can integrate AWS-native Network Load Balancer (NLB) with Cisco ISE for load balancing TACACS traffic. However, traffic might be sent to a Cisco ISE PSN even if the TACACS service is not active on the node as NLB does not support TACACS-based health checks.

NIC Jumbo Frame Support

Cisco ISE supports jumbo frames. The Maximum Transmission Unit (MTU) for Cisco ISE is 9,001 bytes, while the MTU of Network Access Devices is typically 1,500 bytes. Cisco ISE supports and receives both standard and jumbo frames without issue. You can reconfigure the Cisco ISE MTU as required through the Cisco ISE CLI in Configuration Mode.

CHAPTER 5

Additional Installation Information

SNS Appliance Reference

Create a Bootable USB Device to Install Cisco ISE

Use the LiveUSB-creator tool to create a bootable USB device from the Cisco ISE installation ISO file.

Before you begin

- Download LiveUSB-creator to the local system from the following location: https://github.com/lmacken/liveusb-creator/releases/tag/3.12.0
- Download the Cisco ISE installation ISO file to the local system.
- Use an 16-GB or 32-GB USB device.

Step 1 Reformat the USB device using FAT16 or FAT32 to free up all the space.

Step 2 Plug in the USB device to the local system and launch **LiveUSB-creator**.

Step 3 Click **Browse** from the **Use existing Live CD** area and choose the Cisco ISE ISO file.

Step 4 Choose the USB device from the **Target Device** drop-down list.

If there is only one USB device connected to the local system, it is selected automatically.

Step 5 Click **Create Live USB**.
The progress bar indicates the progress of the bootable USB creation. After this process is complete, the content of the USB drive is available in the local system that you used to run the USB tool. There are two text files that you must manually update before you can install Cisco ISE.

Step 6 From the USB drive, open the following text files in a text editor:

- *isolinux/isolinux.cfg* or *syslinux/syslinux.cfg*
- *EFI/BOOT/grub.cfg*

Step 7 Replace the term "**cdrom**" in both the files.

- If you have a 3595, 3615, 3655, or 3695 appliance, replace the term "**cdrom**" with "**hdtsdb1**" in both the files.

Specifically, replace all instances of the "**cdrom**" string. For example, replace

ks=cdrom/ks.cfg

with

ks=hd:sdb1:/ks.cfg

Step 8 Save the files and exit.

Step 9 Safely remove the USB device from the local system.

Step 10 Plug in the bootable USB device to the Cisco ISE appliance, restart the appliance, and boot from the USB drive to install Cisco ISE.

Reimage the Cisco SNS 3500/3600 Series Appliance

The Cisco SNS 3500/3600 series appliances do not have built-in DVD drives. Therefore, to reimage a Cisco ISE hardware appliance with Cisco ISE software, you can do one of the following:

Note The SNS 3500 and 3600 series appliances support the Unified Extensible Firmware Interface (UEFI) secure boot feature. This feature ensures that only a Cisco-signed ISE image can be installed on the SNS 3500 and 3600 series appliances, and prevents installation of any unsigned operating system even with physical access to the device. For example, generic operating systems, such as Red Hat Enterprise Linux or Microsoft Windows cannot boot on this appliance.

- Use the Cisco Integrated Management Controller (CIMC) interface to map the installation .iso file to the virtual DVD device. See Install Cisco ISE Using CIMC, on page 25 for more information.
- Create an install DVD with the installation .iso file and plug in an USB external DVD drive and boot the appliance from the DVD drive.
- Create a bootable USB device using the installation .iso file and boot the appliance from the USB drive. See Create a Bootable USB Device to Install Cisco ISE, on page 43 and Install Cisco ISE Using CIMC, on page 25 for more information.

VMware Virtual Machine

Note The VMware form factor instructions provided in this document are applicable for ISE installed on Cisco Hyperflex as well.

Virtual Machine Resource and Performance Checks

Before installing Cisco ISE on a virtual machine, the installer performs hardware integrity checks by comparing the available hardware resources on the virtual machine with the recommended specifications.

During a VM resource check, the installer checks for the hard disk space, number of CPU cores allocated to the VM, CPU clock speed, and RAM allocated to the VM. If the VM resources do not meet the basic evaluation specifications, the installation terminates. This resource check is applicable only for ISO-based installations.

When you run the Setup program, a VM performance check is done, where the installer checks for disk I/O performance. If the disk I/O performance does not meet the recommended specifications, a warning appears on screen, but it allows you to continue with the installation.

The VM performance check is done periodically (every hour) and the results are averaged for a day. If the disk I/O performance does not meet the recommended specification, an alarm is generated.

The VM performance check can also be done on demand from the Cisco ISE CLI using the **show tech-support** command.

The VM resource and performance checks can be run independent of Cisco ISE installation. You can perform this test from the Cisco ISE boot menu.

Install Cisco ISE on VMware Virtual Machine Using the ISO File

This section describes how to install Cisco ISE on a VMware virtual machine using the ISO file.

Prerequisites for Configuring a VMware ESXi Server

Review the following configuration prerequisites listed in this section before you attempt to configure a VMWare ESXI server:

- Remember to log in to the ESXi server as a user with administrative privileges (root user).
- Cisco ISE is a 64-bit system. Before you install a 64-bit system, ensure that Virtualization Technology (VT) is enabled on the ESXi server.
- Ensure that you allocate the recommended amount of disk space on the VMware virtual machine. See the Disk Space Requirements, on page 22 section for more information.
- If you have not created a VMware virtual machine file system (VMFS), you must create one to support the Cisco ISE virtual appliance. The VMFS is set for each of the storage volumes configured on the VMware host. For VMFS5, the 1-MB block size supports up to 1.999 TB virtual disk size.

Virtualization Technology Check

If you have an ESXi server installed already, you can check if VT is enabled on it without rebooting the machine. To do this, use the **esxcfg-info** command. Here is an example:

```
~ # esxcfg-info |grep "HV Support"
|----HV Support.....3
|----Host Command Line.....grep HV Support
```

If HV Support has a value of 3, then VT is enabled on the ESXi server and you can proceed with the installation.

If HV Support has a value of 2, then VT is supported, but not enabled on the ESXi server. You must edit the BIOS settings and enable VT on the server.

Enable Virtualization Technology on an ESXi Server

You can reuse the same hardware that you used for hosting a previous version of Cisco ISE virtual machine. However, before you install the latest release, you must enable Virtualization Technology (VT) on the ESXi server.

Step 1 Reboot the appliance.

Step 2 Press **F2** to enter setup.

Step 3 Choose **Advanced** > **Processor Configuration**.

Step 4 Select **Intel(R) VT** and enable it.

Step 5 Press **F10** to save your changes and exit.

Configure VMware Server Interfaces for the Cisco ISE Profiler Service

Configure VMware server interfaces to support the collection of Switch Port Analyzer (SPAN) or mirrored traffic to a dedicated probe interface for the Cisco ISE Profiler Service.

Step 1 Choose **Configuration** > **Networking** > **Properties** > **VMNetwork** (the name of your VMware server instance)**VMswitch0** (one of your VMware ESXi server interfaces) **Properties** **Security**.

Step 2 In the Policy Exceptions pane on the **Security** tab, check the **Promiscuous Mode** check box.

Step 3 In the Promiscuous Mode drop-down list, choose **Accept** and click **OK**.

Repeat the same steps on the other VMware ESXi server interface used for profiler data collection of SPAN or mirrored traffic.

Connect to the VMware Server Using the Serial Console

Step 1 Power down the particular VMware server (for example ISE-120).

Step 2 Right-click the VMware server and choose **Edit**.

Step 3 Click **Add** on the Hardware tab.

Step 4 Choose **Serial Port** and click **Next**.

Step 5 In the Serial Port Output area, click the **Use physical serial port on the host** or the **Connect via Network** radio button and click **Next**.

- If you choose the Connect via Network option, you must open the firewall ports over the ESXi server.
- If you select the Use physical serial port on the host, choose the port. You may choose one of the following two options:
  - **/dev/ttyS0** (In the DOS or Windows operating system, this will appear as COM1).
  - **/dev/ttyS1** (In the DOS or Windows operating system, this will appear as COM2).

Step 6 Click **Next**.

42

Step 7 In the Device Status area, check the appropriate check box. The default is Connected.
Step 8 Click **OK** to connect to the VMware server.

Configure a VMware Server

Before you begin

Ensure that you have read the details in the Prerequisites for Configuring a VMware ESXi Server, on page 45 section.

Step 1 Log in to the ESXi server.
Step 2 In the VMware vSphere Client, in the left pane, right-click your host container and choose **New Virtual Machine**.
Step 3 In the Configuration dialog box, choose **Custom** for the VMware configuration and click **Next**.
Step 4 Enter a name for the VMware system and click **Next**.

Tip Tip Use the hostname that you want to use for your VMware host.

Step 5 Choose a datastore that has the recommended amount of space available and click **Next**.
Step 6 (Optional) If your VM host or cluster supports more than one VMware virtual machine version, choose a Virtual Machine version such as Virtual Machine Version 7, and click **Next**.
Step 7 Choose **Linux** and select the supported Red Hat Enterprise Linux version from the **Version** drop-down list.
Step 8 Choose a value from the Number of virtual sockets and the Number of cores per virtual socket drop-down list. Total number of cores should be:

SNS 3600 Series Appliance:

- Small—16
- Medium—24
- Large—24

The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3600 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU Cores or 16 Threads.

Note We strongly recommend that you reserve CPU and memory resources to match the resource allocation. Failure to do so may significantly impact ISE performance and stability.

Step 9 Choose the amount of memory and click **Next**.
Step 10 Choose the **E1000** NIC driver from the Adapter drop-down list and click **Next**.

Note We recommend that you select E1000 to ensure correct adapter order by default. If you choose VMXNET3, you might have to remap the ESXi adapter to synchronize it with the ISE adapter order.

Step 11 Choose **Paravirtual** as the SCSI controller and click **Next**.
Step 12 Choose **Create a new virtual disk** and click **Next**.
Step 13 In the Disk Provisioning dialog box, click **Thick provisioned, eagerly zeroed** radio button, and click **Next** to continue.

Cisco ISE supports both thick and thin provisioning. However, we recommend that you choose thick provisioned, eagerly zeroed for better performance, especially for Monitoring nodes. If you choose thin provisioning, operations such as upgrade, backup and restore, and debug logging that require more disk space might be impacted during initial disk expansion.

Step 14 Uncheck the **Support clustering features such as Fault Tolerance** check box.
Step 15 Choose the advanced options, and click **Next**.
Step 16 Verify the configuration details, such as Name, Guest OS, CPUs, Memory, and Disk Size of the newly created VMware system.
Step 17 Click **Finish**.

The VMware system is now installed.

What to do next

To activate the newly created VMware system, right-click VM in the left pane of your VMware client user interface and choose **Power > Power On**.

Increase Virtual Machine Power-On Boot Delay Configuration

On a VMware virtual machine, the boot delay by default is set to 0. You can change this boot delay to help you choose the boot options (while resetting the Administrator password, for example).

Step 1 From the VSphere client, right click the VM and choose **Edit Settings**.
Step 2 Click the **Options** tab.
Step 3 Choose **Advanced > Boot Options**.
Step 4 From the **Power on Boot Delay** area, select the time in milliseconds to delay the boot operation.
Step 5 Check the check box in the **Force BIOS Setup** area to enter into the BIOS setup screen when the VM boots the next time.
Step 6 Click **OK** to save your changes.

Install Cisco ISE Software on a VMware System

Before you begin

- After installation, if you do not install a permanent license, Cisco ISE automatically installs a 90-day evaluation license that supports a maximum of 100 endpoints.
- Download the Cisco ISE software from the Cisco Software Download Site at http://www.cisco.com/en/US/products/ps11640/index.html and burn it on a DVD. You will be required to provide your Cisco.com credentials.
- (Optional; applicable only if you are installing Cisco ISE on VMware Cloud) The process of installing Cisco ISE on VMware Cloud is exactly the same as that of installing Cisco ISE on VMware virtual machine.

- Cisco ISE virtual machine deployed on VMware cloud in Amazon Web Services (AWS): Cisco ISE can be hosted on software-defined data center (SDDC) provided by VMware Cloud on AWS. Ensure that appropriate security group policies are configured on VMware Cloud (under **Networking and Security > Security > Gateway Firewall Settings**) to enable reachability to on-premises deployment, required devices and services.
- Cisco ISE virtual machine deployed on Azure VMware Solution (AVS): AVS runs VMware workloads natively on Microsoft Azure, where Cisco ISE can be hosted as VMware virtual machine.

Step 1 Log in to the VMware client.
Step 2 For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.
Step 3 Click the **Options** tab.
Step 4 Click **Boot Options**, and in the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note You must change the firmware from **BIOS** to **EFI** in the boot mode of VM settings to boot GPT partitions with 2 TB or more capacity.

Step 5 Click **OK**.
Step 6 Ensure that the Coordinated Universal Time (UTC) and the correct boot order are set in BIOS:
a) If the VM is turned on, turn the system off.
b) Turn on the VM.

The system enters the BIOS setup mode.

c) In the Main BIOS menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.
d) Enter the UTC/Greenwich Mean Time (GMT) time zone.

This time zone setting ensures that the reports, logs, and posture-agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.

e) Using the arrow keys, navigate to the Boot menu and press **Enter**.
f) Using the arrow keys, select CD-ROM drive and press + to move the CD-ROM drive up the order.
g) Using the arrow keys, navigate to the Exit menu and choose **Exit Saving Changes**.
h) Choose **Yes** to save the changes and exit.

Step 7 Insert the Cisco ISE software DVD into the VMware ESXi host CD/DVD drive and turn on the virtual machine.

When the DVD boots, the console displays:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <return>.
boot:
```


Step 8 Use the arrow keys to select **Cisco ISE Installation (Serial Console)** or **Cisco ISE Installation (Keyboard/Monitor)** and press **Enter**. If you choose the serial console option, you should have a serial console set up on your virtual machine. See the VMware vSphere Documentation for information on how to create a console.
The installer starts the installation of the Cisco ISE software on the VMware system. Allow 20 minutes for the installation process to complete. When the installation process finishes, the virtual machine reboots automatically. When the VM reboots, the console displays:

```
Type 'setup' to configure your appliance
localhost:
```

Step 9 At the system prompt, type **setup** and press **Enter**.

Note From Cisco ISE Release 3.0 onwards, the CPUs of the virtualization platform that hosts ISE virtual machines must support (Streaming SIMD Extensions) SSE 4.2 instruction set. Otherwise, certain ISE services (e.g. the ISE API gateway) will not work, and the Cisco ISE GUI cannot be launched. Both Intel and AMD processors have been supporting SSE 4.2 version since 2011.

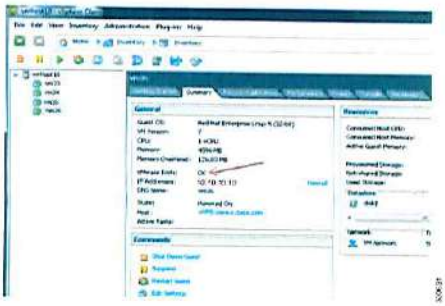
The Setup Wizard appears and guides you through the initial configuration.

VMware Tools Installation Verification

Verify VMWare Tools Installation Using the Summary Tab in the vSphere Client

Go to the Summary tab of the specified VMware host in the vShpere Client. The value in the VMware Tools field should be OK.

Figure 8: Verifying VMware Tools in the vSphere Client



Verify VMWare Tools Installation Using the CLI

You can also verify if the VMware tools are installed using the **show inventory** command. This command lists the NIC driver information. On a virtual machine with VMware tools installed, VMware Virtual Ethernet driver will be listed in the Driver Descr field.

```
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9          , VID: A0  , SN: FCH19xxxxxx
Total RAM Memory: 65750280 kB
CPU Core Count: 16
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.60GHz
CPU 1: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 2: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 3: Model Info: Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.60GHz
CPU 4: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 5: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 6: Model Info: Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.60GHz
CPU 7: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 8: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 9: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 10: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 11: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 12: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 13: Model Info: Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.60GHz
CPU 14: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 15: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /xxx/abc
Disk 0: Capacity: 110.00 GB
NIC Count: 6
NIC 0: Device Name: eth0:
NIC 0: MAC Address: xx:xx:xx:xx:xx:xx
NIC 0: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 1: Device Name: eth1:
NIC 1: MAC Address: xx:xx:xx:xx:xx:xx
NIC 1: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 2: Device Name: eth2:
NIC 2: MAC Address: xx:xx:xx:xx:xx:xx
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3:
NIC 3: MAC Address: xx:xx:xx:xx:xx:xx
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 4: Device Name: eth4:
NIC 4: MAC Address: xx:xx:xx:xx:xx:xx
NIC 4: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 5: Device Name: eth5:
NIC 5: MAC Address: xx:xx:xx:xx:xx:xx
NIC 5: Driver Descr: Intel(R) Gigabit Ethernet Network Driver

(*) Hard Disk Count may be Logical.
```

Support for Upgrading VMware Tools

The Cisco ISE ISO image (regular, upgrade, or patch) contains the supported VMware tools. Upgrading VMware tools through the VMware client user interface is not supported with Cisco ISE. If you want to upgrade any VMware tools to a higher version, support is provided through a newer version of Cisco ISE (regular, upgrade, or patch release).

Clone a Cisco ISE Virtual Machine

You can clone a Cisco ISE VMware virtual machine (VM) to create an exact replica of a Cisco ISE node. For example, in a distributed deployment with multiple Policy Service nodes (PSNs), VM cloning helps you deploy the PSNs quickly and effectively. You do not have to install and configure the PSNs individually.

You can also clone a Cisco ISE VM using a template.

Note For cloning, you need VMware vCenter. Cloning must be done before you run the Setup program.

Before you begin

- Ensure that you shut down the Cisco ISE VM that you are going to clone. In the vSphere client, right-click the Cisco ISE VM that you are about to clone and choose **Power > Shut Down Guest**.
- Ensure that you change the IP Address and Hostname of the cloned machine before you power it on and connect it to the network.

Step 1 Log in to the ESXi server as a user with administrative privileges (root user).

VMware vCenter is required to perform this step.

Step 2 Right-click the Cisco ISE VM you want to clone, and click **Clone**.

Step 3 Enter a name for the new machine that you are creating in the Name and Location dialog box and click **Next**.

This is not the hostname of the new Cisco ISE VM that you are creating, but a descriptive name for your reference.

Step 4 Select a Host or Cluster on which you want to run the new Cisco ISE VM and click **Next**.

Step 5 Select a datastore for the new Cisco ISE VM that you are creating and click **Next**.

This datastore could be the local datastore on the ESXi server or a remote storage. Ensure that the datastore has enough disk space.

Step 6 Click the **Same format as source** radio button in the Disk Format dialog box and click **Next**.

This option copies the same format that is used in the Cisco ISE VM that you are cloning this new machine from.

Step 7 Click the **Do not customize** radio button in the Guest Customization dialog box and click **Next**.

Step 8 Click **Finish**.

What to do next

- Change the IP Address and Hostname of a Cloned Virtual Machine
- Connect a Cloned Cisco Virtual Machine to the Network

Clone a Cisco ISE Virtual Machine Using a Template

If you are using vCenter, then you can use a VMware template to clone a Cisco ISE virtual machine (VM). You can clone the Cisco ISE node to a template and use that template to create multiple new Cisco ISE nodes. Cloning a virtual machine using a template is a two-step process:

Before you begin

Note For cloning, you need VMware vCenter. Cloning must be done before you run the Setup program.

Step 1 Create a Virtual Machine Template, on page 53

Step 2 Deploy a Virtual Machine Template, on page 53

Create a Virtual Machine Template

Before you begin

- Ensure that you shut down the Cisco ISE VM that you are going to clone. In the vSphere client, right-click the Cisco ISE VM that you are about to clone and choose **Power > Shut Down Guest**.
- We recommend that you create a template from a Cisco ISE VM that you have just installed and not run the setup program on. You can then run the setup program on each of the individual Cisco ISE nodes that you have created and configure IP address and hostnames individually.

Step 1 Log in to the ESXi server as a user with administrative privileges (root user).

VMware vCenter is required to perform this step.

Step 2 Right-click the Cisco ISE VM that you want to clone and choose **Clone > Clone to Template**.

Step 3 Enter a name for the template, choose a location to save the template in the Name and Location dialog box, and click **Next**.

Step 4 Choose the ESXi host that you want to store the template on and click **Next**.

Step 5 Choose the datastore that you want to use to store the template and click **Next**.

Ensure that this datastore has the required amount of disk space.

Step 6 Click the **Same format as source** radio button in the Disk Format dialog box and click Next.

The Ready to Complete dialog box appears.

Click **Finish**.

Deploy a Virtual Machine Template

After you create a virtual machine template, you can deploy it on other virtual machines (VMs).

Step 1 Right-click the Cisco ISE VM template that you have created and choose **Deploy Virtual Machine from this template.**

Step 2 Enter a name for the new Cisco ISE node, choose a location for the node in the Name and Location dialog box, and click **Next**.

Step 3 Choose the ESXi host where you want to store the new Cisco ISE node and click **Next**.

Step 4 Choose the datastore that you want to use for the new Cisco ISE node and click **Next**.

Ensure that this datastore has the required amount of disk space.

Step 5 Click the **Same format as source** radio button in the Disk Format dialog box and click **Next**.

Step 6 Click the **Do not customize** radio button in the Guest Customization dialog box.

The Ready to Complete dialog box appears.

Step 7 Check the **Edit Virtual Hardware** check box and click **Continue**.

The Virtual Machine Properties page appears.

Step 8 Choose **Network adapter**, uncheck the **Connected** and **Connect at power on** check boxes, and click **OK**.

Step 9 Click **Finish**.

You can now power on this Cisco ISE node, configure the IP address and hostname, and connect it to the network.

What to do next

- Change the IP Address and Hostname of a Cloned Virtual Machine
- Connect a Cloned Cisco Virtual Machine to the Network

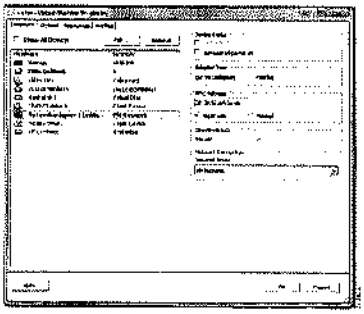
Change the IP Address and Hostname of a Cloned Virtual Machine

After you clone a Cisco ISE virtual machine (VM), you have to power it on and change the IP address and hostname.

Before you begin

- Ensure that the Cisco ISE node is in the standalone state.
- Ensure that the network adapter on the newly cloned Cisco ISE VM is not connected when you power on the machine. Uncheck the **Connected** and **Connect at power on** check boxes. Otherwise, if this node comes up, it will have the same IP address as the source machine from which it was cloned.

Figure 6: Disconnecting the Network Adapter



- Ensure that you have the IP address and hostname that you are going to configure for the newly cloned VM as soon as you power on the machine. This IP address and hostname entry should be in the DNS server. You cannot use "localhost" as the hostname for a node.
- Ensure that you have certificates for the Cisco ISE nodes based on the new IP address or hostname.

Procedure

Step 1 Right-click the newly cloned Cisco ISE VM and choose **Power** > **Power On**.

Step 2 Select the newly cloned Cisco ISE VM and click the **Console** tab.

Step 3 Enter the following commands on the Cisco ISE CLI:

```
configure terminal
hostname hostname
```

The hostname is the new hostname that you are going to configure. The Cisco ISE services are restarted.

Step 4 Enter the following commands:

```
interface gigabit 0
ip address ip_address netmask
```

The ip_address is the address that corresponds to the hostname that you entered in step 3 and netmask is the subnet mask of the ip_address. The system will prompt you to restart the Cisco ISE services. See the *Cisco Identity Services Engine CLI Reference Guide*, for the ip address and hostname commands.

Step 5 Enter Y to restart Cisco ISE services.

Connect a Cloned Cisco Virtual Machine to the Network

After you power on and change the ip address and hostname, you must connect the Cisco ISE node to the network.

Step 1 Right-click the newly cloned Cisco ISE virtual machine (VM) and click **Edit Settings**.

Step 2 Click **Network adapter** in the Virtual Machine Properties dialog box.

Step 3 In the Device Status area, check the **Connected** and **Connect at power on** check boxes.

Step 4 Click **OK**.

Migrate Cisco ISE VM from Evaluation to Production

After evaluating the Cisco ISE release, you can migrate the from an evaluation system to a fully licensed production system.

Before you begin

- When you move the VMware server to a production environment that supports a larger number of users, be sure to reconfigure the Cisco ISE installation to the recommended minimum disk size or higher (up to the allowed maximum of 2.4 TB).
- Please not that you cannot migrate data to a production VM from a VM created with less than 300 GB of disk space. You can only migrate data from VMs created with 300 GB or more disk space to a production environment.

Step 1 Back up the configuration of the evaluation version.

Step 2 Ensure that your production VM has the required amount of disk space.

Step 3 Install a production deployment license.

Step 4 Restore the configuration to the production system.

On-Demand Virtual Machine Performance Check Using the show tech-support Command

You can run the **show tech-support** command from the CLI to check the VM performance at any point of time. The output of this command will be similar to the following:

```
ise-vm.22*admin# show tech | begin "Disk I/O perf"
Running disk IO performance
*********************************
Average Dsk bandwidth writing to disk device: 49 MB/second
Average I/O bandwidth reading from disk device: 192 MB/second
WARNING: VM I/O ASSESSMENT TESTS FAILED!
REASONS: The bandwidth writing to disk must be at least 50 MB/second.
WARNING: and bandwidth reading from disk must be at least 200 MB/second.
WARNING: This VM should only be used for evaluation use only, NOT
WARNING: performance tests to be enforced.
```



```
Disk I/O bandwidth (Dsk) performance test, writing 5GB on to /opt:
3145728000 bytes (3.1 GB) copied, 7.41502 s, 424 MB/s
Disk I/O bandwidth (Fs) performance read test, reading 2GB on /opt:
2147483648 bytes (2.1 GB) copied, 7.41502 s, 290 MB/s
```

Virtual Machine Resource Check from the Cisco ISE Boot Menu

You can check for virtual machine resources independent of Cisco ISE installation from the boot menu.

The CLI transcript appears as follows:

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

Use the arrow keys to select **System Utilities (Serial Console)** or **System Utilities (Keyboard/Monitor)** and press **Enter**. The following screen appears:

```
Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reboot

Enter option [1 - 3] q to Quit
```

Enter **2** to check for VM resources. The output will be similar to the following:

```
*****
***** Virtual Machine Resource Check Result
***** Hard disk(s) total size must be: 600 GigaByte
***** Physical RAM size must be: 16384 MegaByte
***** Number of network interfaces must be: 6
***** Number of CPU cores: 16
***** CPU Speed: 1900.00
***** Verifying CPU requirements...
***** Verifying RAM requirements...
***** Verifying disk partition table.
```

Linux KVM

KVM Virtualization Check

KVM virtualization requires virtualization support from the host processor; Intel VT-x for Intel processors and AMD-V for AMD processors. Open a terminal window on the host and enter the **cat /proc/cpuinfo** command. You must see either the vmx or the svm flag.

- For Intel VT-x:

```
# cat /proc/cpuinfo
Please see the de pae tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc
```



```
aperfmperf eagerfpu pni pclmulqdq dtes64 monitor
ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic popcnt
tsc_deadline_timer aes xsave avx lahf_lm ida arat epb xsaveopt
pln pts dtherm tpr_shadow vnmi flexpriority ept vpid
```

- For AMD-V:

```
# cat /proc/cpuinfo
Please see the de pae tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36 clflush mmx fxsr
dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc
```

Install Cisco ISE on KVM

This procedure explains how to create a KVM on RHEL and install Cisco ISE on it using the Virtual Machine Manager (virt-manager).

If you choose to install Cisco ISE through the CLI, enter a command similar to the following one:

```
#virt-install --name=ise-inst --arch=x86_64 --cpu=host --vcpus=2 --ram=4096

--os-type=linux --os-variant=rhel6 --hvm --virt-type=kvm
--cdrom=/root/vish/Downloads/ise-3.0.0.xx.SPA.x86_64.iso
--disk=/root/vish/ise-inst.qcow,size=200,format=qcow2
--network type=direct,model=virtio,source=eth0,source_mode=bridge
```

Where *ise-3.0.0.xx.SPA.x86_64.iso* is the name of the Cisco ISE ISO image.

Before you begin

Download the Cisco ISE ISO image to your local system.

Step 1 From the virt-manager, click **New**.

The Create a new virtual machine window appears.

Step 2 Click **Local install media (ISO media or CDROM)**, and then click **Forward**.

Step 3 Click the **Use ISO image** radio button, click **Browse**, and select the ISO image from your local system.

a) Uncheck the **Automatically detect operating system based on install media** check box, choose Linux as the OS type, choose supported Red Hat Enterprise Linux version, and click **Forward**.

Supported KVM on QEMU 1.5.3-160

Step 4 Choose the RAM and CPU settings and click **Forward**.

Step 5 Check the **Enable storage for this virtual machine** check box and choose the storage settings.

a) Click the **Select managed or other existing storage** radio button.

b) Click **Browse**.

c) From the Storage Pools navigation pane on the left, click disk **FileSystem Directory**.

d) Click **New Volume**.

A Create storage volume window appears.

e) Enter a name for the storage volume.

f) Choose **raw** from the **Format** drop-down list.

g) Enter the Maximum Capacity.
h) Click **Finish**.
i) Choose the volume that you created and click **Choose Volume**.
j) Click **Forward**.

The Ready to begin the installation screen appears.

Step 6 Check the **Customize configuration before install** check box.

Step 7 Under Advanced options, choose the macvtap as the source for the interface, choose Bridge in the Source mode drop-down list, and click **Finish**.

a) (Optional) Click **Add Hardware** to add additional NICs.

Choose macvtap as the Network source and virtio as the Device model.

b) Click **Finish**.

Step 8 In the Virtual Machine screen, choose the disk device and under Advanced and Performance Options, choose the following options, and click **Apply**.

Field	Value
Disk bus	VirtIO
Cache mode	none
IO mode	native

Step 9 Click **Begin Installation** to install Cisco ISE on KVM.
The Cisco ISE installation boot menu appears.

Step 10 At the system prompt, enter **1** to choose a monitor and keyboard port, or **2** to choose a console port, and press **Enter**.

The installer starts the installation of the Cisco ISE software on the VM. When the installation process finishes, the console displays:

```
Type 'setup' to configure your appliance
localhost:
```

Step 11 At the system prompt, type **setup** and press **Enter**.
The Setup Wizard appears and guides you through the initial configuration.

Microsoft Hyper-V

Create a Cisco ISE Virtual Machine on Hyper-V

This section describes how to create a new virtual machine, map the ISO image from the local disk to the virtual CD/DVD drive, edit the CPU settings, and install Cisco ISE on Hyper-V.

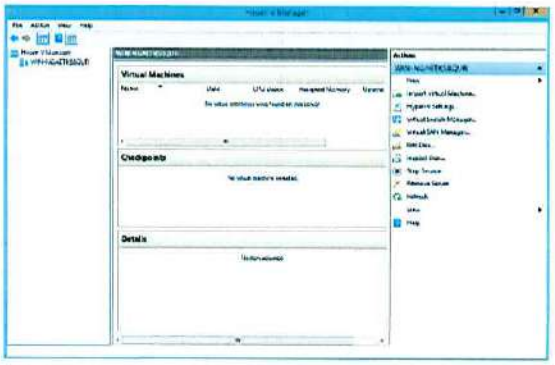
Note Cisco ISE does not support the use of Multipath I/O (MPIO). Hence, the installation will fail if you are using MPIO for the VM.

Before you begin

Download the Cisco ISE ISO image from Cisco.com to your local system.

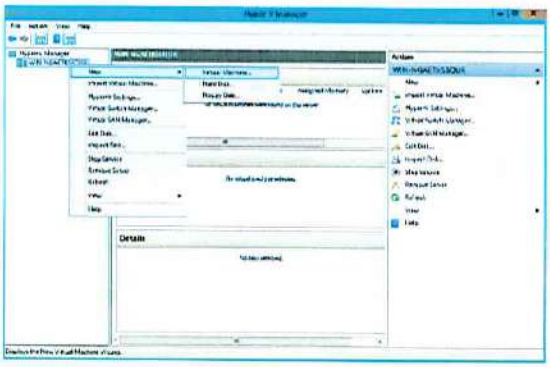
Step 1 Launch Hyper-V Manager on a supported Windows server.

Figure 10: Hyper-V Manager Console



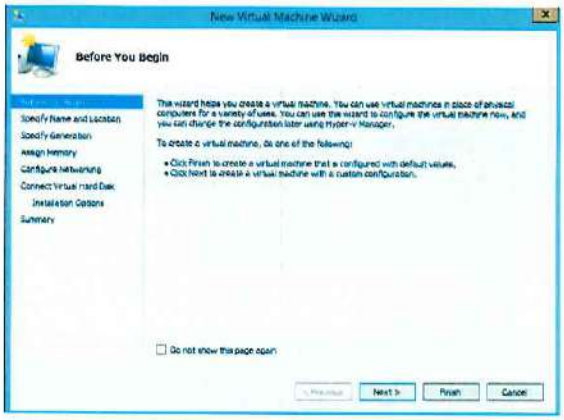
Step 2 Right-click the VM host and click **New > Virtual Machine**.

Figure 11: Create New Virtual Machine



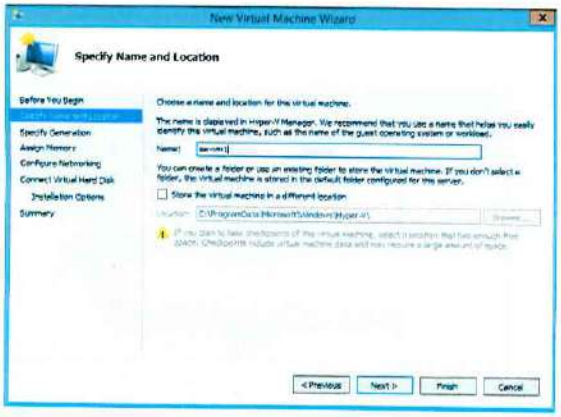
Step 3 Click **Next** to customize the VM configuration.

Figure 12: New Virtual Machine Wizard



Step 4 Enter a name for the VM and (optionally) choose a different path to store the VM, and click **Next**.

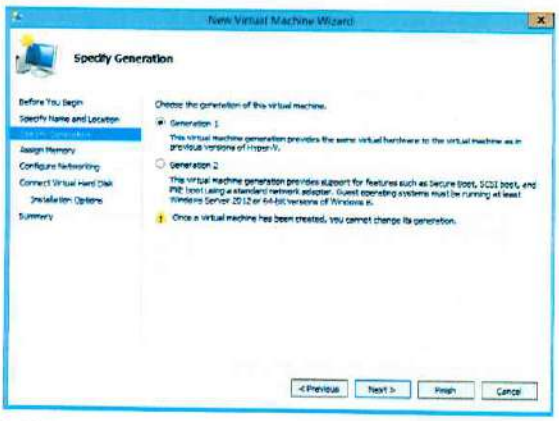
Figure 13: Specify Name and Location



Step 5 Click the **Generation 1** radio button and click **Next**.

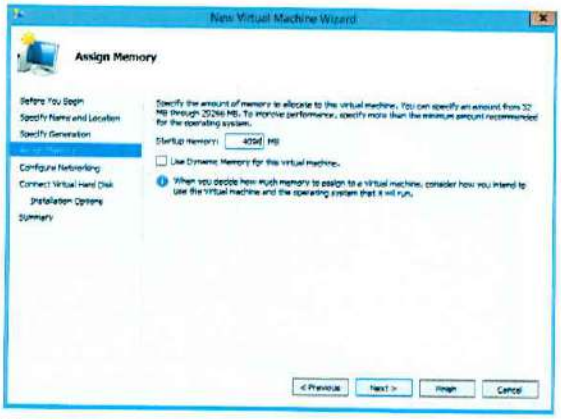
If you choose to create a Generation 2 ISE VM, ensure that you disable the **Secure Boot** option in the VM settings.

Figure 14: Specify Generation



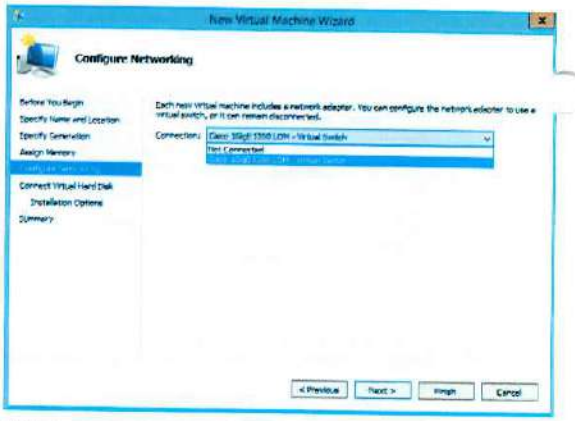
Step 6 Specify the amount of memory to allocate to this VM, for example, 16000 MB, and click **Next**.

Figure 15: Assign Memory



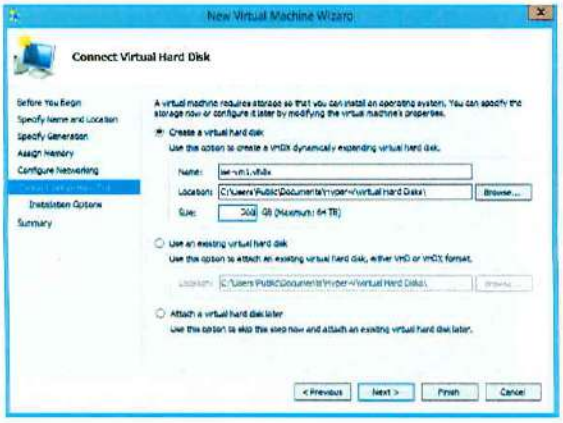
Step 7 Select the network adapter and click **Next**.

Figure 16: Configure Networking



Step 8 Click the **Create a virtual hard disk** radio button and click **Next**.

Figure 17: Connect Virtual Hard Disk

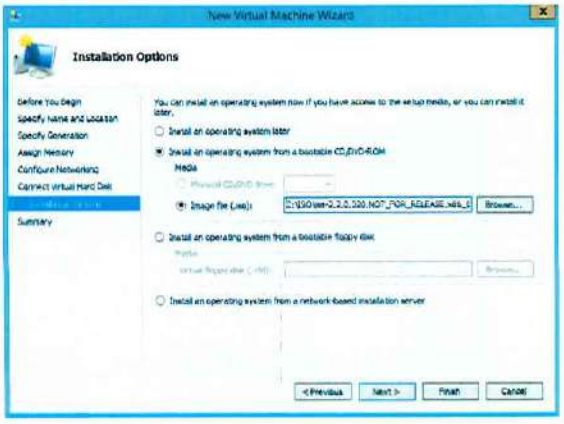


Step 9 Click the **Install an operating system from a bootable CD/DVD-ROM** radio button.

a) From the Media area, click the **Image file (.iso)** radio button.

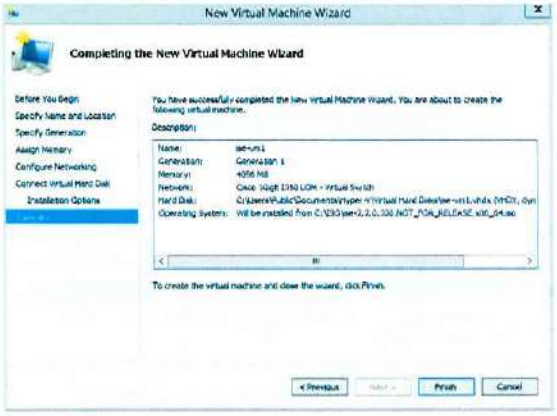
b) Click **Browse** to select the ISE ISO image from the local system and click Next.

Figure 18: Installation Options



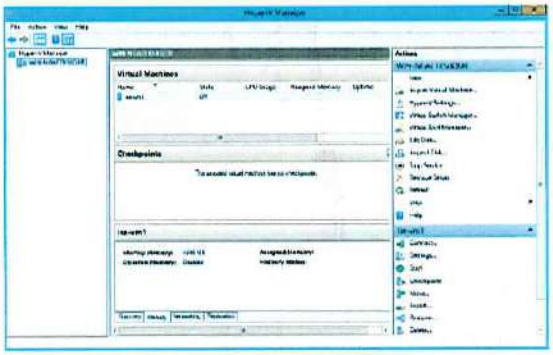
Step 10 Click **Finish**.

Figure 19: Complete the New Virtual Machine Wizard



The Cisco ISE VM is created on Hyper-V.

Figure 20: New Virtual Machine created

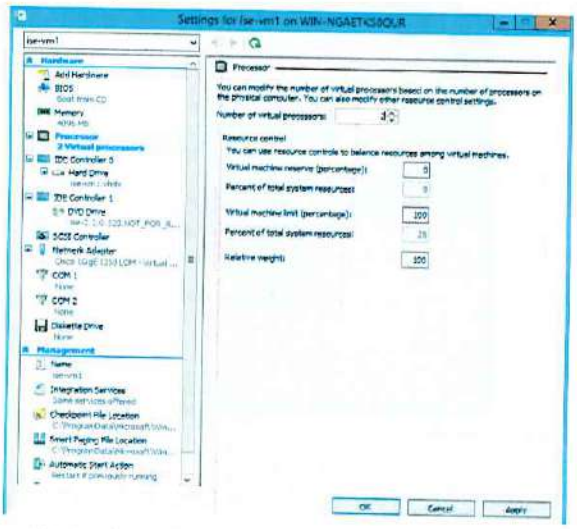


Step 11 Select the VM and edit the VM settings.

a) Select **Processor**. Enter the number of virtual processors, for example, 6, and click **OK**.

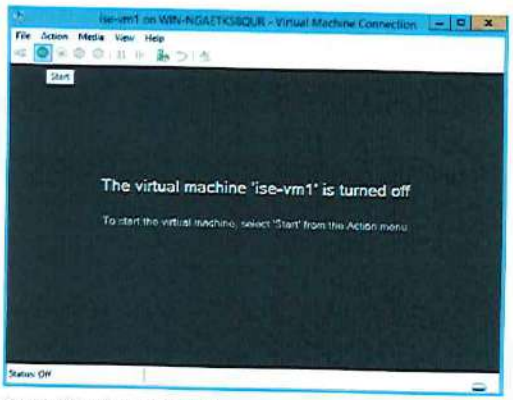
45

Figure 21: Edit VM Settings



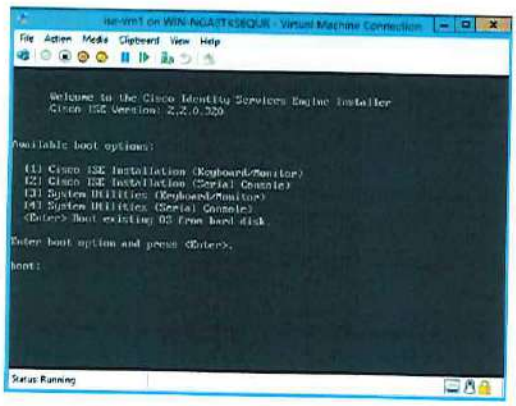
Step 12 Select the VM and click **Connect** to launch the VM console. Click the start button to turn on the Cisco ISE VM.

Figure 22: Start the Cisco ISE VM



The Cisco ISE installation menu appears.

Figure 23: Cisco ISE installation menu



Step 13 Enter 1 to install Cisco ISE using a keyboard and monitor.

Zero Touch Provisioning

Zero Touch Provisioning (ZTP) refers to the uninterrupted provisioning mechanism. It automates Cisco ISE installation, patching, hot patching, and infrastructure service enablement without manual intervention.

ZTP is enabled in Cisco ISE 3.1. We can leverage this feature using two options:

- **Mapping .img file**: This is supported in Virtual Machine (VM) automatic installations, appliances, and OVA installations. It contains mandatory parameters such as hostname, IP Address, IP Netmask, IP Default Gateway, DNS Domain, primary name server, NTP server, system timezone, SSH, username, and password. Optional parameters such as IPV6, patch, hot patch, services, and repository details can also be configured. For more information, see ZTP Configuration Image File.
- **VM User Data**: This is supported in OVA installation and VM automatic installation. It is supported when both .img and user data are configured. It contains mandatory parameters such as hostname, IP Address, IP Netmask, IP Default Gateway, DNS Domain, primary name server, NTP server, system timezone, SSH, username, and password. Optional parameters such as IPV6, patch, hot patch, services, and repository details can also be configured. For more information see VM User Data .

Note TFTP, HTTP, HTTPS and NFS repositories are supported for installation of hot patches and patches on Cisco ISE as part of the ZTP flow. The repositories created during the ZTP flow will not be visible or usable from the Cisco ISE UI.

Before you begin

- For ZTP to trigger installation automatically, the serial console should be enabled for both the VM and the appliance.
- A ZTP configuration image file is required.

The following sections provide information about ZTP.

Automatic Installation in Virtual Machine

The following subsections provide information about automatic installation in the VM.

Automatic Installation in Virtual Machine Using the ZTP Configuration Image File

Step 1 Log in to the VMware client.

Note For an existing VM setup, perform Step 2 to Step 6. For a new VM setup, go directly to Step 7.

Step 2 For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**, and in the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note You must change the firmware from BIOS to EFI in the boot mode of VM settings to boot GPT partitions with 2 TB or more capacity.

Step 5 Click **OK**.

Step 6 Ensure that the Coordinated Universal Time (UTC) and the correct boot order are set in BIOS.

a) If the VM is turned on, turn the system off.
b) Turn on the VM.

The system enters the BIOS setup mode.

c) In the Main **BIOS** menu, using the **arrow keys**, navigate to the **Date and Time** field and press **Enter**.
d) Enter the UTC/Greenwich Mean Time (GMT) time zone.

This time zone setting ensures that the reports, logs, and posture-agent log files from the various node deployment are always synchronized with regard to the time stamps.

e) Using the arrow keys, navigate to the Boot menu and press **Enter**.
f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.
g) Using the arrow keys, navigate to the Exit menu and choose **Exit Saving Changes**.
h) Press Yes to save the changes and exit.

Step 7 Insert the Cisco ISE software DVD into the VMware ESXi host primary CD/DVD drive.

Step 8 Insert the ZTP configuration image file into a secondary CD/DVD drive.

Step 9 Turn on the VM.

When the DVD boots, the console displays the following message:

```
Automatic Installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <Return>.
boot:
```

Note Pressing Enter without entering a boot option does not trigger installation using the hard disk option; it triggers ZTP from Cisco ISE 3.1 onwards.

Step 10 After 150 seconds, the bootup process automatically starts if the prerequisites are met.

Note
- Installation logs can be monitored only through the serial console because ZTP works through the serial console. It can be monitored from the VM console after the setup prompt is displayed.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD/DVD

To leverage ZTP from setup prompt (which is installed through keyboard option till setup) perform the following steps:

1. Install Cisco ISE manually till setup (through boot option 1 or 2) and create the ZTP configuration image file using the above steps.
2. Power off the VM and map the ZTP configuration image file that is created to the CD/DVD drive.
3. Power on the VM. The setup details are picked up from the ZTP configuration file that is mapped to the CD/DVD drive.

Troubleshooting

Issue: If the Automatic installation in the VM is triggered without mapping img file, after 150 seconds, automatic installation is triggered and installation fails saying .img file is not mapped to the CD/DVD drive.

```
***** The ZTP configuration image is missing or empty. Automatic installation flow
  exited.
***** Power off and attach the proper ZTP configuration image or choose manual boot to
  continue.
```

Solution: This error message is seen only through the serial console and not on the VM console. If it happens on an existing VM where Cisco ISE is already installed, hard disk will not be formatted at this state and the existing VM can be recovered by performing these steps: :

1. Turning off the VM.
2. Turning on the VM.

3. Pressing option 5 to boot from hard disk within 150 seconds to load the existing VM.

Issue: If the setup details are invalid in the config file, ZTP installation is stopped and the following message is displayed on the VM Console:

```
Cisco ISE Installation Failed.

Retort Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
```

Solution: This can be resolved by performing the following steps:

1. Create a new configuration .img file with valid details.
2. Power off the VM.
3. Map the new valid image to the CD/DVD drive.
4. Power on the VM. Installation will begin from setup.

Automatic Installation in Virtual Machine Using VM User Data

Step 1 Log in to the VMware client.

Note For an existing VM setup, perform Step 2 to Step 6. For a new VM setup, go directly to Step 7.

Step 2 For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**, and in the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note You must change the firmware from **BIOS** to **EFI** in the boot mode of VM settings to boot GPT partitions with 2 TB or more capacity.

Step 5 Click **OK**.

Step 6 Ensure that the Coordinated Universal Time (UTC) and the correct boot order are set in BIOS:

a) If the VM is turned on, turn the system off.

b) Turn on the VM.

The system enters the BIOS setup mode.

c) In the Main BIOS menu, using the arrow keys, navigate to the **Date** and **Time** field and press **Enter**.

d) Enter the UTC/Greenwich Mean Time (GMT) time zone.

This time zone setting ensures that the reports, logs, and posture-agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.

e) Using the arrow keys, navigate to the **Boot** menu and press **Enter**.

f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.

g) Using the arrow keys, navigate to the **Exit** menu and choose **Exit Saving Changes**.

h) Press **Yes** to save the changes and exit.

Step 7 Insert the Cisco ISE software DVD into the VMware ESXi host primary CD/DVD drive.

Step 8 Insert the ZTP configuration image file into a secondary CD/DVD drive.

Step 9 Configure the VM User Data options.

Note If both .img file and VM user data options are configured in the VM, the user data options will be considered.

Step 10 Turn on the VM.

When the DVD boots, the console displays the following message:

```
Automatic Installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <Return>.
boot:
```

Note Pressing **Enter** without entering a boot option will not trigger the installation using the hard disk option; it will trigger ZTP from Cisco ISE 3.1 onwards.

Step 11 After 150 seconds, the bootup process automatically starts if the prerequisites are met.

Note
- Installation logs can be monitored only through the serial console because ZTP works through the serial console. It can be monitored from the VM console after the setup prompt is displayed.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD/DVD.

To leverage VM User Data option from setup prompt (which is installed through keyboard option till setup), perform the following steps:

1. Install Cisco ISE manually till setup (through boot option 1 or 2).
2. Power off the VM.
3. Configure user-data option mentioned above.
4. Power on the VM . The setup details will be picked from the VM options.

Troubleshooting

Issue: If invalid setup details are entered in the user data option, ZTP installation is stopped and the following message is displayed on the VM Console:

```
Cisco ISE Installation Failed.
```



```
Retort Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
```

Solution: This can be resolved by performing the following steps:

1. Power off the VM.
2. Update user data details with valid data.
3. Power on the VM. Installation will begin from setup.

Automatic Installation in Appliance

The following subsections provide information about automatic installation in the appliance.

Automatic Installation in Appliance Using the ZTP Configuration Image File

Step 1 Log in to the SNS Appliance.

Step 2 Power off the host.

Step 3 Choose **Compute** > **Remote Management** > **Virtual media**.

Step 4 Map the Cisco ISE software ISO and the ZTP configuration image file to the primary CD/DVD drive and secondary CD/DVD drive.

Step 5 Power on the host.

When the appliance boots, the console displays the following message:

```
Please select boot device:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Cisco ISE Installation through ZTP Configuration (Serial Console)
```

Step 6 After 150 seconds, the bootup process automatically starts if the prerequisites are met.

Note
- ZTP works on the SNS Appliance through Vmedia only.
- You must map the .img file in Vmedia before mapping the ISO file.

  Installation logs can be monitored through the serial console as ZTP works only through the serial console. It can be monitored from the KVM console after the setup prompt is displayed.
- Automatic installation in appliance is supported only with the .img file format.

To leverage ZTP from setup prompt (which is installed through keyboard option till setup) perform the following steps:

1. Install Cisco ISE manually till setup (through boot option 1 or 2) and create the ZTP configuration image file using the above steps.
2. Power off the host and map the ZTP configuration image file that is created, to the CD/DVD drive.

3. Power on the host. The setup details should be will from the ZTP configuration file that is mapped to the CD/DVD drive.

Troubleshooting

Issue: If the Automatic installation in the appliance is triggered without mapping img file, after 150 seconds, automatic installation is triggered and installation fails saying .img file is not mapped to the CD/DVD drive.

```
***** The ZTP configuration image is missing or improper. Automatic installation flow
 halted.
***** Power off and attach the proper ZTP configuration image or choose manual boot to
 proceed.
```

Solution: This can be resolved by performing the following steps:

1. Turning off the VM.
2. Turning on the VM.
3. Pressing option 5 to boot from hard disk within 150 seconds to load the existing VM.

Issue: If the setup details are invalid in the config file, ZTP installation is stopped and the following message is displayed on the KVM Console:

```
--------------------------------------------------------------------------------

Cisco ISE Installation Failed

--------------------------------------------------------------------------------

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.

--------------------------------------------------------------------------------
```

Solution: This can be resolved by performing the following steps:

1. Create a new configuration .img file with valid details.
2. Power off the VM.
3. Map the new valid image to the CD/DVD drive.
4. Power on the VM. Installation will begin from setup.

Trigger Automatic Installation using UCS XML APIs

To trigger automatic installation:

1. Get the login session cookie for authentication.
2. Map the Cisco ISE ISO.
3. Map the Configuration Image file.
4. Set the CDROM at first place in the boot order.
5. Enable the Serial Over LAN (SOL).

6. Power restart.
7. Logout.

API URL and request header are same for all methods:

API URL :

```
https://<ucs_server_ip>/nuova
```

Header :

```
Header["Accept"] = "application/xml"
header["Content-Type"] = "application/xml"
```

Step 1: Get the login session cookie for authentication

The aaaLogin method is the login process and is required to begin a session. This action establishes the HTTP (or HTTPS) session between the client and Cisco IMC. This session cookie will be used in upcoming requests to maintain login session.

Request:

```
<aaaLogin inName='admin' inPassword='password'/>
```

Response:

```
<aaaLogin cookie="" response="yes" outCookie="<real_cookie>" outRefreshPeriod="600"
outPriv="admin" outSessionId="17" outVersion="3.0(0.149)"> </aaaLogin>
```

Step 2: Map the Cisco ISE ISO

Configures an ISE ISO file as a vMedia Volume.

Request:

```
<configConfMo cookie='<real_cookie>' dn='sys/svc-ext/vmedia-svc/vmmap-ISE_ISO'
inHierarchical='false'>
<inConfig>
<commVMediaMap dn='sys/svc-ext/vmedia-svc/vmmap-ISE_ISO'
 map='nfs'
 remoteFile='ise_iso_file>'
 remoteShare='nfs_server_path>'
 status='created' volumeName='ISE_ISO' />
</inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/svc-ext/vmedia-svc/vmmap-ISE_ISO"
 cookie="<real_cookie>" response="yes">
<outConfig>
 <commVMediaMap volumeName="ISE_ISO" map="nfs"
  remoteShare='<nfs_server_path>'
  remoteFile="ise_iso_file>"
  mappingStatus="In Progress"
  dn="sys/svc-ext/vmedia-svc/vmmap-ISE_ISO" status="created"/>
  </outConfig>
</configConfMo>
```

Step 3: Map the Configuration Image file

Configures a configuration image as a vMedia Volume.

Request:

```
<configConfMo cookie='<real_cookie>'
dn='sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG' inHierarchical='false'>
<inConfig>
<commVMediaMap dn='sys/svc-ext/vmedia-svc/vmmap=CONFIG-IMG'
  map='nfs'
  remoteFile='config_img_file>'
  remoteShare='<nfs_server_path>'
  status='created' volumeName='CONFIG-IMG' />
</inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/svc-ext/vmedia-svc/vmmap=CONFIG-IMG"
 cookie="<real_cookie>" response="yes">
<outConfig>
 <commVMediaMap volumeName="CONFIG-IMG" map="nfs"
  remoteShare='<nfs_server_path>'
  remoteFile="config_img_file>"
  mappingStatus="In Progress"
  dn="sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG" status="created"/>
  </outConfig>
</configConfMo>
```

Step 4: Set the CDROM at first place in the boot order

Maps the Cisco ISE ISO file that will be picked for installation while power restart.

Request:

```
<configConfMo cookie="<real_cookie>"
inHierarchical="true" dn="sys/rack-unit-1/boot-policy">
  <inConfig>
    <lsBootDef dn="sys/rack-unit-1/boot-policy"  rebootOnUpdate="yes">
      <lsbootVirtualMedia access="read-only" order="1"
dn="sys/rack-unit-1/boot-policy/vm-read-only"/>
    </lsBootDef>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/boot-policy" cookie="<real_cookie>" response="yes">
<outConfig>
  <lsBootDef dn="sys/rack-unit-1/boot-policy" name="boot-policy" purpose="operational"
rebootOnUpdate="no" status="modified" >
  </lsBootDef>
</outConfig>
</configConfMo>
```

Step 5: Enable the SOL

Enables the SOL to view installation logs via telnet.

Request:

```
<configConfMo cookie='<real_cookie>'
dn='sys/rack-unit-1/sol-if'>
<inConfig>
  <solIf dn='sys/rack-unit-1/sol-if' adminState='enable'/>
 </inConfig>
</configConfMo>
```


Response:

```
<configConfMo dn="sys/rack-unit-1/sol-if" cookie="<real_cookie>" response="yes">
<outConfig>
<solIf dn="sys/rack-unit-1/sol-if" adminState="enable" name="SolInterface" speed="115200"
comport="com0" xmlPort="2400" status="modified" /></solIf></outConfig>
</configConfMo>
```

Step 6: Power restart

Triggers Cisco ISE Installation in automatic mode.

Request:

```
<configConfMo cookie='<real_cookie>' dn='sys/rack-unit-1'>
<inConfig><computeRackUnit
dn='sys/rack-unit-1'
adminPower='cycle-immediate'/>
</inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1" cookie="<real_cookie>" response="yes">
<outConfig>
   <computeRackUnit dn="sys/rack-unit-1" adminPower="policy" availableMemory="262144"
model="R2XL-2U3-K9" memorySpeed="2400" name="UCS-C260-M4" numOfAdaptors="0" numOfCores="16"
numOfCoresEnabled="16" numOfCpus="1" numOfEthHostIfs="0" numOfFcHostIfs="0" numOfThreads="32"
operPower="on" originalUuid="19358360-b7f6-4031-8a96-7984f1d35449" presence="equipped"
serverId="1" serial="SAL2224G89K" totalMemory="262144" usrLbl=""
uuid="19358360-b7f6-4031-8a96-7984f1d35449" vendor="Cisco Systems Inc"
cimcResetReason="graceful-reboot
" assetTag="Unknown" adaptorSecureUpdate="Enabled" resetComponents="components"
strictUuidCompatibility="NA" vicPresence="NA" biosScrubPolicy="NA" smartUsbAccess="Disabled"
smartUsbStatus="Disabled" discPostDate="completed" status="modified" >
   </computeRackUnit>
</outConfig>
</configConfMo>
```

Step 7: Logout

Exits the session.

Request:

```
<aaaLogout
     cookie="<real_cookie>"
     inCookie="<real_cookie>"
</aaaLogout>
```

Response:

```
<aaaLogout cookie="" response="yes" outStatus="success"> </aaaLogout>
```

Note For more information on UCS API methods, see:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/api/2-0x/Cisco_IMC_api_for_3rd_party_servers/2-0x/c...html

OVA Automatic Installation

The following sections provide information about automatic installation using the OVA.

OVA Automatic Installation Using the ZTP Config Image File

Step 1 Log in to the VMware client.

Note For an existing VM setup, perform Step 2 to Step 6. For a new VM setup, go directly to Step 7.

Step 2 For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**, and in the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note You must change the firmware from BIOS to EFI in the boot mode of VM settings to boot GPT partitions with 2 TB or more capacity.

Step 5 Click **OK**.

Step 6 Ensure that the Coordinated Universal Time (UTC) and the correct boot order are set in BIOS:

a) If the VM is turned on, turn the system off.

b) Turn on the VM.

The system enters the BIOS setup mode.

c) In the Main **BIOS** menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.

d) Enter the UTC/Greenwich Mean Time (GMT) time zone.

This time zone setting ensures that the reports, logs, and posture-agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.

e) Using the arrow keys, navigate to the Boot menu and press **Enter**.

f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.

g) Using the arrow keys, navigate to the Exit menu and choose **Exit Saving Changes**.

h) Press **Yes** to save the changes and exit.

Step 7 Import the Cisco ISE OVA file into the VMware ESXi.

Step 8 Insert the ZTP config image file into the primary CD/DVD drive.

Step 9 Turn on the virtual machine.

When the DVD boots, the console displays the following message:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk.
Enter boot option and press <Enter>.
boot:
```


Note For an existing VM setup, perform Step 2 to Step 6. For a new VM setup, go directly to Step 7.

Step 2 For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.

Step 3 Click the **Options** tab.

Click **Boot Options**, and in the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note You must change the firmware from BIOS to EFI in the boot mode of VM settings to boot GPT partitions with 2 TB or more capacity.

Step 5 Click **OK**.

Step 6 Ensure that the Coordinated Universal Time (UTC) and the correct boot order are set in BIOS:

a) If the VM is turned on, turn the system off.

b) Turn on the VM.

The system enters the BIOS setup mode.

c) In the Main **BIOS** menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.

d) Enter the UTC/Greenwich Mean Time (GMT) time zone.

This time zone setting ensures that the reports, logs, and posture-agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.

e) Using the arrow keys, navigate to the Boot menu and press Enter.

f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.

g) Using the arrow keys, navigate to the Exit menu and choose **Exit Saving Changes**.

h) Press **Yes** to save the changes and exit.

Step 7 Import the Cisco ISE OVA file into the VMware ESXi.

Step 8 Configure the VM User Data options.

Note If both config file and VM user data options are configured in the VM, the user data options will be considered.

Step 9 Turn on the VM.

When the DVD boots, the console displays the following message:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk.
Enter boot option and press <Enter>.
boot:
```

Note Pressing Enter without entering a boot option will not trigger installation using the hard disk option; it will trigger ZTP from Cisco ISE 3.1 onwards.

Step 10 After 150 seconds, the bootup process automatically starts if the prerequisites are met.

Note
- Installation logs can be monitored only through the serial console because ZTP works through the serial console. It can be monitored from the VM console after the setup prompt is displayed.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD/DVD.

To leverage ZTP from setup prompt (which is installed through keyboard option till setup) perform the following steps:

1. Install Cisco ISE manually till setup (through boot option 1 or 2) and create the ZTP configuration image file using the above steps.
2. Power off the VM.
3. Map the ZTP configuration image file that is created to the CD/DVD drive.
4. Power on the VM. The setup details will be picked up from the ZTP configuration file that is mapped to the CD/DVD drive.

Troubleshooting

Issue: If the setup details are invalid in the config file, ZTP installation is stopped and the following message is displayed on the VM Console:

```
Cisco ISE Installation Failed

Network Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.
```

Solution: This can be resolved by performing the following steps:

1. Create a new configuration .img file with valid details.
2. Power off the VM.
3. Map the new valid image to the CD/DVD drive.
4. Power on the VM. Installation will begin from setup

OVA Automatic Installation Using the VM User Data

Step 1 Log in to the VMware client.

Note
- Installation logs can be monitored only through the serial console because ZTP works through the serial console. It can be monitored from the VM console after the setup prompt is displayed.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD/DVD.

To leverage VM User Data option from setup prompt (which is installed through keyboard option till setup), perform the following steps:

1. Install Cisco ISE manually till setup (through boot option 1 or 2).
2. Power off the VM and configure user-data option mentioned above.
3. Power on the VM. The setup details should be picked from VM options.

Troubleshooting

Issue: If invalid setup details are entered in the user data option, ZTP installation is stopped and the following message is displayed on the VM Console:

```
Cisco ISE Installation Failed

Network Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE

with proper ZTP configuration.
```

Solution: This can be resolved by performing the following steps:

1. Power off the VM.
2. Update user data details with valid data.
3. Power on the VM. Installation will begin from setup.

ZTP Configuration Image File

Create the ZTP configuration image file using the */create_ztp_image.sh ise-ztp.conf iso-ztp.img* command. The script can be executed on RHEL, CentOS, or Ubuntu.

Create the script *create_ztp_image.sh*:

```
#!/bin/bash
#########################################################################
# This script is used to generate ISE ZTP Image with ZTP
# configuration file.
#
# Need to pass ztp configuration file as input.
#
# Copyright (c) 2021 by Cisco Systems, Inc.
# All rights reserved.
```

```
# Note:
# To mount the image use below command
# mount ise_ztp_config.img /ztp
# To mount the image from cdrom
# mount -o ro /dev/sr1 /ztp
#################################################################
if [ -e "$1" ]then
echo "Usage:ZTP <ise-ztp.conf> [out-ztp.img]"
exit 1
elif [ ! -f $1 ]then
echo "File $1 not exist"
exit 1
else
conf_file=$1
fi
if [ -e "$2" ] ;then
Image=ise_config.img
else
Image=$2
fi
mountpath=/tmp/ise_ztp
ztplabel=ISE-ZTP
rm -fr $mountpath
mkdir -p $mountpath
dd if=/dev/zero of=$Image bs=1k count=1440 > /dev/null 2>&1
if [ `echo $?` -ne 0 ];then
echo "Image creation failed\n"
exit 1
fi
mkfs.ext4 $Image -L $ztplabel -F > /dev/null 2>&1
mount -o rw,loop $Image $mountpath
cp $conf_file $mountpath/ise-ztp.conf
sync
umount $mountpath
sleep 1
# Check for automount and umount
automountpath=$(mount | grep $ztplabel | awk '{print $3}')
if [ -e "$automountpath" ];then
umount $automountpath
fi
echo "Image created $Image"
```

Create the sample configuration file *ise-ztp.conf*

```
hostname=ISEHost-40
ipv4_addr=10.126.68.90
ipv4_mask=255.255.255.0
ipv4_default_gw=10.126.68.1
#IPv6 optional
ipv6_addr=2001:420:54ff:44:5056:91/119
ipv6_default_gw=2001:420:54ff:4::1455:1
domain=cisco.com
primary_nameserver=72.163.128.140
# secondary and tertiary are optional
secondary_nameserver=72.163.128.141
tertiary_nameserver=72.163.128.142
primary_ntpserver=ntp.esl.cisco.com
# secondary and tertiary are optional
secondary_ntpserver=ntp1.esl.cisco.com
tertiary_ntpserver=ntp2.esl.cisco.com
timezone=Asia/Kolkata
ssh=true
username=admin
password=Test123
```



```
##Repository Configuration Are optional
repository_name=nfs_repo
repository_protocol=nfs
repository_server_name=10.77.122.11
repository_path=/volume1/vms/infra/patchhotpath
#Patch Information = optional
patch=ise-patchbundle-3.1.0.367-Patch1-21050403.SPA.x86_64.tar.gz
#HotPatches Information = optional
hotpatchversion=apply=CSCvw81602_2.x_MemoryDiagnostics_1-DA.tar.gz,ad=apply=
CSCvw87402_2.x_MemoryDiagnostics_4-DA.tar.gz
#services = optional
ers=true
openapi=true
pxgrid=true
pxGrid_Cloud=true
```

VM User Data

VM user data is supported from ESX 6.5 and later for Cisco ISE installation.

The content of **ise-ztp.conf** should be pasted in the base64encode tool. Use this tool to get the encoded string: https://www.base64encode.org/

Encoded base64 String will be entered in the VM with VM user data in **VM Options > Advanced > Configuration Parameters > Edit Configuration > guestinfo.ise.ztp = [Value] Base Encoded ZTP Configuration**.

CHAPTER 6

Installation Verification and Post-Installation Tasks

Log In to the Cisco ISE Web-Based Interface

When you log in to the Cisco ISE web-based interface for the first time, you will be using the preinstalled Evaluation license.

Note We recommend that you use the Cisco ISE user interface to periodically reset your administrator login password.

Caution For security reasons, we recommend that you log out when you complete your administrative session. If you do not log out, the Cisco ISE web-based web interface logs you out after 30 minutes of inactivity, and does not save any unsubmitted configuration data.

Before you begin

The Cisco ISE Admin portal supports the following browsers for the Admin Portal:

- Mozilla Firefox 72 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 80 and earlier versions
- Microsoft Internet Explorer 11.x

Step 1 After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

Step 2 In the Address field, enter the IP address (or hostname) of the Cisco ISE appliance by using the following format and press **Enter**.

```
https://<IP address or host name>/admin/
```

Step 3 Enter a username and password that you defined during setup.

Step 4 Click **Login**.

Differences Between CLI Admin and Web-Based Admin Users Tasks

The username and password that you configure when using the Cisco ISE setup program are intended to be used for administrative access to the Cisco ISE CLI and the Cisco ISE web interface. The administrator that has access to the Cisco ISE CLI is called the CLI-admin user. By default, the username for the CLI-admin user is admin and the password is user-defined during the setup process. There is no default password.

You can initially access the Cisco ISE web interface by using the CLI-admin user's username and password that you defined during the setup process. There is no default username and password for a web-based admin.

The CLI-admin user is *copied* to the Cisco ISE web-based admin user database. Only the first CLI-admin user is copied as the web-based admin user. You should keep the CLI- and web-based admin user stores synchronized, so that you can use the same username and password for both admin roles.

The Cisco ISE CLI-admin user has different rights and capabilities than the Cisco ISE web-based admin user and can perform other administrative tasks.

Table 15: Tasks Performed by CLI-Admin and Web-Based Admin Users

Admin User Type	Tasks
Both CLI-Admin and Web-Based Admin	• Back up the Cisco ISE application data. • Display any system, application, or diagnostic logs on the Cisco ISE appliance. • Apply Cisco ISE software patches, maintenance releases, and upgrades. • Set the NTP server configuration.
CLI-Admin only	• Start and stop the Cisco ISE application software. • Reload or shut down the Cisco ISE appliance. • Reset the web-based admin user in case of a lockout. • Access the ISE CLI.

Create a CLI Admin

Cisco ISE allows you to create additional CLI-admin user accounts other than the one you created during the setup process. To protect the CLI-admin user credentials, create the minimum number of CLI-admin users needed to access the Cisco ISE CLI.

You can add the CLI-admin user by using the following command in the configuration mode:

```
username <username> password [plain|hash] <password> role admin
```

Create a Web-Based Admin

For first-time web-based access to Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup.

To add an admin user:

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Admin Access > Administrators > Admin Users.**
2. Choose **Add > Create an Admin User.**
3. Enter the name, password, admin group, and the other required details.
4. Click **Submit**.

Reset a Disabled Password Due to Administrator Lockout

An administrator can enter an incorrect password enough times to disable the account. The minimum and default number of attempts is five.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. It does not affect the CLI password of the administrator. After you successfully reset the administrator password, the credentials are immediately active and you can log in without having to reboot the system. .

Cisco ISE adds a log entry in the **Administrator Logins** window. To view this window, click the **Menu** icon (☰) and choose **Operations > Reports > Reports > Audit > Administrator Logins**. The credentials for that administrator ID is suspended until you reset the password associated with that administrator ID.

Step 1 Access the direct-console CLI and enter:

application reset-passwd ise administrator_ID

Step 2 Specify and confirm a new password that is different from the previous two passwords that were used for this administrator ID:

```
Enter new password:
Confirm new password:

Password reset successfully
```


Cisco ISE Configuration Verification

There are two methods that each use a different set of username and password credentials for verifying Cisco ISE configuration by using a web browser and CLI.

Note A CLI-admin user and a web-based admin user credentials are different in Cisco ISE.

Verify Configuration Using a Web Browser

Step 1 After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

Step 2 In the **Address** field, enter the IP address (or host name) of the Cisco ISE appliance using the following format and press Enter.

Step 3 In the Cisco ISE Login page, enter the username and password that you have defined during setup and click **Login.**

For example, entering https://10.10.10.10/admin/ displays the Cisco ISE Login page.

```
https://<IP address or host name>/admin/
```

Note For first-time web-based access to Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup.

Step 4 Use the Cisco ISE dashboard to verify that the appliance is working correctly.

What to do next

By using the Cisco ISE web-based user interface menus and options, you can configure the Cisco ISE system to suit your needs. For details on configuring Cisco ISE, see *Cisco Identity Services Engine Administrator Guide*.

Verify Configuration Using the CLI

Before you begin

To get the latest Cisco ISE patches and keep Cisco ISE up-to-date, visit the following web site: https://software.cisco.com/download/home/283801620/type

Step 1 After the Cisco ISE appliance reboot has completed, launch a supported product, such as PuTTY, for establishing a Secure Shell (SSH) connection to a Cisco ISE appliance.

Step 2 In the Host Name (or IP Address) field, enter the hostname (or the IP address in dotted decimal format of the Cisco ISE appliance) and click **Open**.

Step 3 At the login prompt, enter the CLI-admin username (admin is the default) that you configured during setup and press **Enter.**

Step 4 At the password prompt, enter the CLI-admin password that you configured during setup (this is user-defined and there is no default) and press **Enter**.

Step 5 At the system prompt, enter **show application version ise** and press **Enter.**

Step 6 To check the status of the Cisco ISE processes, enter **show application status ise** and press Enter.

The console output appears as shown below:

```
ise-server/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4930
Database Server                        running          66 PROCESSES
Application Server                     running          8231
Profiler Database                      running          4955
ISE Indexing Engine                    running          8654
AD Connector                           running          9489
M&T Session Database                   running          3059
M&T Log Collector                      running          9271
M&T Log Processor                      running          9129
Certificate Authority Service          running          8968
EST Service                            running          18883
SXP Engine Service                     disabled
TC-NAC Docker Service                  disabled
TC-NAC MongoDB Container               disabled
TC-NAC RabbitMQ Container              disabled
TC-NAC Core Engine Container           disabled
VA Database                            disabled
VA Service                             disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID Service                      disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
```

List of Post-Installation Tasks

After you install Cisco ISE, you must perform the following mandatory tasks:

Table 16: Mandatory Post-Installation Tasks

Task	Link in the Administration Guide
Apply the latest patches, if any	See the section "Software Patch Installation Guidelines" in Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide* for your release.
Install Licenses	See the Cisco ISE Ordering Guide for more information. See Chapter "Licensing" in the *Cisco ISE Administrator Guide* for your release.

Task	Link in the Administration Guide
Install Certificates	See the section "Certificate Management in Cisco ISE" in Chapter "Basic Setup" in the *Cisco ISE Administrator Guide* for your release.
Create Repository for Backups	See the section "Create Repositories" in Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide* for your release
Configure Backup Schedules	See the section "Schedule a Backup" in Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide* for your release.
Deploy Cisco ISE personas	See the section "Cisco ISE Distributed Deployment" in Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

48

CHAPTER 7

Common System Maintenance Tasks

Bond Ethernet Interfaces for High Availability

Cisco ISE supports bonding of two Ethernet interfaces into a single virtual interface to provide high availability for the physical interfaces. This feature is called Network Interface Card (NIC) bonding or NIC teaming. When two interfaces are bonded, the two NICs appear to be a single device with a single MAC address.

The NIC bonding feature in Cisco ISE does not support load balancing or link aggregation features. Cisco ISE supports only the high availability feature of NIC bonding.

The bonding of interfaces ensures that Cisco ISE services are not affected when there is:

- Physical interface failure
- Loss of switch port connectivity (shut or failure)
- Switch line card failure

When two interfaces are bonded, one of the interfaces becomes the primary interface and the other becomes the backup interface. When two interfaces are bonded, all traffic normally flows through the primary interface. If the primary interface fails for some reason, the backup interface takes over and handles all the traffic. The bond takes the IP address and MAC address of the primary interface.

When you configure the NIC bonding feature, Cisco ISE pairs fixed physical NICs to form bonded NICs. The following table outlines which NICs can be bonded together to form a bonded interface.

Table 17: Physical NICs Bonded Together to Form an Interface

Cisco ISE Physical NIC Name	Linux Physical NIC Name	Role in Bonded NIC	Bonded NIC Name
Gigabit Ethernet 0	Eth0	Primary	Bond 0
Gigabit Ethernet 1	Eth1	Backup	
Gigabit Ethernet 2	Eth2	Primary	Bond 1
Gigabit Ethernet 3	Eth3	Backup	
Gigabit Ethernet 4	Eth4	Primary	Bond 2
Gigabit Ethernet 5	Eth5	Backup	

Supported Platforms

The NIC bonding feature is supported on all supported platforms and node personas. The supported platforms include:

- SNS 3500 and 3600 series appliances - Bond 0, 1, and 2
- VMware virtual machines - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)
- Linux KVM nodes - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)

Guidelines for Bonding Ethernet Interfaces

- As Cisco ISE supports up to six Ethernet interfaces, it can have only three bonds, bond 0, bond 1, and bond 2.
- You cannot change the interfaces that are part of a bond or change the role of the interface in a bond. See the above table for information on which NICs can be bonded together and their role in the bond.
- The Eth0 interface acts as both the management interface as well as the runtime interface. The other interfaces act as runtime interfaces.
- Before you create a bond, the primary interface (primary NIC) must be assigned an IP address. The Eth0 interface must be assigned an IPv4 address before you create bond 0. Similarly, before you create bond 1 and 2, Eth2 and Eth4 interfaces must be assigned an IPv4 or IPv6 address, respectively.
- Before you create a bond, if the backup interface (Eth1, Eth3, and Eth5) has an IP address assigned, remove the IP address from the backup interface. The backup interface should not be assigned an IP address.
- You can choose to create only one bond (bond 0) and allow the rest of the interfaces to remain as is. In this case, bond 0 acts as the management interface and runtime interface, and the rest of the interfaces act as runtime interfaces.
- You can change the IP address of the primary interface in a bond. The new IP address is assigned to the bonded interface because it assumes the IP address of the primary interface.

- When you remove the bond between two interfaces, the IP address assigned to the bonded interface is assigned back to the primary interface.
- If you want to configure the NIC bonding feature on a Cisco ISE node that is part of a deployment, you must deregister the node from the deployment, configure NIC bonding, and then register the node back to the deployment.
- If a physical interface that acts as a primary interface in a bond (Eth0, Eth2, or Eth4 interface) has static route configured, the static routes are automatically updated to operate on the bonded interface instead of the physical interface.

Configure NIC Bonding

You can configure NIC bonding from the Cisco ISE CLI. The following procedure explains how you can configure bond 0 between Eth0 and Eth1 interfaces.

Before you begin

If a physical interface that acts as a backup interface (for example, Eth1, Eth3, Eth5 interfaces), is configured with an IP address, you must remove the IP address from the backup interface. The backup interface should not be assigned an IP address.

Step 1 Log in to Cisco ISE CLI with your administrator account.

Step 2 Enter **configure terminal** to enter the configuration mode.

Step 3 Enter the **interface GigabitEthernet 0** command.

Step 4 Enter the **backup interface GigabitEthernet 1** command.
The console displays:

```
% Warning: IP address of interface eth1 will be removed once NIC bonding is enabled. Are you sure
you want to proceed? Y/N [N]:
```

Step 5 Enter Y and press **Enter**.

Bond 0 is now configured. Cisco ISE restarts automatically. Wait for some time to ensure that all the services are up and running successfully. Enter **the show application** status ise command from the CLI to check if all the services are running.

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE SXP Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
```



```
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

Verify NIC Bonding Configuration

To verify if NIC bonding feature is configured, run the **show running-config** command from the Cisco ISE CLI. You will see an output similar to the following:

```
!
interface GigabitEthernet 0
 ipv6 address autoconfig
 ipv6 enable
 backup interface GigabitEthernet 1
 ip address 192.168.114.214 255.255.255.0
!
```

In the output above, "backup interface GigabitEthernet 1" indicates that NIC bonding is configured on Gigabit Ethernet 0, with Gigabit Ethernet 0 being the primary interface and Gigabit Ethernet 1 being the backup interface. Also, the ADE-OS configuration does not display an IP address on the backup interface in the running config, even though the primary and backup interfaces effectively have the same IP address.

You can also run the **show interface** command to see the bonded interfaces.

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST>  mtu 1500
        inet 10.126.107.60  netmask 255.255.255.0  broadcast 10.126.107.255
        inet6 fe80::9aba:82ff:fe85:4ae0  prefixlen 64  scopeid 0x20<link>
        ether 98:ba:82:85:4a:e0  txqueuelen 0  (Ethernet)
        RX packets 1726027  bytes 307536269 (293.2 MiB)
        RX errors 0  dropped 884  overruns 0  frame 0
        TX packets 1235620  bytes 1073397576 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 98:ba:82:85:4a:e0  txqueuelen 1000  (Ethernet)
        RX packets 1726027  bytes 307536269 (293.2 MiB)
        RX errors 0  dropped 884  overruns 0  frame 0
        TX packets 1235620  bytes 1073397576 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        Device memory fe7a0000-fe7bffff

GigabitEthernet 1
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
```

```
ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
RX packets 0  bytes 0 (0.0 B)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 0  bytes 0 (0.0 B)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
device memory 0xfa000000-fa0fffff
```

Remove NIC Bonding

Use the **no** form of the **backup interface** command to remove a NIC bond.

Before you begin

Step 1 Log in to Cisco ISE CLI with your administrator account.

Step 2 Enter **configure terminal** to enter the configuration mode.

Step 3 Enter the **interface GigabitEthernet 0** command.

Step 4 Enter the **no backup interface GigabitEthernet 1** command.

```
% Notice: Bonded Interface bond 0 has been removed.
```

Step 5 Enter Y and press Enter.

Bond 0 is now removed. Cisco ISE restarts automatically. Wait for some time to ensure that all the services are up and running successfully. Enter the **show application status ise** command from the CLI to check if all the services are running.

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# no backup interface gigabitEthernet 1

Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```



```
ise/admin(config-GigabitEthernet)#
```

Reset a Lost, Forgotten, or Compromised Password Using the DVD

Before you begin

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the Cisco ISE Software DVD to start up a Cisco ISE appliance:

- You have a terminal server associated with the serial console connection to the Cisco ISE appliance that is set to exec. Setting it to *no exec* allows you to use a keyboard and video monitor connection and a serial console connection.
- You have a keyboard and video monitor connection to the Cisco ISE appliance (this can be either a remote keyboard and a video monitor connection or a VMware vSphere client console connection).
- You have a serial console connection to the Cisco ISE appliance.

Step 1 Ensure that the Cisco ISE appliance is powered up.

Step 2 Insert the Cisco ISE Software DVD.

Step 3 Use the arrow keys to select **System Utilities (Serial Console)** if you use a local serial console port connection or select **System Utilities (Keyboard/Monitor)** if you use a keyboard and video monitor connection to the appliance, and press **Enter**.

The system displays the ISO utilities menu as shown below.

```
Available System Utilities:
   [1] Recover Administrator Password
   [2] Virtual Machine Resource Check
   [3] Perform System Erase
   [q] Quit and reload
Enter option [1 - 3] q to Quit:
```

Step 4 Enter **1** to recover the administrator password.

The console displays:

```
Admin Password Recovery
This utility will reset the password for the specified ADE-OS administrator.
At most the first five administrators will be listed. To cancel without
saving changes, enter [q] to Quit and return to the utilities menu.

[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4

Enter choice between [1 - 4] or q to Quit: 2
```



```
Password:
Verify password:

Save change and reboot? [Y/N]:
```

St[illegible] Enter the number corresponding to the admin user whose password you want to reset.

[illegible] Enter the new password and verify it.

St[illegible] Enter **Y** to save the changes.

Reset a Disabled Password Due to Administrator Lockout

An administrator can enter an incorrect password enough times to disable the account. The minimum and default number of attempts is five.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. It does not affect the CLI password of the administrator. After you successfully reset the administrator password, the credentials are immediately active and you can log in without having to reboot the system. .

Cisco ISE adds a log entry in the **Administrator Logins** window. To view this window, click the Menu icon (☰) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Administrator Logins**. The credentials for that administrator ID is suspended until you reset the password associated with that administrator ID.

Step 1 Access the direct-console CLI and enter:

application reset-passwd ise administrator_ID

Step 2 Specify and confirm a new password that is different from the previous two passwords that were used for this administrator ID.

```
Enter new password:
Confirm new password:

Password reset successfully
```

Return Material Authorization

In case of a Return Material Authorization (RMA), if you are replacing individual components on an SNS server, be sure to reimage the appliance before you install Cisco ISE. Contact Cisco TAC for assistance.

Change the IP Address of a Cisco ISE Appliance

Before you begin

- Ensure that the Cisco ISE node is in a standalone state before you change the IP address. If the node is part of a distributed deployment, deregister the node from the deployment and make it a standalone node.
- Do not use the **no ip address** command when you change the Cisco ISE appliance IP address.

Step 1 Log in to the Cisco ISE CLI.

Step 2 Enter the following commands:

a) **configure terminal**
b) **interface GigabitEthernet 0**
c) **ip address new_ip_address new_subnet_mask**

The system prompts you for the IP address change. Enter **Y**. A screen similar to the following one appears.

```
ise-13-infra-2/admin(config-GigabitEthernet)# ip address a.b.c.d 255.255.255.0

% Changing the IP address might cause ISE services to restart
Continue with IP address change? Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Identity Mapping Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE pxGrid processes...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Identity Mapping Service...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
```

Cisco ISE prompts you to restart the system.

Step 3 Enter **Y** to restart the system.

View Installation and Upgrade History

Cisco ISE provides a Command Line Interface (CLI) command to view the details of installation, upgrade, and uninstallation of Cisco ISE releases and patches. The **show version history** command provides the following details:

- Date—Date and time at which the installation or uninstallation was performed
- Application—Cisco ISE application
- Version—Version that was installed or removed.
- Action—Installation, Uninstallation, Patch Installation, or Patch Uninstallation
- Bundle Filename—Name of the bundle that was installed or removed
- Repository—Repository from which the Cisco ISE application bundle was installed. Not applicable for uninstallation.

Step 1 Log in to the Cisco ISE CLI.

Step 2 Enter the following command: **show version history**.

The following output appears:

```
ise/admin# show version history
-------------------------------------------------
Install Date: Fri Nov 30 21:48:58 UTC 2018
Application: ise
Version: 3.0.0.XXX
Install type: Application Install
Bundle Filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```


Perform a System Erase

You can perform a system erase to securely erase all information from your Cisco ISE appliance or VM. This option to perform a system erase ensures that Cisco ISE is compliant with the NIST Special Publication 800-88 data destruction standards.

Before you begin

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the Cisco ISE Software DVD to start up a Cisco ISE appliance:

- You have a terminal server associated with the serial console connection to the Cisco ISE appliance that is set to exec. Setting it to *no exec* allows you to use a KVM connection and a serial console connection.
- You have a keyboard and video monitor (KVM) connection to the Cisco ISE appliance (this can be either a remote KVM or a VMware vSphere client console connection).
- You have a serial console connection to the Cisco ISE appliance.

Step 1 Ensure that the Cisco ISE appliance is powered up.

Step 2 Insert the Cisco ISE Software DVD.

Step 3 Use the arrow keys to select **System Utilities (Serial Console)**, and press Enter.

The system displays the ISO utilities menu as shown below:

```
Available System Utilities:

[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[q] Quit and reboot

Enter option [1 - 3] q to Quit:
```

Step 4 Enter **3** to perform a system erase.

The console displays:

```
********** W A R N I N G **********
THIS UTILITY WILL PERFORM A SYSTEM ERASE OF THE DISK DEVICE(S). THIS PROCESS CAN TAKE UP TO 5 HOURS
TO COMPLETE. THE RESULT WILL BE COMPLETE
DATA LOSS OF THE HARD DISK. THE SYSTEM WILL NO LONGER BOOT AND WILL REQUIRE A RE-IMAGE FROM INSTALL
MEDIA TO RESTORE TO FACTORY DEFAULT STATE.

ARE YOU SURE YOU WANT TO CONTINUE? (Y/N): Y
```

Step 5 Enter **Y**.

The console prompts you with another warning:

```
THIS IS YOUR LAST CHANCE TO CANCEL. PROCEED WITH SYSTEM ERASE? (Y/N) Y
```

Step 6 Enter **Y** to perform a system erase.

The console displays:

```
Deleting system disk, please wait...
Writing random data to all sectors of disk device (/dev/sda)...
Writing zeros to all sectors of disk device (/dev/sda)...
Completed: System is now erased.
Press <Enter> to reboot.
```

After you perform a system erase, if you want to reuse the appliance, you must boot the system using the Cisco ISE DVD and choose the install option from the boot menu.

CHAPTER 8

Cisco ISE Ports Reference

Cisco ISE All Persona Nodes Ports

Table 18: Ports Used by All Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Replication and Synchronization	• HTTPS (SOAP): TCP/443 • Data Synchronization/ Replication (JGroups): TCP/12001 (Global) • ISE Messaging Service: SSL: TCP/8671 • Profiler Endpoint Ownership Synchronization/ Replication: TCP/6379	—

Cisco ISE Infrastructure

This appendix lists the TCP and User Datagram Protocol UDP ports that Cisco ISE uses for intranetwork communications with external applications and devices. The Cisco ISE ports listed in this appe[illegible] be open on the corresponding firewall.

Keep in mind the following information when configuring services on a Cisco ISE network:

- The ports are enabled based on the services that are enabled in your deployment. Apart from the ports that are opened by the services running in ISE, Cisco ISE denies access to all other ports.
- Cisco ISE management is restricted to Gigabit Ethernet 0.
- RADIUS listens on all network interface cards (NICs).
- Cisco ISE server interfaces do not support VLAN tagging. If you are installing on a hardware appliance, ensure that you disable VLAN trunking on switch ports that are used to connect to Cisco ISE nodes and configure them as access layer ports.
- The ephemeral port range is from 10000 to 65500. This remains the same for Cisco ISE, Release 2.1 and later.
- VMware on Cloud is supported in Site-to-Site VPN network configuration. Hence, the IP address or port reachability from the network access devices and clients to Cisco ISE must be established without NAT or port filtering.
- All NICs can be configured with **IP** addresses.
- The policy information point represents the point at which external information is communicated to the Policy Service persona. For example, external information could be a Lightweight Directory Access Protocol (LDAP) attribute.

ISE 3.1 Node Communications