



Cisco Community Expert series Webcast

Identity Services Engine: Deployment and Best Practices

Mohammad Azharuddin – Security Customer Support Engineer, #CCIE 58912

Puneesh Chhabra – Security Customer Support Engineer, #CCIE 30128

November 27th 2018

News & Upcoming events



Ask the Expert following the Webcast

Now through Friday November 30th 2018

With
Mohammad Azharuddin
& Puneesh Chhabra

<http://bit.ly/ATE-ISEnov2018>



Mohammad & Puneesh
Customer Support Engineers

Cisco Community – Ask the Expert

Dynamic Multi-point VPN on Cisco routers: Best Practices & Configuration

Till Friday
28th, September 2018

With
Leonardo Peña
Davila

<http://bit.ly/Ask-DMVPN>



The banner features a blue header with the text 'Ask the Expert' and a photo of Leonardo Peña Davila. Below this, the title 'DMVPN on Cisco routers: Best Practices & Configuration' is displayed in white over a background image of two men working at a table with laptops. The Cisco logo is in the bottom left, the dates '26 NOV - 7 DEC, 2018' are in the bottom center, and a 'Join the Discussion' button is in the bottom right.

Ask the Expert

Leonardo Peña Davila

DMVPN on Cisco routers:
Best Practices & Configuration

 CISCO

26 NOV - 7 DEC, 2018

Join the Discussion

Cisco Community – Ask the Expert in Spanish

BGP Attributes- Best practices

Till Friday 7th, December 2018

-Public event-

Adalid Torres

<http://bit.ly/Pregunte-BGP-sp>



Pregunte al Experto

Aclare sus dudas de los Atributos de BGP - Mejores Prácticas

Adalid Torres

¡Haga Preguntas!

19 NOV - 7 DIC, 2018

CISCO

The banner features a blue background with a white laptop icon containing a photo of Adalid Torres. The text 'Pregunte al Experto' is in a white speech bubble. The main title 'Aclare sus dudas de los Atributos de BGP - Mejores Prácticas' is in white. The date '19 NOV - 7 DIC, 2018' and the Cisco logo are at the bottom. A white button with '¡Haga Preguntas!' is in the bottom right. The background shows a man in a blue shirt looking at a tablet on a balcony overlooking a city.

Cisco Community – Webcast in Spanish

Cisco Umbrella- Your Defense Ally

29th November 2018
10hrs CST (utc -6)

-Public event-

Julio Moisa



<http://bit.ly/CiscoUmbrella2018>

©2018 Cisco and/or its affiliates. All rights reserved.

The banner features a blue header with a photo of Julio Moisa on a laptop screen, labeled "Webcast En Vivo" and "VIP 2018". The main image shows a worker in a blue hard hat and safety vest on a scissor lift, looking at a large yellow dome structure. The text "Participe en el Webcast Cisco Umbrella- Tu línea de defensa perimetral" is overlaid on the right. The bottom blue bar contains the "GRUPO INFOTECH" logo, the date and time "JUEVES 29 DE NOVIEMBRE, 2018 10HRS CDT (UTC -6)", and the Cisco logo.

Webcast En Vivo

Participe en el Webcast
Cisco Umbrella- Tu línea
de defensa perimetral

Julio Moisa

GRUPO INFOTECH

JUEVES 29 DE NOVIEMBRE, 2018
10HRS CDT (UTC -6)

CISCO

Become an event Top Contributor!

Participate in Live Interactive Technical Events and much more

<http://bit.ly/EventTopContributors>



A screenshot of the Cisco Community website's "Events Top Contributors" page. The page header includes the Cisco logo and "Cisco Community". Below the header is a search bar and navigation tabs for "Technology & Support", "For Partners", "Customer Connection", "Events", and "Members & Recognition". The main content area shows the breadcrumb "Cisco Community / Events Top Contributors" and the title "Events Top Contributors". A paragraph explains the program: "This program recognizes Cisco experts in the Cisco Community (CSC) that host technical events (Webcasts, Ask the Experts, Tech Talks, and Facebook Forums.) With this program, Cisco recognizes the positive, valuable influence that our top Cisco experts exert on the communities. To learn more, please visit our FAQs". Below this is a "2014 2013" filter and two contributor profiles: Julio Carvajal and Ryota Takao. A small video thumbnail is visible on the right.

Cisco Designated VIPs

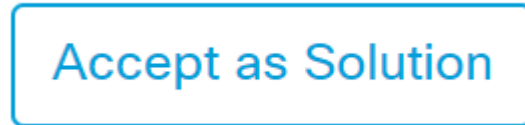
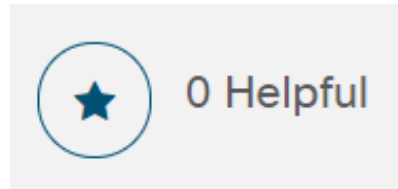


The Cisco Designated VIP program recognizes the top external individual contributors in Cisco's online communities, including the Cisco Support Community (CSC), Cisco Learning Network (CLN) and the Cisco Developers Network (CDN). Cisco Designated VIPs are recognized by their peers for their expertise and tireless contributions, and their abundant participation is vital to community success. With this program, Cisco formally recognizes the positive, valuable influence our top individual members exert on the communities overall. [FAQs](#)

Rate content at the Cisco Community

Help us to recognize the quality content in the community

Rate documents,
Videos & blogs!



Encourage and acknowledge people who
generously share their
time and expertise



Cisco Community Experts



Mohammad Azharuddin
Customer Support Engineer
CCIE #58912



Puneesh Chhabra
Customer Support Engineer
CCIE #30128

Thank You For
Joining Us Today!



Download Today's Presentation
<http://bit.ly/webcast-slides-ISE>

Submit Your Questions Now!

Use the **Q&A** panel to submit your questions and the panel of experts will respond.

They will be answered eventually



Please take a moment to complete the survey at the end of the webcast

New Webex!

The screenshot displays the Cisco Webex Events interface. At the top, the title bar reads "Cisco Webex Events" with standard window controls. Below the title bar is a menu with "File", "Edit", "Share", "View", "Communicate", "Participant", "Event", and "Help". The main content area shows a presentation slide titled "VxLAN Overview" with the subtitle "Overview". The slide features a network diagram of an IP Network (Underlay) cloud. This cloud is connected to four "Edge Device" icons. Each edge device is linked to a "Local LAN Segment", which in turn connects to either a "Physical Host" or "Virtual Hosts" (via a "Virtual Switch"). An "IP Interface" is shown within the cloud. At the bottom of the slide, a URL is provided: <http://opendata.labs.lacnic.net/ipv6stats/graphs/ipv6evo.html>. The interface also includes a "Sharing" bar with a "Screen /presso" button highlighted in red, and a sidebar on the right with options for "Participants (3)", "Q&A", and "Polling". A bottom control bar contains icons for call, video, share, stop, mute, chat, and close.

Please make sure you follow up the presentation in the right screen

Identity Services Engine (ISE) Deployment and Best Practices



Mohammad Azharuddin

Puneesh Chhabra

Security Customer Experience Team

Polling Question 1

Which Cisco ISE persona is responsible for authentications?

- A. Administration Node
- B. Policy Service Node
- C. pxGrid Node



Session Abstract

- Cisco Identity Services Engine (ISE) delivers context-based access control for every endpoint that connects to your network. In addition to providing visibility into all things and users that connect to the network, ISE offers a comprehensive solution for Authentication, automated Device Classification and IoT onboarding, Guest Access, Bring Your Own Device (BYOD), Endpoint Compliance, Software-Defined Segmentation, Context Sharing, Threat-Centric NAC, and controlled access to network devices.
- This session will focus on ISE deployment strategies, overall best practices as well as serviceability tips and tricks to help you gain optimal value and productivity from ISE.

Agenda

- Introducing ISE
- ISE personas and virtual machine hardware sizing
- ISE deployment best practices
- Performance optimization
- Common issues encountered
- Upgrade best practices

You Need the Right Tools to...



See who and what is on your network

Provide guests and contractors
with internet access

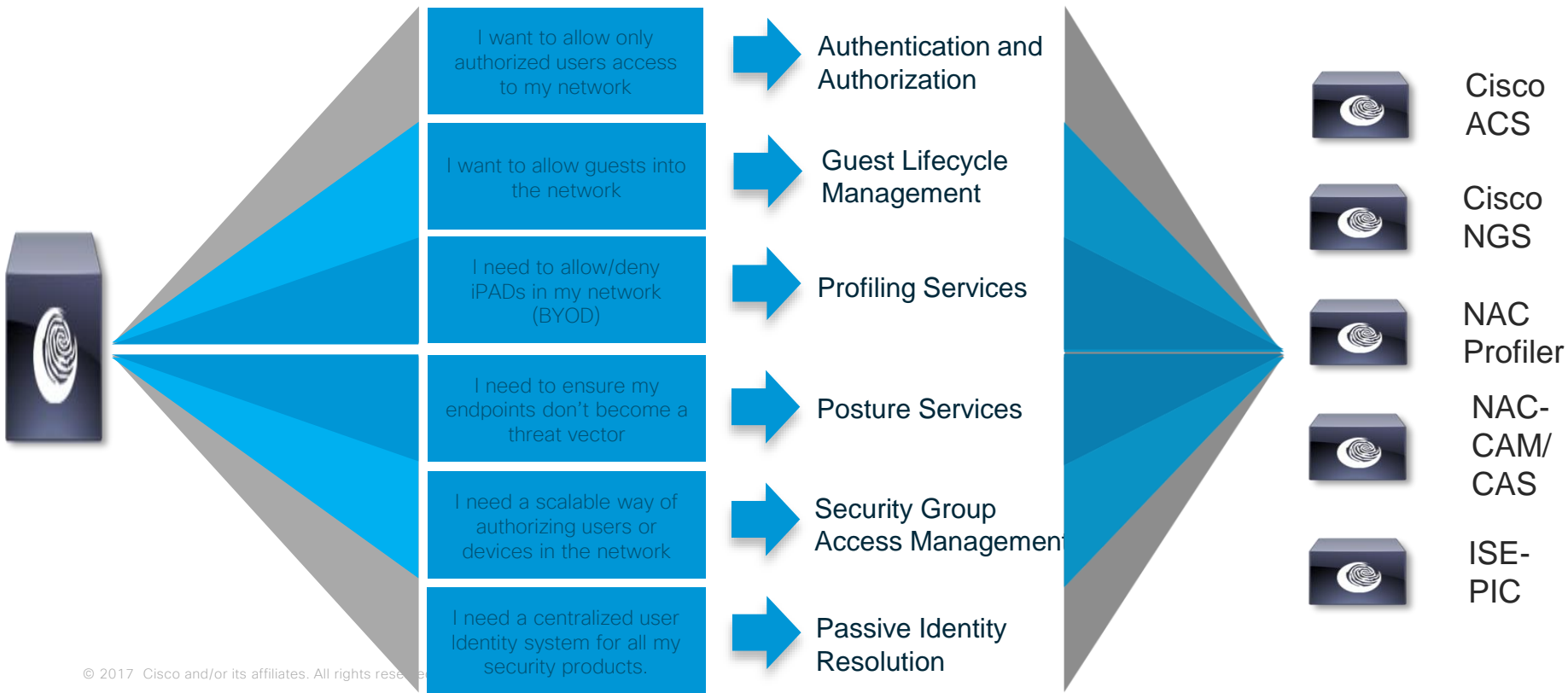
Grant access on a “need to know” basis

Deliver secure admin access to
your network access devices



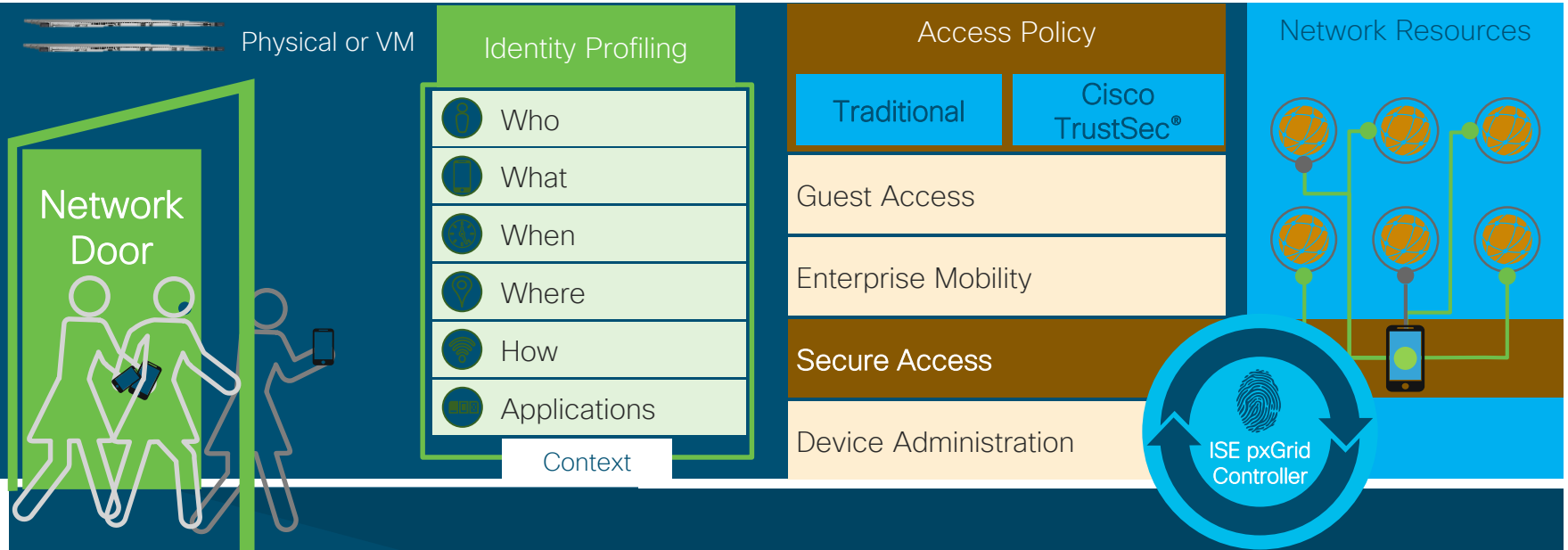
Introducing Identity Services Engine

Introducing Cisco Identity Services Engine (ISE)



Introducing Cisco Identity Services Engine (ISE)

A centralized security solution that automates context-aware access to network resources and shares contextual data



With Cisco Identity Services Engine You Can



See and share rich user and device details



Control all access throughout the network from one place



Stop and contain threats





ISE personas and virtual machine/hardware sizing

Personas



- Policy Service Node (PSN)
 - Makes policy decisions
 - RADIUS/TACACS+ server & provides endpoint/user services



- Policy Administration Node (PAN)
 - Interface to configure policies and manage ISE deployment
 - Replication hub for all database config changes



- Monitoring & Troubleshooting Node (MnT)
 - Interface to reporting and logging
 - Destination for syslog from other ISE nodes and optionally NADs



- pxGrid Controller
 - Facilitates sharing of information between network elements

Basis for VMware Appliance Sizing and Redundancy

New SNS-3500 Series




ISE SNS Appliance Specifications

| Platform | SNS-3415 (34x5 Small) | SNS-3495 (34x5 Large) | SNS-3515 (35x5 Small) | SNS-3595 (35x5 Large) |
|---------------------|---|---|---|--|
| Processor | 1 x QuadCore Intel Xeon CPU E5-2609 @ 2.40 GHz (4 total cores) | 2 x QuadCore Intel Xeon CPU E5-2609 @ 2.40 GHz (8 total cores) | 1 x 6-Core Intel Xeon CPU E5-2620 @ 2.30 GHz (6 total cores) | 1 x 8-Core Intel Xeon CPU E5-2640 @ 2.60 GHz+20MB Cache (8 total cores) |
| Memory | 16 GB | 32 GB | 16 GB | 64 GB |
| Hard disk | 1 x 600-GB 10k SAS HDD (600 GB total disk space) | 2 x 600-GB 10k SAS HDDs (600 GB total disk space) | 1 x 600-GB 10k SAS HDD (600 GB total disk space) | 4 x 600-GB 10k SAS HDDs (1.2 TB total disk space) |
| RAID | No | Yes (RAID 1) | No (1GB FBWC Controller Cache) | Yes (RAID 10) (1GB FBWC Cache) |
| Ethernet NICs | 4x Integrated Gigabit NICs | 4 x Integrated Gigabit NICs | 2 x Integrated GE Ports 4x mLOM GE Ports (6 total LAN ports) | 2 x Integrated GE Ports 4x mLOM GE Ports (6 total LAN ports) |
| Redundant Power? | No (2 nd PSU optional) | Yes | No (2 nd PSU optional) | Yes |

ISE 2.4 Sizing by Deployment/Platform/Persona

Max Concurrent Session Counts by Deployment Model and Platform

- By Deployment

| Deployment Model | Platform | Max Active Sessions per Deployment | Max # Dedicated PSNs / PXGs | Min # Nodes (no HA) / Max # Nodes (w/ HA) |
|---|------------------------------|---------------------------------------|--------------------------------|--|
|  | 3515 | 7,500 | 0 | 1 / 2 |
| | 3595 | 20,000 | 0 | 1 / 2 |
|  | 3515 as PAN+MNT | 7,500 | 5 / 2* | 2 / 7 |
| | 3595 as PAN+MNT | 20,000 | 5 / 2* | 2 / 7 |
|  | 3595 as PAN and MNT | 500,000 | 50 / 2 | 3 / 58 |
| | 3595 as PAN and Large MNT | 500,000 | 50 / 4 | 3 / 58 |

Max Active Sessions != Max Endpoints; ISE 2.1+ supports 1.5M Endpoints

- By PSN

| Scaling per PSN | Platform | Max Active Sessions per PSN |
|--|----------|--------------------------------|
| Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size) | SNS-3515 | 7,500 |
| | SNS-3595 | 40,000 |

Each dedicated pxGrid node reduces PSN count by 1 (Hybrid deployment only)

ISE 2.4 Appliance Support

- Hardware Appliances

- SNS-3515
- SNS-3595



- Virtual Appliances

- Small (based on SNS-3515)
- Medium (based on SNS-3595)
- Large (based on Memory-Enhanced SNS-3595)

No SNS-34x5
Support in ISE 2.4

ISE 2.3 is last
supported release
for SNS-3400
Series

SNS-34x5 End of Life/End of Sale Notice:

<https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/eos-eol-notice-c51-737032.html>

Sizing Production VMs to Physical Appliances

Summary

| Appliance used for sizing comparison | CPU | | Memory (GB) | Physical Disk (GB) ** |
|--------------------------------------|---------|-------------|-------------|-----------------------|
| | # Cores | Clock Rate* | | |
| SNS-3415 | 4 | 2.4 | 16 | 600 |
| SNS-3495 | 8 | 2.4 | 32 | 600 |
| SNS-3515 | 6 | 2.3 | 16 | 600 |
| SNS-3595 | | | | |

* Minimum VM processor clock rate = 2.0GHz per core (same as OVA).

** Actual disk requirement is dependent on persona(s) deployed and other factors. See slide on Disk Sizing.

Warning: # Cores not always = # Logical processors / vCPUs due to Hyper Threading

ISE OVA Templates

Summary

| OVA Template | CPU | | | Virtual Memory (GB) | Virtual NICs (GB) | Virtual Disk Size | Target Node Type |
|--------------|-----------------|------------------|-----------------|---------------------|-------------------|-------------------|------------------|
| | # CPUs | Clock Rate (GHz) | Total CPU (MHz) | | | | |
| Eval | 2 | 2.3 | 4,600 | 8 | 4 | 200GB | EVAL |
| SNS3415 | 4 | 2.0 | 8,000 | 16 | 4 | 200GB | PSN/PXG |
| | | | | | | 600GB | PAN/MnT |
| SNS3495 | 8 | 2.0 | 16,000 | 32 | 4 | 200GB | PSN/PXG |
| | | | | | | 600GB | PAN/MnT |
| SNS3515 | 8 12 | 2.0 | 12,000 | 16 | 6 | 200GB | PSN/PXG |
| | | | | | | 600GB | PAN/MnT |
| SNS3595 | 8 16 | 2.0 | 16,000 | 64 | 6 | 200GB | PSN/PXG |
| | | | | | | 1.2TB | PAN/MnT |

CSCvh71644 - VMware OVA templates for SNS-35xx are not detected correctly...

For 35x5 ISE VMs, HyperThreading is Mandatory

Introducing “Super” MnT

For Any Deployment where High-Perf MnT Operations Required

- Virtual Appliance Only option in ISE 2.4
 - Requires Large VM License
- 3595 specs + 256 GB
 - 8 cores @2GHz min (16000+ MHz)
= 16 logical processors
 - 256GB RAM
 - Up to 2TB* disk w/ fast I/O
- Fast I/O Recommendations:
 - Disk Drives (10k/15k RPM or SSD)
 - Fast RAID w/Caching (ex: RAID 10)
 - More disks (ex: 8 vs 4)

MnT



* CSCvb75235 - DOC ISE VM installation can't be done if disk is greater than or equals to 2048 GB or 2 TB

Cisco Software Notifications

Be Alerted for New ISE Versions, Patches, PSIRTs, Field Notices, EoL, Bugs

Software Download



Downloads Home / Security / Network Visibility and Segmentation / Identity Services Engine / Identity Services

Search...

Expand All Collapse All

Latest Release

2.4.0

Identity Services Engine S

Release 2.4.0

Notifications

Put in the email address and frequency of notification



Cisco Services

Cisco Notification Service

Feedback Sign Up Unsubscribe

Software Updates for Identity Services Engine Software

Product Name: Identity Services Engine Software
Software Type: Identity Services Engine System Software
Release Version: [2.4.0](#)

Alert Type: New File
File Name: [ise-patchbundle-2.4.0.357-Patch1-18052411.SPA.x86_64.tar.gz](#)
File Release Date: 28-MAY-2018

Software Updates for Identity Services Engine Software

Product Name: Identity Services Engine Software
Software Type: Identity Services Engine System Software
Release Version: [2.0.1](#)

Alert Type: New File
File Name: [ise-patchbundle-2.0.1.130-Patch6-18050218.SPA.x86_64.tar.gz](#)
File Release Date: 30-MAY-2018

Find additional information in [Software Downloads](#) index.

Auth Policy Optimization (ISE 2.2 and Earlier)

Leverage Policy Sets to Organize and Scale Policy Processing

Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

- Global Exceptions
Rules across entire deployment
- Wired
- Wireless**
- VPN
- Default
Default Policy Set

Save Order Reset Order

PolicySet Condition

Define the Policy Sets by configuring rules based on the left hand side to change the order.

| Max Auth Rules | Simple Policy Mode | Policy Set Mode (Max Policy Sets=100) |
|--------------------------|--------------------|---------------------------------------|
| Max Authentication Rules | 100 | 200 (2 rules + default) |
| Max Authorization Rules | 600 | 700 (7 rules + default) |

Authentication

| Status | Name | Conditions |
|--------|----------|------------|
| ✓ | Wireless | Wireless |

Authorization

Exceptions (0)

Standard

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|--------|-----------------------------|--|--------------------------------|
| ✓ | Wireless Black List Default | if Blacklist | then Blackhole_Wireless_Access |
| ✓ | Domain_Computer | if AD1:ExternalGroups EQUALS cts.local/Users /Domain Computers | then AD_Login |
| ✓ | Game Consoles - Registered | if (EndPoints:EndPointPolicy EQUALS Game-Console-Registered AND Radius:Called-Station-ID ENDS WITH gaming) | then Game_Console |

Administration > System > Settings > Policy Sets

Advanced Compound Conditions (before ISE 2.3)

Authorization Simple Conditions

For Policy Export go to Administration > System > Backup & Restore > Policy

Edit Add Duplicate Delete

| Name | Expression |
|--|--|
| <input type="checkbox"/> Anomalous Behavior | EndPoints:AnomalousBehaviour EQUALS t |
| <input type="checkbox"/> Anomalous Exception | EndPoints:EndPointPolicy EQUALS Anomal |
| <input type="checkbox"/> Asia | DEVICE:Location EQUALS All Locations#S |
| <input type="checkbox"/> CertRe | |
| <input type="checkbox"/> Europe | #L |
| <input type="checkbox"/> India | #B |
| <input type="checkbox"/> Mobile | e D |
| <input type="checkbox"/> Printer | rs |
| <input type="checkbox"/> SSID1 | ssid |
| <input type="checkbox"/> SSID2 | Radius:Called-Station-ID ENDS_WITH ssid |
| <input type="checkbox"/> US_East | DEVICE:Location EQUALS All Locations#N |
| <input type="checkbox"/> US_West | DEVICE:Location EQUALS All Locations#San Jose |
| <input type="checkbox"/> Wireless_Access | Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 |
| <input type="checkbox"/> Workstation_Devices | EndPoints:LogicalProfile EQUALS Workstations |

First create Simple Conditions. Required to make Advanced Compound Conditions.

Authorization Compound Condition List > New Authorization Compound Condition

Authorization Compound Conditions

* Name



If you switch to the advance view, you can not switch back. Do you want to proceed?

Yes

No

Description

*Condition Expression

Select a condition to insert below

Simple Conditions

```
((Mobile_Devices | Workstation_Devices & SSID1) & US_West) |  
( (Mobile_Devices & SSID2) | (Workstation_Devices & !SSID2) & US_East)
```

SSID1

SSID2

Mobile_Devices

Printer_Devices

Workstation_Devices

Anomalous_Behavior



ISE 2.4 Auth Policy Scale

- Max Policy Sets = 200
(up from 100 in 2.2; up from 40 in 2.1)
- Max Authentication Rules = 1000
(up from 200 in 2.2; up from 100 in 2.1)
- Max Authorization Rules = 3000
(up from 700 in 2.2; up from 600 in 2.1)
- Max Authorization Profiles = 3200
(up from 1000 in 2.2; up from 600 in 2.1)

ISE Policies best practices

- Use compound conditions for differentiation of authentication method

| | | |
|---|-----------------|--|
|  | Corporate Users | if (Wireless_802.1X AND AD1:ExternalGroups EQUALS example.com/SkuchereOU/StaffGR) |
|  | IP Phones | if Cisco-IP-Phone AND Wired_MAB |

- Be as much specific as possible during policy configuration
- Put more specific policies on top
- Move to the polices sets

Polling Question 2

Which of the following services is offered by Cisco ISE?

- A. Firewall
- B. IPS/IDS
- C. NAC



Best Practices



ISE Upgrade Tips & Tricks

Upgrade Readiness Tool (URT)

Available on Cisco.com under ISE Software

Upgrade Readiness Tool (URT) to validate config DB upgrade from 2.0, 2.0.1, 2.1, 2.2, 2.3 to 2.4. This is a signed bundle for image integrity. 29-MAR-2018
[ise-urtbundle-2.4.0.357-1.0.0.SPA.x86_64.tar.gz](#)

- CLI tool used outside of upgrade bundle
- Detect potential upgrade issues BEFORE upgrade.
- No downtime needed to run tool.
- Runs data upgrade on cloned database on Secondary PAN or Standalone node.
- Reports failures/success for each stage as well as time estimate for upgrade.

Introduced in ISE 2.3

```
#####  
# Running Upgrade Readiness Tool (URT) #  
#####  
This tool will perform following tasks:  
1. Pre-requisite checks  
2. Clone config database  
3. Copy upgrade files  
4. Data upgrade on cloned database  
5. Time estimate for upgrade  
  
Pre-requisite checks  
=====  
Disk Space sanity check - Successful  
NTP sanity - Successful  
Appliance/VM compatibility - Successful  
Trust Cert Validation - Successful System  
Cert Validation - Successful Invalid  
MDMServerNames in Authorization Policies  
check -Successful  
6 out of 6 pre-requisite checks passed  
_____  
Clone config database...
```

Upgrade Enhancements

Example URT Outputs



```
- Data upgrade step 93/96, NSFUpgradeService(2.3.0.206)... Done in 0 seconds.
- Data upgrade step 94/96, ProfilerUpgradeService(2.3.0.206)... Done in 1 seconds.
- Data upgrade step 95/96, GuestAccessUpgradeService(2.3.0.206)... Done in 6 seconds.
- Successful
Running data upgrade for node specific data on cloned database
- Successful

Time estimate for upgrade
=====
Estimated time for each node(in mins):
upsdev-vm11(STANDALONE):193

Application successfully installed
upsdev-vm11/admin#
```



```
- Data upgrade step 90/97, networkAccessUpgrade(2.3.0.178)... Done in 0 seconds.
- Data upgrade step 91/97, NetworkAccessUpgrade(2.3.0.182)... Done in 0 seconds.
- Data upgrade step 92/97, CertMgmtUpgradeService(2.3.0.194)... Done in 3 seconds.
- Data upgrade step 93/97, UPSUpgradeHandler(2.3.0.201)... Failed.
- Failed
Final cleanup before exiting...

Collecting log files ...
- Encrypting logs bundle...
Please enter encryption password:
Please enter encryption password again to verify:
Encrypted URT logs(urt_logs.tar.gpg) are available in localdisk. Please reach out to Cisco to debug
% Post-install step failed. Please check the logs for more details.
upsdev-vm11/admin# exit
```

ISE Upgrade: Standard or Backup/Restore Method

Standard Upgrade

Overview Upgrade

Read only mode. Click the Upgrade tab to proceed.

| Node Group - Host Name | Persona | Version - Repository | Status |
|--------------------------|-------------------|----------------------|--------|
| npf-sjca-pap02.cisco.com | Admin SECONDARY | 2.4.0.358 | Active |
| npf-sjca-mm102.cisco.com | Monitor (PRIMARY) | 2.4.0.358 | Active |
| sbg-bgla-pdp01.cisco.com | Policy service | 2.4.0.358 | Active |
| npf-sjca-px02.cisco.com | pxGrid | 2.4.0.358 | Active |
| npf-sjca-pdp01.cisco.com | Policy service | 2.4.0.358 | Active |
| npf-sjca-pdp02.cisco.com | Policy service | 2.4.0.358 | Active |
| npf-sjca-pdp04.cisco.com | | | |
| npf-sjca-px01.cisco.com | | | |
| npf-sjca-mm101.cisco.com | | | |
| npf-sjca-pap01.cisco.com | | | |

1 Review Checklist 2 Download Bundle to Node(s) 3 Upgrade Node(s)

Print Checklist Review the checklist before you begin upgrading the nodes.

Backup ISE

- Configuration and operational data (see Administration > System > Backup & Restore)
- Backup system logs (see Operations > Troubleshoot > Download Logs)
- Export certificates and private keys (see Administration > System > Certificates > System Certificates)

Software

- Review the ISE U
- Confirm valid ISE
- Download the ISE

Credentials

- Make a note of th

Operational Data Purge

- Purge operational
- I have reviewed th

Upgrade - 3 step pro

- Review Checklist
- Download Bundle to Node
- Upgrade Node(s)

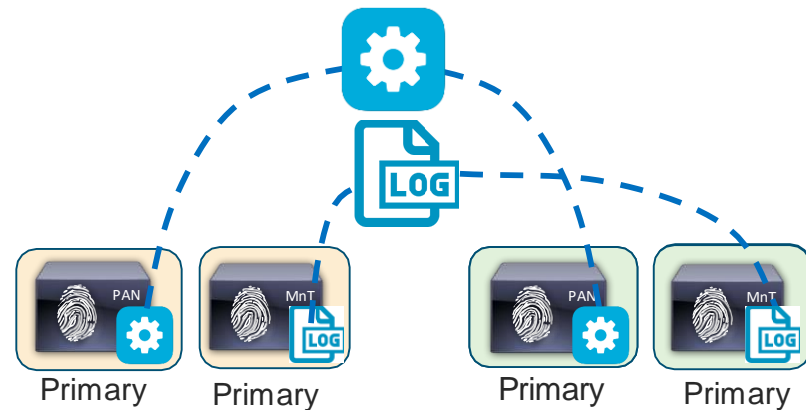
Cancel Upgrade

Deployment (2.4.0.358) New Deployment Upgrade (2.4.0.358) Total estimated time: 348 mins

| Sequence | Node Group - Host Name | Persona | Status |
|----------|--------------------------|-------------------|-----------------------------|
| 1 | npf-sjca-pap02.cisco.com | Admin (SECONDARY) | 0% Upgrading |
| 2 | npf-sjca-pap01.cisco.com | Admin (SECONDARY) | Upgrade queued |
| 3 | | | Select nodes for sequence 3 |

CSCvi38845 Upgrade fails after Feed update due to less heap space -- Requires new Upgrade Bundles to be posted to Software Center

Backup/Restore



Backup/Restore method requires more manual effort, but provides "cleanest" upgrade.

CSCvh57345 Restore of 1.4/2.0/2.0.1 backup fails which taken after Feed update -- Fixed in 2.2 Patch 8 and 2.4

ISE underlying OS upgrade

| ISE Upgrade From \ To | ISE 1.3 | ISE 1.4 | ISE 2.0 | ISE 2.0.1 | ISE 2.1 | ISE 2.2 | ISE 2.3 |
|--------------------------|---------|---------|---------|-----------|---------|---------|---------|
| ISE 1.3 | N/A | No | No | Yes | Yes | N/A | N/A |
| ISE 1.4 | N/A | N/A | No | Yes | Yes | Yes | N/A |
| ISE 2.0 | N/A | N/A | N/A | N/A | Yes | Yes | Yes |
| ISE 2.0.1 | N/A | N/A | N/A | N/A | Yes | Yes | Yes |
| ISE 2.1 | N/A | N/A | N/A | N/A | N/A | No | No |
| ISE 2.2 | N/A | N/A | N/A | N/A | N/A | N/A | No |



ISE Post upgrade tasks/issues

- If you had enabled certificate-based authentication for administrative access to Cisco ISE (Administration > Admin Access) before upgrade and used Active Directory as your identity source, after upgrade, you will not be able to launch the ISE login page because Active Directory join is lost during upgrade. If you run in to this issue, from the Cisco ISE CLI, start the ISE application in safe mode using the following command:
 - *application start ise safe*
- This command brings up the Cisco ISE node in safe mode. Perform the following tasks:
 - Log in to the Cisco ISE user interface using the internal administrator account.
 - If you do not remember your password or if your administrator account is locked, see the [Cisco Identity Services Engine Hardware Installation Guide Cisco Identity Services Engine Hardware Installation Guide](#) for information on how to reset an administrator password.
 - Join Cisco ISE with Active Directory.



ISE Post upgrade tasks/issues contd..

- Ensure that you have Reverse DNS lookup configured for all Cisco ISE nodes in your distributed deployment in the DNS server(s). Otherwise, you may run into deployment-related issues after upgrade.



ISE Post upgrade tasks/issues contd..

- If you have created SFTP repositories using RSA keys, then when you upgrade the Secondary Administration node to a later release, the SFTP repository becomes inaccessible because the RSA keys were generated from the Primary Administration node.
- After you upgrade, if you want to access the SFTP repository, you can do one of the following:
 - Regenerate the RSA keys from the new Primary Administration node.
 - After upgrade, promote the new Secondary Administration node to be the Primary Administration node.

Radius servers configuration recommendations

- **Server timeout** - recommended value between 5-10 seconds. Avoid using of default 2s, it is too aggressive
- **RFC 3576** - enable COA support for this server. For ISE keep it always enabled

| | |
|---------------------------|--|
| Server Index | 14 |
| Server Address(Ipv4/Ipv6) | 10.48.17.252 |
| Shared Secret Format | ASCII ▾ |
| Shared Secret | ●●● |
| Confirm Shared Secret | ●●● |
| Key Wrap | <input type="checkbox"/> (Designed for FIPS customers) |
| Port Number | 1812 |
| Server Status | Enabled ▾ |
| Support for RFC 3576 | Enabled ▾ |
| Server Timeout | 5 seconds |

WLAN configuration recommendations

Use the same server for Authentication and Accounting

- This will ensure that single PSN will be an exclusive holder of session/endpoint data
- Accounting Start/Stop/Update won't trigger endpoint ownership change

The screenshot shows the 'AAA Servers' configuration page in a network management interface. It has three tabs: 'Layer 2', 'Layer 3', and 'AAA Servers'. Below the tabs, there is a heading 'Select AAA servers below to override use of default servers on this WLAN'. Underneath, there is a section for 'Radius Servers' with a checkbox for 'Radius Server Overwrite interface' which is currently unchecked. Below that, there are two columns: 'Authentication Servers' and 'Accounting Servers'. Both columns have a checked 'Enabled' checkbox. There are two rows of server configurations, 'Server 1' and 'Server 2'. Each row has a dropdown menu for the server IP and port. For Server 1, the dropdowns are 'IP:10.48.17.252, Port:1812' and 'IP:10.48.17.252, Port:1813'. For Server 2, the dropdowns are 'IP:10.48.17.118, Port:1812' and 'IP:10.48.17.118, Port:1813'. The dropdown menus for both columns in both rows are highlighted with a blue border.

| | Authentication Servers | Accounting Servers |
|----------|----------------------------|----------------------------|
| Server 1 | IP:10.48.17.252, Port:1812 | IP:10.48.17.252, Port:1813 |
| Server 2 | IP:10.48.17.118, Port:1812 | IP:10.48.17.118, Port:1813 |

WLAN configuration recommendations (continue)

- **AAA Override** – allow applying of authorization attributes returned by server
- **Session Timeout** – 10 hours is recommended value
- **Client Exclusion** – ignore client authentication attempts after failed one. Recommended value is 180 seconds
- **NAC State** – Enable COA support for WLAN

The screenshot displays the 'Advanced' configuration page for WLAN. Several settings are highlighted with blue boxes:

- Allow AAA Override**: Enabled
- Coverage Hole Detection**: Enabled
- Enable Session Timeout**: 28800 (Session Timeout (secs))
- Client Exclusion**: Enabled 180 (Timeout Value (secs))
- NAC State**: Radius NAC

Other visible settings include:

- DHCP**: DHCP Server Override; DHCP Addr. Assignment Required
- OEAP**: Split Tunnel Enabled
- Management Frame Protection (MFP)**: MFP Client Protection Optional
- DTIM Period (in beacon intervals)**: 802.11a/n (1 - 255) 1; 802.11b/g/n (1 - 255) 1
- Static IP Tunneling**: Enabled
- Wi-Fi Direct Clients Policy**: Disabled
- Maximum Allowed Clients**: 0
- Maximum Allowed**: 200



AD Integration Best Practices

- **DNS** servers in ISE nodes must have all relevant AD records (A, PTR, SRV)
- Ensure **NTP** configured for all ISE nodes and AD servers
- Configure **AD Sites and Services**
(with ISE machine accounts configured for relevant Sites)
- Configure Authentication Domains (**Whitelist domains** used) (ISE 1.3)
- Use **UPN/fully qualified usernames** when possible to expedite user lookups
- Use **AD indexed attributes*** when possible to expedite attribute lookups
- **Run Scheduled Diagnostics** from ISE Admin interface to check for issues.

* Microsoft AD Indexed Attributes:

<http://msdn.microsoft.com/en-us/library/ms675095%28v=vs.85%29.aspx>

<http://technet.microsoft.com/en-gb/library/aa995762%28v=exchg.65%29.aspx>



ISE avoiding melting

Suppression for Anomaly clients and for logging should always be enabled.

- **Anomaly client suppression** – send access-reject to client immediately (during reject interval) if two or more unsuccessful attempts with the same scenario being detected from the same client during detection interval
- **Log suppression**– logging only first successful authentication for client, for all subsequent authentication only authentication count will be updated.



Distributed Deployment Basics

- Certificate Trust List (CTL) of the primary node is populated with the appropriate Certificate Authority (CA) certificates that can be used to validate the HTTPS certificate of the standalone node.
- The fully qualified domain name (FQDN) of the standalone node that you are going to register, must be DNS-resolvable from the primary Administration ISE node.



Per Node limit

- 40k concurrent sessions per 3595 (ISE 2.1+)
- PSN will remove oldest active session when limit is exceeded
[SessionLifecycleNotifier][] cpm.nsf.session.internal.LRUagingAlgorithm -:::::- Removing session from cache 87bcd1780009655756550D61 as the current session size is max: 40000
- 4500 maximum concurrent EAP sessions
- PSN will not accept any new EAP sessions if limit is exceeded
prrt.log logs: WARN , 1295104912 ,NIL-CONTEXT,Hit EAP session count limit. Dropping request!,RADIUSHandler.cpp:509
- 30 maximum concurrent guest sessions
- Minimum Disk IO – Read = 300 MB/sec & Write = 50 MB/ sec



Per Deployment limit

- 50 PSNs per deployment
- 40k active sessions per 3595
- 500k total active sessions
- $50 \times 40 \text{ k} = 2000\text{k} \neq$ Total supported active sessions
- The limitation of 500k is due to Admin and MNT nodes
- Maximum latency between nodes $\leq 300\text{ms}$

Polling Question 3

What is the maximum number of Admin nodes we can have in a Cisco ISE deployment?

- A. 1
- B. 2
- C. 3 or more



Some important Document Guide Links for ISE Upgrade

ISE Upgrade Path:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/upgrade_guide/b_ise_upgrade_guide_23/b_ise_upgrade_guide_23_chapter_010.html#id_15402

ISE Upgrade Procedure:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/upgrade_guide/b_ise_upgrade_guide_23/b_ise_upgrade_guide_23_chapter_010.html#id_15401

Pre-Upgrade Tasks:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/upgrade_guide/b_ise_upgrade_guide_23/b_ise_upgrade_guide_23_chapter_01.html#prepareforupgrade

Post-Upgrade Tasks:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/upgrade_guide/b_ise_upgrade_guide_23/b_ise_upgrade_guide_23_chapter_0100.html#reference_FE2938C15CD64E48B4CB19BF843C624A

Full performance and Scaling guide:

<https://communities.cisco.com/docs/DOC-68347>

Thanks!

Submit Your
Questions Now!



Use the Q&A panel to submit your
questions, our expert will respond

Ask the Expert following the Webcast

Now through Friday November 30th 2018

With
Mohammad Azharuddin
& Puneesh Chhabra

<http://bit.ly/ATE-ISEnov2018>



Mohammad & Puneesh
Customer Support Engineers

Collaborate within our Social Media



Twitter

- @Cisco_Support
- <http://bit.ly/csc-twitter>

Facebook

- Cisco Community
- <http://bit.ly/csc-facebook>

Learn About Upcoming Events

We invite you to review our Social Media Channels

YouTube

- Cisco Community
- <http://bit.ly/csc-youtube>



App

- Cisco Technical Support



LinkedIn

- Cisco Community
- <http://bit.ly/csc-linked-in>



Cisco has support communities in other languages!

If you speak Spanish, Portuguese, Japanese, Russian or Chinese we invite you to participate & collaborate



[Comunidad de Cisco](#)
Spanish

[Comunidade da Cisco](#)
Portuguese

[思科服务支持社区](#)
Chinese

[Сообщество Cisco](#)
Russian

[シスココミュニティ](#)
Japanese



More IT Training Videos and Technical Seminars on the Cisco Learning Network

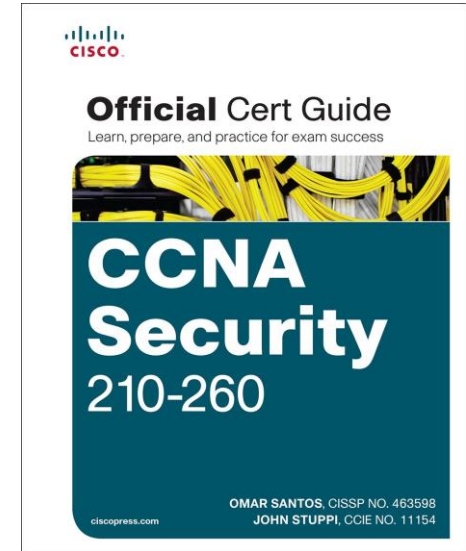
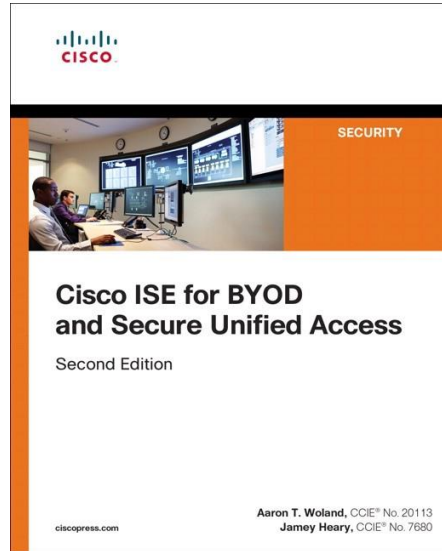
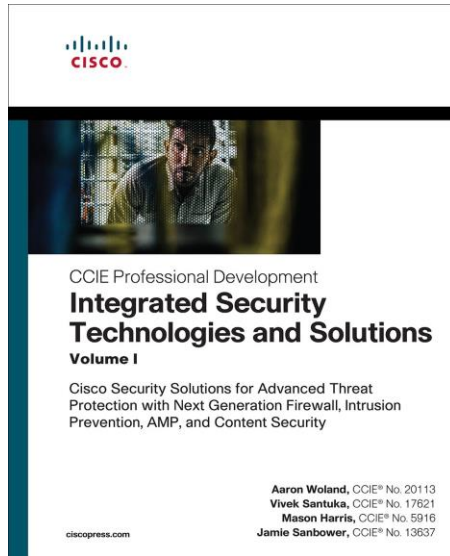
View Upcoming Sessions Schedule

<https://cisco.com/go/techseminars>

Thank you for participating, you earned a discount!

Redeem your 35% discount offer by entering code: CSC when checking out.

<http://bit.ly/Community-CiscoPress2018>



Thank you for Your
Time!

Please take a moment to complete the
survey



Thanks For Joining today!

