Cisco Identity Services Engine (ISE) 3.x

A cloud-enabled approach to increase visibility into policy controls and zero-trust

Providing secure access to trusted users and endpoints is getting harder and harder to achieve. The problem of identifying and controlling endpoints as they request access to trusted resources has been exacerbated by trends around cloud migration, mobility, and the proliferation of the Internet of Things (IoT)-connected devices. But as the cloud, mobility, and IoT all possess great possibilities to unlock innovation as well as save organizational resources, these new paradigms have introduced more questions and complexity when it comes to securing data and m aintaining compliance across the expanding perimeter.

Zero trust with least privilege access is a vital cybersecurity principle that addresses these challenges. It recommends granting only the minimum level of system/network access based on the least level of privilege required to allow users and endpoints to carry out their missions as required by business objectives. Unrequired access extends the network attack surface, increases the risk for the organization, and allows the lateral movement of threats.

By controlling access to only what is needed to reach business outcomes, the organizational risk is reduced, and compliance is assured.

The complexity of today's networks makes the implementation of the least privilege approach to providing network access a daunting challenge. Without having the visibility to properly identify network endpoints, controlling access with segmented zones of trust is not only not recommended, but it could also cause disastrous effects in the workplace, shutting down businesscritical functions, especially in IoT environments.

Solving more for customers in Cisco ISE:

Where and how customers consume their security has evolved, and to lead in this transition, we are kicking off our cloud-enabled approach with ISE VMs deployable from the cloud (AWS and Azure). Here are few critical customer problems we are solving.

- When a user or a device access an application sitting in datacenter or cloud, the traffic traverses different paths (LAN, SDWAN, Data Center, Cloud). These domains are managed by different policy controllers that are managed by different personas such as Network Operationss or Security Operations or Data Center administrators who may not talk to each other. This could result in policy loopholes. In addition each of these policy controllers have different policy constructs for implementing access and segmentation policy. Maintaining consistent policy for a simple user to application access becomes a nightmare due to its complexity.

  With common policy Cisco ISE learns the context of users, devices and applications from all sources and assigns a label called Security Group Tag (SGT) to these entities. Cisco ISE then becomes an context exchange hub to share the user, device and application context and assigned SGTs to all policy controllers across both network and security domain. Now an SGT becomes a common identifier for both source (user and device) and destination (application) for creating unique policies across the policy controller. This simplifies the process of creating a consistent policy no matter what policy controller you use.
- Customers want fast, lightweight security, so we delivered agentless posture to solve the internal debate between speed of delivery and protection.
- Customers evolve from essential to advanced use cases to gain value and provide secure network access; we have evolved our licensing structure to match.

Added visibility

Identifying and classifying network devices and resources is a critical first step in building a zero-trust strategy around network segmentation and creating zones of trust for policy decisions and enforcement. Within this recent release of ISE and across our Secure Access portfolio, we have increased our ability to see and identify what is connecting to the network to build visibility-based network segmentation and policy control into the network itself without the use of agents.

What’s new in ISE?

Solving for visibility and enabling zero trust is why we are delivering a bold, cloud-centric approach to network access and control. ISE focuses on three key pillars to enable customers to solve their secure access challenges and build a zero-trust workplace: added visibility to increase efficiency and reduce network downtime, enhanced security and time-saving flexibility.

Improved visibility

pxGrid Direct Visibility has improved transparency from the last iteration of Cisco ISE (ISE 3.2) and now customers get improved endpoint attributes via external databases such as Service Now. Whether the data comes from endpoints, users, devices or which apps are running over the network and its different attributes, it provides a lot of information such as the device type, device owner and other things like whether the device is operational.

In the latest version of Cisco ISE 3.4, there are two new pxGrid Direct enhancements that will strengthen the synergy between Cisco ISE and pxGrid. The first enhancement will allow customers to immediately synchronize data from pxGrid Direct Connectors. Currently Cisco ISE can synchronize a full data base update once a week or less (minimum once every 12 hours), with incremental updates every day (incremental updates minimum once every hour). With immediate synchronization, there is no longer a need to wait until once a week or until the end of the day. Any and all updates can be made immediately without waiting.

The second enhancement grants the ability to push updates immediately to Cisco ISE. This new feature is called pxGrid Direct Push and will allow a continuous synchronization of Cisco ISE without any lag. In other words, whenever a single record is adjusted, the change will immediately be sent to Cisco ISE.

A Cisco-only feature called Wi-Fi Edge Analytics will allow network admins to mine data from Apple, Intel and Samsung devices to better improve profiling. Cisco Catalyst 9800 wireless controllers will pass along endpoint-specific attributes, such as model, OS version, firmware, among others, to ISE via RADIUS. From there this information will be used to profile common endpoints found on the network.

Getting this network data in an easily accessible fashion allows the network admin to make better decisions. This data can then be spun to run the network in a more efficient manner allowing for a safer network and less time spent on translating information.

Cloud-enabled actionable visibility

By embracing cloud-based solutions, organizations are gaining actionable visibility and increased context to inform the policy decision points in a zero-trust framework. ISE extends its open standards-based ecosystem, pxGrid, into the cloud, with pxCloud. Customers are able to take the knowledge from cloud-based security intelligence and analytics solutions to gain an actionable arm of defense at the network enforcement points throughout the network. This level of integration increases an organization's overall security posture with automated threat containment to prevent the lateral movement of malware, stopping sophisticated attacks such as ransomware, while future protecting existing security investments and increasing their ROI.

Increased flexibility with Agentless posture

To see everything and to make obtaining complete visibility and control "touchless," we support an Agentless posture to ensure all devices are identified, and remain in omplicance, without having to install anything on the device or endpoint. Agentless posture increases flexibility and accelerates time to value with ease of deployment while solving the internal debate between the speed of delivery of network resources and increasing risk. On top of Agentless posture, ISE also enables running scripts on each and every endpoint connected to the network to gain better visibility.

AI-augmented visibility through integration with AI endpoint analytics

Dynamic visibility extends beyond a static list, simple identifiers, or single levels of authentication such as ID/password or MAC address. Single identifiers, when coupled together, can start to build the identity of a user or endpoint. ISE uses Cisco AI Endpoint Analytics to track multiple data sources while leveraging machine learning to automatically analyze and classify unknown devices based on their behavior, adding a new level of assurance to the identity of the endpoint. Device profiles are continuously and dynamically updated via a baseline of behavior, posture, and threat analytics from our pxGrid ecosystem to ensure levels of trust are maintained to limit organizational risk and maintain compliance.

Visibility for now and the future

We have increased the capabilities within ISE to improve device identification and classification with increased support for MDM (mobile device management) and MUD (manufacture usage description) as well as overcoming challenges with shared MAC addresses with Unique Device ID. ISE extended integrations into solutions such as Cisco Cyber Vision, and Cisco DNA Center™ increases and automates visibility and control into IoT devices to ensure visibility based segmentation can be implemented without disrupting business objectives.

Enhanced security

Customers can now take ISE to the cloud. With cloud-supported deployments, integration with cloud-native solutions, and identity directories, ISE is giving organizations the flexibility they require to enable cloudfirst strategies while providing secure access and supporting zero trust.

PAC-less now supported

Protected Access Credentials (PAC) is a credential generated by Cisco that is sent to Cisco ISE allowing for TrustSec devices authentication. When a device needs identification later, the PAC file can be sent again. Support of a PAC-less communication was developed and supported by Cisco ISE in efforts to make the network run smoother.

When a device that supports PAC-less communication connects to a network, newer switches and network devices now know whether a device supports PAC. Once the determination is understood, the findings are sent to Cisco ISE. If PAC is not supported, Cisco ISE will recognize this resulting in a PAC-less double check. Older devices that still use PAC will still be covered and behave the way that it always has.

Keeping aware of your active directory site

This new feature provides Active Directory Site Awareness so customers have more control over Domain Controllers (DC) and in the priority in which the Policy Service Nodes (PSN) are selected. Situations when a domain controller is unavailable, Cisco ISE will automatically choose the next DC available. When the original domain controller comes back online, the current protocol is for Cisco ISE to stick with the current DC and not return to the original one selected.

While automation is a hallmark of Cisco ISE there are times when customers better understand which domain controller is best due endpoint proximity. In addition there are cases where the customer knows when a particular domain controller performs better than the one that Cisco ISE chooses and may want to override Cisco ISE’s decision.

In these cases, Cisco allows the flexibility for our customers to supercede the Cisco ISE selection algorithm. This provides a peace of mind for customers who will be safe in the knowledge that the domain controller that they chose originally is the one that will be connected once the DC is restored.

It is a credential generated by ISE as part of the EAP-FAST protocol.

The strength is in the chip

The new TPM Chip (for supported hardware) is a response to the need for increased security. Found on the new SNS-3700 models and in some virtual environments, the TPM chip is a dedicated chip where sensitive information can be stored. Previously if Cisco ISE uses a password to connect to a data base, it was stored in the file system, which is less secure. But now with the information housed on the TPM Chip, it is proven to be more difficult to access thus providing a more secure place for information to be stored.

Enabling a cloudcentric approach

Organizations are looking to the cloud first as they build their infrastructure as well as deploy services and solutions. ISE is enabling this strategic approach with pxCloud, our open and standards-based integration platform. pxCloud enables integration with cloud-native Software-as-a-Service (SaaS) security solutions. Organizations are able to enhance their security visibility and intelligence to gain more context as they look to automate threat containment and improve policy decisions and enforcement without having to deploy anything on-premises.

ISE in and with the cloud

ISE is deployable from the cloud to enable customers' cloud-first approach and to increase customer flexibility in the deployment of ISE to provide secure access. We have also integrated with Azure AD to better support our customers migrating into the cloud through single sign-on to expand our cloud-centric strategy. Furthermore, with ISE, customers can deploy an ISE node in an ESX infrastructure running on AWS.

Cloud-enabled actionable visibility

With increased visibility and context from the cloud, organizations are now better informed to confidently create access policies to reduce organization risk, without risking business objectives and preventing the connection. With cloudenabled visibility, customers gain an active arm of protection from passive security solutions to automate threat containment Customers can bring together silos of visibility and intelligence to extend interoperability and take a platform approach in solving their secure access challenges.

Open integrations to extended ecosystem

pxCloud extends the ISE ecosystem and furthers our open and interoperable stance within solving customers' challenges. The ISE ecosystem of trusted and validated partners confirms Cisco's commitment to overcoming complexity in the network with solutions that are interoperable and support a platform approach to gain simplicity, automation, and accelerate value.

Time-saving flexibility

In everything we do, we need to be customercentric. And overcoming complexity to ensure that our customers can accelerate their value is a core principle guiding our innovations and design. ISE has answered this challenge by hardening and improving its core functions, and with a focus on interoperability and platform integrations, customers will be able to accelerate their value as well as the value of existing solutions without an increase in investment.

Automating temporary connections

Dynamic Reauthentication Times is a time-saving feature that allows the administrator to set up a temporary policy where a group of devices—not expected to stay on the network for a long time—are placed in a particular bucket. This bucket is "dumped" or removed from the network at a particular time that is set by the administrator. This allows the administrator to set up a designated time prior to expel the end devices in that temporary bucket concurrently once that designated period is complete. This provides a sort of temporary segmentation that continues the Cisco ISE tradition of least privilege where users are allowed to access only the information that they need.

When using this feature, Cisco ISE ignores the default session timeout and calculates for each endpoint upon connecting to the network. This is done in a way that all endpoints will get the session timeout at the exact same time, regardless to the time they authenticated. The end time value is something that Cisco ISE procures using pxGrid Directs.

Reduce your reboot time by 40%

Rebooting Cisco ISE is something that can take more than 20 minutes and results in taking ISE offline for that amount of time. Thanks to this new feature, rebooting of Cisco ISE will now take a much shorter time–often seeing a reboot reduction savings of 40%. Typically a reboot of Cisco ISE is usually called for when upgrading software or adding new services or reauthorizing new certifications. While rebooting ISE is something that doesn't happen every day, when it is needed, it is now a faster process.

Splits means less time to upgrade

With Split Upgrades your nodes are broken up into two separate groups: the Primary Policy Administration Node (PPAN) and Secondary Policy Administration Node (SPAN). With the nodes split, it allows the network to divide the update and complete the new software revision on the PPAN first before starting on SPAN. While the PPAN updates, the network's security responsibility shifts to the SPAN. When it comes time for the SPAN to update, it reverts back to the PPAN. This shortens the upgrade process and becomes more predictable and runs without network interruption. Customers will no longer have to worry about a lack of network functionality when they see an ISE update request. Once installed, their networks will be up-to-date with the latest and greatest in security.

The Unknown becomes quantifiable

There are instances where clusters of unidentified endpoints can be found on the network. Using AI/ML Profiling and Multi-Factor Classification (MFC) will allow customers to quickly identify clusters of identical unknown endpoints via a cloudbased ML engine. From there, the devices can be reviewed by proposed profiling policies via the ML engine and have the devices labeled as either MFC Hardware Manufacturer, MFC Hardware Model, MFC Operating System and MFC Endpoint Type.

What this means is that grouping unknown endpoints on the network has become much easier. A network admin can then create a profile and rules for that group of devices making it more difficult forthe devices to roam the network.

Increase efficiency while reducing downtime

ISE's Controlled Application Restart benefits network admins by saving them time and eliminating a lot of the headaches that come with managing network security. They are now given the ability to control the replacement of the ISE administrative certificate allowing them the ability to plan for maintenance once their current certificate expires. Prior to this new feature, a certification replacement required a complete reboot, which can cause some admins to allow the certification to lapse.

Stay up-to-date without the roadblocks

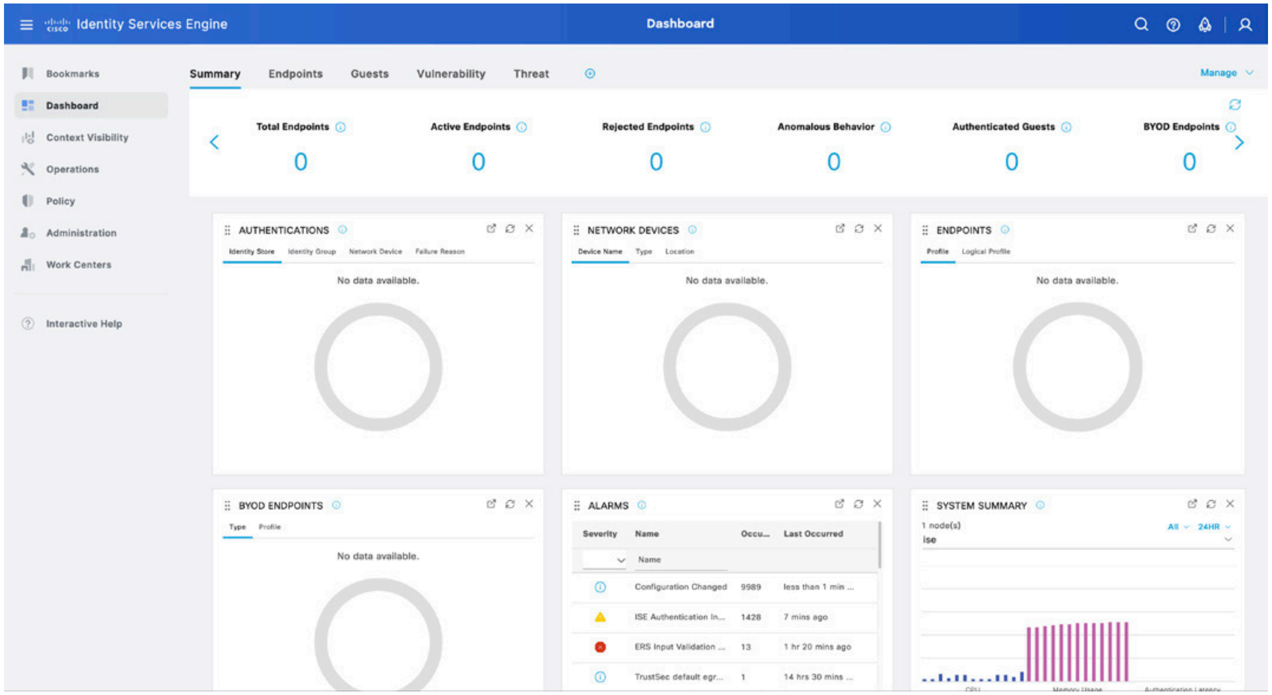
Not every customer has the most up-to-date end points–and this is especially true when it comes to IoT devices. Thanks to Cisco ISE Cipher Control, ISE provides the network admin with the ability to edit a list of ciphers that can be disabled so that customers can be compliant with the latest security standards. This is done with the option to select which ciphers should be ignored using authentication.

Simplified user experience

Guided workflows enable customers to quickly configure ISE for advanced secure access use cases. These simplified workflows allow organizational flexibility to adapt to changing organizational needs, and the threat landscape. No longer will IT be caught reacting to every market shift and instead will be able to take back control of the network. An immediate benefit of guided workflows is removing the complexity barrier to achieving network segmentation, a key component of the zero-trust framework.

Easy ISE: Ease the onboard experience for customers and guests

Granting access to guests has been made simple. Guest Auto-Login gives guests the flexibility to log in, without credentials, after sponsor approval, and we have made multiple enhancements to improve on the guest user experience.



Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests	BYOD Endpoints
0	0	0	0	0	0

AUTHENTICATIONS: No data available.

NETWORK DEVICES: No data available.

ENDPOINTS: No data available.

BYOD ENDPOINTS: No data available.

ALARMS

Severity	Name	Occu...	Last Occurred
ⓘ	Configuration Changed	9989	less than 1 min ...
⚠	ISE Authentication In...	1428	7 mins ago
✖	ERS Input Validation ...	13	1 hr 20 mins ago
ⓘ	TrustSec default egr...	1	14 hrs 30 mins ...

SYSTEM SUMMARY

1 node(s)

ise

The bridge to possible

Benefits of 3.x

- **Cloud-enabled visibility:** Extend interoperability into the cloud. Enhance visibility for access decisions. Embrace the flexibility required to be cloud-driven.
- **A simplified user experience:** A user experience with a focus on simplicity unlocks advanced use cases to rapidly accelerate value and protection.
- **Added flexibility:** Agentless posture and support for Endpoint Scripts allows the visibility required to ensure compliance. You no longer need to choose between the speed of delivery of services and protection.
- **Increased visibility through integration with AI Endpoint Analytics:** With AI-augmented visibility, customers can leverage machine learning to properly identify, classify, and verify device identification for effective policy management and network control.
- **Secure Access from the cloud:** Enable a cloud-driven approach to unifying visibility and control across campus and branch deployments with ISE from the cloud.

Learn more about Cisco Identity Services Engine

cisco.com/go/ise

Resources:

- ISE Solution Overview
- Dynamic Visibility AAG
- Visibility-Driven Segmentation AAG
- Automated Threat Containment AAG

Supporting documentation

- Release Notes
- Data Sheet
- Licensing FAQ
- End-User Documentation Hub