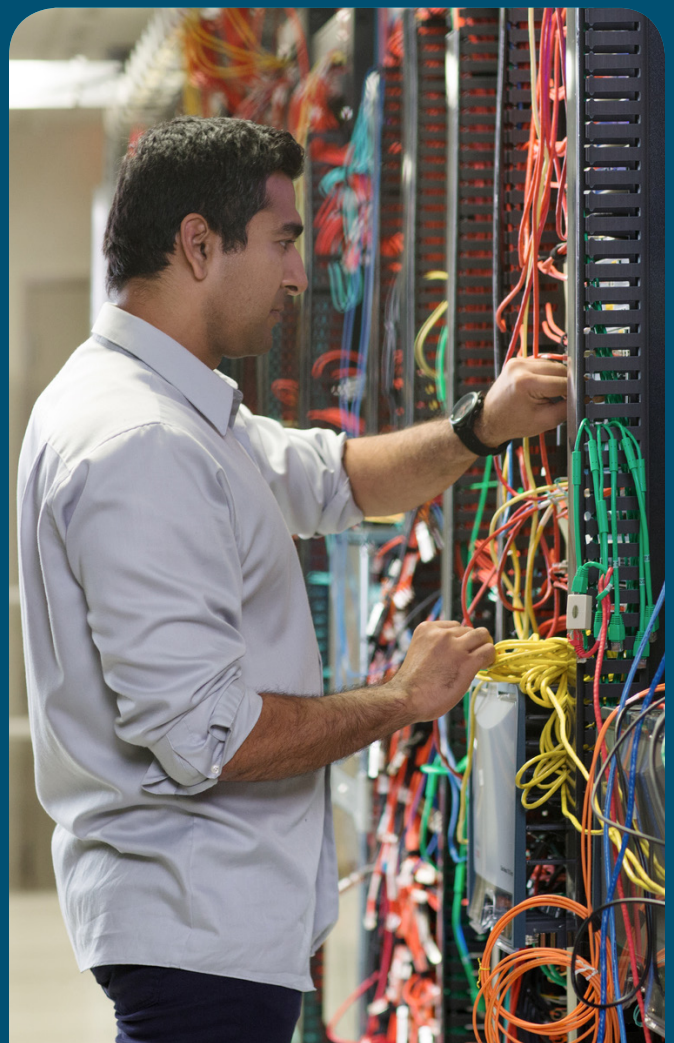
Cisco Identity Services Engine and Tanium—Better Together

Automated solution for network access control and comply to connect.

There is no silver bullet in IT security; however, many times a solution of point products working together can get you close, maybe silver plated. At Cisco, we see many customers deploy and maintain multiple security products, sometimes 40+ products, to achieve the goals, requirements, and mandates set forth by industry standards or internal and government policies. The common problem that we see with this approach is that the individual products do what they are designed to do well but work only within that "silo of excellence" and therefore lack visibility, enforcement, and execution that can be had with an integrated solution architecture. Cisco and Tanium have partnered together to bring an integrated architecture for network access and comply to connect.

To build an integrated architecture, the systems in use must do what they do well and integrate with other products not only from the same vendor, but also from third parties. The assumption that every security product will be from one vendor is not common or possible to cover all the required security requirements of our customers. Cisco realized that a common communication language was needed and created a new communication protocol to enable better integration and orchestration. Cisco® Platform Exchange Grid (pxGrid) protocol is designed around the assumption that multiple vendors will need the same information and should receive it in the same language at the same time.



ISE

Control all network access from one place

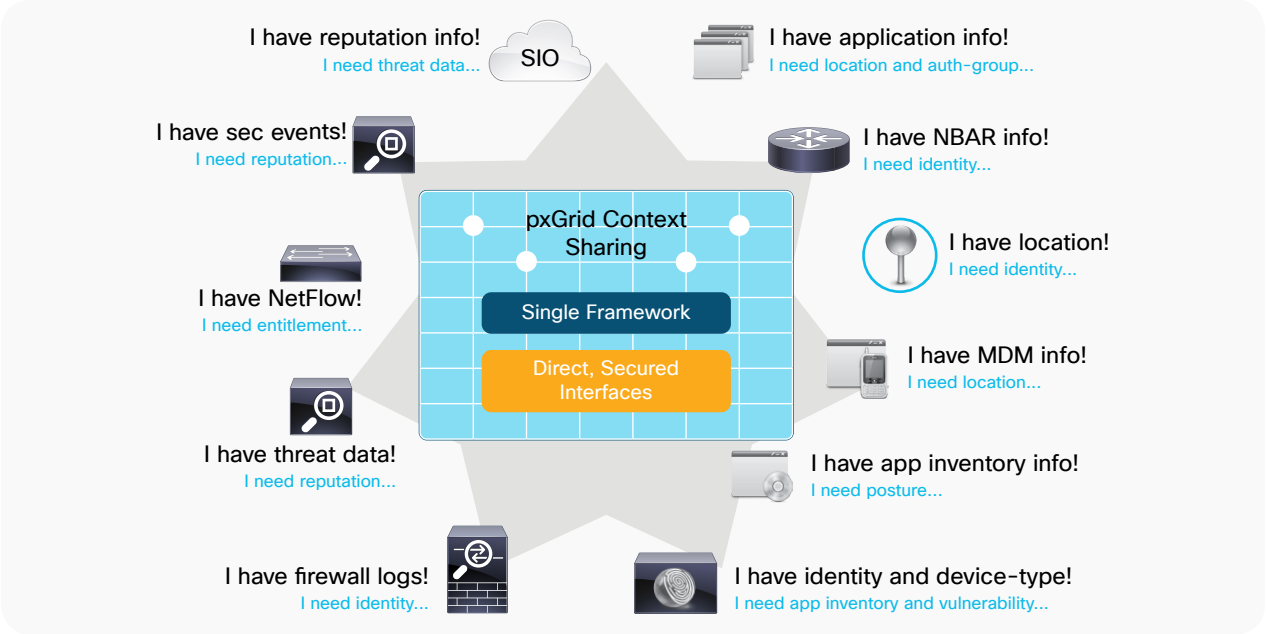
Simplify access across wired, wireless, and VPN connections. Policies are cascaded across all types of access points and software-defined segmentation.

Stop and contain threats

Reduce risks and contain threats by dynamically controlling network access. Identity Services Engine (ISE) can assess vulnerabilities and apply threat intelligence.

See and share rich user and device details

Users and devices are shown in a simple, flexible interface. ISE shares details through pxGrid with partner platforms to make them user, device, and network aware.



pxGrid works by using a publisher/subscriber framework with topics for multiple functions like the following.

- **Context sharing:** The session topic provides session context for each end device as it connects to the network and authenticates via 802.1X/MAB. The session notification shares information such as username, MAC address, device type/profile, assigned policy, Security Group Tag (SGT), and more. Subscribers to the session topic can ingest this data and use it for immediate attribution, passive authentication, and more.
- **Adaptive Network Control (ANC):** Quick and dynamic change on the network is the key to blocking threats and keeping the network secure. The ANC topic allows subscribers to enact policy-based network changes to individual endpoints based on triggers in the subscribers solution.
- **Context-In:** The pxGrid Context-In allows providers to publish context data into ISE for device context/profiling and threat information. The context published from the provider can then be used in policy for network access–level changes.
- **Dynamic topics:** Providers can develop their own topic for sharing of data of their choosing with other pxGrid consumers.

Tanium

Gain visibility

Complex, distributed networks reduce vision. Know your endpoints whether on-premises, cloud, or remote.

Unify teams

Resilience requires unity. Align security, risk, and operations teams around one common view of actionable data.

Operate with speed

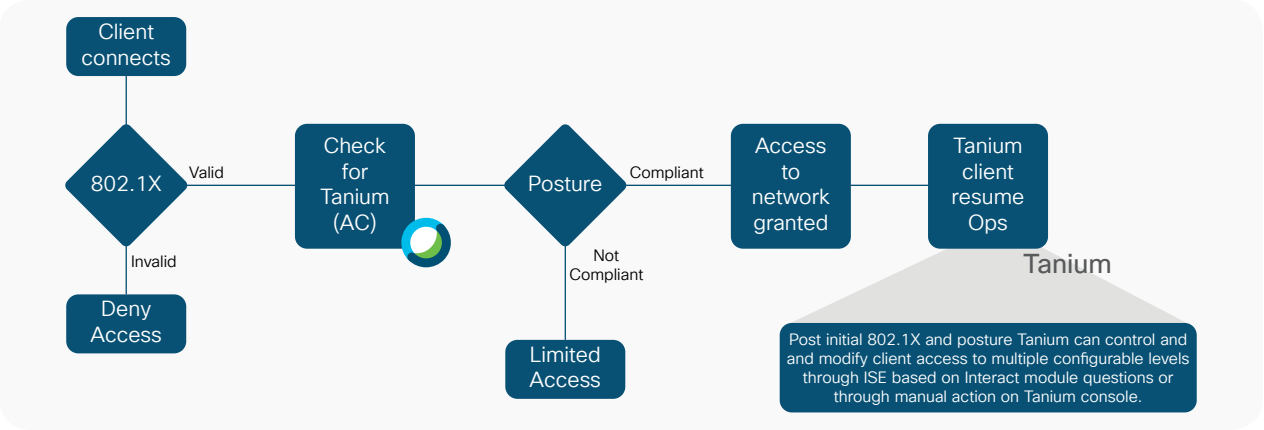
Act in an instant with confidence. Scale without slowing down in the world's largest, most complex environments.

C22-741641-00 12/18

Cisco ISE NAC with Tanium Discover, Interact, and Comply

Customers that have deployed Cisco ISE and Tanium now have the ability to seamlessly connect the two systems for automated threat control and containment using pxGrid ANC. Cisco ISE and Tanium's out-of-the-box ability provides orchestrated compliance enforcement at the onset of network access with ISE as well as continuous compliance and dynamic access control with Tanium.

Cisco ISE starts the process with authenticating the endpoint onto the network via 802.1X and/or MAB, or MAC Address Bypass, upon initial connection and periodically based on policy. After authentication with supported operating systems, the ISE compliance checks for and enforces the presence and status of the Tanium client. If the client is not running, it can be started, or if the client is not present, the endpoint is restricted from full access to the network and can be placed into a network segment where deployment can be performed. Once the endpoint is found in compliance with the Tanium agent requirements, it is then granted access to the protected network. After this initial interrogation, the Tanium client and server can communicate, and based on customer-defined policies and queries, Tanium can use pxGrid and ISE to set the appropriate network policy for that particular client.



The orchestration between the two platforms enables both products to do what they do best and work together through pxGrid to increase the capability and effectiveness of their platforms. As network security requirements change and evolve, the integration will enable the administrators of each platform to execute change and enforcement quickly and with confidence that both solutions will work together to deliver.

For more information, visit the following links

www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

www.cisco.com/c/en/us/products/security/pxgrid.html

https://docs.tanium.com/network_quarantine/network_quarantine/index.html