Cisco TrustSec 2.0

PB662693

Physical boundaries are disappearing. Businesses need to support a mobile workforce and manage outsourcers, all collaborating on a range of devices from PCs and tablets to smartphones. In addition, the changing IT landscape of virtualization and cloud computing demands a new definition of “identity,” and more effective protection for valuable information assets that may now reside off-premises. In this Borderless Networks environment, it becomes critical to establish visibility and appropriate access control for all users and devices.

Cisco TrustSec®, the security component of the Cisco Borderless Network Architecture, provides visibility into and control of who and what is connected to the network. Cisco TrustSec allows organizations to embrace the rapidly changing business environment of mobility, virtualization, and collaboration while enforcing compliance, maintaining data integrity and confidentiality, and establishing a consistent global access policy. Cisco TrustSec integrates with the Cisco SecureX Architecture™ to allow the Cisco security portfolio to take advantage of the network-based identity context for full context-aware firewalling and policy enforcement.

Cisco TrustSec 2.0 Customer Benefits

The Cisco TrustSec 2.0 system release enhances the flexibility of role-based access control for businesses by:

- Simplifying the management of security policy and access control for all users and access types - wired, wireless, and VPN
- Empowering users to securely collaborate on any device, including consumer IT devices like smartphones and tablets
- Enabling comprehensive support of all user needs via complete security lifecycle services, from guest access to security posture, and profiling
- Delivering and expanding on authorization and segmentation solutions that address compliance requirements
- Using the Cisco networking infrastructure as the secure, resilient, and scalable foundation for role-based access control

Cisco TrustSec 2.0 Solution Highlights

Table 1 describes the solution highlights in Cisco TrustSec 2.0.

Table 1. Solution Benefits for Cisco TrustSec 2.0

Features	Description	Benefits
Unified Policy with Cisco Identity Services Engine Software 1.0	The Cisco Identity Services Engine offers centralized policy creation and provisioning for all network access scenarios - wired, wireless, and VPN. With the convergence of Cisco Network Admission Control (NAC) Manager and Server, NAC Guest Server, and Cisco Secure Access Control Server (ACS) into the same appliance, Cisco TrustSec deployments and the decision to deploy overlay or infrastructure integrated mode is now simplified.	All-in-one-access and policy platform for better operational efficiencies.
Complete Lifecycle Services: • Integrated profiling • Posture • Guest access	The following Lifecycle Services are integrated on the Identity Services Engine: • New integrated profiling capabilities automate the identification of wired and wireless devices, from smartphones and tablets to printers and IP phones, enabling organizations to define an access policy for categories of devices. • Posture support with 802.1X helps to ensure that endpoints do not become a threat vector. • Guest access features such as sponsor portals and guest access configuration provide flexible access control options for guests, including limiting the duration of access or restricting guests to Internet only access. This capability is now integrated within the Identity Services Engine along with the other Lifecycle Services.	Integrated Lifecycle Services on the same platform enables operational simplicity in deployments and support of user needs.
Security group access expanded platform and deployment support	Security group access - the scalable, flexible method to authorize and enforce users and devices in the network through their roles - now expands to support authorization at the aggregation and WAN layer. • Tagging and enforcement (Security Group Tags (SGT) and Security Group Access Control Lists (SGACL)) are now supported on the Cisco Catalyst® 6000 Series Switches enabling policy enforcement at the campus aggregation layer. • Tagging and control plane propagation of the roles (Security Exchange Protocol (SXP) and Security Group Tagging (SGT)) on the Cisco ASR 1000 Series Aggregation Services Router platforms expand authorization for extranet or WAN aggregation use cases. In addition, security group access is supported in Cisco Virtual Desktop Infrastructure (VDI) environments as well. VDI users are tagged in the data center after authentication, and enforcement restricts access to the appropriate virtual or physical data center assets.	Simplified, topology-independent method of authorizing branch and extranet users.
Wireless 802.1X enhancements	In addition to the ability to profile wireless devices in the network, wireless deployments now support RADIUS change of authorization (CoA) methods to authorize users to access the network after meeting security policies.	Flexible security services and authorization for wireless users.

Cisco TrustSec 2.0 Product Components and Features

Table 2 summarizes the products and features available in Cisco TrustSec 2.0.

Table 2. Cisco TrustSec 2.0 Releases

Product/Component	Feature Details	Release and Availability
Identity Services Engine	• Platforms: 1121/3315 3355/3395 Vmware • Integrated authentication, authorization, and accounting (AAA) policy server. 802.1X with guest, profiler, and posture services on the same appliance	Identity Services Engine Software 1.0
Catalyst 2960 and 3750/3560 Series	• Platforms: 2960, 2960S - Identity features include 802.1X authentication, MAB (MAC Authentication Bypass), multi-authentication, multi-domain authentication, flex authentication, CoA • Platforms: 3560, 3560E, 3560X, 3750, 3750E, 3750X - 802.1X authentication, MAB (MAC Authentication Bypass), multi-authentication, multi-domain authentication, flex authentication, CoA, SXP	Cisco IOS® Software Release 12.2.55SE3
Catalyst 6500 Series*	• 802.1X authentication, MAB (MAC Authentication Bypass), multi-authentication, multi-domain authentication, flex authentication, CoA, SXP	12.2(33)SXI7 (SUP 32/SUP 720)
	• Features in SXI7 and SXP IPv6, VRF Aware support	12.2(33)SXJ1 (SUP 32)*
	• Security Group Access: SXP, SGT, SGACL	12.2(50)SY (SUP2T)
Nexus 7000 Series	• Security Group Access: SXP, SGT, SGACL	5.2.1
Cisco Secure Access Control System	• FIPS 140-2 Level 1 compliance • Windows 2008 R2 support for authentication and authorization • Internet Explorer 8 support for Administrator Interface • SHA-256-signed CA certificate support • Cryptographic module enhancements for FIPS - RADIUS key wrap (Key Encryption Key (KEK) and Message Authentication Code Key (MACK)), key zeroization	Cisco Secure Access Control System 5.2 (shipping)
Cisco AnyConnect™ Secure Mobility Client	Integration of 802.1X supplicant and MACSec supplicant	Cisco AnyConnect 3.0
Cisco ASR 1000 Series Aggregation Services Routers	SGA (Security Group Access) integration; SXP	Cisco ASR 1000 Series 15.1(3)S (XE 3.4.0)
Cisco Wireless LAN Controller	• Profiling with wireless • Enforcement on Cisco Wireless LAN Controller instead of inline Policy Enforcement Point (PEP)	Cisco Unified Wireless Network Software Release 7.0 MR1 (7.0.116)

* For Catalyst 6500 Series, SUP 720 will be validated in the next TrustSec release, which is TrustSec 2.1.

Note:

- TrustSec 2.0 and systems testing provides validated use cases, features and platforms for a specific systems release. Features not included in TrustSec 2.0 may still be supported on platforms, but not validated at the systems level.
- The Cisco Catalyst 4500 Series is not supported in TrustSec 2.0 due to features/image availability during systems testing timeframes. The Catalyst 4500 Series platforms will be supported in the TrustSec 2.1 systems release.

Upgrade Paths

The Identity Services Engine comes with a migration tool that assists customers in migrating from Cisco Secure Access Control System 5.X deployments to Cisco Identity Services Engine. For details, please refer to the Identity Services Engine migration documents.
http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html.

Also, note that the Cisco Identity Services Engine is only available under the Cisco Authorized Technology Provider program.

To upgrade to a new release of Cisco IOS Software, please refer to the switch migration documents.

Ordering Information

To place an order, visit the Cisco Ordering Tool. To download software, visit the Cisco Software Center.

Cisco Services

Cisco Services makes networks, applications, and the people who use them work better together.

Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

For More Information

For more information about the Cisco TrustSec solutions, visit http://www.cisco.com/go/trustsec or contact your local account representative.

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 www.cisco.com/go/offices.

Printed in USA C25-662693-03 03/12