Secure Mobility

Klaus Lenssen

Senior Business Development Manager Security

Complete Your Online Session Evaluation

Please complete the online evaluation under

www.cisco.at/expo2008/feedback

The first 100 to complete the survey will receive a copy of Don Tapscott´s book “Wikinomics”.

We very much appreciate and value your feedback, many thanks!

Business in Motion

Business Mobility Requirements Differ from Consumer Mobility

Secure, manage and audit **device** usage/policies/access

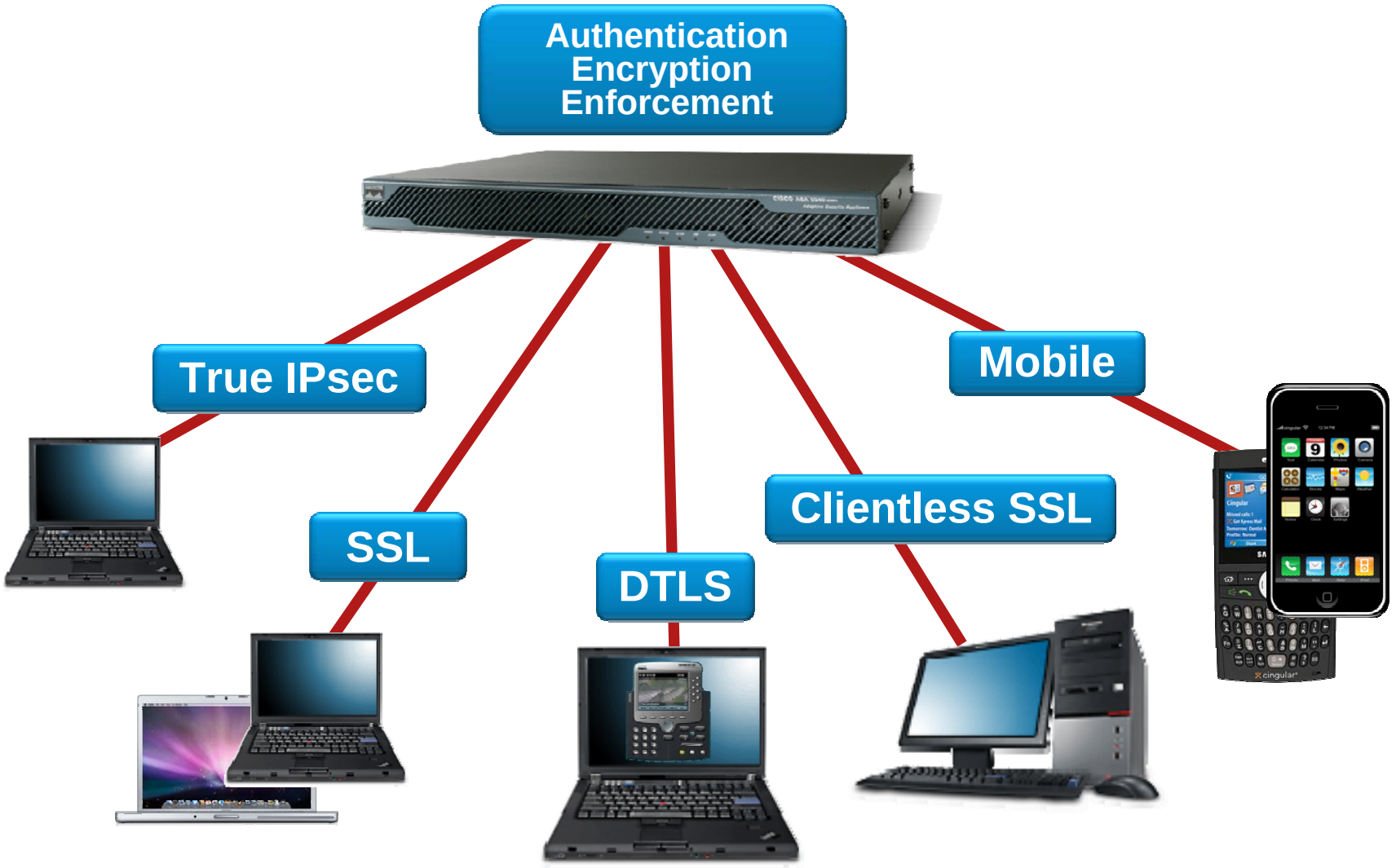
Integrate multiple **networks** from personal to private to public

Enable **applications** to securely access information across multiple networks

Enforce role-aware **user** experience irrespective of connection

Anytime, Anywhere over Any Network: Not exactly…. rather Right Application, Right User, Right Policies

Unified Secure Access

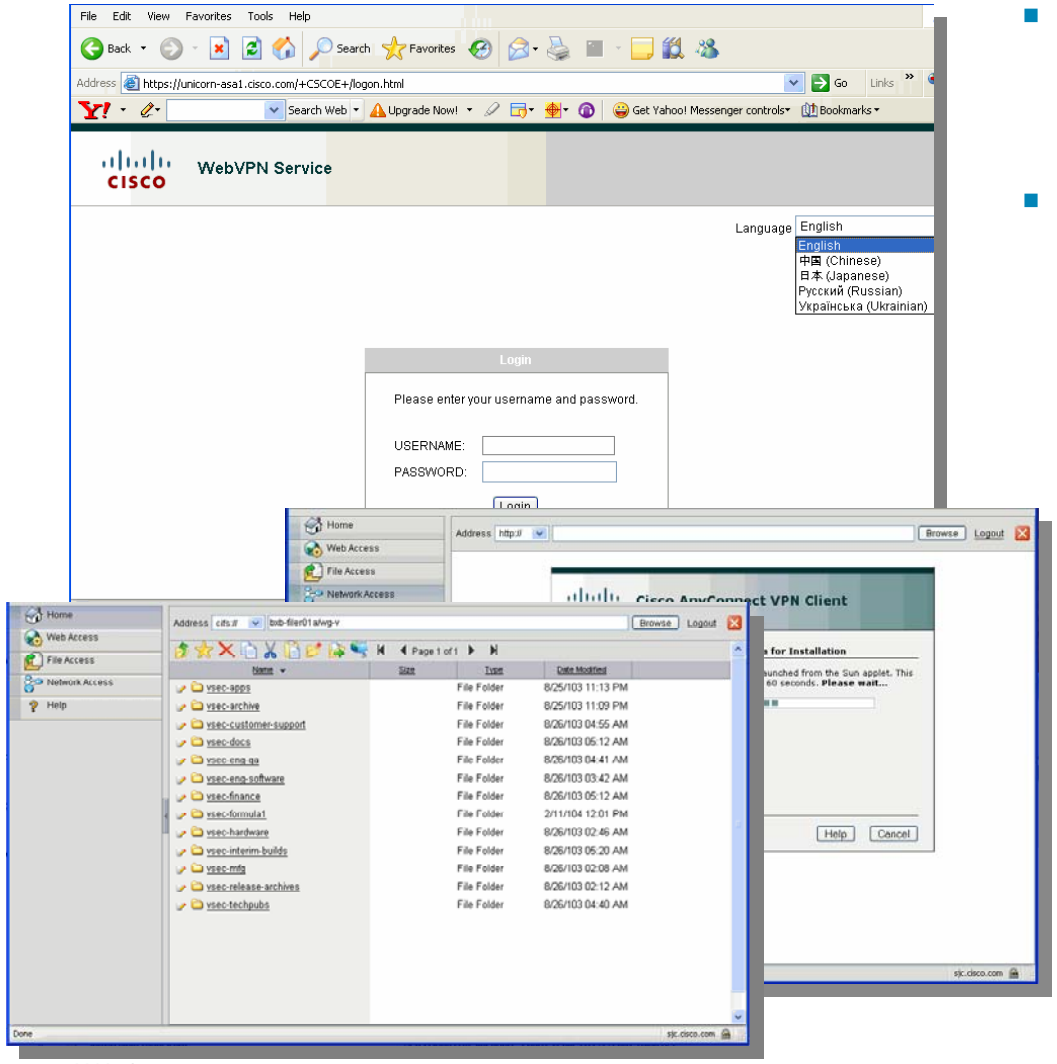


Cisco Security on iPhone

- **Cisco VPN technology**
- **Integrated in iPhone**
- **Secure intranet access**
- **Critical applications**
- **Cisco ASA and PIX**

For End-Users, Seamless Access Anywhere

Personalized application and resource access



- **Personalized homepage**

  Localizable, RSS feeds, personal bookmarks, etc.

- **Delivers web-based and traditional applications**

  Sophisticated web and other applications delivered seamlessly to the browser

  SAML Single Sign-On (SSO) – verified with RSA Access Manager

Intuitive user experience

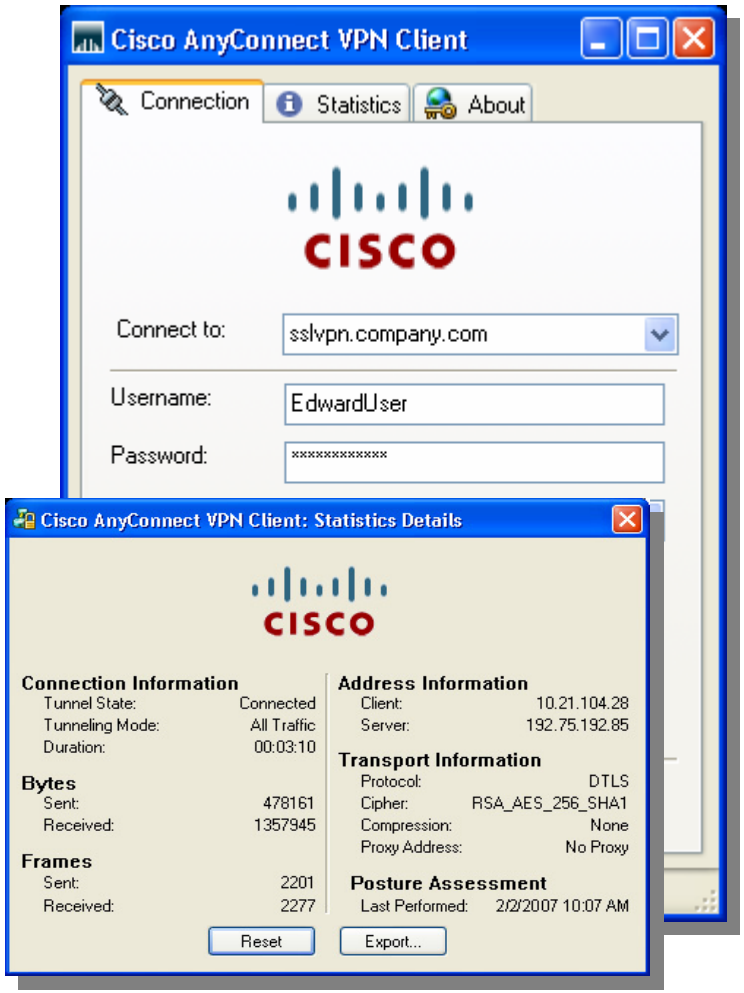
Drag and Drop file access and webified file transport

Delivers key applications beyond the browser

Smart Tunnels deliver more applications without admin privileges

For End-Users, Access for All Applications

Cisco AnyConnect VPN Client for secure remote productivity



- **Extends the in-office experience**
  - LAN-like full-network access, supports latency sensitive apps like voice (via DTLS transport)
- **Access across platforms**
  - Windows 2K / XP (x86/x64) / Vista (x86/x64)
  - Mac OS X 10.4 & 10.5, Linux Intel
  - Windows Mobile 5 Pocket PC Edition (Coming soon)
- **Always up to date**
  - Remotely installable and configurable to minimize user demands
- **No-hassle Connections**
  - No reboots required
  - Stand-alone, Web Launch, Portal Connection
  - Start Before Login (2K/XP)
  - MSI – Windows Pre-installation package

For End-Users, Access for All Applications
Datagram Transport Layer Security (DTLS)

- **Limitations of TLS (HTTPS/SSL) with SSL VPN tunnels**

  TLS is used to tunnel TCP/IP over TCP/443

  TCP requires retransmission of lost packets

  Both application **and** TLS wind up retransmitting when packet loss is detected.

- **DTLS solves the TCP over TCP problem**

  DTLS replaces underlying transport TCP/443 with UDP/443

  DTLS uses TLS to negotiate and establish DTLS connection (control messages and key exchange)

  Datagrams only are transmitted over DTLS

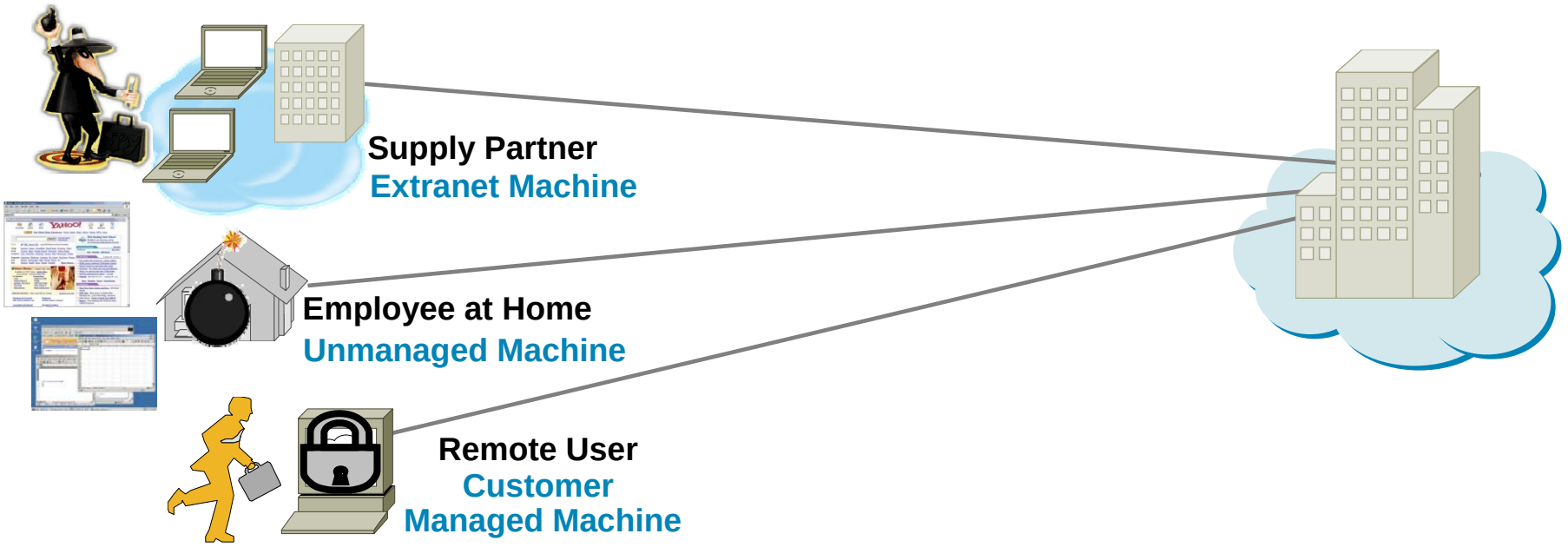
- **Other benefits**

  Low latency for real time applications

  DTLS is optional and will automatically fallback to TLS (HTTPS)

Unique Security Challenges on the Endpoint

SSL VPN Brings New Points of Attack



Before SSL VPN Session

- Who owns the endpoint?
- Endpoint security posture: AV, personal firewall?
- Is malware running?

During SSL VPN Session

- Is session data protected?
- Are typed passwords protected?
- Has malware launched?

Post SSL VPN Session

- Browser cached intranet web pages?
- Browser stored passwords?
- Downloaded files left behind?

Cisco Secure Desktop (Secure Vault)
How it Works

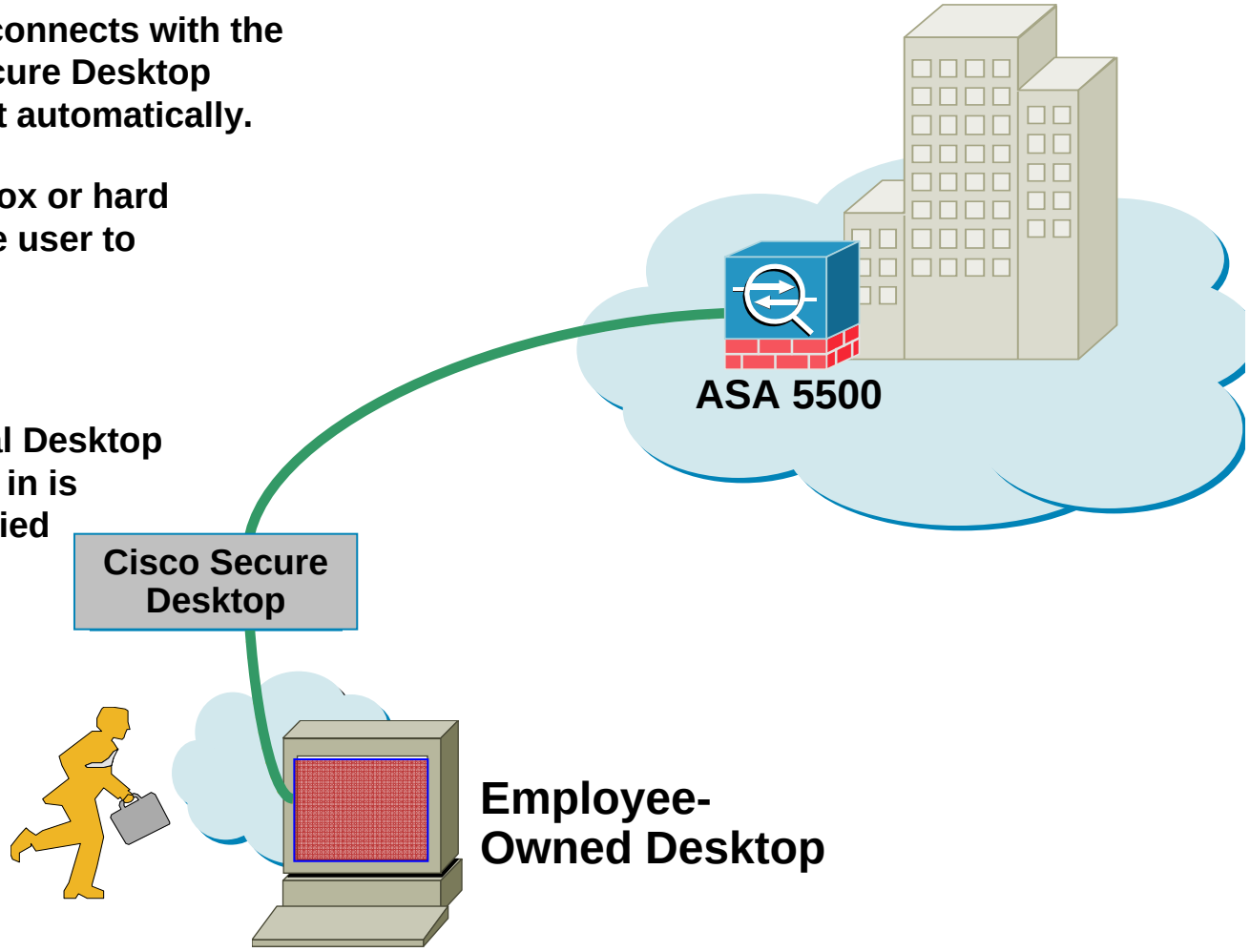
Step One: A user on the road connects with the concentrator and the Cisco Secure Desktop is pushed down to the endpoint automatically.

Step Two: An encrypted sandbox or hard drive partition is created for the user to work in

Step Three: The user logs in

Step Four: At Logout the Virtual Desktop that the user has been working in is eradicated and the user is notified

Note: CSD download and eradication is seamless to the user. If the user forgets to terminate the session auto-timeout will close the session and erase session information



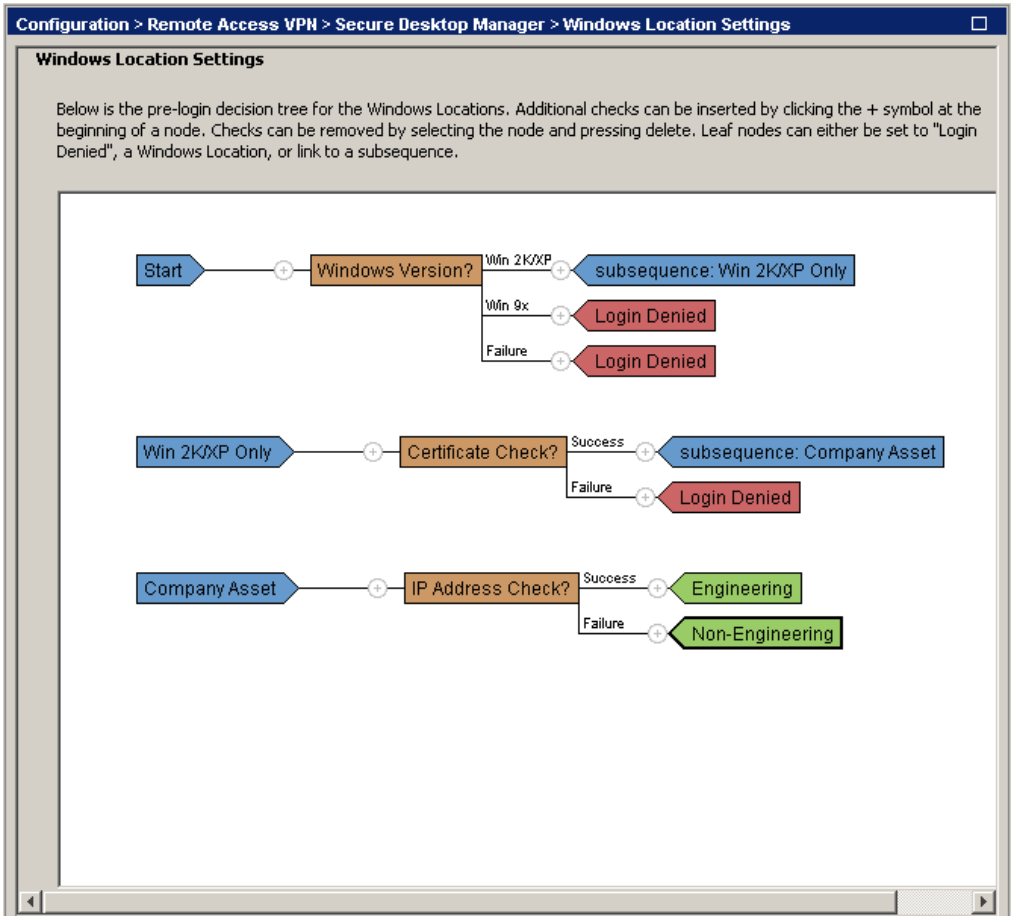
Comprehensive EndPoint Security

- Cisco Secure Desktop (CSD) now supports checking for hundreds of pre-defined products, updated frequently
  - Anti-virus, anti-spyware, personal firewall, and more
- Administrators can define custom checks including running processes
- Posture policy presented visually to simplify configuration and troubleshooting (Pre-login sequence and Dynamic Access Policies)
- Cisco Secure Desktop consists of four features:
  - Host Scan (Windows)
  - Advanced Endpoint Assessment provides remediation and periodic rechecking capabilities (licensed option)
  - Secure Vault (Windows 2K/XP)
  - Cache Cleaner (Windows, Mac OS X, and Linux)

Cisco Secure Desktop

Pre-login Decision Tree

- Supported Checks
  - Registry check
  - File check
  - Certificate check
  - Windows version check
  - IP address check
- Leaf Nodes
  - Login denied
  - Location
  - Subsequence
- Visual policy simplifies administrative configuration



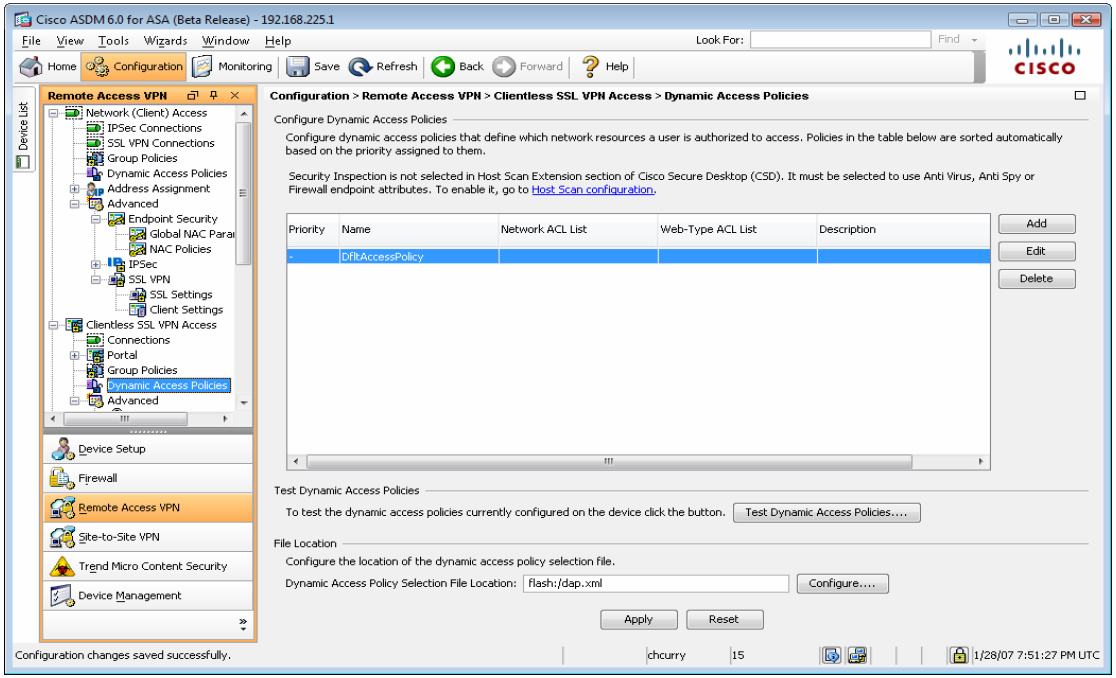
Comprehensive EndPoint Security Dynamic Access Policies (DAP)

The Dynamic Access Policy (DAP) is defined as a collection of access control attributes associated with a specific tunnel or session.

The DAP is dynamically generated by selecting and/or aggregating attributes from one or more DAP records.

The DAP records are selected based on the **endpoint security information** of the remote device and/or the **AAA authorization information** of the authenticated user.

DAP will be generated and then applied to the user's tunnel or session.



Cisco SSL VPN Summary

Simple and Secure Access from Anywhere

- Broad access from anywhere
- User-friendly interfaces
- World-class security
- Flexible, controlled access options
- Intuitive management
- Fully integrated with the Cisco Self-Defending Network

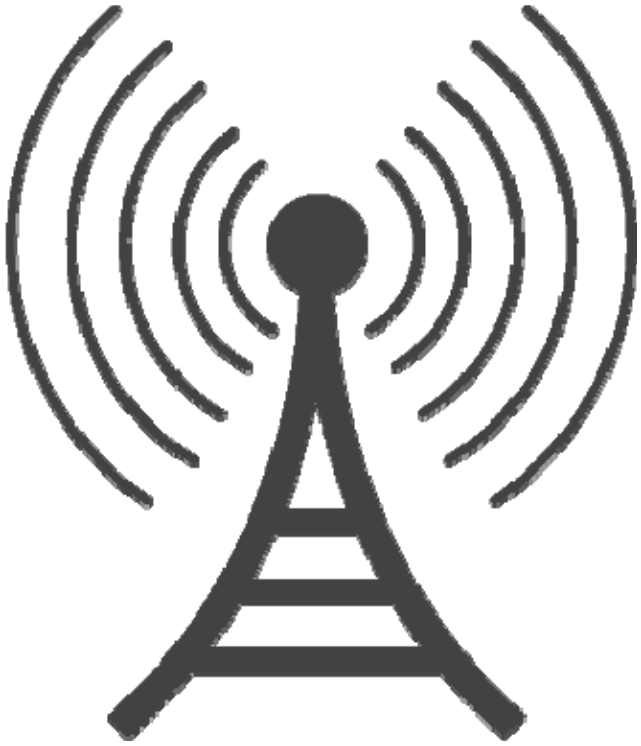
www.cisco.com/go/sslvpn

Secure Guest Access

The Enterprise Hotspot

Enterprises are the most important hotspot destination for business partners in a connected world.

- Provide network access to visitors
- Presents a professional and secure access to visitors
- Enable improved productivity from vendors and contractors
- Strengthen collaboration between employees and partners



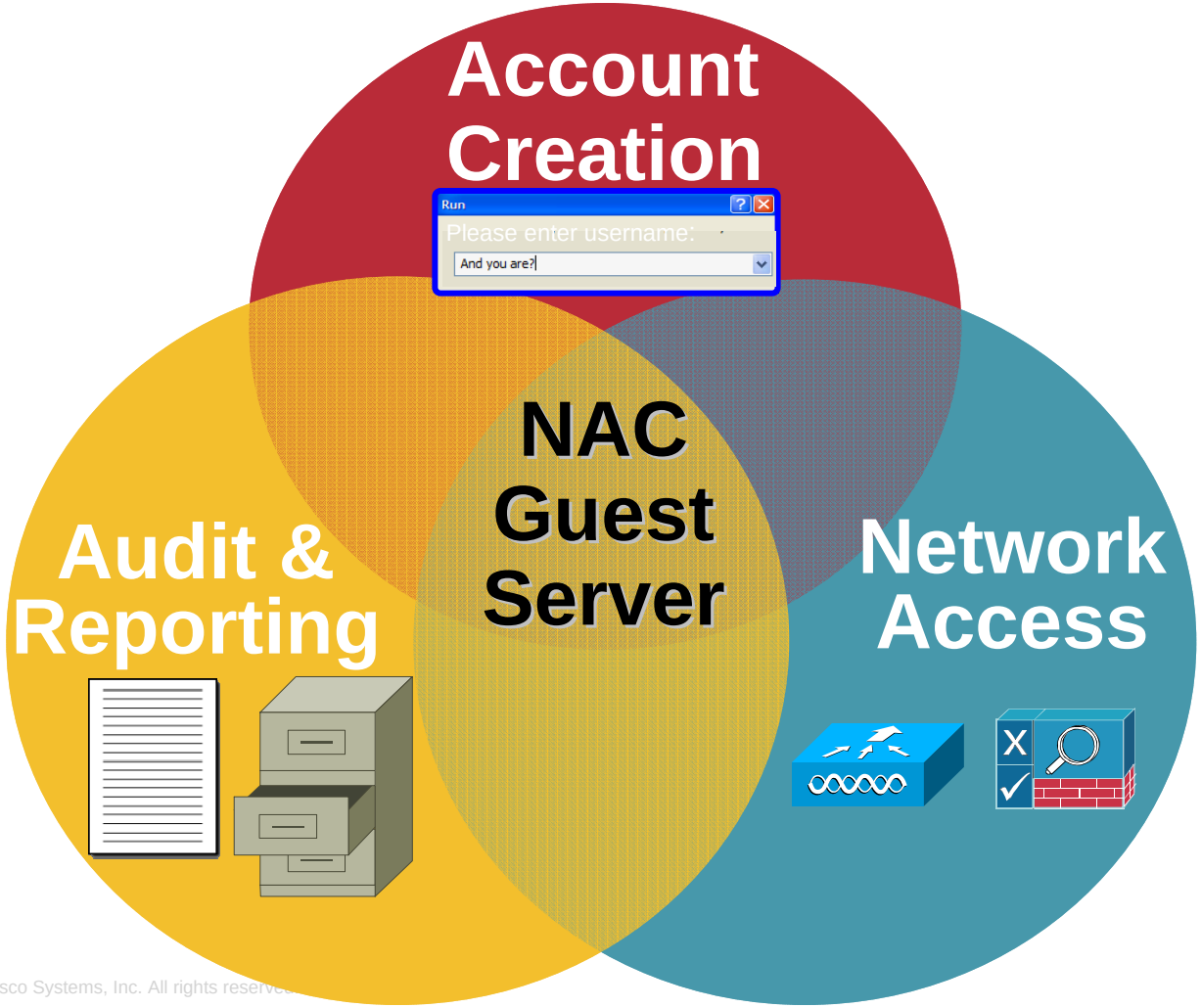
Provide Guest Access in a seamless, secure manner

Guest Access Considerations

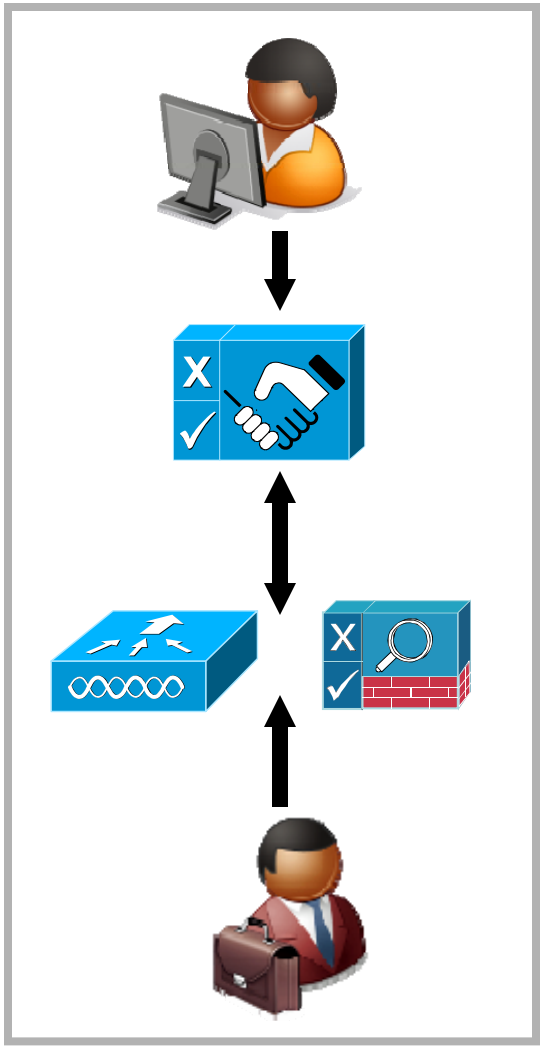
Ease of use	Provisioning of user accounts Receptionist, help desk, any user
Integration with network infrastructure	Reduce infrastructure upgrades Avoid parallel network infrastructure
Auditing and accountability	Know who is doing what Know who created which account
Cost	Cost of implementation Cost of ongoing management

Delivering Guest Access

Cisco NAC Guest Server Unites guest access functions



Four Key Components of Guest Access



SPONSOR

The internal user who wants to be able to provide internet access to their guest

NAC GUEST SERVER

Enables sponsor to create guest account; audits; provisions account on network enforcement device

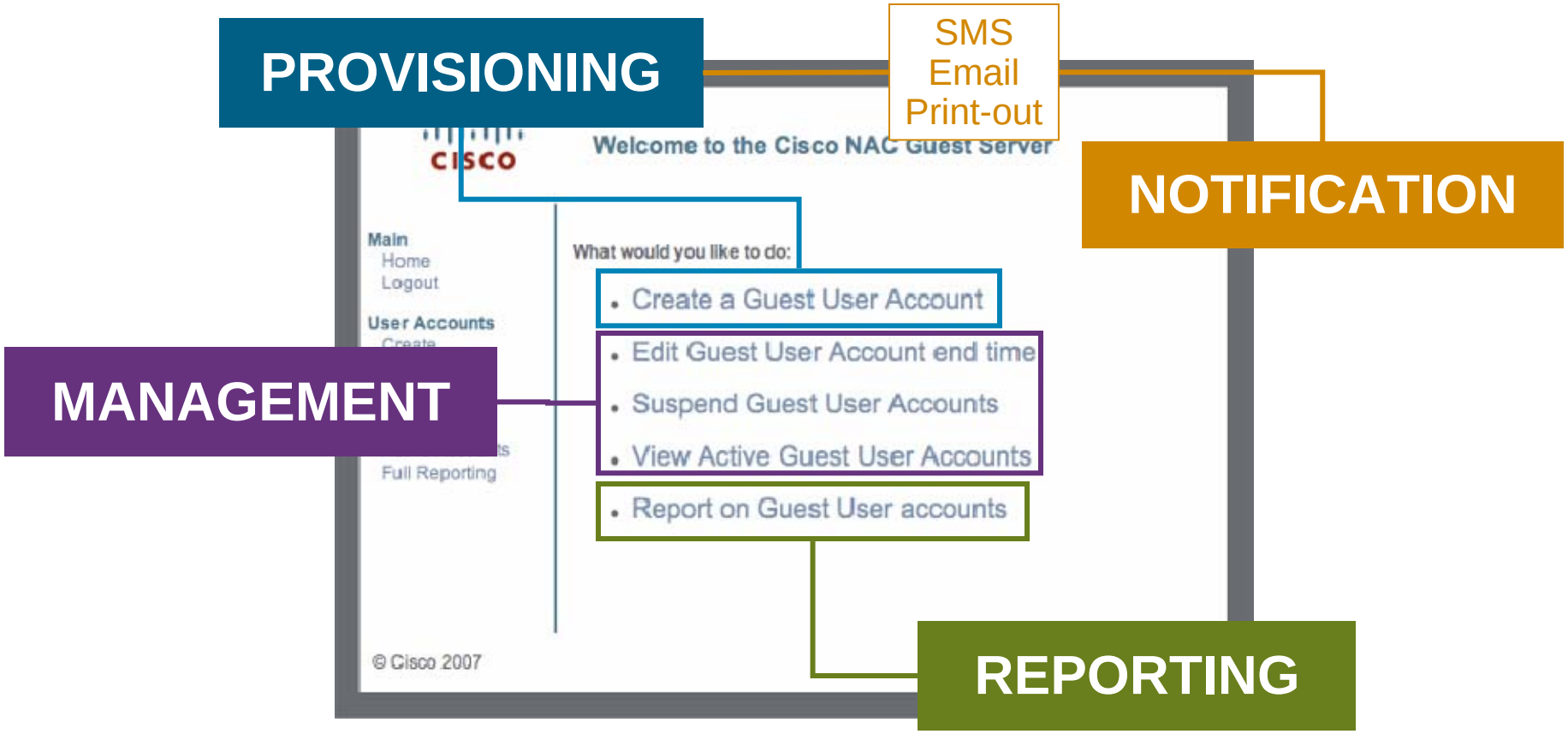
NETWORK ENFORCEMENT DEVICE

Web re-direction, authentication and provides access. Wireless LAN Controller or NAC Appliance

GUEST

The visitor who needs network access (usually internet only, but could be more)

Managing the Guest User Lifecycle



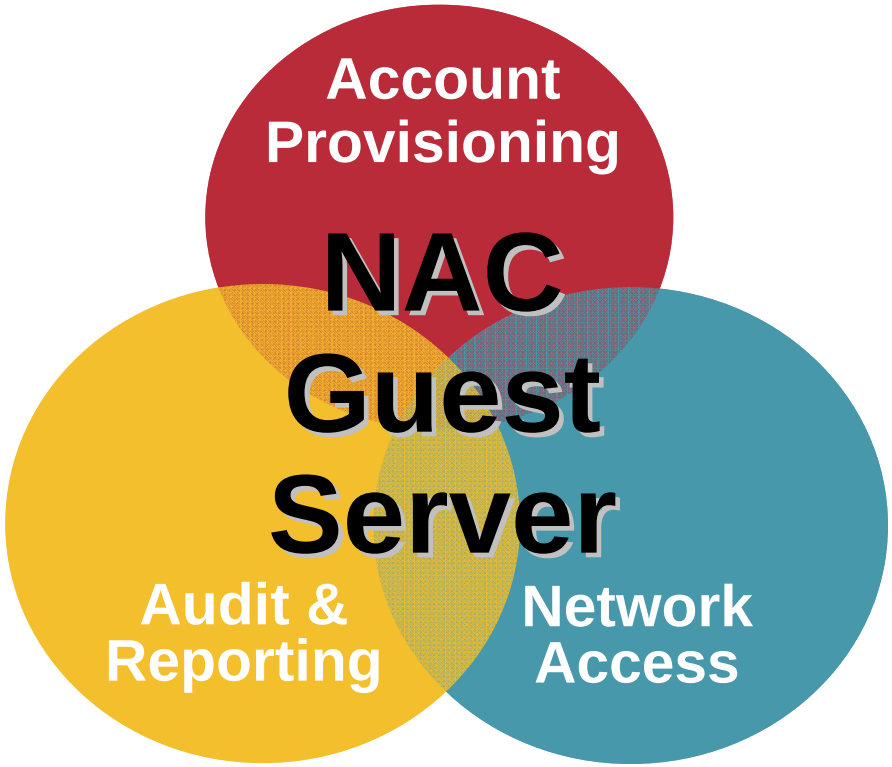
Provisioning

- Who should create user accounts?
  - Receptionist/Lobby Ambassador
  - IT Security
  - Managers
  - Anyone
- NAC Guest Server lets you choose based upon your security policy
- Allowing anyone to create accounts provides increased usage and will be just as secure

- Reduced Cost
- Full Audit Trail
- Speed of access
- Ease of use

Summary

- Providing Guest Access brings increased
  - Collaboration
  - Productivity
  - Cost Savings
- Security is paramount
  - Accountability
  - Audit
- Cisco NAC Guest Server integrates Guest Access
  - Ease of Provisioning
  - Network Integration
  - Audit and Reporting

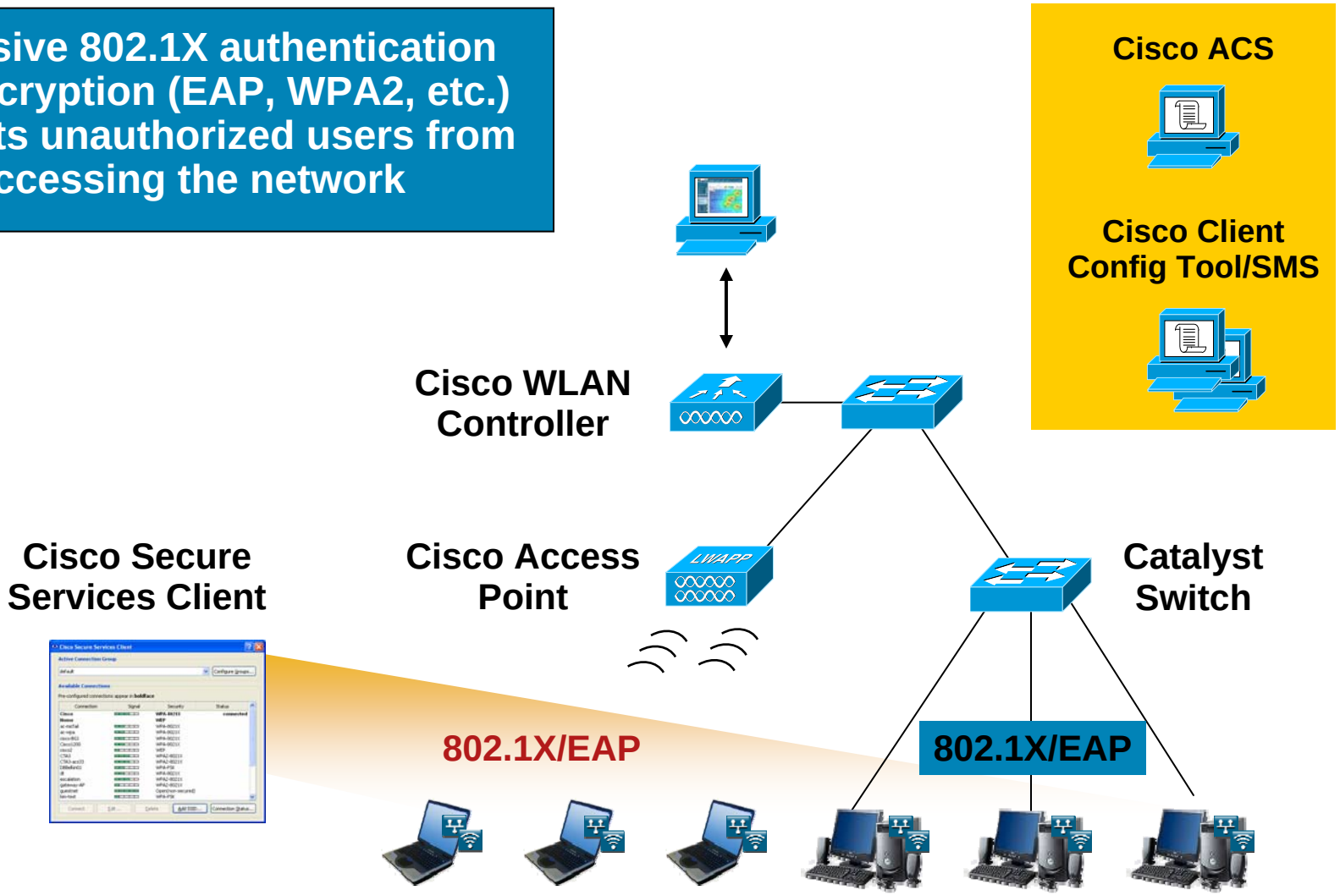


- Unifies guest access across Cisco NAC Appliance and Cisco Wireless LAN Controllers

Cisco Secure Services Client 5.1

Network Architecture

Extensive 802.1X authentication and encryption (EAP, WPA2, etc.) prevents unauthorized users from accessing the network



Introducing Cisco Secure Services Client

Secure and Managed Connectivity to Wired and Wireless Networks

- Client Services:

  Mobility, Security, Management, Identity & Cisco Compatible Extensions

- Key Features:

  802.1X authentication for wired and wireless devices

  Broad support for encryption and authentication standards

- Target Customers:

  Enterprises with wired and wireless devices

Single Client for Uniform Security & Services

- Cisco Solution Support:
  - **Network Admission Control**
  - **Cisco Secure ACS**
  - **Identity Based Network Security**
  - **Cisco Unified Wireless Network**

Cisco Secure Services Client

Features

- Unified wired and wireless client
- Support for industry standards
- Endpoint integrity
- Single sign-on capable
- Enabling of group policies
- Administrative control

Benefits

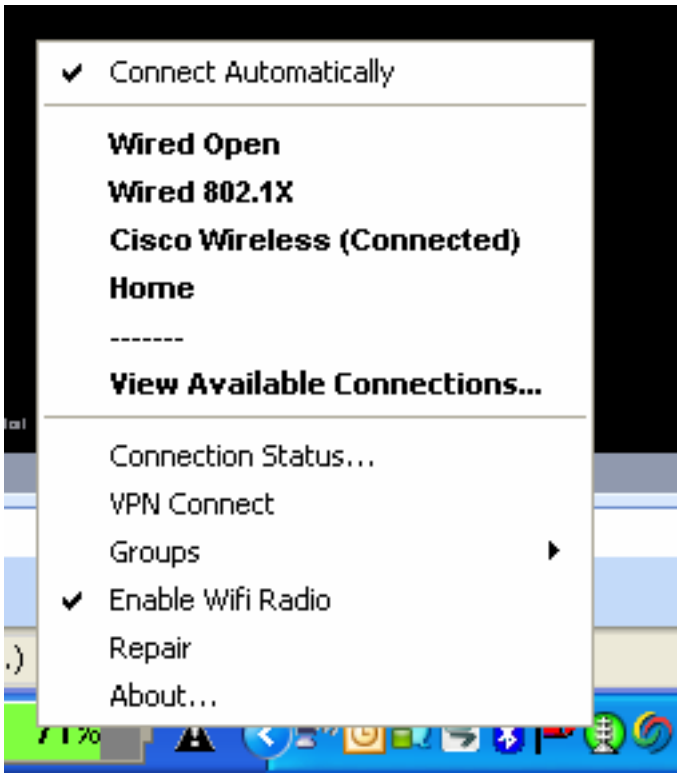
- Reduces client software
- Simple, secure device connectivity
- Minimizes chances of network compromise from infected devices
- Reduces complexity
- Restricts unauthorized network access
- Centralized provisioning

Drivers for Cisco Secure Services Client

What End Users want	Balancing the Needs of End Users and IT Administrators	What IT Administrators need
Intuitive - Easy to configure & use		Adhere to enterprise security policies
Immediate access to network without intervention		No user tampering - No override
Connectivity at office, home and public hotspots		Easy to Manage – Easy to Deploy
Status at a glance		No Wireless When Wired
Manage from the tray icon		

Simple User Interface

- Most user interaction done from the tray icon
- Users manage home and roam profiles - IT manages office profile
- Users are unable to override the office profile
  - All deployed profiles are locked
  - 802.1X profiles are deployed and not configurable by the user
- Two Click Connect to an open beaconing access point - Eliminates the need for the insecure and cumbersome "ANY" SSID

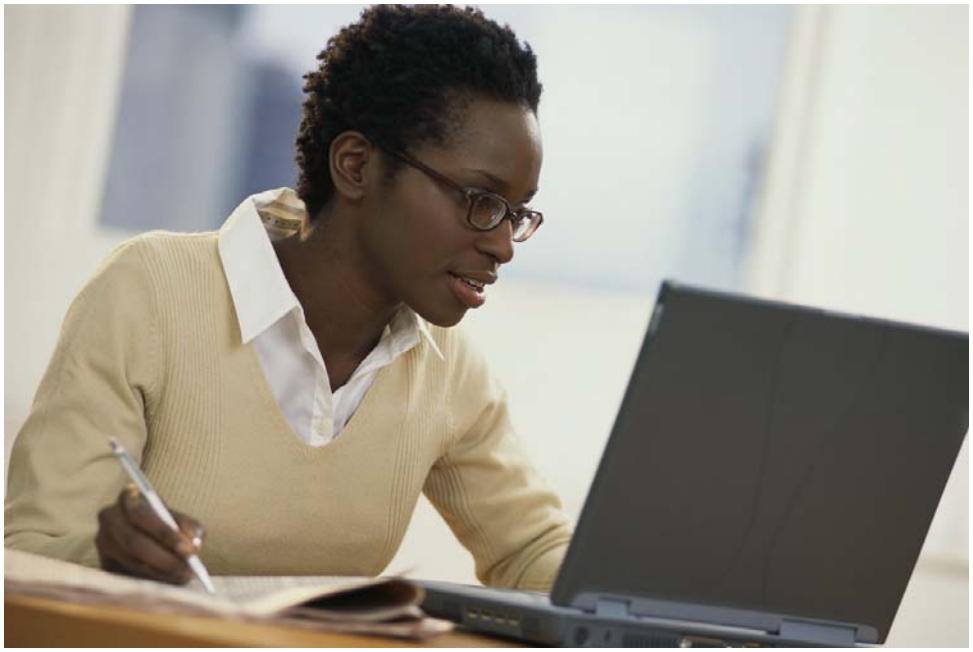


Campus Settings

- Moving from building to building
  - Walking outside
  - Enclosed walkways
  - Driving
- Laptop – Fully powered, suspended or hibernating
- Goal - Resume connection without having to re-enter credentials but do not keep sessions overnight

No Wireless When Wired

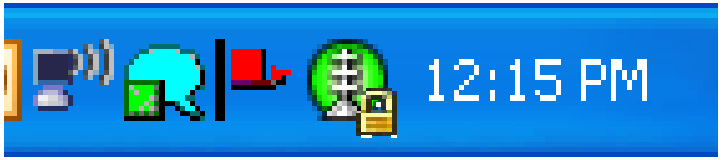
- Prefer wired when in automatic mode
- Override with manual mode
- One connection at a time



Home / Open Hotspot

VPN Not Active

VPN Active



- Automate the user experience – set it up once
- Automatically connect to the SSID (open, WPA-Personal, etc.)
- Prompt for VPN credentials and connect without requiring the user to open the VPN Client
- Remember the VPN credential until logout