



# Securing Complexity with NAC Appliance (Cisco Clean Access): A Technical View

**NAC Appliance Technical Marketing Team**  
**June 2006**

# Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
4. **NAC Appliance Technical Benefits**

# The Challenge of Securing Complexity

This is a story about network security.



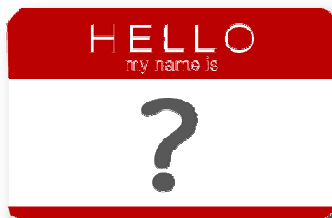
Specifically, how you can have compromising productivity.



security without

More to the point, your company may already be bristling with network defenses, but you still have one glaring vulnerability—

**your network users.**



# Productivity Causes Complexity



WHAT SYSTEM IS IT?

Windows, Mac or Linux  
Laptop or desktop or PDA  
Printer or other corporate asset

WHO OWNS IT?

Company  
Employee  
Contractor  
Guest  
Unknown

WHERE IS IT COMING  
FROM?

VPN  
LAN  
WLAN  
WAN

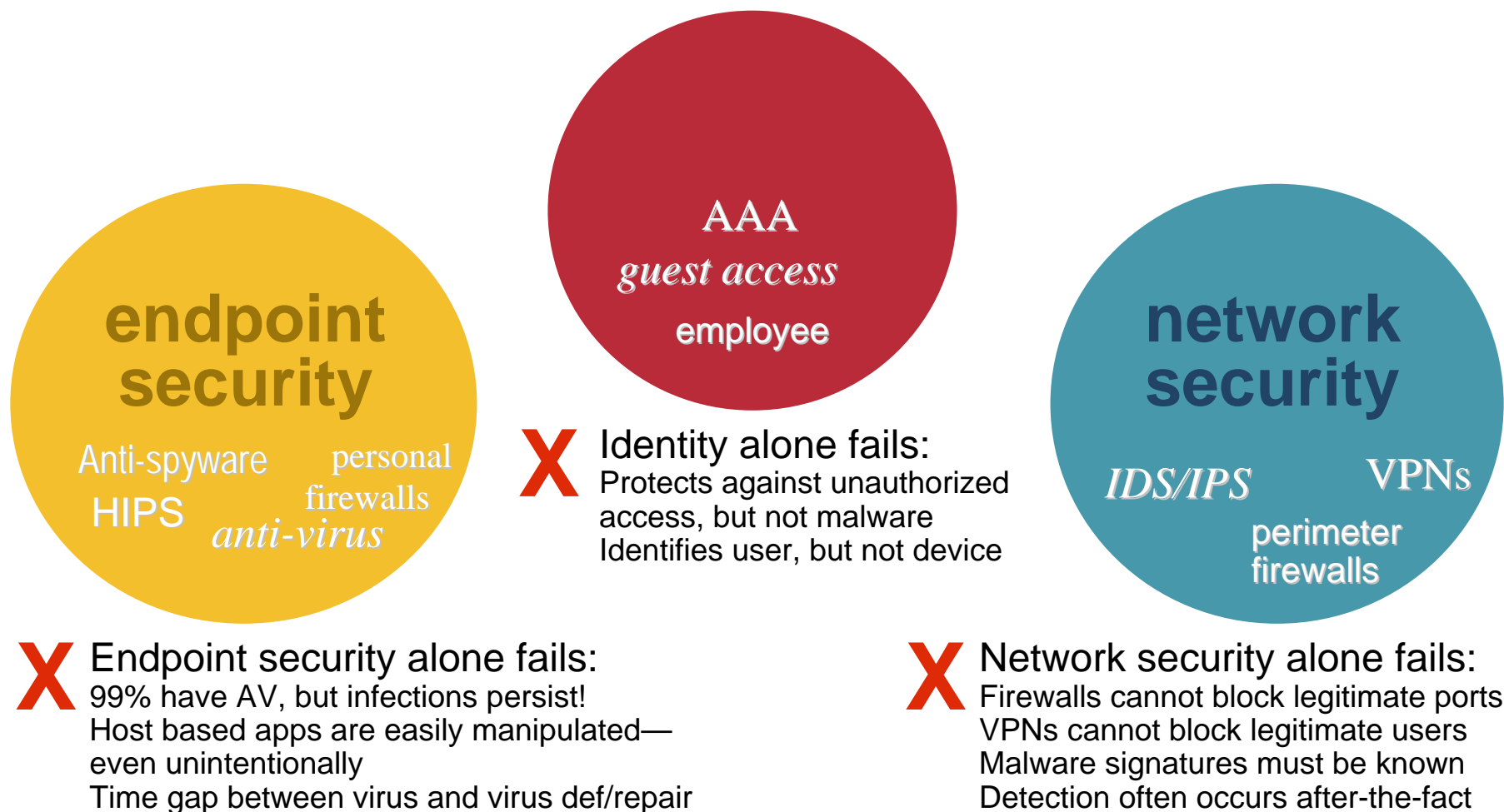
WHAT'S ON IT?  
IS IT RUNNING?

Anti-virus, anti-spyware  
Personal firewall  
Patching tools

WHAT'S THE PREFERRED  
WAY TO CHECK/FIX IT?

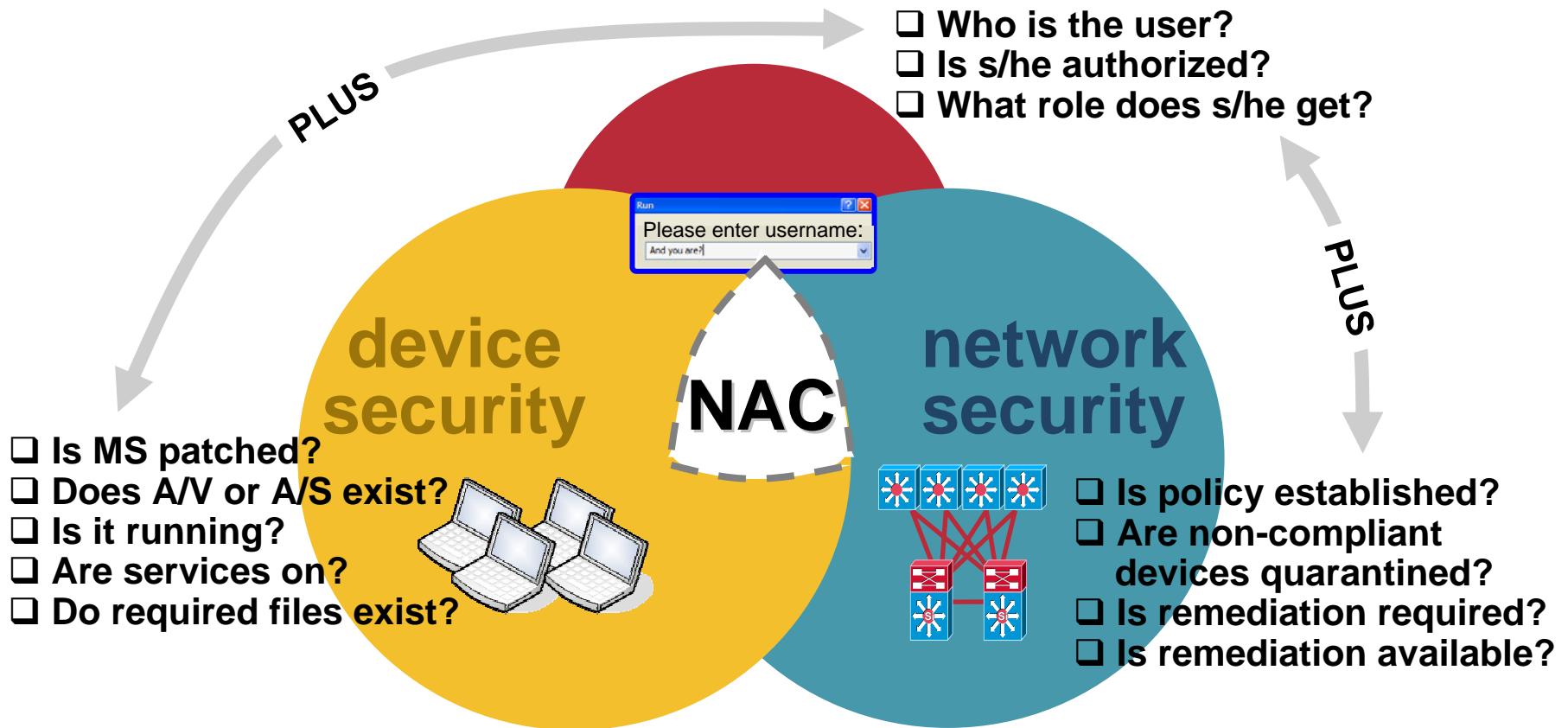
Pre-configured checks  
Customized checks  
Self-remediation or auto-remediation  
Third-party software

# Complexity Demands Defense-in-Depth



# What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.



# Four Key Capabilities of NAC

## SECURELY IDENTIFY DEVICE & USER

Uniquely identifies users and devices, and creates associations between the two

## ENFORCE CONSISTENT POLICY

Assess and enforce a ubiquitous policy across the entire network

## QUARANTINE AND REMEDiate

Acts on posture assessment results, isolates device, and brings it into compliance

## CONFIGURE AND MANAGE

Easily creates comprehensive, granular policies that map quickly to user groups and roles

### WHAT IT MEANS

### WITHOUT IT ...

Critical to associate users and devices with roles to know which policies apply; prevents device spoofing.

A decentralized policy mechanism (e.g. on endpoint) can leave gaping security holes.

Just knowing a device is non-compliant is not enough—someone still needs to fix it.

Policies that are too complex or difficult to create and use will lead to abandonment of project.

**A robust NAC solution must have all four capabilities.**

# Before We Continue, You May Be Asking ...

- **Do I need separate products for my VPN users, my LAN users, my unmanaged users?**
- **Am I your guinea pig? What's your experience in deploying NAC?**
- **Is this going to take months to deploy?**
- **How can I be sure that this product will fit MY situation?**
- **Do I need to upgrade my entire infrastructure?**



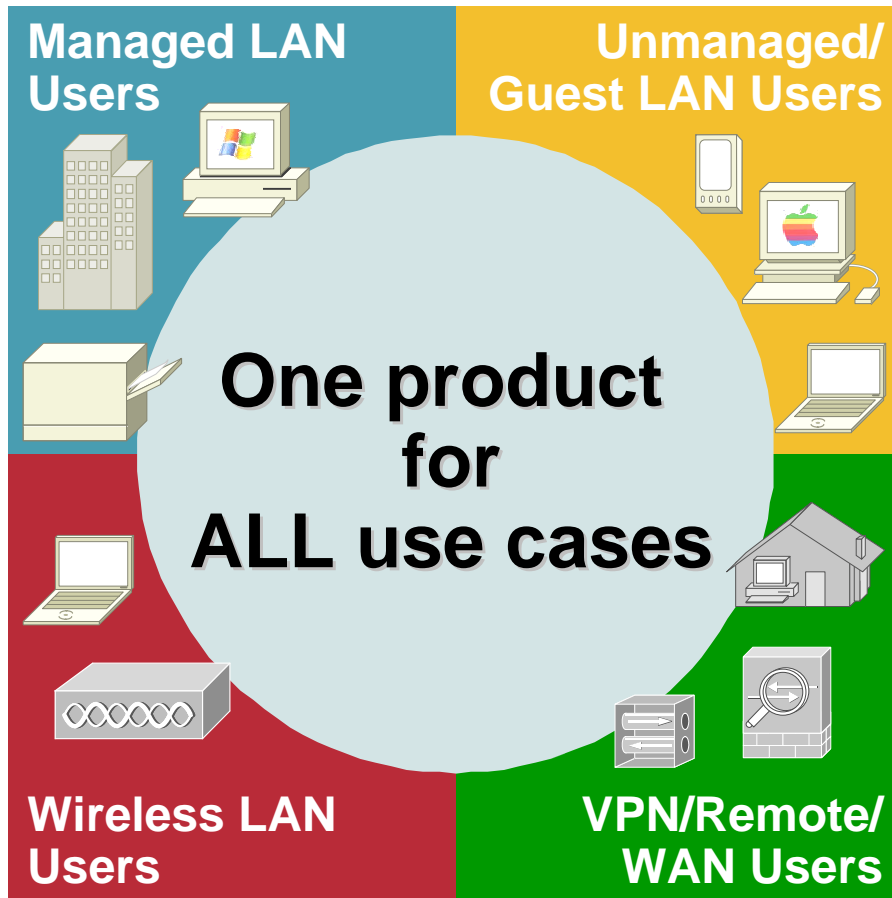
# Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
4. **NAC Appliance Technical Benefits**



# NAC Appliance

1.



2.

**600+ customers across all use cases:  
No. 1 NAC solution**

3.

**Most deployments ready under 5 days**

4.

**Scales from 100 users to 100,000+ user,  
across 150+ locations**

5.

**Does not require infrastructure upgrade**

# NAC Appliance Enforces Compliance

**Who's on?  
What's on?**

**Securely  
Identify  
Device & User**

**Authenticates and  
authorizes users**  
(local db, RADIUS,  
LDAP, Kerberos, AD,  
etc.)

**Supports all access  
methods** (LAN,  
wireless, remote/VPN,  
WAN)

**What are the  
requirements  
for access?**

**Enforce  
Consistent  
Policies**

**Centralized policy  
supports multiple  
user roles**

**Scans for infections,  
port vulnerabilities,  
hotfixes, AV, AS,  
services running,  
and files**

**What are the  
steps to meet  
requirements?**

**Quarantine  
And  
Remediate**

**Isolates non-  
compliant devices  
using MAC and IP  
addresses; effective  
at a per-user level**

**Network-based, self-  
guided remediation**  
  
**Helpdesk integration**

**How do I create  
or modify  
requirements?**

**Configure  
And  
Manage**

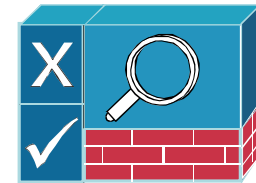
**Pre-configured  
checks simplify  
policy configuration  
and rule creation**

**Web-based interface  
for easy  
management of  
roles, policies, and  
remediation steps**

# NAC Appliance (formerly known as Clean Access) Components

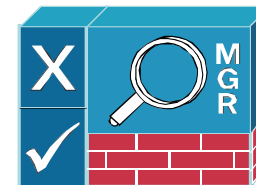
- **Cisco Clean Access Server**

Serves as an in-band or out-of-band device for network access control



- **Cisco Clean Access Manager**

Centralizes management for administrators, support personnel, and operators



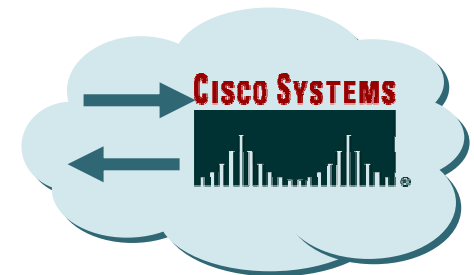
- **Cisco Clean Access Agent**

Optional lightweight client for device-based registry scans in unmanaged environments



- **Rule-set Updates**

Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



# Sampling of Pre-Configured Checks

## Critical Windows Updates

Windows XP, Windows 2000,  
Windows 98, Windows ME



## Anti-Virus Updates



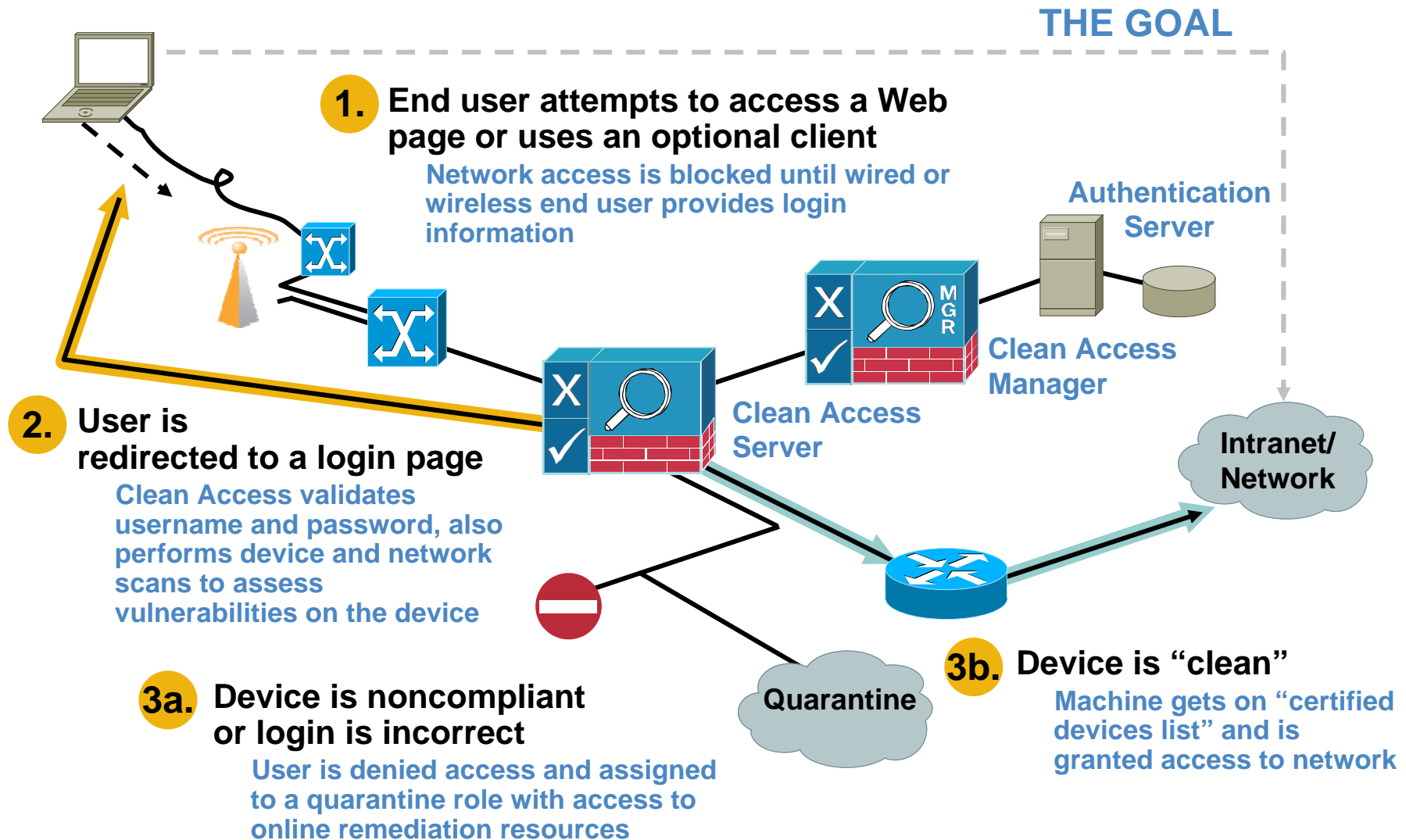
## Anti-Spyware Updates

## Other 3<sup>rd</sup> Party Checks



**Customers can easily add customized checks**

# Product User Flow Overview



# User Experience with Agent

Login  
Screen



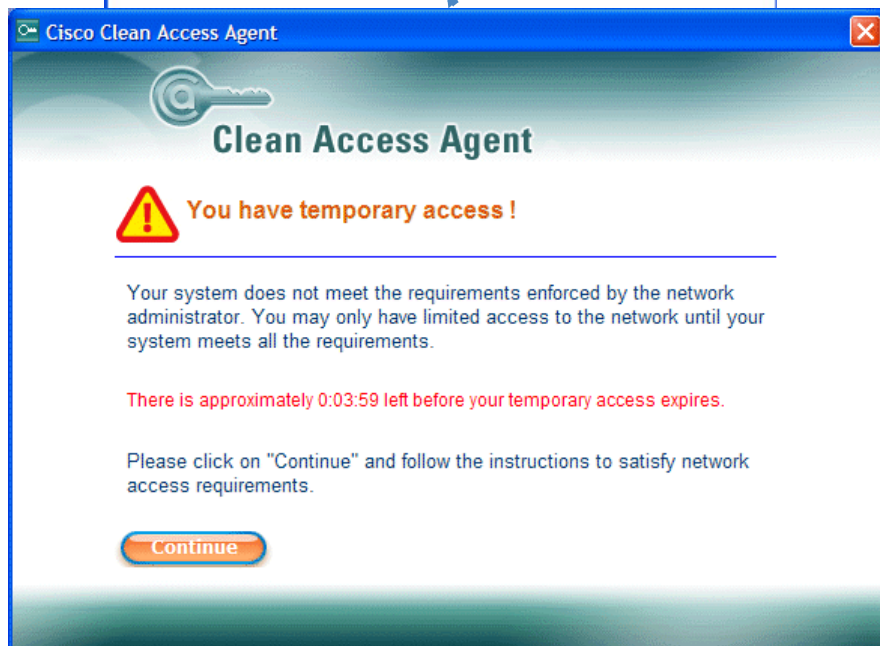
The login screen for the Cisco Clean Access Agent. It features a blue header with the Cisco logo and the text 'Clean Access Agent'. Below the header, there is a prompt 'Please enter your user name and password:' followed by input fields for 'User Name' (containing 'cisco') and 'Password'. There is a 'Remember Me' checkbox and a prompt 'Please select your authentication provider:' with a dropdown menu showing 'Local DB'.

**Scan is performed**

(types of checks depend on user role)

**Scan fails**

**Remediate**



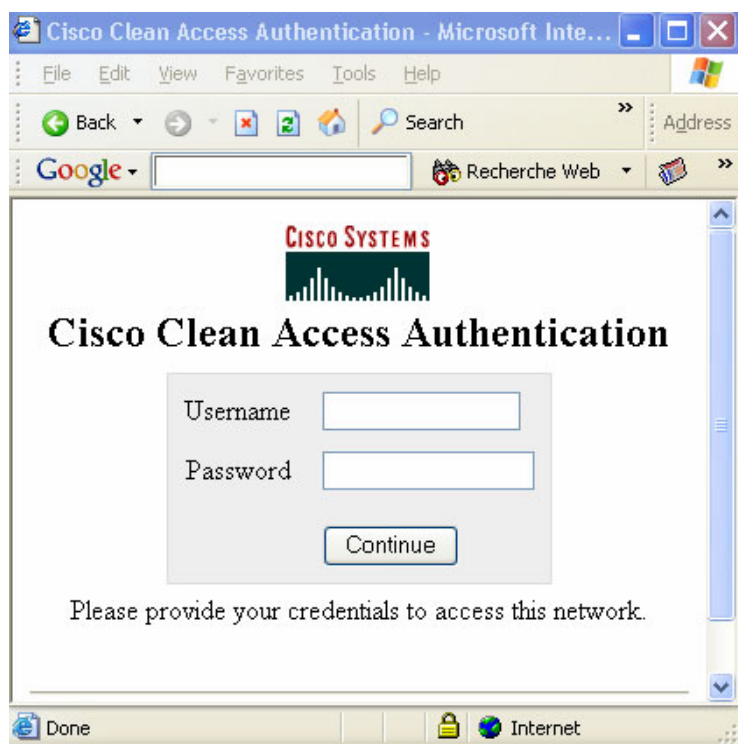
The remediate screen for the Cisco Clean Access Agent. It features a blue header with the Cisco logo and the text 'Clean Access Agent'. Below the header, there is a yellow warning icon and the text 'You have temporary access !'. A message states: 'Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.' Below this, it says 'There is approximately 0:03:59 left before your temporary access expires.' At the bottom, there is a 'Continue' button.



The remediate screen for the Cisco Clean Access Agent. It features a blue header with the Cisco logo and the text 'Clean Access Agent'. Below the header, there is a yellow warning icon and the text 'Please download and install the required software before accessing the network.' Below this, there is a section titled 'Required Software' with a timer '(0:03:10 left)'. It lists the 'Name' as 'Anti-Spyware (Optional) Software', the 'Version', and the 'Location' as 'http://www.lavasoft.com/support/download/'. A 'Description' follows, stating: 'Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.' At the bottom, there are three buttons: 'Go To Link', 'Next', and 'Cancel'.

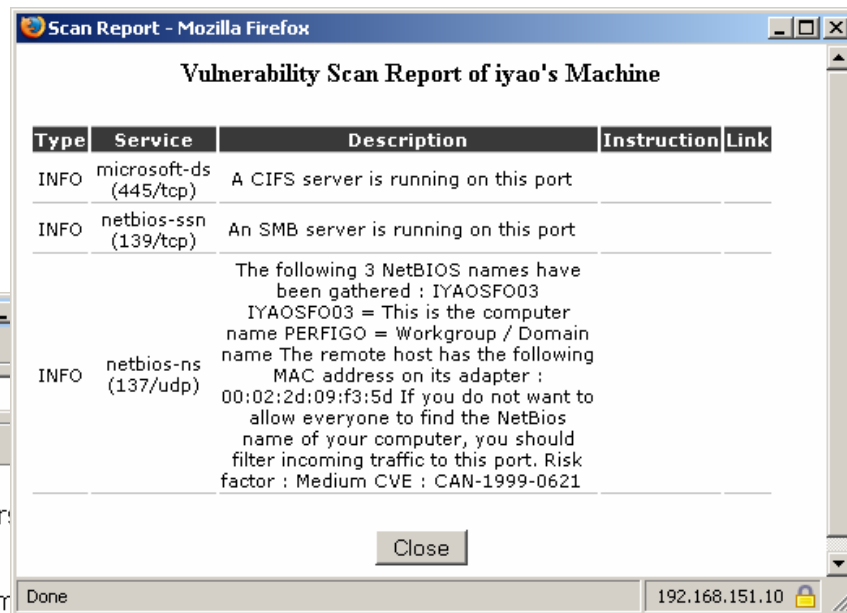


# User Experience via Web Browser



**Login  
Screen**

**Scan is performed**  
(types of checks depend on user role/OS)



**Guided self-remediation**

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

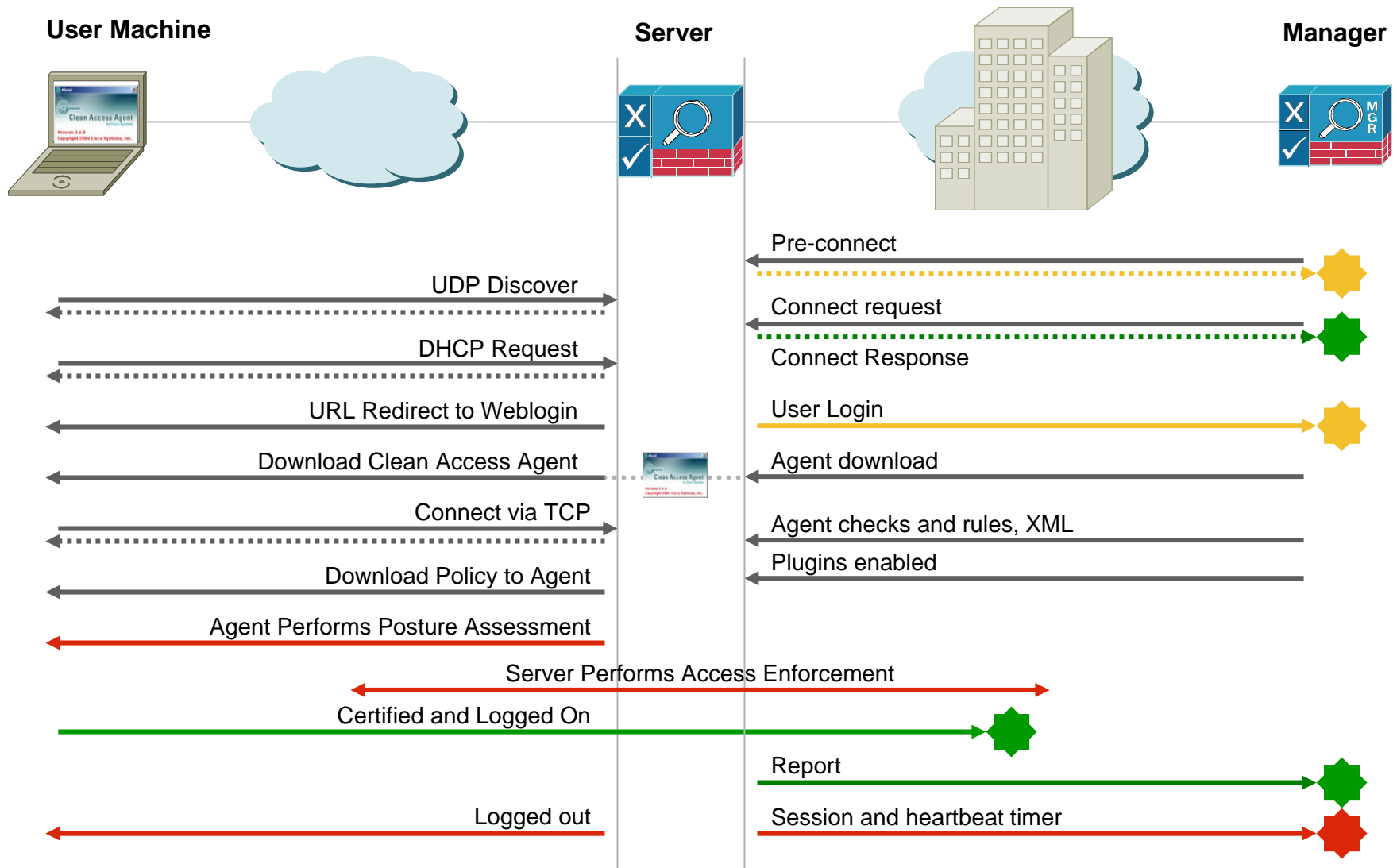
The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact

Accept

Decline



# NAC Appliance Protocol Flow



# NAC Appliance Sizing

**Super Manager**



manages up to 40

Users = online, concurrent

**Enterprise and Branch Servers**

**Standard Manager**



manages up to 20

**Enterprise and Branch Servers**

**Manager Lite**



manages up to 3

**Branch Office or SMB Servers**



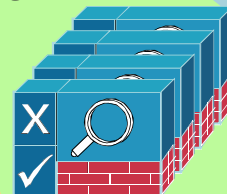
100 users



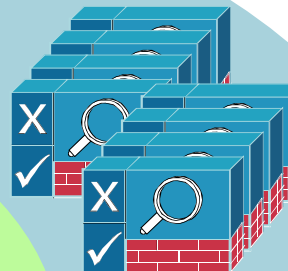
250 users



500 users



1500 users each





1500 users each

# Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
  - Management Console
  - Checks, Rules, Requirements
4. **NAC Appliance Technical Benefits**



# Tour of Features: Management Console



**Switch Management**

- Profiles
- Devices

**User Management**

- User Roles
- Auth Servers
- Local Users

**Monitoring**

- Summary
- Online Users
- Event Logs
- SNMP

**Administration**

- CCA Manager
- User Pages
- Admin Users
- Backup

## Cisco Clean Access Manager

Version 3.6.2

Device Management > Clean Access Servers > 172.19.106.1

Status Network Filter Advanced Authentication Misc

IP DHCP DNS Certs IPSec L2TP PPTP PPP

Clean Access Server Type: NAT Gateway

☐ Enable L2 strict mode for Out-of-Band Virtual Gateway

☐ Out-of-Band Real-IP Gateway

IP Address: 172.19.106.13 IP Address: 10.10.10.1

Subnet Mask: 255.255.255.0 Subnet Mask: 255.255.255.0

Default Gateway: 172.19.106.1 Default Gateway: 10.10.10.1

☐ Set management VLAN ID: ☐ Set management VLAN ID:


(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)

Update Reboot

- The Clean Access Manager (CAM) uses a GUI front-end for administration and management
  - Flat HTML, no Java or Active-X controls necessary
- Changes are only made once in the active CAM, replication takes care of the rest
- Communication between the CAS and the CAM is protected by SSL and shared passwords
- Clean Access Server administration is controlled centrally through the Clean Access Manager

**Note:** NAC Appliance is formerly known as Clean Access

# CAM Manages All Clean Access Servers



## Cisco Clean Access Manager

Version 3.6.2

- Device Management
  - CCA Servers**
  - Filters
  - Roaming
  - Clean Access
- Switch Management
  - Profiles
  - Devices
- User Management
  - User Roles
  - Auth Servers
  - Local Users
- Monitoring
  - Summary
  - Online Users
  - Event Logs
  - SNMP
- Administration
  - CCA Manager
  - User Pages
  - Admin Users
  - Backup

Device Management > Clean Access Servers > 172.19.106.13

StatusNetworkFilterAdvancedAuthenticationMisc

IP · DHCP · DNS · Certs · IPSec · L2TP · PPTP · PPP

Clean Access Server Type:

NAT Gateway

Virtual Gateway

RealHP Gateway

NAT Gateway

Out-of-Band Virtual Gateway

Out-of-Band RealHP Gateway

Out-of-Band NAT Gateway

☐ Enable L3 support

☐ Enable L2 strict mode for

Trusted Interface (to protected network)

IP Address172.19.106.13

Subnet Mask255.255.255.192

Default Gateway172.19.106.1

☐ Set management VLAN ID: 0

☐ Pass through VLAN ID to managed network

Untrusted Interface (to managed network)

IP Address10.10.10.1

Subnet Mask255.255.255.0

Default Gateway10.10.10.1

☐ Set management VLAN ID: 0

☐ Pass through VLAN ID to protected network

(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)

Update

Reboot

Session Number  
Presentation\_ID

© 2006 Cisco Systems, Inc. All rights reserved.

C97-347999-00 05/06

Cisco Public

21

# Pre-Configured Checks

**Updates of Clean Access Agent and pre-configured checks are downloaded automatically at designated intervals**

**Cisco Clean Access Manager** Version 3.6.2

Device Management > Clean Access

**Certified Devices** | **General Setup** | **Network Scanner** | **Clean Access Agent**

Distribution • Rules • Requirements • Role-Requirements • Reports • **Updates**

Current Version of Cisco Checks & Rules: **10183**  
Current Version of CCA Agent Upgrade Patch: **3.6.2.0**  
Current Version of Supported AV/AS Product List: **37**  
Current Version of Default Host Policies: **5**  
Current Version of OS Detection Fingerprint: **1**

**Update Settings**

☒ Automatically check for updates every  hours

☒ Check for CCA Agent upgrade patches

☒ Use an HTTP proxy server to connect to the update server

Proxy Address:

Proxy Port:

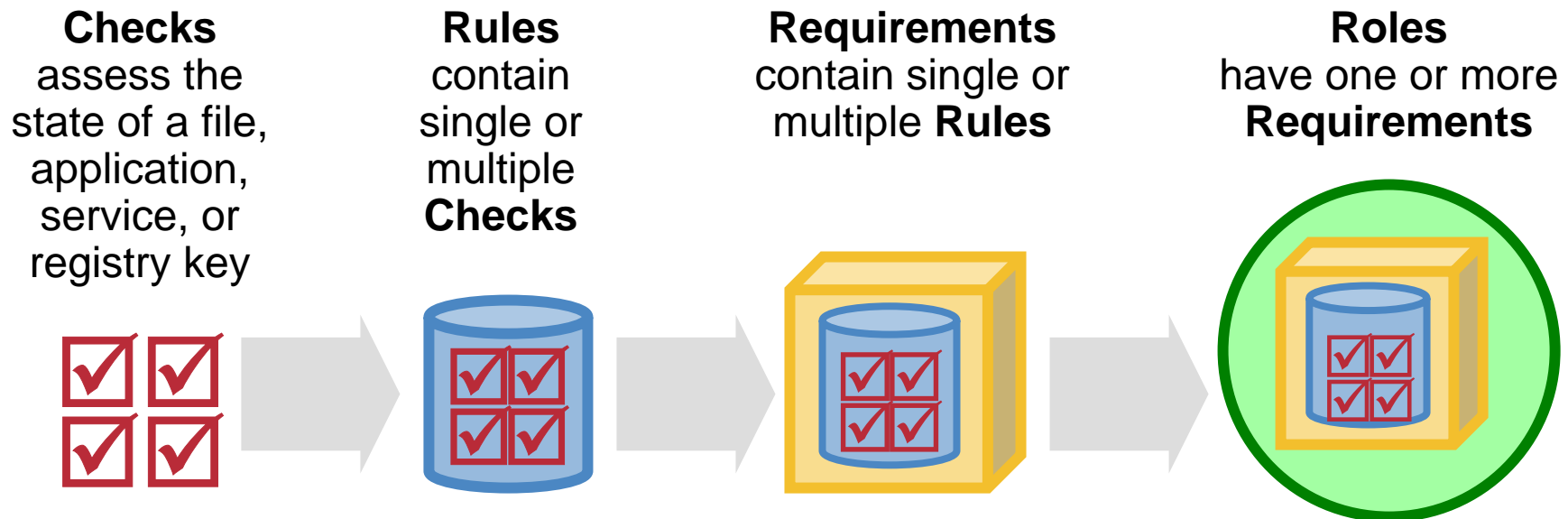
Proxy Username:

Proxy Password:

- **Proxy capabilities for customer who do not allow direct internet connections**
- **SSL encryption and certificates secure traffic between Cisco and the CAM**

# Posture Validation Overview

**NAC Appliance posture validation is a hierarchical process with either pre-loaded or custom profiles**



# Checks and Rules: An Example

## Checks

assess the state of a  
file, application, service,  
or registry key



**Is anti-spyware installed?**  
(application present, file present)  
**Is anti-spyware up-to-date?**  
(file version > or = )  
**Is anti-spyware running?**  
(service / exe running)

## Rules

assemble individual  
checks together to make  
a posture assessment



**Anti\_Spyware\_Installed\_Check**  
**AND**  
**Anti\_Spyware\_UptoDate\_Check**  
**AND**  
**Anti\_Spyware\_Running\_Check**



# How Checks Look in the Manager

This is an example of a registry key CHECK for a Windows Hotfix:

**Cisco Clean Access Manager** Version 3.6.2

Device Management > Clean Access

**Certified Devices** | **General Setup** | **Network Scanner** | **Clean Access Agent**

**Distribution** · **Rules** · **Requirements** · **Role-Requirements** · **Reports** · **Updates**

**Check List** | **View Check** | **Rule List** | **New Rule** | **New AV Rule** | **New AS Rule** | **AV/AS Su**

**Info**

Check Category: Registry Check Check Type: Registry Key

Check Name: pc\_HotFix888113\_9x

Registry Key: HKLM \ Software\Microsoft\Active Setup\Installed Components

Operator: exists

Check Description: Critical Update 888113

Operating System: ☐ Windows All ☐ Windows XP ☐ Windows 2000  
☒ Windows ME ☒ Windows 98

☐ Automatically create rule based on this check

\* Cisco created checks cannot be edited. Create a copy of the check if you intend to change it.

# How Rules Look in the Manager

This is an example of a Windows Hotfix RULE with multi-level check logic:

**Cisco Clean Access Manager** Version 3.6.2

Rule Name

pr\_XP\_Hotfixes

Rule Description

Windows XP Hotfixes

Operating System

☐ Windows All ☒ Windows XP ☐ Windows 2000  
☐ Windows ME ☐ Windows 98

Rule Expression

pc\_HotFix896423\_XP&pc\_HotFix901214\_XP&pc\_HotFix896422\_XP&pc\_HotFix896424\_XP&pc\_HotFix896358\_XP&pc\_HotFix913446\_XP&pc\_HotFix891781\_XP&pc\_HotFix885250\_XP&pc\_HotFix888113\_XP&pc\_HotFix902400\_XP&pc\_HotFix904706\_XP&{(pc\_Windows-XP-SP2&pc\_HotFix912919\_XP&pc\_HotFix908519\_

Use checks and operators to create an expression. If a rule condition is true, the client is considered in compliance with the rule.  
  
Operators are "&" (and), "|" (or), "!" (not), and "()" (eval priority parens).  
  
Ex: *check1 & (check2 | check3)*

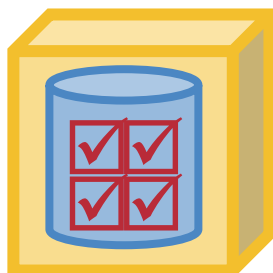
\* Cisco created rules cannot be edited. Create a copy of the rule if you intend to change it.

Checks for Selected Operating System			
Name	Category	Type	OS
pc_Hotfix828035	Registry Check	Registry Key	Win ( XP )
pc_Hotfix823182	Registry Check	Registry Key	Win ( XP )
pc_Hotfix824146	Registry Check	Registry Key	Win ( XP )
pc_Hotfix825119	Registry Check	Registry Key	Win ( XP )
pc_Hotfix835732	Registry Check	Registry Key	Win ( XP )
pc_Hotfix828741	Registry Check	Registry Key	Win ( XP )
pc_Hotfix823559	Registry Check	Registry Key	Win ( XP )
pc_Hotfix329390	Registry Check	Registry Key	Win ( XP )
pc_Hotfix323255	Registry Check	Registry Key	Win ( XP )
pc_Symantec_Client_Firewall	Registry Check	Registry Value	Win ( XP )

# Requirements and Roles

## Requirements

tie remediation actions directly to a rule



## Roles

determine which requirements and which security filters apply



### Remediation methods include:

- File Distribution (“[Download antispyware.exe](#)”)
- Link Distribution (“[windowsupdate.com](#)”)
- Local Check (text instructions or messages)
- Definition Update (direct launch of supported AV or AS)

### Option to dynamically assign VLANs

Apply individual URL redirection per role, as well as Acceptable Usage Policies, User Pages, and more

# How Requirements Look in the Manager

Remediation as required by **REQUIREMENTS** can be manual, automatic, optional, or enforced:

**Cisco Clean Access Manager** Version 3.6.2

Device Management > Clean Access

Certified Devices

General Setup

Network Scanner

Clean Access Agent

Distribution

Rules

Requirements

Role-Requirements

Reports

Updates

Requirement List

Edit Requirement

Requirement-Rules

Requirement Type 

AV Definition Update

☒ Do not enforce requirement

Priority 4

Antivirus Vendor Name 

McAfee, Inc.

\*Note: Vendors without products supported by this requirement type (ALWIL Software, America Online, Inc., EarthLink, Inc., Microsoft Corp., SOFTWIN, Zone Labs LLC) are not listed in the Antivirus Vendor Name list.

Requirement Name 

McAfee AV Definition Update

Description 

You must download the latest McAfee AV definition file:

Operating System 

☐ Windows All ☒ Windows XP ☒ Windows 2000

☐ Windows ME ☐ Windows 98

Save Requirement

Cancel

If the user has one of the following listed products installed, he/she can use the Update button provided by CCA Agent to update the virus definition file if this requirement fails.

# How Roles Look in the Manager

Fine-tuning for  
timers, agents,  
and policies on  
a per-ROLE  
basis:

Device Management > Clean Access

Certified Devices   General Setup   Network Scanner   Clean Access Agent

User Role: consultant

Operating System: ALL  
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

☐ Require use of Clean Access Agent  
Clean Access Agent Download Page Message (or URL):  
<b>Network Security Notice:</b> This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this

☒ Show [Network Scanner User Agreement page](#) to web login users

☒ Enable pop-up scan vulnerability reports from User Agreement page

☒ Require users to be certified at every web login

☐ Show Network Policy to Clean Access Agent users  
Network Policy Link:

☐ Exempt certified devices from web login requirement

☒ Block/Quarantine users with [vulnerabilities](#) in role: Quarantine Role (15 minutes)

Show quarantined users User Agreement Page of: quarantine role

Update   Cancel

# How Roles Look in the Manager

More options  
based on user  
ROLE (called  
“FTE” in this  
case):

User Management > User Roles

List of Roles | **New Role** | Traffic Control | Bandwidth | Schedule

☐ Disable this role

Role Name:

Role Description:

Role Type:

\*VPN Policy:

\*Dynamic IPsec Key: ☐ Enable ☒ Disable

\*Max Sessions per User Account ( ☐ Case-Insensitive ):  (1 - 255; 0 for unlimited)

Retag Trusted-side Egress Traffic with VLAN (In-Band):  (0 - 4095, or leave it blank)

Out-of-Band User Role VLAN:  (0 - 4095)

\*After Successful Login Redirect to: ☒ previously requested URL  
☐ this URL:  (e.g., http://www.cisco.com/)

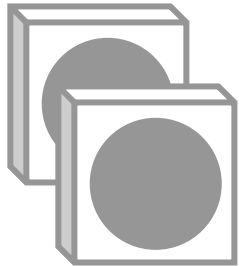
Redirect Blocked Requests to: ☒ default access blocked page  
☐ this URL or HTML message:

\*Roam Policy: ☒ Deny ☐ Allow

\*Show Logged-on Users: ☒ IPsec info ☐ PPP info  
☒ User info ☒ Logout button

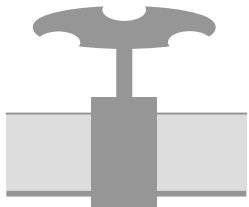
(\*only applies to normal login role)

# Filters and Bandwidth



**SECURITY FILTERS** behave the same as Access Control Lists with additional <http://weblink> and Layer 2 protocol capabilities.

Each role has its own filter, with access levels controlled by the system administrator.



**BANDWIDTH CONTROLS** allow for either per-user or per-role restrictions.

Common for remediation and guest access applications.

# How Filters Look in the Manager

At-a-glance  
display of Filters  
by User Roles:

**Cisco Clean Access Manager** Version 3.6.2

User Management > User Roles

List of RolesNew RoleTraffic ControlBandwidthSchedule

IP · Host

All RolesUntrusted -> TrustedSelect

[Add Policy to All Roles](#)

Unauthenticated Role

[Add Policy](#)

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*;*	172.19.106.12 /255.255.255.255 ;*	<input checked="" type="checkbox"/>			
Allow	ALL TRAFFIC	*	*	<input type="checkbox"/>			
Allow	UDP	DNS <sup>†</sup>					
Block	ALL						

Agent Quarantine Role

[Add Policy](#)

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*;*	172.19.106.12 /255.255.255.255 ;*	<input checked="" type="checkbox"/>			
Allow	ALL TRAFFIC	*	*	<input type="checkbox"/>			
Allow	UDP	*;*	*:53				
Block	ALL						

Network Scan Quarantine Role

[Add Policy](#)

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
--------	----------	-----------	---------	--------	------	-----	------



# How Bandwidth Controls Look

**Bandwidth control on a per-user and per-role basis:**

**Cisco Clean Access Manager** Version 3.6.2

User Management > User Roles

List of Roles

New Role

Traffic Control

**Bandwidth**

Schedule

Role Name:

Agent Quarantine Role

Upstream Bandwidth

Kbits/sec

(the minimum recommended value is 100; use -1 for unlimited)

Downstream Bandwidth

Kbits/sec

(the minimum recommended value is 100; use -1 for unlimited)

Burstable Traffic

(from 1 to 10; the burst rate is determined by multiplying this number by the bandwidth)

Shared Mode

All users share the specified bandwidth

All users share the specified bandwidth

Each user owns the specified bandwidth

Description

Save

Cancel

# Clean Access Manager: Back-end Authentication Integration

**Flexible back-end authentication options allow for fast integration to existing networks: Kerberos/NTLM, RADIUS, LDAP, AD, local db**

The screenshot displays the Cisco Clean Access Manager web interface, Version 3.6.2. The breadcrumb navigation shows 'User Management > Auth Servers'. The 'New Server' tab is selected, showing a form for adding a new authentication server. The form includes fields for Authentication Type (set to Kerberos), Domain Name (CISCO.COM), Server Name (auth.cisco.com), and Description. A dropdown menu for Default Role is open, showing options like Unauthenticated Role, Allow All, Guest, Consultant, ScanTest (highlighted), TAC, Dormitory Student, printer, Chicago\_users, and Nowhere. At the bottom are 'Add Server' and 'Cancel' buttons.

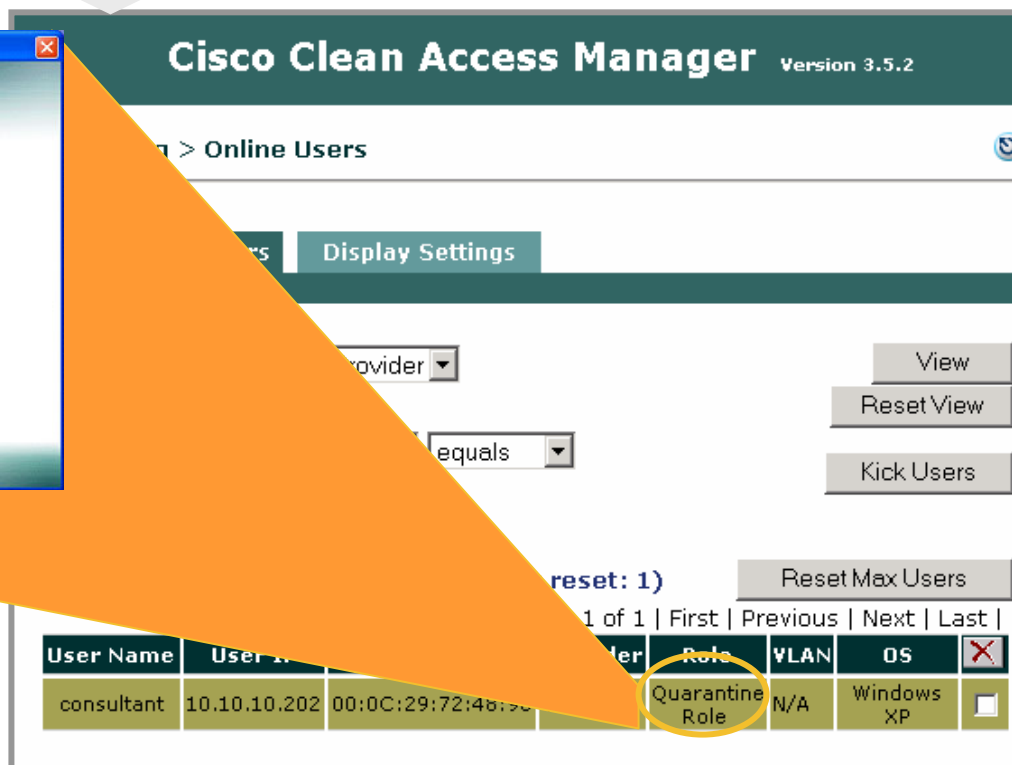
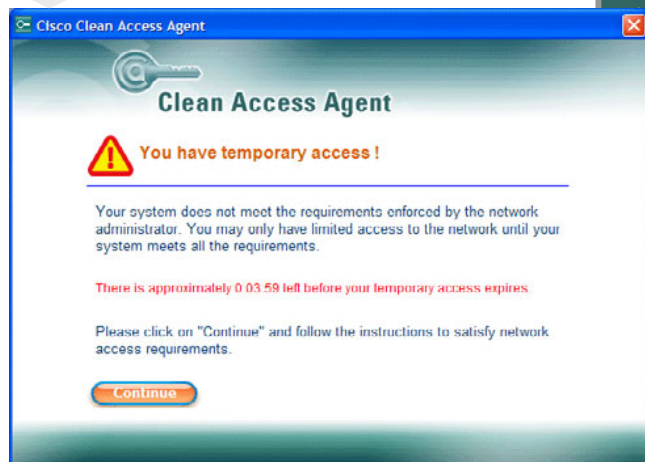
Cisco Clean Access Manager Version 3.6.2	
User Management > Auth Servers	
List of Servers   <b>New Server</b>   Mapping Rules   Auth Test   Account	
Authentication Type	Kerberos
Domain Name	CISCO.COM
Server Name	auth.cisco.com
Description	
Provider Name	
Default Role	Unauthenticated Role
<div>Unauthenticated Role</div> <div>Allow All</div> <div>Guest</div> <div>Consultant</div> <div><b>ScanTest</b></div> <div>TAC</div> <div>Dormitory Student</div> <div>printer</div> <div>Chicago_users</div> <div>Nowhere</div>	
<div>Add Server</div> <div>Cancel</div>	

- **Map users attributes and rights directly to Roles and Filters**
- **Add operators and conditions to mapping rules to dial in the desired access rights**

# Admin Control with Real-Time Information

USER

ADMIN



**Logs can be viewed locally or sent via Syslog to an off-box collection engine for custom reports**

# Fine-Tuning Administrator Access

**Multiple administrator user accounts for NOC, help desk operators, etc.**

**Cisco Clean Access Manager** Version 3.6.2

Administration > Admin Users

Admin Users

Admin Groups

List • Edit

☐ Disable this group

Group Name

Help-Desk

Description

Customized permissions for help desk

Access Control Policy:

Clean Access Servers

Default Clean Access Server Access: read only

Clean Access Server 172.19.106.13: read only

Module Features

Default Feature Access: read only

Clean Access Servers Management : read only

Device Filters (MAC & Subnet): full control

Roaming : read only

Certified & Floating Devices : full control

Network Scanner (Nessus) : read only

Clean Access Agent : read only

Switch Management : read only

# Clean Access Manager Benefits Summary

- **Centralized and scalable management and policy configuration**
- **Pre-configured checks drastically reduce “Day 2” support and maintenance**
- **Full access to the rules engine can create a posture assessment for any application**
- **Flexible remediation options give users as much power as desired to self-repair, reducing help desk dependence**

# Agenda

1. **Securing Complexity**
2. **NAC Appliance Product Overview**
3. **NAC Appliance Features In-Depth**
4. **NAC Appliance Technical Benefits**



# NAC Appliance Technical Benefits

## Product Experience

With 500+ deployments, Cisco understands the technical impact on your network

## Defense-in-Depth

NAC Appliance is a self-contained, proactive way to enforce policy compliance on all incoming devices

## Rapid Setup Easy Mgmt

Pre-configured rulesets and checks make it easy to setup, maintain, modify, and expand

## Flexible Deployment

Broad deployment options means that NAC Appliance fits into your network the way you need it to

## Future Proof

NAC Appliance is core to Cisco's strategic NAC vision and can be leveraged across all future deployment options



# Q&A



# CISCO SYSTEMS

