



Enabling Contractor Provisioning Cisco NAC deployments



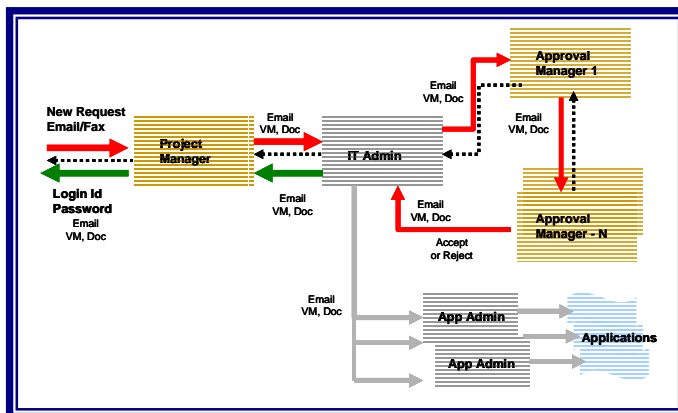
Introduction

Corporate computing environments are becoming more complex. The presence of large number of applications in a high computing environment coupled with the presence of knowledge workers, working from within the organization and remotely, the issues related to timely resource access/revocation are plenty.

- Provide network access to several thousand temporary users like contractors that are retained and periodically assigned across multiple projects.
- Reduce the time needed and eliminate potential errors during the user provisioning process which currently mandates multiple information exchanges between project managers, IT administrators and managers.
- Automate the de-provisioning of users when the associated project is completed to maximize IT security.
- Establish a means to document the approval process for user accounts which is essential to achieve regulatory compliance.
- Ability to provision contractors locally or remotely, while ensuring network access to these users 24/7.
- Significantly reduce help desk calls associated with password resets as users access the resources across time zones.

Apere Contractor Provisioning Solution with Cisco NAC

- IMAG provisioning solution integrates seamlessly with Cisco's NAC solution, with minimal field configuration
- IMAG provides a comprehensive user account approval process based on a self-service creation mechanism with remote access via the internet for external users
- With IMAG, user requests are routed thru a company defined approval process, which is documented to ensure compliance and for forensics purposes.
- IMAG automatically de-provisions user accounts when needed and appropriate reminders are sent to administrators and end users.
- IMAG uses patented technology to provide disaster recovery over Enterprise's WAN with deployments across two different physical locations.
- IMAG's Self-Service Password Reset Portal enabled enterprise to reduce help desk costs and improve IT productivity.
- IMAG can be configured for high availability with active passive fail over

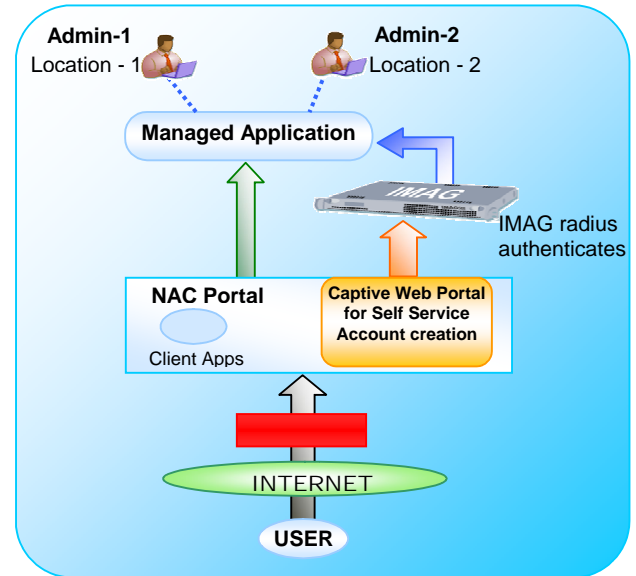
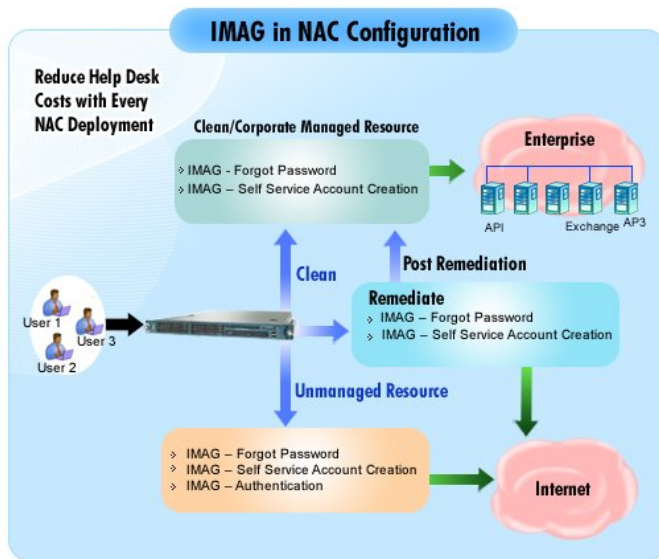


Productivity Challenges – To provision new contractors or consultants' enterprises currently use elaborate manual, email/VM process to get approvals from project managers and application managers before providing any access to applications. It takes 1-3 weeks before providing required access, leading to loss of productivity. Several times the status of requests is not known.

Security and Compliance Challenges – Accounts need to be removed timely for security and compliance reasons. The process needs to be documented and reproduced for forensics and compliance reporting.

The Solution – Cisco NAC and Apere IMAG

Configuration



Self-Service Account Request and Password Management

IMAG can be easily configured into NAC web portal. The procedure is described in the following section. Contractors or temporary users can click on the self service request portal for requesting new accounts or password resets.

IMAG’s user self help portal for requesting account creation and password reset can be accessed using a browser. A simple workflow process allows the provisioning administrator to obtain approval from appropriate authorizers within the organization, if needed. This significantly reducing the time and effort needed to create new accounts, while eliminating potential errors. Users can request accounts for certain duration of time.

IMAG’s intuitive work flow process ensures that required e-mails indicating the status of account creation are automatically sent to the appropriate administrators and authorizers in addition to the user. Status of the account is updated on the self-service account creation portal, enabling the user to view account status at any time. IMAG can send reminder e-mails, on a configurable basis, for account expiration, password expiration

etc. This enables the user to efficiently manage the accounts on their own, eliminating IT intervention.

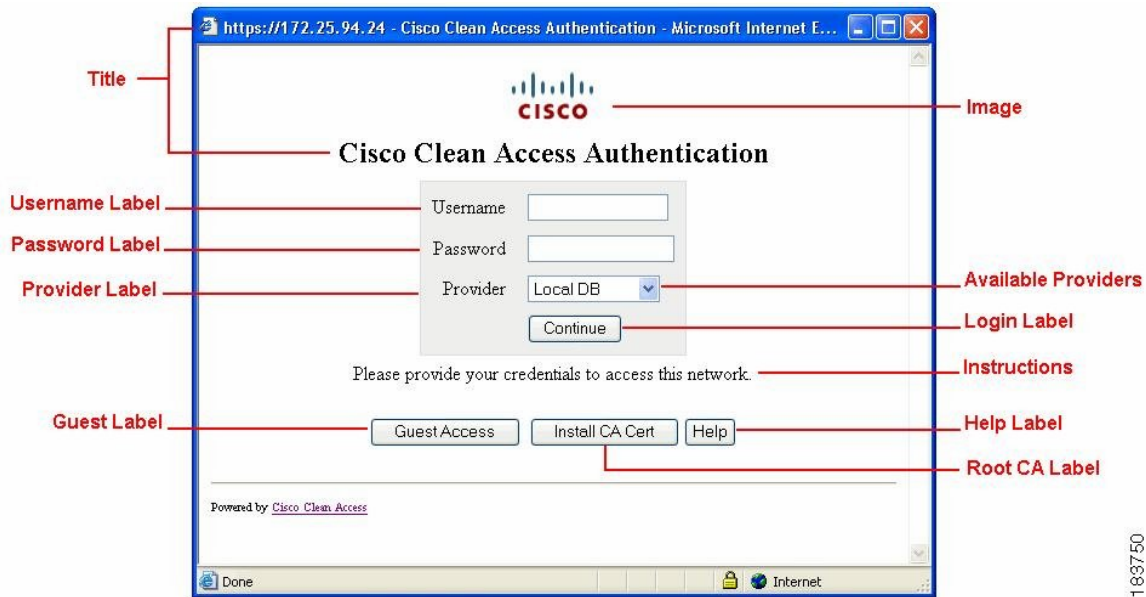
Once a user's account is successfully created through the IMAG self-service portal, it is automatically added to an authoritative list of user accounts which enables an IT Administrator to leverage IMAG's Identity Management platform to maintain and manage that account from a centralized location. A user who obtains an account created through the IMAG self-service portal can also reset their password, as needed, again eliminating IT intervention.

IMAG provides a reporting tool to administrators to generate various reports of user activities within the self service portal. These reports can be queried, viewed and stored based on the period required i.e., daily, weekly, monthly.

In summary, IMAG's self-service portal enables administrators to cost effectively manage the contractor account provisioning process, maximizing their productivity by providing quick and secure access, and ensuring regulatory compliance.

Cisco NAC Integration Steps

Cisco NAC Web login screen looks as follows:



The items listed in red can be customized. To allow users access to self service account creation and self service password reset services running on IMAG, following steps can be followed:

1. Change Web login page to Frame based. To change the format of the page from the default frameless format, use the following steps:

- a. From **Administration > User Pages > Login Page > List**, click the **Edit** button next to the page to be customized.
- b. The **General** sub tab page appears by default.
- c. From the **Page Type** dropdown menu, choose **Frame-Based** option.
Frame-based—This sets the login fields to appear in the left frame of the page, and allows you to configure the right frame with your own customized content (such as organizational logos, files, or referenced URLs).

Administration > User Pages 🔄

Login Page

File Upload

List · Add · **Edit**

General
Content
Style

Enable this login page

VLAN ID
(separate multiple VLANs with a comma)

Subnet (IP/Mask) /

Operating System ▼

Page Type ▼

Page Description

Web Client (ActiveX/Applet) ▼

Use web client to detect client MAC address and Operating System.

Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

183505

- d. Leave other settings at their defaults.
- e. Click **Update** to save your changes.

2. Customize the instructions on the login page to guide the users to click on the links to create self service accounts and self service password. This can be done from Administration -> User Pages -> Login Page -> List -> Edit -> Content as shown in the figure below.

Administration > User Pages

· ·

| |

Image: Title:

<input checked="" type="checkbox"/> Username Label	<input type="text" value="Username"/>	<input checked="" type="checkbox"/> Password Label	<input type="text" value="Password"/>
<input checked="" type="checkbox"/> Login Label	<input type="text" value="Continue"/>	<input type="checkbox"/> Provider Label	<input type="text" value="Provider"/>
Default Provider:	<input type="button" value="Local DB"/>	Available Providers:	<input type="checkbox"/> Local DB

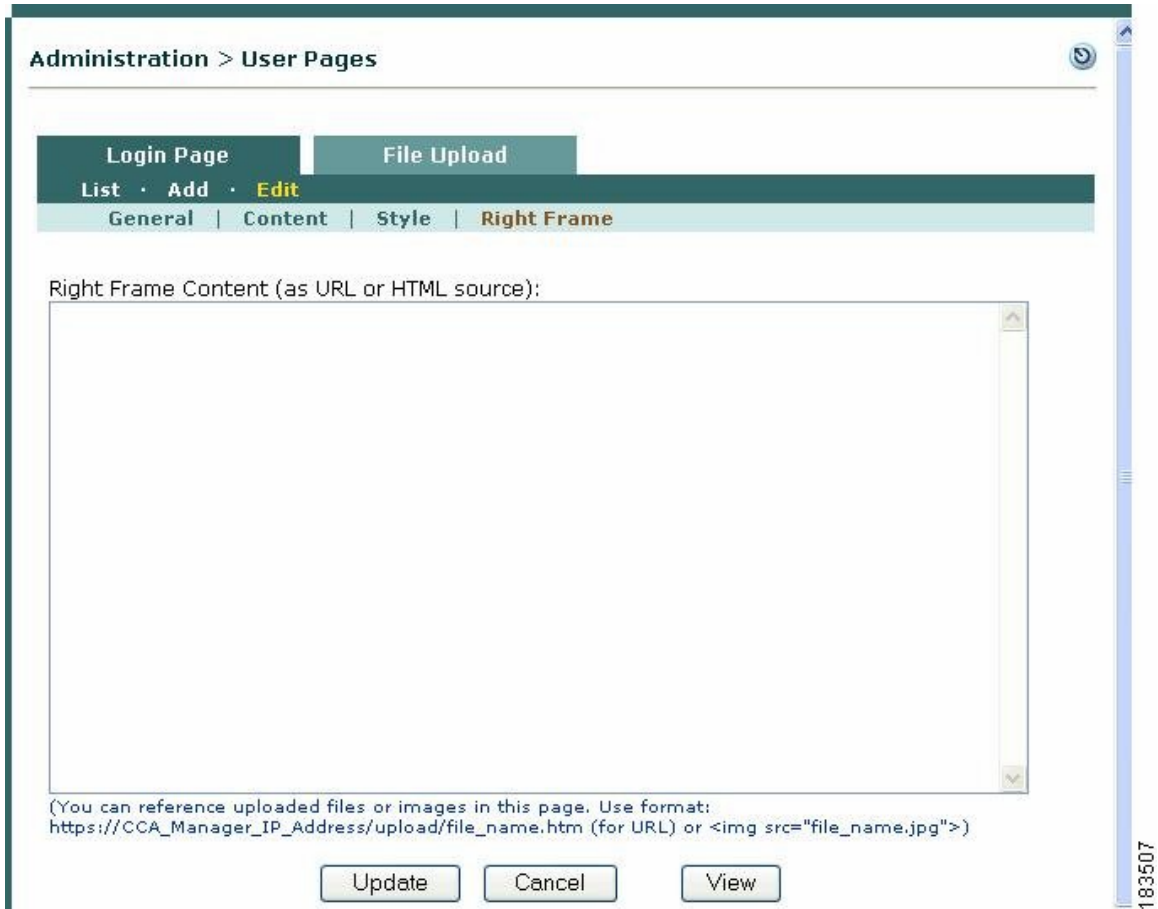
Instructions:

<input type="checkbox"/> Guest Label	<input type="text" value="GuestAccess"/>	<input type="checkbox"/> Root CA Label	<input type="text" value="Install CA Cert"/>
<input type="checkbox"/> Help Label	<input type="text" value="Help"/>	Root CA File:	<input type="button" value="Clean Access CA Cert"/>

Help Contents:

183504

3. In the right side of the login page frame, Administrator can add link to the self service portal running on IMAG. This can be done from Administration -> User Pages -> login Page -> List -> Edit -> Right Frame as shown in the figure below.



The administrator can enter the URL, https://IMAG_IP_ADDRESS/ServicePortalLinks.jsp. It is important to make sure that there are traffic policies created to allow access to the server's pointed by the URL.

Target Market Segments		Request	ID Admin	Approvals Compliance	Provision	Notification
Health Care Large Institutions Kaiser, Blue Shield etc & Hospitals	Visiting Doctors, Temporary Nurses Insurance Audits	■	■	■	■	■
Fortune 1000 Construction, Oil & Gas, Insurance Executive Centers	Contractors Remote Offices Off-Shore Entities	■	■	■	■	■
Academia Universities, Schools	Students Visiting Faculty Temp Admins	■	■	■	■	■
Financial Fund Managers, Banks, Insurance	Insurance Agents Finance Advisors Auditors	■	■	■	■	■

Contact Info

US Headquarters

2635 North First St
 Suite 212, San Jose,
 CA, 95134
 Toll Free: +1-877-875-9476
 Phone: +1-408-434-1001
 Fax: +1-408.434.1002

India Research and Development Office

Apere India Pvt Ltd
 Plot # 14, Huda Colony
 Road # 02, Banjara Hills
 Hyderabad - 500 033
 Phone: +91-40-44308080
 Fax: +91-40-44308

E-mail: app@apere.com