FORESCOUT

Guest Access

Providing safe network access to partners, contractors and visitors

Organizational Challenges

- Protect sensitive systems and data
- Securely enable hassle-free, multi-level guest access with little or no manual intervention
- Comply with regulatory mandates
- Enable visitors, contractors, customers and employees to use their own devices while enforcing appropriate network access
- Simplify rather than complicate network access control

Technical Challenges

- Enable secure, limited guest access that's non-intrusive, easily deployed and properly segmented from the internal network
- Discover and remediate devices that do not meet organizational policies and standards
- Discover, assess and monitor devices to detect anomalous behavior
- Enable secure wired or wireless guest access
- Gain comprehensive visibility and control of guest devices—with or without security agents
- Prevent infected or non-compliant devices from spreading malware across the network

Enabling guest access to your network may sound simple, but it requires balancing the needs of the guest for a painless user experience with the absolute necessity of keeping the network safe and your IT staff sane. ForeScout Technologies has a proven history of helping organizations offer guest access while maintaining the highest levels of cybersecurity and staff satisfaction.

The Challenge

How do you allow guests on your network to connect directly to the Internet while making sure they don't gain entry into network segments and servers where they have no business being? That's the challenge in a nutshell, and it's quite a technological feat when you consider that guest traffic runs on the organization's network infrastructure right alongside high-value corporate computing traffic. Of course another complicating factor is the potential danger that underlies every connection, as there is always the possibility that the user behind the guest device you're authorizing is hostile to your network and organization.

Those are the stakes. ForeScout CounterACT® is the solution. It provides the guest access web application that allows customers, visitors, consultants, contractors and other non-employees to access the network based on your policies. Wired or wireless access can range from Internet-only to full network admission. But CounterACT takes network access control well beyond simple guest access—preventing unauthorized access as well as orchestrating defense against viruses, worms and zero-day threats.

The Solution

ForeScout CounterACT delivers value in three distinct ways:

See ForeScout CounterACT provides visibility into a wide range of devices—managed and unmanaged, corporate and personal, wired and wireless—even personally owned Bring Your Own Device (BYOD) endpoints as well as Internet of Things and rogue devices. CounterACT identifies and analyzes guests' devices and applications—determining the device user, owner, operating system, configuration, software, services, patch state and the presence of security agents. In addition, CounterACT continuously monitors devices, ports and connections.

> Thanks to ForeScout CounterACT, we have been able to clean up our entire network and implement secure access for employee notebooks and guest devices. Everything has been very smooth right from day one."
>
> **— Steffen Appel, Group Leader WAN/Security at SOKA-BAU (insurance services) Wiesbaden, Germany**

Control CounterACT automates guest access enrollment and control by deciding how guest devices should comply with your security policies and selecting the appropriate onboarding options. Based on what it sees, CounterACT allows you to restrict the access of non-compliant devices, limit access to Internet-only, quarantine any device within a secure VLAN or grant access to appropriate corporate VLAN segments. In addition, it can validate and enforce endpoint compliance to ensure security patches are up to date and antimalware software is installed and running. CounterACT simplifies this process for 802.1X, non-802.1X and mixed environments—without requiring manual intervention.

Orchestrate ForeScout CounterACT's ability to see and control unmanaged devices minimizes the dangers inherent in providing access to guests. However, protecting network infrastructure requires immediate response to security incidents, and that can only be possible with intelligence sharing among security solutions. Plug-and-play integrations made possible by ForeScout Extended Modules extend CounterACT's See and Control capabilities to more than 70 leading network, security, mobility and IT management products.* For example, Enterprise Mobility Management (EMM) solutions extend secure access to smartphones and tablets. In addition, Endpoint Protection Platform (EPP) tools automate policy-driven endpoint compliance through shared insights on device protection status and endpoint enforcement, monitoring and policy compliance reporting. These bidirectional integrations enable a unified and automated security response while reducing the cost and complexity of securing network infrastructure.

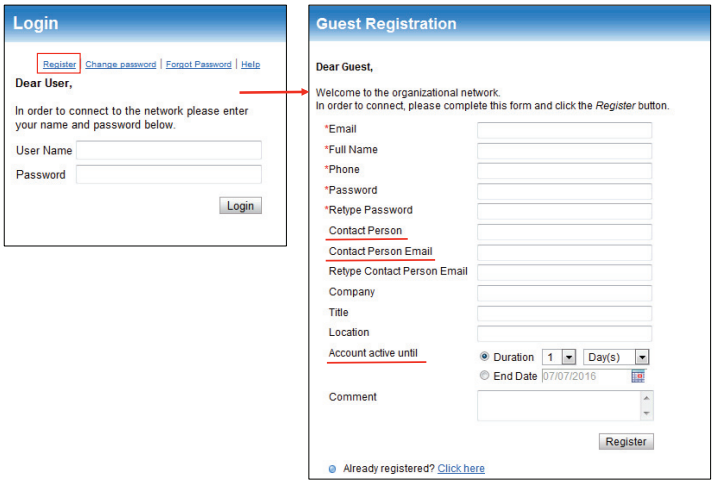
Types of Guest Access: Three Key Use Cases

As soon as CounterACT determines that a device attempting to access the network is unmanaged, it is segmented into a restricted VLAN. Users of Windows, Mac and Linux devices are presented with a log-in screen. After these unknown guests enter basic identifying information, they are classified as registered guest users and given Internet-only access. If, however, the user is a partner or contractor—or an employee accessing the network with their personally owned device—they can gain higher-level network access based on your policies and their role in the organization.

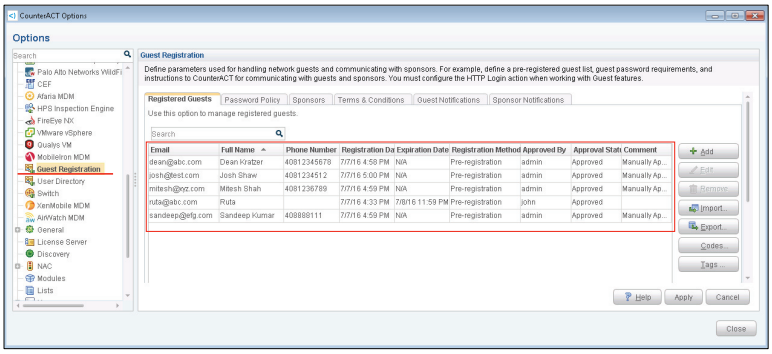
These trusted users can register as guests but will have a second option of logging in with their corporate credentials or "sponsor-approved" authorization information (via Active Directory or an LDAP-based directory). Based on policies and user profile, these users are likely to be granted access ranging from Internet/email-only to full corporate network access. As for rogue devices and hackers, they are locked out. The best they can do is register and gain Internet-only access.

In addition to access control, CounterACT provides a broad range of automated remediation options to ensure that guest devices accessing the network are compliant with policies and up to date with regard to operating systems, applications and antivirus software.

#1 Self-registration by guest using the Guest captive portal



#2 CT operator Pre/Early registration from CounterACT GUI



#3 Sponsor Portal individual guest entry and Bulk Import for multiple guest entry

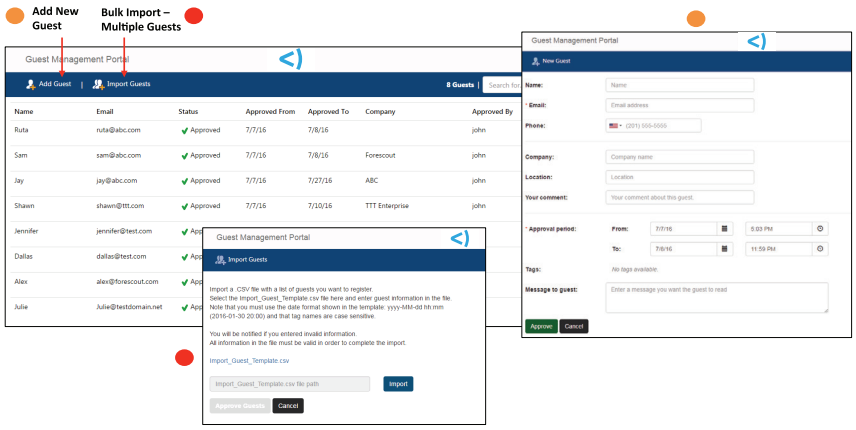


Figure 1: Guest registration log-in screens based on user profile.

*As of January 2016

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591