

ENTERPRISE GUEST ACCESS

Product Overview

Whether large or small, companies have guests. Guests can be virtually anyone who conducts business with the company but is not an employee. Many of these guests require some form of network access in order to be productive. Providing a guest user secure Internet access, let alone access to files on your network or extranet, is anything but simple. You can't afford to let your guest users access your sensitive corporate network resources.

For companies of all sizes, Juniper Networks Enterprise Guest Access supports secure, authorized network resource access, manages guest network usage, and reduces the threats that come with unauthorized guest users and their compromised devices.

Product Description

Juniper Networks® Enterprise Guest Access is a comprehensive appliance that addresses all of your guest user network access requirements. Enterprise Guest Access is based on the award winning Juniper Networks Unified Access Control solution. With the Enterprise Guest Access appliance, you can easily authenticate guest users and contractors, assess the health state of their devices, control their access to your network and its sensitive resources, and coordinate your network access policies, security, and regulatory compliance across even the most distributed of network environments.

Enterprise Guest Access is quick and easy to deploy and use, employing a simplified guest user administration interface that allows even the most nontechnical of users to create guest user access credentials and rights. It takes the burden of setting up guest user network access off the shoulders of your already overburdened IT staff, and it enables your administrative and support teams to take on this somewhat mundane yet crucially important task.

Purpose-built for small to medium sized businesses (SMBs) as well as enterprises and agencies with many guests or visitors, the Enterprise Guest Access appliance delivers wired and wireless guest network access control (NAC) seamlessly through a single, small, inline network appliance and license, without any agents to deploy or maintain. The Enterprise Guest Access appliance delivers two separate functions—guest user provisioning and authentication, and guest user access enforcement.

Enterprise Guest Access Architecture and Key Components

All-In-One Appliance

Enterprise Guest Access is an all-in-one, inline appliance that delivers role-based access control for guests, partners, and contractors. The Enterprise Guest Access appliance delivers agentless (browser-based) wired and wireless NAC for guest users seamlessly from a single appliance. The slim, sleek, small form-factor Enterprise Guest Access appliance supports secure, authorized network resource access, manages network use, and reduces the threat of unauthorized users and compromised devices. The Enterprise Guest Access appliance authenticates guest users and contractors, and assesses the health state of their devices before granting them network access.

Guest User Authorization

The Enterprise Guest Access appliance also ensures that only authorized guest users can log into and access those areas of your network to which they are authorized access based on their identity and device integrity. It integrates and leverages Juniper's Host Checker functionality, used in tens of thousands of Juniper Networks SA Series SSL VPN Appliances and IC Series Unified Access Control Appliances, enabling you to define policy that scans guest user devices attempting to connect to your network for a variety of security applications and states, including custom endpoint checks. It also enables you to create and enforce network access based on time and duration. In this way, Enterprise Guest Access enables you to deliver differentiated network access for various guest user categories such as one-time guest users, contractors, vendors, and others.

Secure Network Access

The Enterprise Guest Access appliance enables and builds a Layer 2 bridge to ensure secure network access. With Layer 2 bridging enabled, your guest users are provided with an IP address from your corporate network. Since the Enterprise Guest Access appliance is inline, it is the first place that your guest users will come to when they attempt to access your network. The Enterprise Guest Access appliance will first serve the guest user a web-based captive portal page when access is attempted. Users will use their guest credentials, which include the user name and password provided to them by your guest access administrator. They will log in and be provided with a network session. During the deployment of Enterprise Guest Access, you will have created resource access policies on the appliance which direct guest users to resources that are provisioned on the network and to which they have authorized access (for example, the Internet). User traffic has no other route to the corporate network except through the Layer 2 Enterprise Guest Access appliance bridge. Users and guests are connected to the external interface, and protected resources are connected to the internal interface.

Provisioning and Management

The Enterprise Guest Access appliance also simplifies guest user network access provisioning and management. Access is controlled through an enterprise customizable web-based captive portal, directing users to input their guest access credentials—created and provided to the guest user by your receptionist or any corporate sponsor—to gain authenticated, authorized access to your network and resources. Guest user access credentials are as simple as a user name and password. Guest user network access may be provisioned for up to 200 guest users on a single Enterprise Guest Access appliance. And, identity information of guest users is stored in a database on the appliance, which is perfect for addressing regulatory compliance audits.

Since its operation does not require that an agent be downloaded to the user's device, Enterprise Guest Access works with devices running most major operating system platforms, including Microsoft Windows, Apple Mac OS, and Linux. Being agentless means that Enterprise Guest Access requires no configuration on a guest user's device, and using a web-based captive portal means it needs zero configuration to set up, greatly simplifying its deployment and use.

Guest Administrator Accounts

A limited number of guest administrator accounts may be created. Your IT or technical staff can provision a local user or employee with limited administration rights to provide temporary access accounts for external guest users. Guest user account manager information is stored in a database local to the enterprise guest access appliance. This is useful for administrator tracking and regulatory compliance audits. Provisioning of numerous guest user account managers, typical for an office or site which is without reception or administrative staff, can be easily undertaken. Authenticated access for guest user account managers to the enterprise guest access appliance is accomplished natively or by interfacing with and leveraging existing SMB or enterprise authentication data stores, such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP), and authentication, authorization, and accounting (AAA) capabilities.

Time-Based Network Access Policies

The Enterprise Guest Access appliance enables guest user accounts to be created based on flexible, time-based network access policies. Guest user accounts may be created with a specific start and end time. For example, guest user network access might start at 9:00 a.m. and end at 5:00 p.m. Guest user accounts may also be created for a specific hourly duration, such as guest user network access being allowed for 8 hours. Guest user access can also be limited by the administrator to a specific number of days, in an hours-based format, such as for 24 hours, 48 hours, or up to 72 hours. Enterprise Guest Access affords you flexibility and control in the management of guest user network access.

Network Access Control

The Enterprise Guest Access appliance also provides a simple to deploy, easy to administer way of addressing NAC, while providing an upgrade path to Juniper's comprehensive network and application access control solution, Unified Access Control, at any time by leveraging the access and security policies already created and instituted by the SMB or enterprise with the Enterprise Guest Access appliance. This saves both time and cost.

Enterprise Guest Access Network Diagram

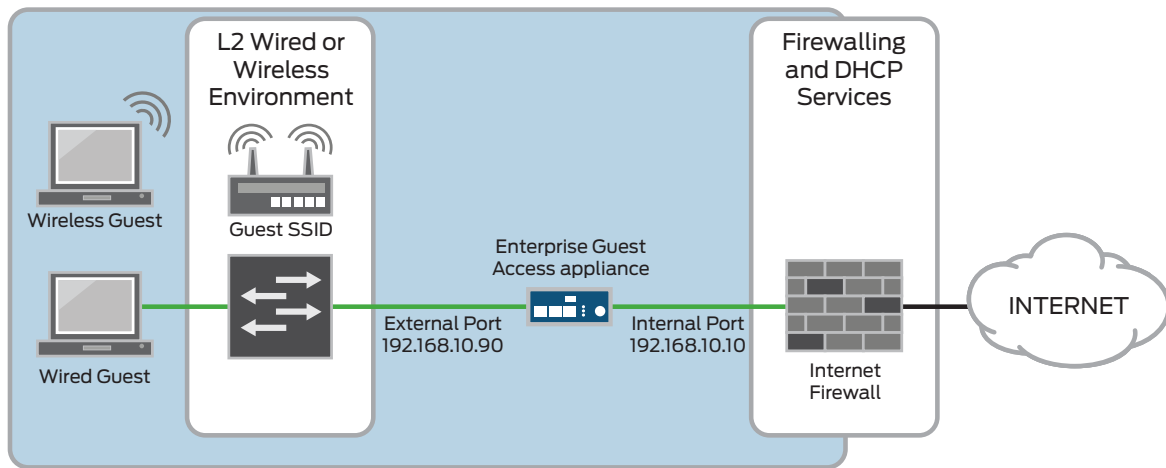
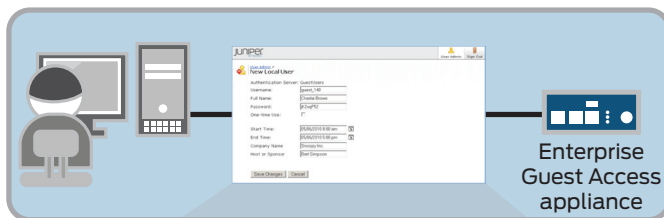


Figure 1: Juniper Networks Enterprise Guest Access

Figure 1 provides a high-level view of Juniper Networks Enterprise Guest Access. In this diagram, the Enterprise Guest Access appliance is connected inline between the wireless and wired guest users, and the Internet firewall. The Enterprise Guest Access appliance, as the inline enforcement point, blocks guest traffic until users have typed their credentials into the captive portal served to them by the Enterprise Guest Access appliance and have been authenticated for network access.

Enterprise Guest Access Sample Workflow

1. Guest access administrator creates a guest user account on the Enterprise Guest Access appliance.

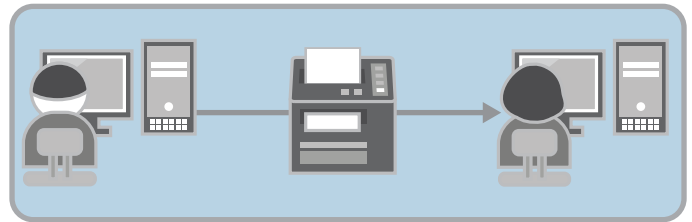


The screenshot shows the Juniper Enterprise Guest Access web interface for creating a new local user. The form includes the following fields and values:

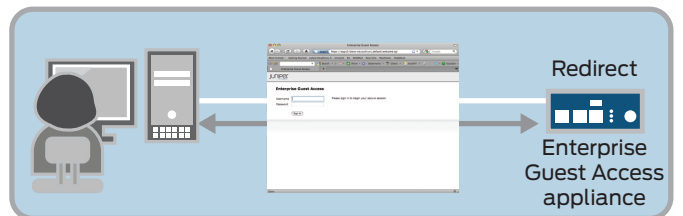
Authentication Server:	GuestUsers
Username:	guest_140
Full Name:	Charlie Brown
Password:	jk2xqF52
One-time Use:	<input type="checkbox"/>
Start Time:	05/06/2010 8:00 am
End Time:	05/06/2010 5:00 pm
Company Name:	Snoopy Inc.
Host or Sponsor:	Bart Simpson

Buttons for 'Save Changes' and 'Cancel' are visible at the bottom.

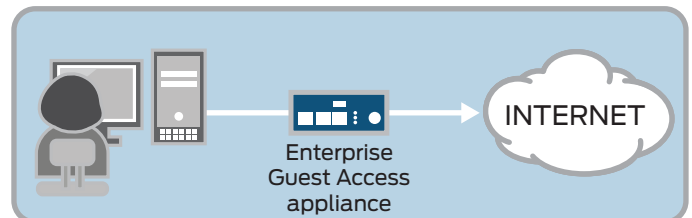
2. Guest access administrator provides credentials to the guest user, typically via hard copy printout.



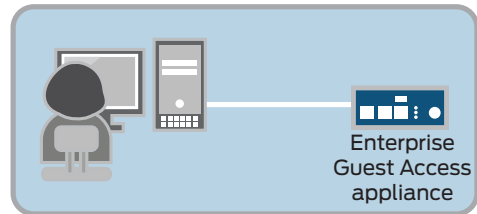
3. Guest user attempts to access the network, and access is redirected to the Enterprise Guest Access appliance, which serves the guest user a customized web-based captive portal page in which the guest user types in credentials.



4. When authentication is successful and the device being used meets the predefined security and access control policies, guest user is allowed to access the areas of the network to which authorization has been granted.



5. When guest user's account expires, the Enterprise Guest Access appliance automatically logs the user off of the network and does not allow network access until the guest receives new, updated guest user credentials.



Features and Benefits

Enterprise Guest Access offers a number of important features and benefits.

FEATURE	BENEFIT
Sleek, small form-factor appliance design	The Enterprise Guest Access appliance takes up less space and is not meant to be hidden away in a networking closet, making it easier to deploy and use.
Agentless	No agent to deploy on a guest user's endpoint device means the Enterprise Guest Access appliance is a zero configuration solution, simple to deploy and maintain, and for a guest user to operate, minimizing guest-related help desk or support calls.
Identity- and role-based guest access	Limit guest user access based on the user's identity or role. Know which guest users are on your network and when. Store guest user data for regulatory compliance audits.
Comprehensive pre-authentication endpoint integrity checks and posture assessment	The Enterprise Guest Access appliance's support of Host Checker ensures that a guest's endpoint device meets a previously decided baseline of security and access policy before it can be granted access to the network and its resources.
Support for wired and wireless guest access	Ensures that endpoint devices will meet a baseline security criteria—regardless of the guest user's access method, whether wired or wireless—and that the user will be authenticated before being allowed to access the network.
Consistent endpoint baselining across the network	For medium to large enterprises with many guest users, the Enterprise Guest Access appliance ensures that a minimum baseline of endpoint device security and access policy, and endpoint integrity is met and maintained.
Secure network access for up to 200 guest users	Purpose-built to address the network access control needs of SMBs and enterprises with many guest users.
Simplified guest user creation	Enables the administrative and support staff of an SMB or enterprise to create and distribute guest user access rights and credentials, relieving the already overworked IT staff of this task.
Secure Layer 2 bridge	The secure Layer 2 bridge of the Enterprise Guest Access appliance provides guest users with an IP address, ensuring their secure network access.
Flexible time-based guest user network access	Limits guest user network access based on specific hours, a specific number of hours, or a specific number of days (in hours).
Guest administrator user database	The list of guest administrators, stored in a database local to the Enterprise Guest Access appliance as determined by the organization, can be used to address regulatory compliance requirements.
Guest user database	The list of guest users passing policy checks and receiving guest access rights and credentials to access the network is stored in a database on the Enterprise Guest Access appliance, helping to address regulatory compliance needs.
Consistent access control	The Enterprise Guest Access appliance, when deployed in smaller branch offices or sites, can ensure that an enterprise secures its distributed network, whether remote or local, with consistent, identity-enabled access control and shared security policies.
Simple upgrade to full-blown NAC	Delivers a simple upgrade path to IC Series Unified Access Control Appliances delivering comprehensive network and application access control for small to large enterprises and government agencies while leveraging existing, previously developed policies.

Specifications

Dimensions (W x H x D)

- 7.73 x 4.31 x 1.65 in
(19.64 x 10.95 x 4.2 cm)

Weight

- 1.98 lb (900 g)

Rack mountable

- Yes, with optional tray

A/C power supply

- 100-240 VAC, 1A 50-60 Hz, 30 W maximum

System battery

- CR2032 3 V lithium coin cell

Efficiency

- 80% or greater at full load

Material

- Aluminum

Fans

- One 40 mm fan

LEDs

- Power, HDD activity, hardware alert

Ports

- RJ45 serial (console port)
- Two RJ45 Ethernet 10/100/1000 (traffic)
- USB

Operating temp

- 41° through 104° F (5° through 40° C)

Storage temp

- -40° through 158° F (-40° through 70° C)

RH (operating)

- 8% - 90% noncondensing

RH (storage)

- 5% - 95% noncondensing

Altitude (operating)

- 10,000 ft maximum

Altitude (storage)

- 40,000 ft maximum

Safety certifications

- EN 60950-1: 2006 (2nd Edition)

Emissions certifications

- EN 55022 Class B: 2006, EN 55024+A1+A2: 1998, EN 300 386 v1.4.1: 2008

Warranty

- 90 days
- Can be extended with support contract

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

MODEL NUMBER	MODEL NAME AND DESCRIPTION
Enterprise Guest Access Base System	
MAG2600	Enterprise Guest Access Appliance Base System
Endpoint License	
MAGX600-GUEST-ACCESS	Enterprise Guest Access License

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.