celestix

WSA

www.celestix.com/wsa

Comprehensive secure remote access to network resources for any user and from any location, based on trust and compliance with corporate policy

Celestix WSA delivers secure, anywhere access to corporate resources with Microsoft Forefront® Unified Access Gateway (UAG) 2010. Through a centralized management portal, organizations can securely publish applications to any users from a range of endpoints and locations, including managed and unmanaged PCs and mobile devices.

Highlights

- Secure publishing of on premise applications regardless of type
- Seamless integration with Microsoft applications such as SharePoint, Exchange and OCS/Lync
- Control access to cloud based applications such as Salesforce, Google Apps, and Office 365
- Enables a variety of access methods including SSL VPN, SSTP, and DirectAccess
- Endpoint device health control and manage out capability
- Control access based on endpoint compliance against policy
- Multiple server array deployment
- Integrated single sign on and authentication options
- Granular access policies
- Supports Windows Server 2008 (x64)
- Built-in firewall
- SQL logging
- Reduces total cost of ownership by consolidating infrastructure
- Reduces support costs by simplifying connectivity for users

WSA supports a combination of connectivity options such as SSL VPN, Windows DirectAccess and SSTP as well as built-in configurations and policies. WSA integrates a deep understanding of the applications published, the health of the device being used to gain access, and the user's identity to enforce granular access controls and policies.

Seamless and secure remote connectivity with DirectAccess

With WSA and Windows 7/8/8.1, mobile workers can seamlessly and securely access the corporate network using DirectAccess. WSA appliances can be configured as DirectAccess servers enabling domain computers to transparently connect to the network regardless of that user's location, without requiring any additional user input.

Integrated security

WSA limits risk through a combination of access policies, endpoint health inspection, and user authorization information. Administrators can set up policies that specify prerequisites that endpoints must meet for each transaction. Endpoint health can be inspected using built-in UAG policies or through integration with Network Access Protection (NAP).

Simplified remote access

WSA consolidates and standardizes access to corporate resources through a single platform. The result is a simplified ongoing management and user experience security and corporate compliance.

Designed for the **Microsoft** network

celestix

www.celestix.com/wsa

WSA APPLIANCE

Features

Administration

- Celestix COMET management console
- Web UI and wizards
- Integrates with Active Directory
- Front panel display and jog dial
- Includes standard configurations for enterprise applications and extensive customization capabilities
- Units are shipped pre-hardened with comprehensive policy configurations

Logging and reporting

- Supports monitoring, logging, and reporting for management and accounting
- Event monitoring of users, applications, and time periods
- Event logger records system usage and user activities and send alerts to the administration console
- Event query tool with pre-configured templates for full reporting capabilities
- SQL logging

High availability

- One-button system recovery
- Remote drive service
- Load balances traffic to array members, using integrated Network Load Balancing (NLB) or a hardware load balancer

Endpoint access controls

- Endpoint policy allows administrators to define compliance checks and verify endpoint settings such as active security software
- Delivers a standard SSL VPN portal and login pages for easy setup, customization, and administration
- Built-in certificate authority that grants a trusted endpoint certificate for a specific machine on request
- Integrates Windows Server 2008 NAP technology to verify client endpoint compliance against NAP policies

Connectivity options

- DirectAccess
- Remote port and socket forwarding over an SSL tunnel
- Remote Desktop Gateway (RDG)
- Network-level SSL VPN, with support for both the SSTP and Network Connector protocols

UAG 2010 licensing

- Includes OS license
- Requires a Client Access License (CAL) for each named or authenticated device or user

Models



	WSA 3400	WSA 6400	WSA 8400
Recommended users*	up to 500	500 - 5,000	5,000 - 15,000
Form factor	1U	1U	2U
CPU	Intel i5	Intel E3	2 x Intel E5
Number of processors	4 Cores	4 Cores	12 cores (hyperthreading)
Memory	8 GB	16 GB	16 GB
Cache	6 MB	6 MB	15 MB
Hard drive	SATA-II 120 GB available storage	SATA-II 120 GB available storage 2 x 160 GB hot-swappable hard drive	SATA-II 300 GB available storage 4 x 160 GB hot-swappable hard drive
Hot-swappable fans	-	–	■
Power supply	220W auto-switching universal 110/220V AC power supply	Redundant hot-swappable power supply 2 x 250W	Redundant hot-swappable power supply –2 x 500W
Disk mirror RAID	-	RAID 1	RAID 6
Gigabit ethernet ports	6	6	8
Dimensions (H x W x L)	1.75" x 17.3" x 13.0"	1.75" x 17.3" x 21.5"	3.5" x 17.4" x 23.25"

■ Standard with base unit
– Not available
* Performance guidelines only. Actual performance may vary depending upon networking and application environment.

Celestix Networks, Inc.
3125 Skyway Court
Fremont, California 94539

USA +1 510 668 0700
UK +44 (0) 118 959 6198

Japan +81 03 5210 2991
Singapore +65 6781 0700

info@celestix.com