

White Paper

Celestix WSA and DirectAccess - Comprehensive, secure remote access to corporate resources



Celestix WSA Unified Access Gateway appliance delivers secure, anywhere-access to messaging, collaboration, and other resources, increasing productivity while maintaining compliance with policy. Celestix WSA Unified Access Gateway provides a single solution for administrators to deliver access and implement granular policies based on the user's identity and the health of the device.

Overview

Celestix WSA Unified Access Gateway delivers comprehensive, secure remote access to corporate resources for employees, partners, and vendors from a diverse range of endpoints and locations, including managed and unmanaged PCs and mobile devices.

Building on the secure remote access capabilities in Microsoft Intelligent Application Gateway 2007, Celestix WSA UAG draws on a combination of connectivity options, ranging from SSL VPN to Windows® DirectAccess, as well as built-in configurations and policies. These enable Celestix WSA to provide centralized and easy management and thereby reduce management costs. In addition, Celestix WSA integrates a deep understanding of the applications published, the state of health of the devices being used to gain access, and the user's identity to enforce granular access controls and policies.

Key Features and Benefits

Access anywhere

Empowers users to be productive from virtually any device or location

Celestix WSA acts as a consolidated gateway from a diverse range of endpoints and locations, providing access through a single portal. Remote users—employees, partners, and customers—can access Web and non-Web applications and gain full VPN access to corporate networks including internal file shares and client server applications.

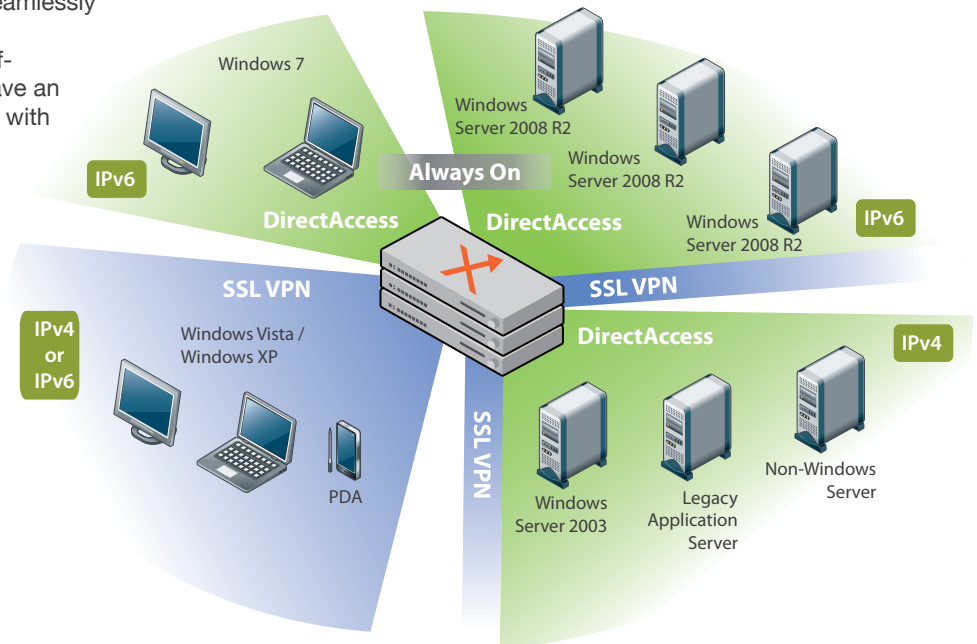
Simplifies secure remote access

Celestix WSA supports a wide range of Microsoft applications, including Microsoft SharePoint®, Microsoft Exchange Server, Remote Desktop Services, and Microsoft Dynamics® CRM through predefined optimizer modules. These modules include optimum settings and rules for securing specific applications and are based on deep research into application

Seamless and secure remote connectivity with DirectAccess

With DirectAccess in Windows 7 and Windows Server® 2008 R2, mobile workers can seamlessly and securely access the entire corporate network—file shares, intranet, and line-of-business applications—wherever they have an Internet connection. Celestix UAG works with DirectAccess to:

- Extend these benefits to legacy applications and resources, and support down-level and non-Windows clients through integrated SSL VPN capabilities and other connectivity options.
- Limit exposure associated with connecting unmanaged, down-level, and non-Windows clients through granular access controls and policies.
- Protect the DirectAccess gateway with a hardened edge solution and built-in firewall.
- Simplify deployment using built-in wizards and tools.
- Support scalability and ongoing administration through built-in array management and integrated load balancing.



behavior, browser-server interactions, and endpoint requirements. UAG also supports third-party applications such as CRM, ERP, and HR. Administrators can publish the following types of applications using Celestix WSA:

- Web applications and Web farms via reverse proxy.
- RemoteApps through a Forefront UAG portal by using Remote Desktop Services (Terminal Services) with an integrated Remote Desktop Services Gateway.
- Non-Web applications over a secure connection using socket or port forwarding as well as VPN connections

Extends Windows DirectAccess

Forefront UAG delivers DirectAccess to legacy applications and resources running on existing infrastructure and supports down-level and non-Windows clients through integrated SSL VPN capabilities and other connectivity options.

Integrated security

Enhances security and increases corporate compliance

- Limits exposure through a combination of granular access policies, deep endpoint health inspection, and user authorization information.

- Enables administrators to set up policies that specify prerequisites that endpoints must meet for each transaction. They can implement these using built-in Celestix WSA or Network Access Protection (NAP) policies downloaded from a Network Policy Server (NPS).

Enables a variety of strong authentication methods

- Integrates with Active Directory® and easily overlays a wide variety of third-party authentication solutions and repositories, allowing for strong authentication and enforcement through granular policies. This helps ensure that only authorized users or groups can access particular applications or execute transactions.
- Leverages credentials provided during a session to enable single sign-on to internal applications.

Simplified management

Reduces total cost of ownership by consolidating infrastructure

Delivers remote access connectivity through a combination of VPN, SSL VPN, Web publishing, and DirectAccess. This enables organizations to standardize and consolidate a disparate infrastructure onto one cost-effective platform.

Simplifies deployment and ongoing management

- Offers out-of-the-box appliance solution.
- Facilitates the grouping of multiple Celestix WSA appliances into an array. All array members share the same configuration and can be managed as a single entity.
- Uses wizards to simplify initial deployment and key ongoing tasks.
- Easily integrates Celestix WSA through Microsoft SQL Server® and management through System Center Operations Manager.

Reduces support costs by simplifying connectivity for users

Typically security and access technologies are fragmented, resulting in a complex user experience. Celestix WSA consolidates access to corporate resources, simplifying the user's experience and reducing support calls and their costs.

For more information about WSA appliances, contact Celestix today at:

	Americas	+1 510 668.0700
	United Kingdom	+44 (0) 118 959 6198
	Singapore	+65 6781.0700
	India	+91 44 3910 3530

