# celestix

## Celestix SecureAccess
### Solution Brief

Celestix SecureAccess is a comprehensive remote access solution designed not only to simplify the deployment of Windows-based remote access technologies, but also enhance the manageability and features that not found in standard Microsoft DirectAcess. Organizations that deploy Celestix SecureAccess for their remote access needs will find a solution that provides the best and most secure remote access experience by taking advantage of the unique capabilities of each supported client platform.

## Features and Benefits

Deploying complex connectivity customizations without specific experience or with limited time actually increases Organizational risk for information security. The Celestix SecureAccess appliance provides a more secure, cost-efficient deployment option.

### Setup Simplicity

Administrators can configure the IP address, subnet mask, default gateway, and static routes in minutes, without the need for a keyboard, mouse, or monitor. The platform also features a compact appliance form factor, allowing our devices to be mounted in any standard 19" equipment rack. Hardware-integrated disaster recovery is also included.

### Centralized Administration

The SecureAccess includes the HTML5-based management console, which is cross-platform friendly and enables remote management using any browser on any device. The web UI centralizes general Windows Server administration and Remote Access (RA) configuration, so administrators can go to one place to customize the deployment. Administrative efficiency can offset appliance costs by saving IT staff hours.

### Seamless Multi-factor Authentication Integration

Celestix MFA multi-factor authentication integrates seamlessly out-of-the-box with the Celestix SecureAccess Appliance to provide a simple solution to complex password requirements and maximizes security.

### Trusted Hardware

Our hardware has undergone extensive testing, and minimizes the attack surface by engineering just the services and applications that are necessary for security and connectivity. Hardware is hardened based on expertise gained through years of experience in networking security.

### Access Multiplicity

Every Organization is different, there is no "one size fits all" scheme for remote access. Celestix SecureAccess provides for multiple access scenarios and the supporting functions they require. Secure access strategies can include managed/unmanaged devices, application publishing, and facilitation for public and private cloud connectivity.
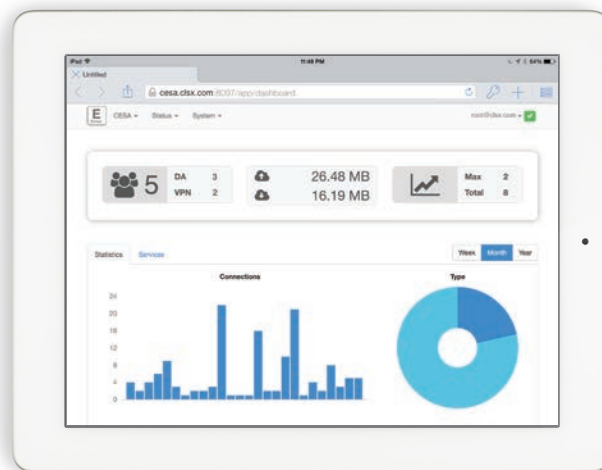
**Expanded Functionality**

Celestix SecureAccess improves upon current Server 2012 functionality with exclusive features. Reporting, alerting, and monitoring tools both simplify daily management and support compliance requirements. Real-time connection management provides greater control over user access to resources.

**More Client Coverage**

DirectAccess, as awesome as it is, only works for domain-joined Windows clients that are running either Windows 7 Enterprise/ Ultimate Edition, or Windows 8.x and later Enterprise Edition. Celestix SecureAccess extends DirectAccess experience for roaming users even for Windows Professional editions and Mac OSX computers. The innovative SecureAccess feature gives both Windows Professional and Mac users the seamless, transparent always-on VPN experience that Windows Enterprise have enjoyed for years. Remote users automatically connect to the office network when they have an Internet connection.

**Future Ready**

Future enhancements can be added through updates to both Remote Access and the SecureAccess platform. Examples include virtualization, SSO enhancements, and forms-based authentication. By allowing Organizations to leverage new features, Celestix SecureAccess continues to provide value for the investment.

## Celestix SecureAccess vs. Generic Windows Server 201x White Box

Organizations may wonder whether an appliance provides worthwhile advantages over deploying a generic Windows Server 2012 R2 white box. While Server 2012 offers a host of connectivity features, most companies don't have specialized or in-depth knowledge regarding best configuration practices for the features that are now included. To help IT departments handle an ever-increasing scope of services, reducing complexity while maintaining security is essential to advance organizational goals.

Celestix strives to deliver high value to our customers. Our appliances save installation time, ease configuration tasks, and reduce licensing costs. They are hardened for security and undergo extensive, purpose-specific testing. Celestix also adds functionality not available in standard Server 2012 deployments. Imminent product releases will provide a wealth of additional features that will continue to return on connectivity investments.

| Features | Celestix SecureAccess | Microsoft DirectAccess |
|---|---|---|
| Delivery Platform | Physical and virtual appliance | Software |
| Operating System | Hardened Windows Server 2012 R2/ Windows Server 2016 | Windows Server 2012 R2/Windows Server 2016 |
| Management Tool | Celestix Comet Web UI | Windows Interface |
| Web-based interface | 🟢 | 🔴 |
| Supported clients | Any Windows edition and Mac OSX | Windows 7,8,10 Enterprise only |
| • Windows 7,8,10 Enterprise | 🟢 | 🟢 |
| • Windows 7,8.10 Professional and below | 🟢 | 🔴 |
| • Mac OSX | 🟢 | 🔴 |
| • iOS | Available in late 2017 | 🔴 |
| Remote Access 'Kill Switch' | 🟢 | 🔴 |
| Protocols Supported | Domain Join or Non-domain joined for SecureAccess | Domain Join |
| Methods of Authentication supported | Domain Authentication / Radius / Certificate | Domain Authentication / Radius / Certificate |
| Settings delivery | Distributed to the client via Group Policy, SecureAccess Offline or SCCM | Distributed to the client via Group Policy |
| Reporting | Enhanced | Limited |
| Device Management | 🟢 | 🔴 |
| Hardened OS | 🟢 | 🔴 |
| Support | 24x7x365 support available | Limited troubleshooting documentation and phone support. |

🟢 Available    🔴 Not Available

# celesti**x**

## Supported Remote Access Scenarios

Celestix SecureAccess solution supports the following secure remote access scenarios.

**DirectAccess for Managed Windows Clients** – DirectAccess leverages existing Windows platform technologies to provide seamless and transparent, always-on, bi-directional remote access for corporate-managed Windows devices. DirectAccess clients must be deployed using the Enterprise SKU (Windows 7 Ultimate is also supported) and must be domain-joined. Client configuration is performed exclusively using Active Directory Group Policy, making client provisioning as simple as adding a computer account to a security group. DirectAccess allows remote clients to access on-premises resources in the same way they do inside the corporate network. This streamlined, familiar access improves productivity and reduces help desk support costs.

**SecureAccess client** extends DirectAccess experience for roaming users even for Windows Professional editions and Mac OSX computers.

**Client-Based VPN for Non-Managed Clients** – To provide support for non-managed clients, the Celestix SecureAccess platform also includes traditional VPN access using protocols such as IKEv2, SSTP, L2TP/IPsec, and PPTP. Supported VPN clients are available natively in Windows and most other desktop and mobile operating systems.

**Web Application Proxy (WAP) for Application Publishing** – Often it is desirable to simply provide remote access to an application individually as opposed to providing low-level network connectivity for remote users. The WAP functionality allows organizations to securely publish on-premises web-based applications such as Exchange Outlook Web App (OWA) and SharePoint quickly and easily.

**Remote Desktop Gateway** – Many organizations have chosen to implement a Virtual Desktop Infrastructure (VDI) solution to address the diverse requirements for secure remote access to internal applications and services.  Celestix SecureAccess enables secure remote access to on-premises VDI deployments using firewall-friendly transports and provides improved performance over earlier releases.

**Site-to-Site VPN** – Organizations can deploy Celestix SecureAccess to enable cross-premises network connectivity to public cloud providers or to establish secure remote branch office connectivity.

## Deployment Options

### Hardware Appliance

The Celestix SecureAccess E Series is delivered on our advanced hardware appliance platform and ensures the best security and performance for remote access deployments. The E Series is a dedicated, purpose-built hardware platform that features a certified configuration with predictable performance. It is available in a variety of models to meet the needs of organizations large and small. The E Series greatly simplifies the deployment and ongoing management for corporate remote access. It also includes features that ease the configuration and monitoring for remote access such as a proprietary web-based management console, interactive drill-down reporting, streamlined client troubleshooting, and proactive session management.

### Virtual Appliance

Many organizations today are moving away from hardware-based devices and instead are deploying only virtualized solutions. To address these needs, Celestix has introduced a virtual edition of their popular E Series appliance platform. The V Series is available as a software download that will automatically configure an existing virtual machine as a Celestix E Series appliance. The V Series includes all of the same features provided by the hardware appliance versions including. In addition, the V Series is fully supported by Celestix global support.

While the V series doesn't provide the same predictable performance of our dedicated, purpose-built hardware appliances, it can be an effective alternative to deploying hardware for many small to mid-sized organizations.

# celestix

## Celestix Rapid Pilot Services

Celestix provides evaluation services for organizations seeking to perform proof of concept or pilot deployments of DirectAccess and the Celestix SecureAccess appliances.

Our evaluation program provides the following services:

- Technical and business requirement review
- Develop evaluation criteria and time-line
- Installation and configuration of the appliance(s)
- Validation of infrastructure and client configuration
- Up to 30 days of PoC Support across 20 clients (on Windows 10 Enterprise PCs) and 10 SecureAccess clients (on Windows 10 Professional or Mac PCs)*
- Access to Celestix DirectAccess Experts

*Subject to change based on need

Technical Requirements

- Celestix SecureAccess physical appliance or virtual appliance
- Enterprise PKI
- DirectAccess client natively available on Windows 10 Enterprise
- SecureAccess client for Mac or Windows 10 Pro computers
- Active Directory
- IPv6 Capable DNS Servers