

# SECURITY YOU NEED FOR THE NETWORK YOU HAVE



Celestix Appliances für  
Microsoft Forefront

**msa**

Microsoft Internet Security  
& Acceleration Server 2006  
Appliance

**wsa**

Microsoft Intelligent  
Application Gateway 2007  
Appliance

**CLB**

Celestix Load Balancer

**HOTPin**

2FA - Lösung für die Celestix  
WSA Appliance ohne Token



# Warum einen ISA Server? Und warum als Appliance?

## **Der ISA Server gehört zur Microsoft Forefront-Familie, der neuen Produktreihe für den Security-Bereich.**

Gesehen haben Sie sie sicher schon oft, aber haben Sie sich auch schon einmal eingehender mit dem Celestix Appliances für den Microsoft ISA und den IAG Server beschäftigt? Realisieren Sie deutlich preiswerter als mancher Mitbewerber sichere VPN Verbindungen, kombiniert mit einer Application Layer Firewall und einem Webproxy mit Caching-Funktion.

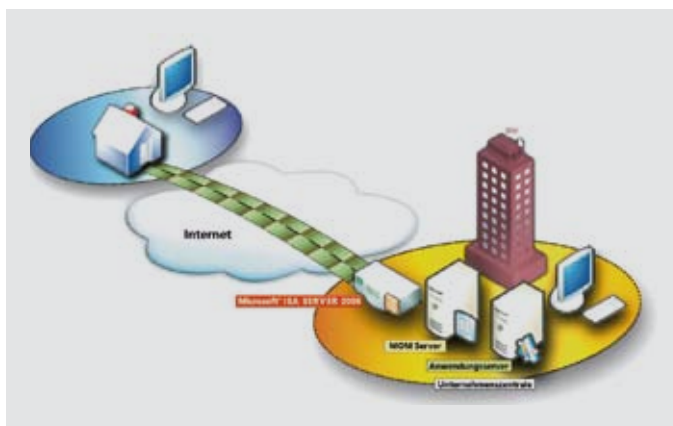
Der ISA-Server von Microsoft auf einer Celestix-Appliance ermöglicht einen sicheren Fernzugriff auf unterschiedlichste Unternehmensanwendungen. So gewährleisten Sie, dass Mitarbeiter im Außendienst oder im Home Office problemlos auf Daten und Anwendungen in der Firma zugreifen können. Sie können den Zugriff auch per Authentifizierung oder mittels Zertifikate überwachen.

Eine der am häufigsten veröffentlichten Anwendungen im Unternehmensbereich ist Microsoft „Exchange“. Der ISA-Server unterstützt alle Versionen des Exchange-Servers und bietet als zwischengeschaltete Authentifizierungsstelle – oder auch „Man in the Middle – effiziente Absicherungsmechanismen. Somit wird gewährleistet, dass keine ungewollten Zugriffe auf den Exchange-Server stattfinden.

In Verbindung mit einem Exchange-Server kann der ISA folgende Web Client Services veröffentlichen: Outlook Web Access, Outlook RPC/HTTP(s), Outlook Mobile Access und Exchange ActiveSync. Somit können übrigens auch Firmen-Smartphones ohne weiteren Service Ihres Providers Mails empfangen und versenden.



Microsoft®  
Internet Security &  
Acceleration Server



Neben den Publishingfunktionen des ISA-Servers, bleibt der ISA-Server immer noch eine der weltweit am häufigsten installierten Web-proxy mit Caching-Lösungen. Die Vorteile einer Celestix-Appliance-Lösung liegen vor allem in der auf die Anforderungen des ISA-Servers abgestimmten Hardware (high performance appliance platform) und dem gehärteten Windows Betriebssystem – das heißt, alle Services, die Sie unter dem ISA-Server nicht benötigen werden „ausgeschaltet“ und unterstützen die Sicherheit des ISA-Servers zusätzlich. Der ISA-Server selbst ist nach dem “Common Criteria EAL 4+” vom deutschen BSI zertifiziert.

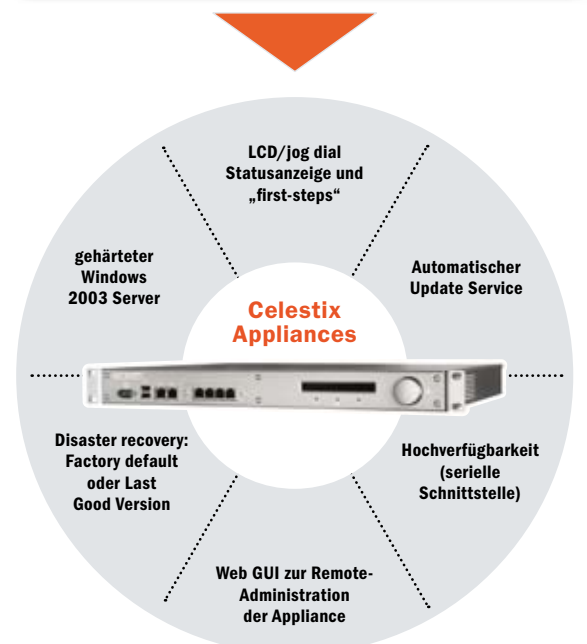
Alle Celestix Appliances verfügen über eine versteckte Partition, von der aus Sie Ihre Appliance auf „Factory Default“ oder eine von Ihnen abgespeicherte „Last Good Version“ zurücksetzen können. Hiermit werden Ihnen Ausfallzeiten erspart. Die Konfiguration des ISA-Servers kann außerdem auch noch auf ein gesondertes Backup gesichert werden.

Celestix baut für Microsoft hochwertige Appliances, auf denen sowohl ein gehärteter Windows Server 2003, als auch der ISA/ IAG Server bereits installiert ist. Ergänzt wird die Box durch eine von Celestix entwickelte Web-Oberfläche zur Fernwartung des jeweiligen Servers.

Sie können Ihren Kunden eine geschlossene Komplettlösung bereitstellen – Sie müssen nichts mehr installieren und haben keinen Ärger mehr mit überflüssigen Bestandteilen des Betriebssystems. Sie kaufen alle Lizenzen zusammen: Hardware, Betriebssystem & Software und haben nur einen Supportweg. Sie können optional Kaspersky Antivirus und Websense Websecurity einbinden, die Produkte stehen auf der Appliance zum Download bereit und integrieren sich nach der Installation in die Weboberfläche.

Das Upgrade auf das Threat Management Gateway (TMG) – dem Nachfolger vom ISA Server ist in dem Support bereits enthalten – Sie bekommen dann von Celestix das Image des neuen Betriebssystems und die neue Software. Die Hardware ist bereits auf 64bit umgestellt. Die Konfiguration werden Sie übernehmen können. Das TMG wird Ende des Jahres auf den Markt kommen und wird optional Forefront Antivirus und einen URL-Filter enthalten. Weitere Features werden HTTPS-Scanning, Email-Security und die Integration von „Stirling“ (Management Server).

Überzeugen Sie sich selbst von der Qualität und der Performance der Appliances und bestellen Sie sich für 14 Tage ein Testgerät bei Wick Hill!



# Vertrauen in Technik – das „common criteria“ ELA4+

## Viele Kunden aus dem öffentlichen Bereich legen Wert auf eine Zertifizierung Ihres Produktes vom BSI (Bundesamt für Sicherheit in der Informationstechnik).

Als Grundlage für die Prüfung der Vertrauenswürdigkeit von IT-Produkten dienen verschiedene Sicherheitskriterien, unter anderem den CC- „Common Criteria“ (Harmonisierung aller relevanten Sicherheitskriterien und weltweit anerkannter Standard ISO/IEC 15048). Sie bieten durch die Normierung als Standard ISO/IEC 15048 erstmalig einen umfangreichen Katalog von vordefinierten Sicherheitsfunktionalitäten und somit eine international anerkannte Sprache zur Beschreibung von IT-Sicherheit. Internationale Abkommen gewährleisten eine weltweite Anerkennung der Zertifizierungsergebnisse nach den CC. Das Ergebnis der Prüfung nach CC (Sicherheitsfunktionalität, EAL-Stufe, Stärke der Sicherheitsfunktionen) wird durch das BSI-Sicherheitszertifikat bestätigt.

Die Sicherheitskriterien schaffen Vergleichbarkeit der Ergebnisse unabhängiger Prüfungen und Bewertungen der Sicherheit. Dies wird durch Bereitstellung einer gemeinsamen Menge von Anforderungen an die Sicherheitsfunktionen von IT-Produkten und an die geprüften Vertrauenswürdigkeitsmaßnahmen erreicht. Das Evaluationsverfahren führt ein Maß für das Vertrauen ein, indem die Sicherheitsfunktionen dieser Produkte und Systeme und die Vertrauenswürdigkeitsmaßnahmen den Anforderungen genügen.

Das BSI-Sicherheitszertifikat macht IT-Produkte transparent durch die exakte Beschreibung der Sicherheitsleistung des IT-Produktes in Verbindung mit den abzuwehrenden Bedrohungen und einer Bewertung, die angibt, wie stark die Sicherheitsfunktionen sich diesen Bedrohungen widersetzen vertrauenswürdig durch die Prüfung aller Aspekte wie Vertraulichkeit, Integrität und Verfügbarkeit vom Entwurf über die Produktion und die Auslieferung bis zum Einsatz des IT-Produktes direkt nutzbar durch eine genaue Beschreibung der Administration und der Einsatzumgebung des IT-Produktes und durch Aufzeigen von Schwachstellen mit Hinweisen, wie mögliche Auswirkungen verhindert werden können passend für Ihren Bedarf wenn das Zertifikat bestätigt, dass das IT-Produkt dem Sicherheitsprofil Ihrer Anwendung und Einsatzumgebung entspricht.





**Celestix MSA™ Security Appliances bieten für den Einsatz der Microsoft ISA Server-Firewall eine einzigartige Kombination aus Performance, Zuverlässigkeit, umfassendem Support und günstigem Preis. All dies macht die Celestix MSA-Familie zum unangefochtenen Marktführer bei ISA Server-Appliances.**

## Features und Nutzen

### EINFACHER EINSATZ

Celestix MSA Appliances sind serienmäßig voll ausgestattet und einsatzbereit, ohne dass zusätzliche Software installiert werden muss. Die einzigartige Celestix SlingSHOT™ Appliance Engine mit Jog-Dial und LED-Display erlaubt dem Benutzer die direkte Einrichtung der Anfangsparameter, wie z.B. der IP-Adresse, auf einfachstem Wege. Die Installation benötigt kaum mehr als 15 Minuten vom Auspacken bis zur voll funktionstüchtigen Firewall. Ein einziger Ansprechpartner sowohl für Hardware- als auch für Softwaresupport sorgt dafür, dass Fragen, die trotz aller Einfachheit auftreten können, umgehend und unkompliziert beantwortet werden.

### NAHTLOSE INTEGRATION IN DIE MICROSOFT-INFRASTRUKTUR

Der ISA Server 2006 integriert sich nahtlos in die bekannten Microsoft-Anwendungen wie Sharepoint, Exchange Server und ActiveDirectory. Der ISA Server ist die einfachste und direkte Methode, um externen Usern Zugriff auf Unternehmensanwendungen wie E-Mail, Web-Services oder Sharepoint-Services zu gewähren und gleichzeitig volle Zugangskontrolle und Einhaltung der Richtlinien zu gewährleisten.

### BENUTZERFREUNDLICHKEIT

Celestix hat den ISA Server noch benutzerfreundlicher gemacht. Es wurde eine webbasierte Managementschnittstelle hinzugefügt, mit der sämtliche Parameter der ISA Firewall gesteuert und überwacht werden können. Standard-Management-Methoden werden ebenfalls unterstützt, jedoch empfinden die meisten User die webbasierte Steuerung als einfacher. Die webbasierte Schnittstelle ist Bestandteil der Celestix SlingSHOT Appliance Engine - keine andere Appliance verfügt darüber.

### ERWEITERTE STATE-OF-THE-ART SECURITY

MSA Appliances laufen unter dem Microsoft Internet Security and Acceleration (ISA) Server 2006, einer der modernsten Application-Layer-Firewalls der dritten Generation auf dem Markt. Celestix erweitert die Sicherheit des ISA Server durch Vorhärtung des Betriebssystems und garantiert damit Sicherheit gegen alle bekannten Sicherheitslücken und Exploits.

### FEATURES

- Microsoft ISA Server 2006
- Nahtlose Integration in Ihre Microsoft IT Infrastruktur
- Breitgefächerte Performancemodelle
- Betriebsfertige Auslieferung
- Web GUI für einfache Konfiguration und Steuerung
- LCD Frontpanel und Jog Dial für einfache Konfiguration und Echtzeit-Statusanzeige
- Wiederherstellung der letzten funktionierenden Version oder Werkseinstellungen per Knopfdruck
- Installation einer kompletten Firewall, VPN- und Caching-Lösung in weniger als 15 Minuten
- gemanagter Softwareupdate-Service
- Garant für Zuverlässigkeit: Redundanz, Failover, Load Balancing
- Voller Support durch Celestix: Ein Ansprechpartner für alle Service-Angelegenheiten
- Umfangreichste Ausstattung und höchste Performance im Preissegment

### AUSGELEGT FÜR:

- Microsoft ISA Server 2006
- Nahtlose Integration in Ihre Microsoft IT Infrastruktur
- Breitgefächerte Performancemodelle
- Betriebsfertige Auslieferung
- Web GUI für einfache Konfiguration und Steuerung
- LCD Frontpanel und Jog Dial für einfache Konfiguration und Echtzeit-Statusanzeige
- Wiederherstellung der letzten funktionierenden Version oder Werkseinstellungen per Knopfdruck
- Installation einer kompletten Firewall, VPN- und Caching-Lösung in weniger als 15 Minuten
- gemanagter Softwareupdate-Service
- Garant für Zuverlässigkeit: Redundanz, Failover, Load Balancing
- Voller Support durch Celestix: Ein Ansprechpartner für alle Service-Angelegenheiten
- Umfangreichste Ausstattung und höchste Performance im Preissegment
- Vollständige Bandbreite an Sicherheitsanwendungen im Unternehmensnetzwerk
- Mit wachsenden Netzwerkanforderungen skalierbar
- Maximale Verfügbarkeit
- Nahtlose Integration in Netzwerk und Active Directory
- Application Publishing (Reverse Proxy)
- Internet-Proxy
- VPN-Gateway





MSA Series	MSA3000i	MSA4000i	MSA5000i	MSA6000i	MSA3000b
<b>Processor</b>	Intel® Pentium Dual-Core	Intel® Core 2 Duo	Dual-Core Intel® Xeon®	Dual-Core Intel® Xeon®	Intel® Pentium Dual-Core
Clock Speed/FSB	2.0GHz/800MHz	2.40Hz/800MHz	3.0GHz/1333MHz	3.0GHz/1333MHz	2.0GHz/800MHz
Memory	2GB	2GB	4GB	4GB	2GB
Platform	Scorpio-X	Scorpio-X	Pyxis	Pyxis	Scorpio-X
Foot Print	1U	1U	1U	2U	1U
SSL Cypto card	nein	(900 TPS, 100 Mbps)	(17,000 TPS, 2.5 Gbps)	(17,000 TPS, 2.5Gbps)	nein
Mirror Hard Drives	nein	nein	nein	ja	nein
Redundant Power Supplies	nein	nein	nein	ja	nein
<b>Microsoft ISA</b>	Workgroup Edition				Enterprise Branch Edition
Deployment type	Education, Small/ Medium Size business	Education, Mid size enterprise	Government, Mid Large enterprise	Government, Mid Large enterprise	Remote/Branch office
Type of broadband	T-1 or DSL	T-1	T-1 or T-3	T-3	T-1 or DSL
Ideal for	Proxy and Web filtering, secure application publishing, gateway anti-virus scanning, Remote access, Firewall.				All the features in (i) + NLB array size up to 2 + Required CSS management
<b>Performance</b>					
Firewall (Mbps)	1,500	2,370	3,438	3,438	1,500
ISA forward proxy (Mbps)	144	320	499	499	144
ISA forward proxy (TPS)	877	1.924	2.994	2.994	877
ISA + WSS (TPS)	538	1.005	2.082	2.082	538
ISA + WSS (Mbps)	88	166	345	345	88
ISA + KAV (TPS)	138	263	427	427	138
ISA + KAV (Mbps)	22	43	70	70	22
ISA + WSS + KAV (TPS)	127	223	406	406	127
ISA + WSS + KAV (Mbps)	20	36	66	66	20
<b>Concurrent Users</b>					
ISA Forward Proxy	550	1.250	3.000	3.000	550 (scalable to 1.100)
ISA + WSS	-	650	2.000	2.000	300 (scalable to 600)
ISA + KAV	150	250	550	550	150 (scalable to 300)
ISA + WSS + KAV	-	150	500	500	75 (scalable to 150)
VPN	100	100	100	100	100

MSA Series	MSA4000b	MSA6000b	MSA5000e	MSA6000e	MSA8000e
<b>Processor</b>	Intel® Core 2 Duo	Dual-Core Intel® Xeon®	Dual-Core Intel® Xeon®	Dual-Core Intel® Xeon®	2 x Quad-Core Intel® Xeon®
Clock Speed/FSB	2.40Hz/800MHz	3.0GHz/1333MHz	3.0GHz/1333MHz	3.0GHz/1333MHz	2.5GHz / 1333MHz
Memory	2GB	4GB	4GB	4GB	4GB
Platform	Scorpio-X	Pyxis	Pyxis	Pyxis	Hydrus
Foot Print	1U	2U	1U	2U	2U
SSL Cypto card	(900 TPS, 100 Mbps)	(17,000 TPS, 2.5 Gbps)	(17,000 TPS, 2.5 Gbps)	(17,000 TPS, 2.5 Gbps)	(17,000 TPS, 2.5 Gbps)
Mirror Hard Drives	nein	ja	nein	ja	ja
Redundant Power Supplies	nein	ja	nein	ja	ja
<b>Microsoft ISA</b>	Enterprise Branch Edition		Enterprise Edition		
Deployment type	Regional branch	Regional office	Government, Mid enterprise	Government, Large enterprise	Government, ISP, Larger enterprise
Type of broadband	T-1	T-3	T-1 or T-3	T-3	T-3
Ideal for	All the features in (i) + NLB array size up to 2 + Required SS management		All the features in (i) series + NLB array size up to 32 + Loadbalancing + High availability		
<b>Performance</b>					
Firewall (Mbps)	2,370	3,438	3,438	3,438	3,752
ISA forward proxy (Mbps)	320	499	499	499	532
ISA forward proxy (TPS)	1.924	2.994	2.994	2.994	3.192
ISA + WSS (TPS)	1.005	2.082	2.082	2.082	2.320
ISA + WSS (Mbps)	166	345	345	345	385
ISA + KAV (TPS)	263	427	427	427	752
ISA + KAV (Mbps)	43	70	70	70	124
ISA + WSS + KAV (TPS)	223	406	406	406	664
ISA + WSS + KAV (Mbps)	36	66	66	66	110
<b>Concurrent Users</b>					
ISA Forward Proxy	1,250 (scalable to 2,500)	3,000 (scalable to 6,000)	3,000 (scalable to 96,000)	3,000 (scalable to 96,000)	7,000 (scalable to 224.000)
ISA + WSS	650 (scalable to 1,300)	3,000 (scalable to 6,000)	2,000 (scalable to 64,000)	2,000 (scalable to 64,000)	3,000 (scalable to 96,000)
ISA + KAV	250 (scalable to 500)	550 (scalable to 1,100)	550 (scalable to 17,600)	550 (scalable to 17,600)	1,500 (scalable to 48,000)
ISA + WSS + KAV	150 (scalable to 300)	500 (scalable to 1,000)	500 (scalable to 16,000)	500 (scalable to 16,000)	1,500 (scalable to 48,000)
VPN	100	100	4000	4000	4000

Stand 03 2009; Änderungen und Irrtümer vorbehalten\*

# Warum einen IAG Server? Und warum als Appliance?



Microsoft®  
**Internet Security &  
Acceleration Server**



## **Microsoft Intelligent Application Gateway 2007 auf einer Celestix WSA Appliance Celestix hat für Microsofts Intelligent Application Gateway eine leistungsfähige Appliance entwickelt – Die Celestix WSA -Appliance.**

Mit dem IAG kombiniert Microsoft den ISA Server 2006 und das Intelligent Application Gateway der Firma Whale Communications zu einer performanten und gleichzeitig sicheren Fernzugriffslösung über SSL-VPN. Die Edge Security- und Access-Produkte der Microsoft Forefront-Familie, der Internet Security and Acceleration (ISA) Server 2006 und das Intelligent Application Gateway (IAG) 2007 leisten einen entscheidenden Beitrag zum Schutz Ihrer IT-Umgebung gegen Gefahren aus dem Internet. Gleichzeitig unterstützen sie Ihre Anwender mit schnellem, policy-basiertem Zugriff auf Unternehmens-Anwendungen und -Daten:

- **Sicherer Remote-Access: Zugriff für Mitarbeiter, Partner und Kunden – praktisch unabhängig vom Gerät und Standort**
- **Sicherheit für Zweigniederlassungen: Verbesserte Connectivity und**
- **Sicherheit für Remote-Standorte**
- **Internet-Zugriffsschutz: Wirkungsvollere Abschirmung der IT-Infrastruktur gegen Gefahren aus dem Internet**

Mit dem Intelligent Application Gateway können Sie Ihren Anwendern ein Portal zur Verfügung stellen, auf dem über eine SSL-VPN Verbindung die Anwendungen bereitgestellt werden. Durch die Firewallinstanz des ISA-Servers wird bei der IAG-Appliance volle Sicherheit gewährleistet. Sie können das Portal optisch an Ihre Firma anpassen und alle Icons etc verwenden, die sie möchten.

Mit einem IAG haben Sie außerdem die Möglichkeit, den Zugriff granular zu steuern. Somit können Sie nicht nur den Zugriff per Authentifizierung oder Zertifikat gewährleisten, sondern Sie können auch bestimmen, welche Softwarepakete installiert sein müssen für einen vollen Zugriff, welchen Signaturstand das Antivirenprogramm hat und auf welchem Windows Patchlevel der Client steht.

Ob Internetcafe, Firmenlaptop oder fremdes Firmennetzwerk: Das IAG schafft Transparenz und Sicherheit, weil die Clients beim Zugriff überwacht werden und der Umfang des Zugriffes vorher festgelegt wird. Diese Endpoint-Überprüfung ist an Ihre Bedürfnisse anpassbar und eines

der wichtigsten Features des IAG. Erfüllt ein Client Ihre Anforderungen nicht, werden seine Zugriffsrechte heruntergesetzt um Datenverluste zu minimieren. Erfüllt der Nutzer alle Ihre Anforderungen, kann er über das IAG-Portal von zu Hause aus so arbeiten, als säße er im Büro. Nachdem der Nutzer sich ausgeloggt hat, werden alle Sitzungsrückstände von seinem Client entfernt.

Wenn Sie ein Intelligent Application Gateway nutzen, müssen Sie nicht zwei Instanzen konfigurieren (ISA und IAG), weil dies der IAG-Server übernimmt. Das heißt, dass man auf dem ISA-Server keinerlei Policies konfigurieren muss um die Erreichbarkeit des IAG-Portals zu gewährleisten.

Den Möglichkeiten bei der Einrichtung der Policy sind mit einem Intelligent Application Gateway keine Grenzen gesetzt – Sie können die Freigabe von Anwendungen auf Gruppen und einzelne Nutzer herunter brechen und hier jeweils nach den sich einwählenden Clients unterscheiden.

Alle Celestix Appliances verfügen über eine versteckte Partition, von der aus Sie Ihre Appliance auf „Factory Default“ oder eine von Ihnen abgespeicherte „Last Good Version“ zurücksetzen können. Hiermit werden Ihnen Ausfallzeiten erspart. Die Konfiguration des ISA-Servers kann außerdem auch noch auf ein gesondertes Backup gesichert werden.

Celestix baut für Microsoft hochwertige Appliances, auf denen sowohl ein gehärteter Windows Server 2003, als auch der ISA/ IAG Server bereits installiert ist. Ergänzt wird die Box durch eine von Celestix entwickelte Web-Oberfläche zur Fernwartung des jeweiligen Servers.

Sie können Ihren Kunden eine geschlossene Komplettlösung bereitstellen – Sie müssen nichts mehr installieren und haben keinen Ärger mehr mit überflüssigen Bestandteilen des Betriebssystems. Sie kaufen alle Lizenzen zusammen: Hardware, Betriebssystem & Software und haben nur einen Supportweg. Sie können optional Kaspersky Antivirus und WebSense Websecurity einbinden, die Produkte stehen auf der Appliance zum Download bereit und integrieren sich nach der Installation in die Weboberfläche.

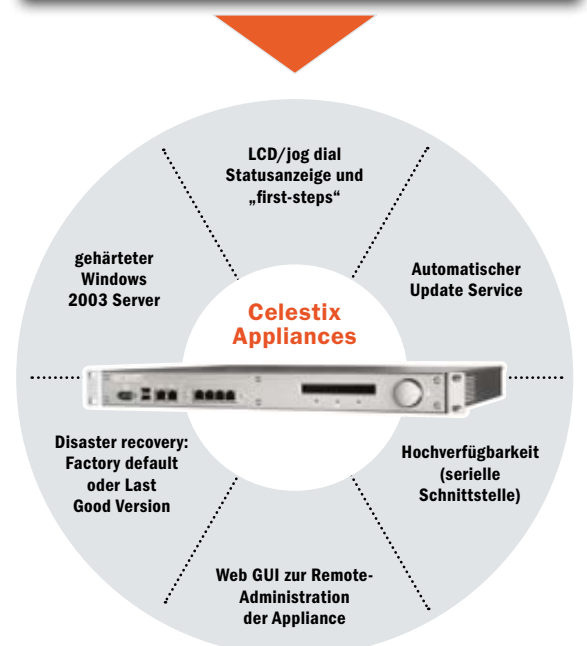
Das Upgrade auf das Unified Access Gateway (UAG) – dem Nachfolger vom IAG Server ist in dem Support bereits enthalten – Sie bekommen dann von Celestix das Image des neuen Betriebssystems und die neue Software. Die Konfiguration werden Sie übernehmen können. Das UAG soll Anfang des Jahres 2010 auf den Markt kommen.

**INTEGRIERTE SICHERHEIT**




Microsoft  
**Internet Security & Acceleration Server 2006**

Microsoft  
**Intelligent Application Gateway 2007**





### Umfassende und sichere Fernzugriffslösung

Bei den WSA™ SSL VPN-Appliances von Celestix™ handelt es sich um hochleistungsfähige Zugriffssicherheitslösungen. Diese bieten auf der einen Seite ein Höchstmaß an Schutzvorkehrungen und garantieren auf der anderen Seite einen einfachen Zugriff von außerhalb auf unternehmenskritische Anwendungen.

Wir leben heute in einer Welt, in der es in virtuellen Umgebungen keine Grenzen mehr gibt. Um eine möglichst hohe Effizienz zu gewährleisten, müssen Unternehmen ihren Mitarbeitern einen zuverlässigen Zugriff auf das Netzwerk garantieren, unabhängig von Standort und Zeit. Informationen und Daten werden zum höchsten Gut für ein Unternehmen und der Remote Access auf das Netzwerk damit zu einem absoluten „Muss“. Außendienstmitarbeiter eines Unternehmens sind auf den uneingeschränkten Zugriff auf Anwendungen wie E-Mail, Auftragserfassung und -status, Instant Messaging und Intranet angewiesen, damit der Geschäftsbetrieb stabil und zuverlässig funktioniert. Unternehmenskritische Daten gilt es massiv zu schützen. Innerhalb der Firmenmauern scheint diese Übung noch relativ überschaubar – schwierig wird es jedoch einen Zugriff von außerhalb abzusichern. Hier spielen viele Komponenten, die nur schwer zu kontrollieren sind, eine gewichtige Rolle. Angriffe über das Internet gehören zum am schnellsten wachsenden Bereich der Cyber-Kriminalität. Deshalb müssen sämtliche Unternehmen, ob groß oder klein, stets wachsam sein. Die WSA SSL VPN-Anwendungen von Celestix unterstützen IT-Verantwortliche in ihrem Bemühen, die Zugänglichkeit der Informationsbestände so zur Verfügung zu stellen, wie es gewünscht wird. Das heißt, auf der einen Seite nur den tatsächlich autorisierten Anwendern einen Zugriff zu erlauben, und gleichzeitig vor äußeren Attacken zu schützen. Die Celestix WSA-Appliance kombiniert die Leistungsfähigkeit der Celestix Scorpio-Anwendungshardware und der Engine-Software „SlingSHOT™“ mit Microsofts Intelligent Application Gateway 2007 und dem Internet Security and Acceleration Server 2006. Zusammen bilden sie die derzeit fortschrittlichste, auf dem Markt erhältliche SSL-Zugriffslösung für Virtual Private Networks (VPN).

### ZUGRIFFSKONTROLLE

Sichere und zuverlässige Authentifizierung - schützt die Anwender vor unliebsamen Attacken und beschleunigt den Zugriff für autorisierte Benutzer.

### SCHUTZ DER RESSOURCEN

Der integrierte Anwendungsschutz gewährleistet die Unversehrtheit und Sicherheit der Netzwerk- und Anwendungsinfrastruktur.

### ABSICHERUNG VON INFORMATIONEN

Die konsequente Durchsetzung von Richtlinien (Policies) hilft bei der Einhaltung gesetzlicher und unternehmens-interner Anforderungen (Compliance). Auf diese Weise werden Risiken und Verantwortlichkeiten beim Zugriff auf sensible Unternehmensdaten minimiert.

### DIE WICHTIGSTEN MERKMALE AUF EINEN BLICK

- Einfach zu installierende und sichere Fernzugriffslösung
- Eine einzige Plattform für den Fernzugriff von Mitarbeitern und Geschäftspartnern
- Zugriff auf Unternehmensanwendungen und -ressourcen - unabhängig vom Client
- Branchenführende Endpunktsicherheit, einmalige Anmeldung für Web-Anwendungen (Single Sign-On), granulare Zugriffskontrolle und Schutz vor Bedrohungen (Threat Prevention)
- Die skalierbaren Anwendungen werden den Fern- und Extranet-Zugriffsanforderungen von Unternehmen jeder Größe gerecht
- Web-basierte, grafische Benutzeroberfläche (GUI) für die Fernverwaltung
- Frontpanel mit LC-Display zur einfachen Netzwerkkonfiguration und Statusanzeige
- One button-System zur Wiederherstellung der Werkseinstellungen und letzten fehlerfreien Version
- Echter Gigabit-Netzwerkdurchsatz
- PCI-Express-Architektur
- Update-Services

### UMFASSENDE UND SICHERER ZUGRIFF

Die WSA-Appliance beinhaltet folgende Features: SSL-VPN, eine Firewall für Web-Anwendungen sowie einen Endpoint-Security Ansatz, der Zugriffskontrolle, Autorisierung und Inhaltsprüfung für eine Vielzahl von Geschäftsanwendungen ermöglicht. Zusammen sorgen diese Funktionalitäten dafür, dass mobile Mitarbeiter und Außendienstmitarbeiter von einem breiten Spektrum von Geräten und Standorten, wie öffentlich zugänglichen Computern, PCs und mobilen Geräten, auf einfache und flexible Weise von einem sicheren Zugriff profitieren können. WSA ermöglicht es IT-Administratoren außerdem, die Einhaltung von Richtlinien zur Nutzung von Anwendungen und Informationen mithilfe einer benutzerdefinierten Remote-Access-Policy (Fernzugriffsrichtlinie) umzusetzen.

Funktion	Konnektivität		Zugriffsrichtlinie	Anwendungssicherheit		Endpoint Security
	Single Sign-on	Nutzung als Portalseite	Zugriffsbeschränkung auf Anwendungsbereiche	Funktionen sperren	Anwendungs-Firewall	Attachment Wiper
<b>Application Optimizer</b>						
<b>Exchange Outlook Web Access</b>	ja	k.A.	ja	Upload/ Download	Teilweise positiv	ja
<b>SharePoint Portal Server</b>	ja	ja	ja	Upload/ Download/Bearbeiten	Uneingeschränkt positiv logisch	ja
<b>Domino Web Access</b>	ja	k.A.	ja	Upload/ Download	Uneingeschränkt positiv logisch	ja
<b>IBM WebSphere</b>	ja	ja	ja	Upload/ Download/Bearbeiten	Teilweise positiv	ja
<b>SAP Portal</b>	ja	ja	ja	Upload/ Download/Bearbeiten	Nur negativ	ja
<b>EMC Documentum Webtop</b>	ja	ja	ja	Upload/ Download/Bearbeiten	Teilweise positiv	ja
<b>Dynamics</b>	ja	k.A.	ja	Upload/ Download/ Bearbeiten/ Exportieren	Teilweise positiv	ja

## Konnektivitätsmodule

### CLIENT/SERVER CONNECTOR

Der Client/Server Connector bietet sofort einen sicheren Zugriff auf geschäftskritische Client-/Server-Anwendungen wie Microsoft Exchange, Lotus Notes, Citrix, Microsoft Terminal Services, FTP und Telnet. Gleichzeitig gewährleistet er eine einfache Konfiguration für weitere Client-/Server-Anwendungen dank eines generischen Tools zur Anwendungsdefinition.

### TUNNELING-MODI

- **Port-Weiterleitung (Port Forwarding):**  
Die Client-Komponente reagiert auf eine spezifische lokale Adresse an einem bestimmten lokalen Port und veranlasst die Anwendung, den TCP-Datenverkehr an diese Adresse zu senden und nicht an die echte IP-Adresse des Anwendungsservers. Der SSL VPN-Client kapselt den abgefangenen Datenverkehr ein und schickt diesen dann verschlüsselt zum Gateway. Dieser Modus funktioniert optimal bei Anwendungen, die statische TCP-Ports nutzen, oder bei Anwendungen, die einen HTTP- oder SOCKS-Proxy unterstützen.
- **Socket-Weiterleitung (Socket Forwarding):**  
Die Client-Komponente koppelt sich mit der SPI-Schnittstelle (Service Provider Interface) von Microsoft Winsock. Sie nutzt die LSP-/NSP-Schnittstellen (Layered Service Provider/Name Space Provider) von Windows und bietet Socket-Handling auf niedriger Ebene. Zudem zeichnet sie sich durch die volle Unterstützung sämtlicher Winsock-Anwendungen aus – wie TCP und dynamische Ports.

### APPLICATION OPTIMIZER

WSA beinhaltet mehrere Intelligent Application Optimizer: Integrierte Softwaremodule mit vorkonfigurierten Einstellungen für den sicheren Fernzugriff auf häufig genutzte Unternehmensanwendungen. Diese Optimizer bieten Endpoint-Security, Application Publishing und Filterung von Serveranfragen nach Standardwerten für individuelle Anwendungen. So soll ein flexibles Gleichgewicht zwischen einem effizienten Geschäftsablauf bei maximaler Netzwerk- und Datensicherheit erreicht werden. Standardmäßig integriert sind benutzerdefinierte, granulare Zugriffsrichtlinien- und Sicherheitsfunktionen für Microsoft Exchange Server und SharePoint® Portal Server sowie für zahlreiche Geschäftsanwendungen wie SAP, IBM Domino und Lotus Notes.

### NETWORK CONNECTOR

Der Network Connector erlaubt es Administratoren, Fernverbindungen zu installieren, zu betreiben und zu verwalten, die Nutzern über eine virtuelle, sichere und transparente Verbindung die volle Konnektivität auf Netzwerkebene bieten. Darüber hinaus profitieren die Nutzer von derselben Funktionalität, als wären sie direkt mit dem Unternehmensnetzwerk verbunden.

- Das Network-Connector-Modul weist externen Nutzern eine lokale IP-Adresse zu. So können sie aus der Ferne über eine sichere Verbind-

gung auf Netzwerkebene (gemeinsame Ordner) auf Unternehmensserver und komplexe Systeme wie File Shares und interne Datenbanken zugreifen.

- Das Network-Connector-Modul tunnelt nahezu jedes IP-basierte Protokoll und unterstützt daher auch Voice over IP (VoIP).
- Die Fähigkeit des Network Connectors, auf Grundlage der Benutzeridentität eine Direktverbindung zu den unterschiedlichen Servern in den Abteilungen herzustellen, hat beträchtliche Vorteile für die Sicherheit, weil keine vollkommen offene Verbindung auf Netzwerkebene vom SSL VPN-Gateway direkt zum LAN für alle Nutzer notwendig ist.
- Er bietet Administratoren die Möglichkeit, die Verbindung unmittelbar nach der Benutzeranmeldung (User Login) mithilfe eines vordefinierten Scripts, nach einer Compliance-Prüfung oder auf Abruf seitens des Benutzers aufzubauen, indem dieser nach der Autorisierung das Network-Connector-Symbol auf der Portalseite anklickt.

### VON DEN VORTEILEN BEIDER SEITEN PROFITIEREN

Die WSA mit dem integrierten ISA Server 2006 stellt eine gemeinsame Anwendung für den Schutz des Netzwerkperimeters, des Fernzugriffs und der SSL- und IPsec-Verbindungen auf Anwendungsebene zur Verfügung. Die Integration von SSL VPN in die bestehende Microsoft-Infrastruktur unterstützt den sicheren Zugriff auf die Anwendungen und Services von Microsoft und anderen Anbietern über eine einzige Anwendung. Die WSA-Appliance zeichnet sich durch ein neues, verbessertes und kostengünstiges Design aus, das die Betriebskosten reduzieren hilft und die Nutzung mehrerer Geräte von unterschiedlichen Anbietern für verschiedene Zugriffsmethoden überflüssig macht. Die IT-Abteilung Ihres Unternehmens kann nun eine konsolidierte Sicherheitslösung einführen, die flexibel und einfach einzusetzen ist.

### PERIMETERSCHUTZ

Der ISA Server sorgt in Verbindung mit dem Intelligent Application Gateway (IAG) für die erforderliche Netzwerktrennung und die Überwachung von ein- und ausgehenden Inhalten. Dabei bietet er zusätzliche Funktionalität für den Schutz des Netzwerkes, um eine Vielzahl von Internet-Bedrohungen abzuwehren. Die konsolidierte Anwendung stellt eine flexible, softwaregesteuerte Lösung dar, die neben umfassender Sicherheit auch der Forderung nach Leistungsfähigkeit, Verwaltbarkeit und Skalierbarkeit gerecht wird. Die Kombination von Stateful Packet Filtering, Circuit Filtering, Application-Layer Filtering, Web-Proxy und Endpunktsicherheit in einer einzigen Anwendung gibt dem Administrator vielfältige Möglichkeiten zur Konfiguration eines richtliniengesteuerten Zugriffs auf Anwendungen und Netzwerkressourcen.

ISA Server bietet die Möglichkeit zur Filterung des Datenverkehrs, anstatt mit einer mechanistischen Lösung aufzuwarten. Dabei werden drei Arten von Firewall-Funktionalitäten bereitgestellt: Packet Filtering auch Circuit-Layer Filtering genannt, Stateful Filtering und Application-Layer Filtering. Dank der Fähigkeit, eine regelbasierte Filterung auf den gesamten Datenverkehr anzuwenden, der die Netzwerkgrenze passiert,

kann die konsolidierte Lösung Bedrohungen wie beispielsweise Würmer oder Malware, die von authentifizierten Benutzern ausgehen können, direkt abwehren.

## Produktmerkmale

### SKALIERBARKEIT

**Benutzer:** Unterstützt eine unbegrenzte Benutzeranzahl auf einem einzigen Gateway.

**Hochverfügbarkeit:** Linear skalierbar auf bis zu 64 hochverfügbare Knotenkonfigurationen.

### ZUGRIFFSRICHTLINIE

#### Endpunkt-Compliance-Prüfungen





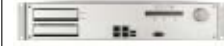
Die Endpunktrichtlinie erlaubt es Administratoren, Compliance-Prüfungen mithilfe von Standardvariablen zu definieren, wie zum Beispiel der Präsenz von Sicherheitssoftware und IAG-spezifischen Komponenten wie dem Attachment Wiper. Unterstützt komplexe Regeln für Endpunktrichtlinien mit flexibel anpassbaren Compliance-Prüfungen, bei denen Boolesche Operationen zum Einsatz kommen.

### VERWALTBARKEIT

**SSL VPN-Portal:** Bietet einen zentralen Zugangspunkt (Single Access Point) für Anwendungen, unterstützt aber auch mehrere Zugangspunkte mit eigenen Richtlinienparametern, wie Partner-Extranets und Mitarbeiterportale, auf einem einzigen Gateway.

#### Umfassende Rahmenbedingungen für Richtlinien (Policy Framework):

- Standardeinstellungen für den Anwendungszugriff und Standardkonfigurationen für Endpunktrichtlinien (Endpoint Policies), um einen minimalen Integrationsaufwand und geringe laufende Verwaltungskosten sicherzustellen.
- Unterstützt das Intelligent Application Toolkit für die Definition von positiv logischen Regelsätzen, URL-Filter zur Ergänzung der Optimizer-Einstellungen und die Entwicklung von Richtlinien (Policies) für personalisierte oder proprietäre Anwendungen.
- Unterstützt das Intelligent Application Template, das die Rahmenbedingungen zur Entwicklung eines Application Optimizers sowohl für generische Web-Anwendungen als auch für komplexe Unternehmensanwendungen liefert, die Komponenten, Web-Parts und Objekte beinhalten.

Product	Celestix WSA3000	Celestix WSA4000	Celestix WSA6000	Celestix WSA8000	Celestix WSA8000h
					
<b>System</b>					
<b>Form Factor</b>	1U compact rack	1U compact rack	2U compact rack	2U compact rack	2U compact rack
<b>Dimensions (WxDxH)</b>	17.5" x 14.38" x 1.75"	17.5" x 14.38" x 1.75"	17.5" x 17.5" x 3.5"	17.5" x 19.75" x 3.5"	17.5" x 19.75" x 3.5"
<b>Processor</b>	Intel® Pentium Dual-Core	Intel Core 2 Duo	Dual-Core Intel Xeron	2 x Xeon Quad Core	2 x Xeon Quad Core
<b>Front Bus Speed/Cache</b>	800MHz/1MB	800MHz/21MB	1066MHz/4MB	1333MHz/12MB	1333MHz/12MB
<b>Chipset Chipset</b>	Intel 945GV	Intel 945GV	Intel 945GV	Intel 5100P	Intel 5100P
<b>Memory (667MHz DDR2)</b>	2GB	2GB	3GB	4GB	4GB
<b>Hard Drive (SATA-II)</b>	80GB	80GB	Hot swappable 3 x 80GB (RAID 5) + 1x 80GB hot spare	2 x 73GB SAS RAID 1	2 x 73GB SAS RAID 1
<b>Disk Speed</b>	7,200 rpm	7,200 rpm	7,200 rpm	15,000 rpm	15,000 rpm
<b>LCD Panel</b>	40x2 Character	40x2 Character	40x2 Character	40x2 Character	40x2 Character
<b>Gigabit NICs (PCIe)</b>	6	6	6	4	4
<b>SSL Accelerator/HSM</b>	nein/nein	ja/nein	ja/nein	ja/nein	ja/ja
<b>Ports</b>	2 x Serial Ports/Console 3 x USB 2.0 Ports	2 x Serial Ports/Console 3 x USB 2.0 Ports	2 x Serial Ports/Console 3 x USB 2.0 Ports	1 x Serial Ports/Console 3 x USB 2.0 Ports	1 x Serial Ports/Console 3 x USB 2.0 Ports
<b>Power</b>	300W Universal AC input 100V~240V 50/60Hz	300W Universal AC input 100V~240V 50/60Hz	300W Universal AC input 100V~240V 50/60Hz (redundant & hot swappable)	500W Universal AC input 100V~240V 50/60Hz (redundant & hot swappable)	500W Universal AC input 100V~240V 50/60Hz (redundant & hot swappable)
<b>Appliance Software</b>					
<b>Microsoft IAG</b>	3.7	3.7	3.7	3.7	3.7
<b>Bundled User Licenses</b>	10	10	10	10	10
<b>Recommended max. users</b>	<1,000	<2,500	<5,000	<15,000	<15,000
<b>Recommended concurrent users</b>	up to 500	up to 1,000	up to 2,500	up to 8,000	up to 8,000
<b>Restore to factory default</b>	ja	ja	ja	ja	ja
<b>Restore to last known good version</b>	ja	ja	ja	ja	ja
<b>Update services</b>	ja	ja	ja	ja	ja
<b>Hardened OS</b>	Embedded Windows Server 2003	Embedded Windows Server 2003	Embedded Windows Server 2003	Embedded Windows Server 2003	Embedded Windows Server 2003



## HIGHLIGHTS

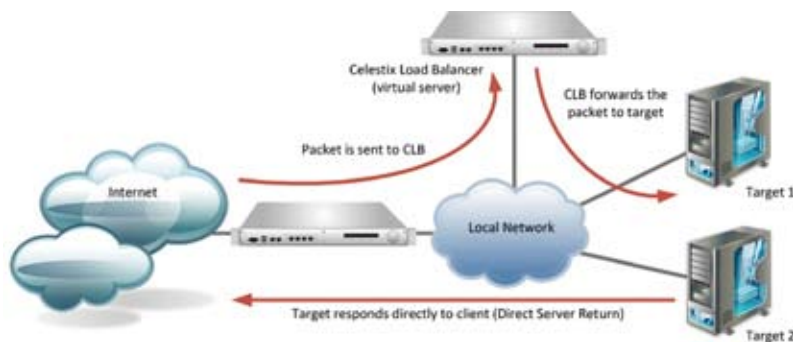
- Layer 2 (Ethernet)-basierter Software Load Balancer
- Layer 4 Load Balancing
- Sitzungspermanenz basierend auf Client-Adresse und optionalem Quellport
- Backup-Targets (Hosts) können für einen Ausfall aller primären Targets spezifiziert werden
- Server Health Check Engine per PING, TCP, Socket Open und frei konfigurierbarem UDP Health Check Agent
- Änderungen in Echtzeit per Email und SNMP-Traps
- Mehr Zuverlässigkeit durch Betrieb in Aktiv-Passiv-Clustern
- Unterstützung mehrfacher Instanzen der Load Balancer Session, sowie paket-/byte-basiertes Reporting für jede Instanz
- Benutzerfreundliches UI für Konfiguration und Reporting
- Benutzerfreundlicher Konfigurations-Wizard zum Konfigurieren von Instanzen, Targets und Netzwerken
- Kinderleichte Installation – betriebsbereit in nur 20 Minuten
- Distributions-Methoden: SimpleWeighted Round Robin, Zufall, Client Address Hashing und "Least Resource" auf Basis der Information vom Agent
- Unterstützung für Direct Server Return (DSR)-Betrieb
- Unveränderte Client-Adressen auf IP-Level
- Hohe Verfügbarkeit für Multi-Node dank Standard-VRRP (Virtual Router Redundancy Protocol)
- "All Service Load Balancing" auf Basis von IP-Adressen ermöglicht Unterstützung nahezu aller Protokolle (z.B. aktives FTP, RTSP/RTP/RTCP, DNS etc.)
- Session-Tabelle mit bis zu 16 Millionen Sessions gleichzeitig
- Volle Unterstützung für Session-Tabellen-State Replication/Session-Synchronisierung zwischen VRRP Amster und Backup



**Der Celestix Load Balancer (CLB) ist eine einfach zu bedienende und gleichzeitig eine der kosteneffektivsten IP Load Balancing-Lösungen auf dem Markt. Das System garantiert Zuverlässigkeit, Performance und hohe Verfügbarkeit Ihrer Anwendungen. Der CLB verfügt über Failover-Fähigkeiten für den Fall eines Serverausfalls und die Möglichkeit, Traffic über mehrere Server zu verteilen.**

## SERVER LOAD BALANCING

Der CLB nutzt mehrere Methoden des Load Balancing zur Umverteilung des Traffic über mehrere Server, darunter das Simple Weighted Round-Robin, Zufallsverteilung, Client-Adress-Hashing und „Least Resource“ auf Basis von Information von einem Agent. Durch die Verwendung einer eingebauten Health Check Engine ist der CLB in der Lage, den Traffic bei einem Serverausfall nahtlos umzuschalten.



## EINSATZDIAGRAMM

Der Celestix CLB bietet Failover und Redundanz für viele gängige Enterprise Services, wie zum Beispiel:

- Web-Anwendungen (Microsoft Sharepoint, Microsoft Outlook Web Access, etc.)
- Security-Gateways (Firewalls, SSL VPN, URL filtering, SPAM, Anti-Virus, etc.)
- Microsoft Terminal Services
- Server mit SMTP-Service

Der CLB basiert auf der Celestix Scorpio X Appliance-Plattform der vierten Generation. Dank der sorgfältigen Abstimmung bietet die Scorpio X ein hervorragendes Preis-Leistungs-Verhältnis für eine Hardwareplattform.

## DIE SLINGSHOT APPLIANCE ENGINE BEINHALTET:

- Setup, Routing, NIC-Konfiguration, lokale User, Software-Updates
- Reboot/Restart, Betrachten von Logfiles, fortlaufendes Monitoring etc.
- Fortschrittliche Software zum updaten der Engine
- Disaster Recovery – System-Rollback auf Werkseinstellung per Knopfdruck
- Maßgeschneiderte Appliance Hardware-Plattform
- LCD/Jog-Dial für sofortige Inbetriebnahme und Statusanzeige
- Optimiertes Celestix Motherboard für hohe Zuverlässigkeit
- 1U-Gehäuseform mit halber Bautiefe für Montage ohne Schienen



# HOTPin

**Hohe Sicherheit zum günstigen Preis mit Zwei-Faktor-Authentifizierung**

## ÜBERBLICK

Formular-Grabber, Keylogger und Phishing sind nur einige der Mittel, mit denen Hacker die Daten für User-Logins stehlen.

Der Verkauf gestohlener IDs ist ein lukratives Geschäft. Das wirft die Frage auf: Wer befindet sich eigentlich gerade in ihrem Netzwerk? Benutzer-Authentifizierung ist daher das Sicherheitsthema der Stunde.

Zwei-Faktor-Authentifizierungssysteme (2FA) identifizieren User über eine Frage, deren Antwort nur der Nutzer kennt (z.B. ein Passwort oder eine PIN), sowie über etwas, das der Benutzer besitzt (z.B. ein Hardware-Token oder eine Karte). HOTPin™ ist das neue 2FA von Celestix. Celestix hat HOTPin™ von Anfang an auf höchste 2FA-Sicherheit mit Einmal-Passwörtern ausgelegt – diese werden äußerst kostengünstig auf Benutzerhandys oder PCs übertragen. HOTPin ist das erste 2FA-System, das vollständig mit Microsoft IAG 2007 SSL VPN-Software integriert ist. HOTPin ist die 2FA-Sicherheitslösung für den IAG und kommt auf der WSA™ Appliance zum Einsatz, der weltweit meistverkauften IAG-Appliance.

## HOTPIN™ SENKT KOSTEN

In der Regel sind die Kosten pro Benutzer für 2FA-Systeme sehr hoch. Normale Hardware-Tokens, wie sie in herkömmlichen 2FA-Systemen zum Einsatz kommen, schlagen schnell mit bis zu 150 Dollar pro Benutzer zu Buche. Im Gegensatz

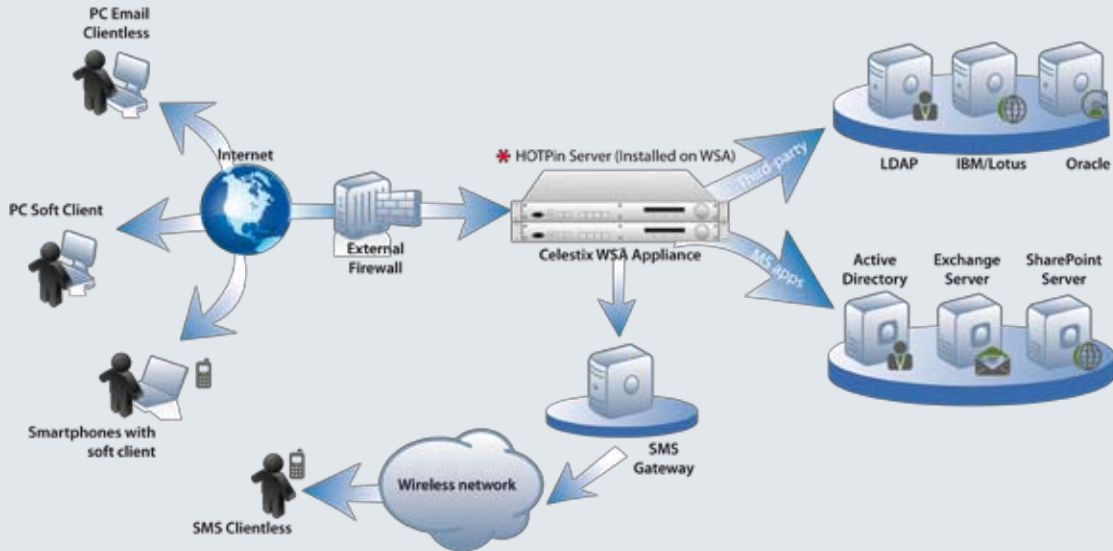
**HOTPin**  
2FA for Celestix WSA SSL VPN Appliance

Hervorragend geeignet für Extranet-Partner, Bankkunden, Patienten, sowie andere vorübergehende Benutzer, da nach kurzfristiger Benutzung die Notwendigkeit für HardwareTokens entfällt. Die Nutzerlizenz kann sofort neu vergeben werden.

- Mehr Vertrauen durch offene OTP-Standards
- Geringe Kosten: Vermeidung teurer HardwareTokens und geringere Kosten für Server Software
- Komfort: Einfachere Benutzung und Steuerung ohne gesonderte HardwareTokens
- Bessere Erfüllung von PCI, SOX, HIPPA und weiteren Bestimmungen
- Macht Mitarbeiter mobil
- Dank neuester Technik bleiben Sie bei 2FA auf dem neuesten Stand.
- Zuverlässiger Betrieb dank hoher Interoperabilität mit Microsoftstrukturen
- On-Box-Integration mit IAG 2007 SSL VPN für schnelle Installation und einfache Steuerung
- Vollständige Lösung: Celestix bietet Hardware, Software, professionelle Services und Support aus einer Hand.
- Mehr Umweltschutz: Es landen keine ausgedienten HardwareTokens auf der Deponie

dazu senden die Celestix HOTPin™-Systeme die Einmalpasswörter an das Handy des Benutzers, und eliminieren so die Kosten für teure Hardware-Tokens mit nur einer Funktion.

Die serverseitige Applikation HOTPin™ wird als Plug-In auf Appliances der Celestix WSA™-Reihe eingesetzt. Dabei nutzen WSA-Appliances die IAG-Software, um für Remote-Benutzer eine sichere Netzwerkverbindung durch Erzeugung von SSL-VPNs herzustellen. Das HOTPin Server-Plugin steuert Benutzer-Credentials und authentifiziert die Benutzer. HOTPin nutzt dabei HOTP, einen HMAC-basierten Algorithmus zur Erzeugung von Einmal-Passwörtern. Im Gegensatz zu Algorithmen anderer Anbieter handelt es sich bei HOTP um einen offenen Standard, der bereits ausgiebig von Sicherheitsexperten und führenden Wissenschaftlern untersucht wurde. HOTPin bringt die Einmal-Passwörter durch zwei verschiedene Wege auf das Handy: per Clientless Mode und per Client Mode. Im Clientless Mode erzeugt die HOTPin Server-Applikation Einmalpasswörter und schickt sie per SMS auf das Mobiltelefon oder den PC des Anwenders. Der Clientless Mode ist hervorragend für Benutzer ohne Smartphone geeignet. Für den Client Mode lädt sich der Benutzer die HOTPin Client-Software auf sein Smartphone oder den PC herunter. Die HOTPin Client-Software generiert das Einmalpasswort direkt auf dem Smartphone oder PC. Der Vorteil des Client Mode besteht darin, dass unabhängig von der Funknetzabdeckung Einmalpasswörter zur Verfügung gestellt werden. HOTPin besitzt auch einen Windows-Client, der auf dem PC installiert werden kann und Einmalpasswörter direkt auf den Desktop liefert.



**Folgende Clients werden derzeit von HOTPin im Client Mode unterstützt:**



HOTPin Client for RIM BlackBerry



HOTPin Client for Windows Mobile 5/6, Pocket PCs



HOTPin Client for Apple iPhone



HOTPin Client for Standard Win32 Software Devices

**PROFESSIONAL SERVICES**

Celestix bietet Entwicklungsdienstleistungen an, damit Sie HOTPin und IAG-Lösungen präzise auf Ihren persönlichen Einsatzzweck abstimmen

können. Mehr Informationen finden Sie unter: [http://www.wickhill.de/products/celestix/uk\\_index\\_g.php](http://www.wickhill.de/products/celestix/uk_index_g.php) oder per E-Mail: info@wickhill.de

**Technischer Support**

Telefon: +49 (0)40 - 23 73 01 - 25  
Mo.-Do. 8-18 Uhr, Fr. 8-17:30 Uhr

**Internal Sales**

Telefon: +49 (0)40 - 23 73 01 - 0  
Mo.-Fr. 8-18 Uhr

Fax: +49 (0)40 - 23 73 01 - 80

**Vertriebs- und  
Technische Schulungen**

Wir schulen Sie auf das richtige Level, damit  
Sie ihren Kunden optimal beraten können.

**Installations-Unterstützung**

Unsere Techniker unterstützen Sie bei der  
Installation vor Ort beim Kunden.

**24Plus Austausch Service**

Sie bzw. Ihre Kunden profitieren von dem  
Austausch zum nächsten Arbeitstag. Durch  
24Plus! reduzieren Sie Ihren Stress und  
unnötige Ausfallzeiten im Falle eines Hard-  
waredefektes. Dieses PLUS gibt es nur bei  
Wick Hill.