



Uniwersalne produkty SSL VPN zapewniają najlepsze doświadczenia związane z dostępem do wszystkich aplikacji



**Produkty Citrix Access Gateway są rodziną udoskonalonych urządzeń SSL VPN, umożliwiających użytkownikom kontrolowany dostęp do wszystkich aplikacji oraz zasobów koniecznych do zapewnienia ich wydajności. Citrix Access Gateway to uniwersalne produkty zapewniające bezpieczny dostęp do dowolnej aplikacji lub protokołu sieciowego, w tym do rozproszonych aplikacji Windows® i UNIX®, aplikacji internetowych, sieciowych zasobów plików, a nawet usług telefonii korzystającej z aplikacji głosowych VoIP – i to bez konieczności dostosowywania do wymogów klienta czy sieci WWW. Polityki dostępu określają poziom dostępu użytkownika w oparciu o reguły zdefiniowane przez administratora i analizę punktu końcowego.**

Dzięki Citrix Access Gateway organizacje mogą przezwyciężyć problemy związane z innymi rozwiązaniami VPN, takimi jak trudności z przechodzeniem przez zaporę sieciową i serwer proxy, złożoność dystrybucji oprogramowania klienckiego, ograniczone wsparcie dla aplikacji i skomplikowane zarządzanie nimi.

Szeroki wachlarz urządzeń i edycji sprawia, że Access Gateway może zaspokoić potrzeby organizacji każdej wielkości, od małych firm po najbardziej wymagające globalne korporacje:

**Citrix Access Gateway Standard Edition** to proste we wdrożeniu i zarządzaniu oraz najbardziej efektywne kosztowo rozwiązanie bezpiecznego zdalnego dostępu na rynku. Urządzenie Access Gateway instaluje się w części sieci poza zaporą, w strefie DMZ – zabezpiecza ono cały ruch w sieci przy użyciu standardowego protokołu SSL. Zdalni użytkownicy uzyskują połączenie dzięki łatwemu w obsłudze, pobieranemu z sieci WWW i automatycznie aktualizowanemu klientowi, ciesząc się takim samym dostępem do aplikacji, jak gdyby znajdowali się fizycznie w sieci lokalnej.

**Citrix Access Gateway Advanced Edition** umożliwia dostęp większej liczbie użytkowników z większej liczby urządzeń, w tym kiosków internetowych i urządzeń przenośnych. Rozbudowana technologia SmartAccess™ umożliwia elastyczną, precyzyjną, opartą na regułach kontrolę dostępu, w tym ścisłą integrację z serwerem Citrix Presentation Server™.

**Citrix Access Gateway Enterprise Edition** to najlepsze rozwiązanie dla wymagających środowisk korporacyjnych, oferujące maksymalną skalowalność, wydajność, wysoką dostępność i rozbudowane możliwości zarządzania. Zintegrowane opcje przyspieszające i optymalizujące działanie aplikacji dodatkowo zwiększają wydajność zdalnego dostępu, redukując przy tym koszty.

## Bezpieczny, skalowalny dostęp dla mobilnych profesjonalistów

Urząd ds. Wyroków w Zawieszeniu, Zwolnień Warunkowych i Ułaskawień Stanu Południowa Karolina (The South Carolina Department of Probation, Parole and Pardon Services, SCDPPPS) pomaga zresocjalizowanym przestępcom w powrocie do społeczeństwa, dbając przy tym o ochronę bezpieczeństwa publicznego. Wyzwaniem dla organizacji było zapewnienie swym pracownikom w terenie bezpiecznego dostępu do znajdujących się w sieci informacji o poszczególnych przypadkach. Niestety jej sieć IPSec VPN sprawiała trudności z przechodzeniem przez zaporę sieciową i stawiała duże wymagania związane ze wsparciem technicznym.

Urząd SCDPPPS zastosował zatem bramkę Citrix Access Gateway, która jest konkurencyjna cenowo, zapewnia proste i błyskawiczne wdrożenie oraz dysponuje łatwym w obsłudze klientem, niewymagającym ręcznej instalacji i aktualizacji. Po wdrożeniu rozwiązania firmy Citrix rozbudowana aplikacja kliencka PowerBuilder, używana przez pracowników SCDPPPS, zaczęła pracować z za zapory sieciowej bez jakiegokolwiek modyfikacji kodu.

Bezpieczny, skalowalny dostęp dla mobilnych profesjonalistów.

## Większe bezpieczeństwo danych dzięki monitorowaniu i regulowaniu dostępu użytkowników

Klient Access Gateway maskuje wewnętrzne adresowanie sieci, co w połączeniu ze sterowaniem rozdzielania tunelowania skutecznie blokuje pospolite robaki sieciowe. „Białe listy” aplikacji pozwalają administratorom ściśle kontrolować aplikacje klienckie i ich wersje, które mogą komunikować się z określonymi serwerami zaplecza. Kombinacja logowania i ciągłego skanowania punktów końcowych w czasie rzeczywistym sprawia, że urządzenie użytkownika pozostaje bezpieczne dla sieci korporacyjnej przez cały czas połączenia. Wersja Advanced Edition, dzięki wprowadzeniu opcji SmartAccess™ z systemem sygnalizacyjno-reagującym („sense-and-respond”), umożliwia nie tylko udzielenie czy odmowę dostępu do aplikacji, ale również aktywne kontrolowanie tego, co użytkownik może robić z uzyskanymi informacjami. Na przykład, na podstawie urządzenia, z którego następuje dostęp i/lub jego lokalizacji, możliwa jest kontrola uprawnień użytkowników do przeglądania, drukowania, modyfikowania lub zapisu informacji.

## Zaspokojenie potrzeb największych korporacji

Access Gateway Enterprise Edition zapewnia niespotykany dotąd zestaw cech, takich jak wysoka dostępność zdalnego dostępu do pojedynczego centrum przetwarzania danych oraz możliwość tworzenia kompletnego rozwiązania do usuwania skutków awarii obejmującego wiele lokalizacji geograficznych.



Dzięki zaawansowanym opcjom bezpieczeństwa, takim jak uwierzytelnianie za pomocą karty SmartCard i zapobieganie atakom typu odmowa usługi, organizacje mogą być pewne bezpieczeństwa swoich danych i aplikacji. Użytkownicy zaś, dzięki wiodącym na rynku rozwiązaniom służącym kompresji i akceleracji, mogą uzyskać jeszcze lepsze wrażenia związane ze zdalnym dostępem.

## Prostsza administracja i niższe koszty

W porównaniu z podejściem tradycyjnym Access Gateway, uniwersalne rozwiązania SSL VPN firmy Citrix radykalnie upraszczają zarządzanie. Administratorzy mogą je szybko i łatwo instalować, konfigurować i wdrażać, bez uszczerbku dla bezpieczeństwa i przy znacznie obniżonym koszcie eksploatacji.

Zapewnienie dostępu użytkownikom nie generuje kosztów i nie wywołuje komplikacji związanych z instalacją, konfiguracją, aktualizacją i obsługą techniczną oprogramowania klienckiego na każdym urządzeniu.

## Przegląd cech

		Platinum Edition	Enterprise Edition	Advanced Edition
Cecha	Korzyść			
Uniwersalne rozwiązanie SSL VPN – obsługa wszystkich aplikacji i protokołów	Podnosi wydajność umożliwiając użytkownikom dostęp do wszystkich potrzebnych im aplikacji i zasobów. Obniża koszty – nie ma potrzeby utrzymywania osobnej infrastruktury SSL i IPSec VPN, aby obsłużyć wszystkie aplikacje.	•	•	•
Automatycznie pobierany i aktualizowany klient VPN	Automatycznie pobiera klienta VPN do urządzenia podczas nawiązywania połączenia z bramką Citrix Access Gateway. Dodatkowa korzyść dla użytkowników to posiadanie zawsze najnowszej wersji oprogramowania klienckiego. Zmniejsza uciążliwość instalowania, utrzymywania i zapewnienia obsługi technicznej oprogramowania na urządzeniu klienckim.	•	•	
Nieadministracyjny klient VPN	Zapewnia połączenie sieciowe dla klienta w przypadku, gdy użytkownik nie ma uprawnień administratora urządzenia. W razie potrzeby program instalacyjny klienta powraca do nieadministracyjnego trybu instalacji.	•	•	•
Ciągły dostęp	Automatycznie wznowia sesje po utracie połączenia z siecią lub przechodzeniu między sieciami. Poprawia wrażenia użytkowników związane z korzystaniem z problematycznych sieci, takich jak publiczny bezprzewodowy Internet, oraz zwiększa wydajność użytkowników przy poruszaniu się pomiędzy różnymi sieciami.	•	•	•
Dostęp z urządzeń bez klienta	Zapewnia bezpieczny dostęp do dokumentów, sieciowych zasobów plików i poczty elektronicznej z dowolnego urządzenia wyposażonego w przeglądarkę, włącznie z kioskami internetowymi i urządzeniami małych rozmiarów, takimi jak PDA. Umożliwia użytkownikom dostęp do korporacyjnych zasobów IT z dowolnych urządzeń, które są zabezpieczone i nie pozwalają na pobieranie żadnego oprogramowania.		•	
Integracja z portalem	Pozwala administratorom skonfigurować dowolny interfejs użytkownika, na przykład Microsoft® SharePoint™ czy IBM® WebSphere™, jako domyślną stronę startową dla określonych użytkowników lub ich grup.		•	•
Obsługa aplikacji głosowych VoIP	Zapewnia dostęp do popularnych telefonów programowych VoIP. Obniża wydatki na telekomunikację pracowników w delegacji lub świadczących pracę na odległość.	•	•	•
Konfiguracja zapewniająca dużą dostępność	Łączy urządzenia w aktywne/pasywne pary, zapewniając kontynuację sesji w przypadku awarii urządzenia nadrzędnego. Zapewnia dostępność usługi VPN, bez konieczności inwestycji w oprogramowanie do obsługi aplikacji innych producentów.			•
Opcja globalnego równoważenia obciążenia serwerów (GSLB, Global Server Load Balancing)	Ustala kolejność łączenia klienta z najlepszymi serwerami VPN pod względem dostępności, sprawności, bliskości i czasu reakcji.			•
Przyspieszenie transferu	Przyspiesza uzyskanie dostępu do aplikacji i zasobów dzięki szyfrowaniu SSL poza serwerem, kompresji stron WWW i optymalizacji TCP. Zapewnia optymalne wrażenia związane ze zdalnym dostępem użytkownikom korzystającym z łączy o niskiej przepustowości lub cechujących się długim czasem oczekiwania.			•
Zintegrowane skanowanie punktu końcowego	Urządzenia klienckie są skanowane zgodnie z kryteriami określonymi przez administratora w celu zapewnienia właściwych ustawień takich elementów, jak aktualne oprogramowanie bezpieczeństwa i wersje systemów operacyjnych. Zapewnia to, że urządzenie nie narazi na niebezpieczeństwo sieci, do której jest podłączone.	•	•	•
Kwarantanna	Umożliwia urządzeniom klienckim, które nie przejdą pomyślnie skanowania punktu końcowego, ograniczony dostęp do serwerów w celu zainstalowania najnowszych baz wirusów, aktualizacji systemu operacyjnego itd. Zdalni użytkownicy mogą z łatwością zaktualizować swoje urządzenia, by mogły one spełnić ustalone wymogi.		•	•
Kontrola dostępu na podstawie scenariuszy	W zależności od tego, kim jest użytkownik, jakie są wyniki analizy punktu końcowego oraz lokalizacja sieci klienta, mechanizm reguł dynamicznie ustala dostępność poszczególnych zasobów.		•	•
Kontrola uprawnień do działania	Administratorzy określają nie tylko, które dane są dostępne, ale również, jakie działania (np. drukowanie, zapisywanie, uruchamianie, przeglądanie) użytkownik może podejmować. Poziom dostępu jest automatycznie rekonfigurowany wraz z przemieszczaniem się użytkowników do innych urządzeń, lokalizacji i rodzajów połączenia.		•	
Czyszczenie pamięci podręcznej przeglądarki	Usuwa obiekty i dane gromadzone w pamięci lokalnej przeglądarki podczas sesji SSL VPN. Zabezpiecza poufne informacje firmy przed pozostaniem w pamięci zdalnych urządzeń.			•

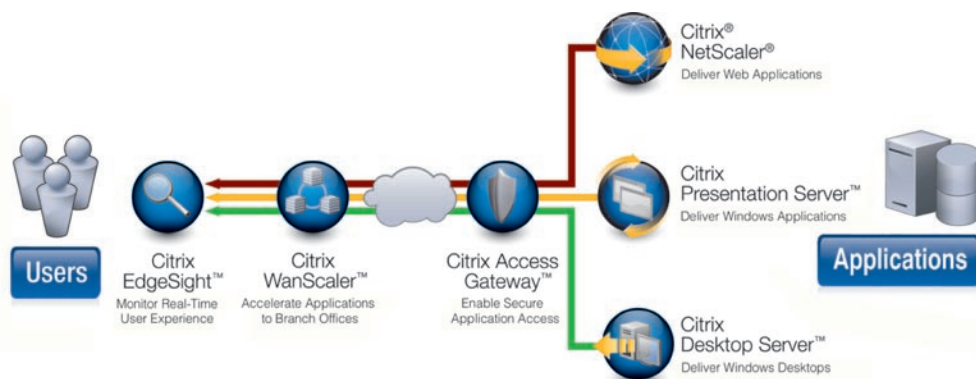
		Platinum Edition	Enterprise Edition	Advanced Edition
Cecha	Korzyść			
Wyłączenie lub włączenie rozdzielania tunelowania	Kontrola dotycząca tego, czy lokalna sieć użytkownika wraz z dostępem do Internetu będzie dostępna podczas sesji Access Gateway. Jeśli zdalny komputer jest jednocześnie połączony bezpośrednio z Internetem i siecią VPN, poprzez ataki za pośrednictwem Internetu osoby niepowołane mogłyby uzyskać dostęp do sieci korporacyjnej. Wyłączenie rozdzielania tunelowania zmniejsza zagrożenie złośliwym atakiem.	•	•	•
Rozwinięte sterowanie rozdzielaniem tunelowania	Rozdzielanie tunelowania można wyłączyć na poziomie klienta, w celu zamknięcia bezpośredniego dostępu do Internetu, przy jednoczesnym umożliwieniu dostępu do zasobów podsieci lokalnej klienta. Zmniejsza zagrożenie złośliwym oprogramowaniem, umożliwiając jednocześnie użytkownikom dostęp do drukarek sieciowych i innych zasobów lokalnych.			•
Uwierzytelnianie RADIUS i LDAP	Uwierzytelnia użytkowników na podstawie danych przechowywanych na serwerach LDAP lub RADIUS. Organizacje mogą wykorzystać istniejące katalogi z danymi uwierzytelniającymi.	•	•	•
Uwierzytelnianie dwuskładnikowe	Zapewnia dwuskładnikowe uwierzytelnianie użytkowników za pomocą znaczników RSA SecurID® and Secure Computing SafeWord™.	•	•	•
Uwierzytelnianie za pomocą karty elektronicznej	Zapewnia efektywne i wygodne uwierzytelnianie użytkowników za pomocą kart elektronicznych zgodnych ze standardami branżowymi.			•
Obsługa certyfikatów klienta	Przed udostępnieniem chronionych zasobów można sprawdzić poprawność certyfikatów w celu weryfikacji urządzeń klienckich.	•	•	•
Certyfikaty bezpieczeństwa	Model urządzenia z serii 9000 z opcją sprzętową FIPS spełnia wymagania normy FIPS 140-2 na poziomie 2.			•
Zapobieganie atakom typu odmowa usługi	Chroni zasoby przed najczęstszymi atakami typu odmowa usługi, takimi jak ataki typu SYN czy przepelnienie żądaniami HTTP GET.			•
Administracja oparta na rolach	Tworzy użytkowników i grupy administracyjne, z których każda może mieć niepowtarzalne uprawnienia administracyjne. Określa reguły bezpieczeństwa gwarantujące, że administratorzy wykonują tylko minimalny zestaw operacji wynikający z ich roli.			•
Nadzór nad działaniami użytkowników	Monitoruje i prowadzi zapis kontrolny działań użytkowników. Umożliwia pełny wgląd we wszystkie działania zapewniając bezpieczeństwo usług i danych.	•	•	•
Nadzór nad działaniami administratorów	Monitoruje wszystkie zmiany w konfiguracji dokonane przez administratorów. Zapewnia pełną odpowiedzialność administratorów poprzez zapis kontrolny wszystkich działań administracyjnych.			•
Obsługa protokołu SNMP	Bramka Access Gateway obsługuje protokół SNMP, który służy do przekazywania danych pomiarowych dotyczących stanu technicznego i wydajności. Jest on zintegrowany z istniejącymi systemami zarządzania i monitorowania sieci.	•	•	•
Serwery syslog	Bramka Access Gateway obsługuje zapisywanie plików dziennika systemowego na zdalnych serwerach syslog. Zbiera ona wszystkie logi w jednej lokalizacji, co ułatwia administrowanie.	•	•	•
Wiele wirtualnych serwerów sieci VPN	Pojedyncze urządzenie może emulować wiele sieci SSL VPN poprzez hostowanie jednego lub większej liczby serwerów wirtualnych – każdego z unikalnym IP, pełną nazwą domeny i certyfikatem. To obniża całkowity koszt eksploatacji dzięki konsolidacji sprzętu i punktów zarządzania.			•
Połączenia inicjowane przez serwer	Urządzenia klienckie mogą być konfigurowane według niepowtarzalnych adresów, co umożliwia nawiązywanie połączeń z sieci chronionej. Rozwiązanie to ma szeroki zakres zastosowań, takich jak tryb aktywny FTP, komunikatory internetowe i oprogramowanie do zarządzania systemami.			•
Obsługa VLAN	Obsługuje znakowanie na podstawie protokołu 802.1q, umożliwiając trasowanie pakietów do właściwego segmentu sieci VLAN. Umożliwia administratorom szybkie wdrożenie SSL VPN w sieciach z istniejącymi topologiami VLAN.			•

## Specyfikacje sprzętowe

Model Access Gateway				
	2000	7000	9000	9000 z opcją FIPS
Rozmiary	1,7" W x 16,8" S x 14,1" G (1U) 4,3 cm W x 42,6 cm S x 35,8 cm G	1,75" W x 17,25" S x 18,75" G (1U) 4,4 cm W x 43,8 cm S x 47,6 cm G	3,5" W x 17" S x 16" G (2U) 8,9 cm W x 43,2 cm S x 40,6 cm G	3,5" W x 17" S x 16" G (2U) 8,9 cm W x 43,2 cm S x 40,6 cm G
Waga	23 funty (10,4 kg)	28 funtów (12,17 kg)	34 funty (15,4 kg)	34 funty (15,4 kg)
Zasilanie	Zasilacz 260 W prądu przemiennego z czujnikiem temperatury. Prąd przemienny: 100–240 V, 60–50 Hz, 5–3 A	Prąd przemienny w pełnym zakresie: 90–264 V, 47–63 Hz, 250 W	Prąd przemienny w pełnym zakresie: 90–264 V, 47–63 Hz, 335 W	Prąd przemienny w pełnym zakresie: 90–264 V, 47–63 Hz, 335 W
Maksymalna liczba sesji	1000 równoległych (połączenia z siecią VPN) lub 2000 równoległych (połączenia z serwerem Presentation Server)	200 równoległych	5000 równoległych	5000 równoległych
Porty sieciowe	2 x 10/100/1000 BASE-T	6 x 10/100 BASE-T 2 x 10/100/1000 BASE-T	4 x 10/100/1000 BASE-T + 1 x 10/100/1000 BASE-T lub 4 x 1000 BASE-T-SX Fiber ports + 1 x 10/100/1000 BASE-T	4 x 10/100/1000 BASE-T + 1 x 10/100/1000 BASE-T lub 4 x 1000 BASE-T-SX Fiber ports + 1 x 10/100/1000 BASE-T
Dostępność w edycji	Standard Edition, Advanced Edition	Enterprise Edition	Enterprise Edition	Enterprise Edition
Gwarancja	1 rok na sprzęt; 1 rok na utrzymanie oprogramowania; dostępne są rozszerzone plany obsługi technicznej	1 rok na sprzęt; 90 dni na utrzymanie oprogramowania; dostępne są rozszerzone plany obsługi technicznej	1 rok na sprzęt; 90 dni na utrzymanie oprogramowania; dostępne są rozszerzone plany obsługi technicznej	1 rok na sprzęt; 90 dni na utrzymanie oprogramowania; dostępne są rozszerzone plany obsługi technicznej

## Sześć kluczowych elementów wydajnego systemu zdalnego dostępu do aplikacji

Dostęp do aplikacji dla wszystkich użytkowników – najwyższa wydajność, bezpieczeństwo i elastyczność, najniższy koszt.



**Citrix® NetScaler®** do dostarczania aplikacji internetowych — zoptymalizuj wszystkie aplikacje internetowe, korzystając ze zintegrowanego rozwiązania sieciowego, które zwiększa wydajność, poprawia bezpieczeństwo i zdecydowanie zmniejsza obciążenie serwerów.

**Citrix Presentation Server™** do dostarczania aplikacji działających w systemie Windows — możesz zaoszczędzić miliony na kosztach administracji i wyeliminować zagrożenia dla danych, instalując aplikacje Windows w centrum obliczeniowym, a następnie udostępniając je użytkownikom przez sieć w postaci zwirtualizowanej lub strumieniowej.

**Citrix Desktop Server™** do dostarczania pulpitów — zmniejsz koszty, nakłady pracy administracyjnej i zagrożenie bezpieczeństwa związane z pracą na stacjach roboczych, wirtualnie dostarczając pulpity Windows z centrum danych; w ten sposób poprawisz także komfort użytkowników.

**Citrix Access Gateway™** do bezpiecznego dostępu do aplikacji — udostępni pojedynczy, bezpieczny punkt dostępu do wszystkich aplikacji, który automatycznie dostosowuje zasady dostępu w zależności od scenariuszy użytkownika.

**Citrix WanScaler™** do przyspieszania aplikacji używanych przez użytkowników w oddziałach — natychmiast popraw wydajność aplikacji dostarczanych przez sieci WAN, zmniejszając jednocześnie zużycie pasma nawet o 75%.

**Citrix EdgeSight™** do monitorowania działania systemu z perspektywy użytkowników — zagwarantuj, że wszystkie aplikacje zawsze działają zgodnie z określonymi parametrami biznesowymi, monitorując ich wydajność z perspektywy użytkowników.

### Informacje o firmie Citrix:

Citrix Systems (NASDAQ: CTXS) jest globalnym liderem i najbardziej zaufanym dostawcą infrastruktury do dostarczania aplikacji. Ponad 200 tys. organizacji z całego świata polega na firmie Citrix w zakresie dostarczania dowolnych aplikacji do użytkowników w dowolnym miejscu, przy zachowaniu najwyższej wydajności, bezpieczeństwa i najniższych kosztów. Do klientów firmy Citrix należą 100% firm z listy Fortune100 i 98% z listy FortuneGlobal500, a także setki tysięcy małych przedsiębiorstw i zaawansowanych użytkowników. Citrix ma około 6200 partnerów w ramach kanału dystrybucyjnego i sojuszu, działających w ponad 100 krajach. Roczne przychody wyniosły w 2006 r. 1,1 miliarda USD. Więcej informacji można uzyskać na stronie [www.citrix.com](http://www.citrix.com).

©2007 Citrix Systems, Inc. Wszelkie prawa zastrzeżone. Citrix®, Citrix Application Firewall™, Citrix Presentation Server™, Citrix Application Gateway™, Citrix Access Gateway™, Citrix Password Manager™, NetScaler®, AppCache™, AppCompress™, AppExpert™, Request Switching®, GoToMeeting™, GoToAssist™, GoToMyPC® oraz Deep Stream Inspection™ są znakami towarowymi firmy Citrix Systems, Inc. i/lub jednej lub więcej firm od niej zależnych i mogą być zarejestrowane w Biurze Patentów i Znaków Towarowych USA (United States Patent and Trademark Office) i w innych krajach. Windows® jest zarejestrowanym znakiem towarowym firmy Microsoft Corporation w Stanach Zjednoczonych. UNIX® jest zarejestrowanym znakiem towarowym konsorcjum The Open Group w Stanach Zjednoczonych i innych krajach. Wszelkie inne znaki towarowe i zarejestrowane znaki towarowe należą do swoich właścicieli.

## Citrix Worldwide

### Worldwide headquarters

Citrix Systems, Inc.  
851 West Cypress Creek RoadFort  
Lauderdale, FL 33309  
USA  
Tel: +1 (800) 393 1888  
Tel: +1 (954) 267 3000

### European headquarters

Citrix Systems International GmbH  
Rheinweg 9, 8200 Schaffhausen  
Switzerland  
Tel: +41 (0)52 6 35 77-00

### Asia / Pacific headquarters

Citrix Systems Hong Kong Ltd.  
Suite 3201, 32nd Floor  
One International Finance Centre  
1 Harbour View Street, Central  
Hong Kong  
Tel: +852 2100 5000

### Citrix Online Division

Citrix Online Division  
5385 Hollister Avenue  
CA 93111, Santa Barbara  
USA  
Tel: +1 (805) 690 6400

### Selected European subsidiaries

**Citrix Systems GmbH**  
Am Söldnermoos 17  
85399 Hallbergmoos / München  
Germany  
Tel: +49 (0)811 83-0000

**Citrix Systems Poland Sp. z o.o.**  
Warsaw Financial Centre  
ul. E. Plater 53  
00-113 Warsaw  
Poland  
Tel: +48 (22) 528 6615

**Representative office  
of Citrix Systems Int. GmbH**  
Regus BC, Smolensky Passage  
Smolenskaya sq.,3  
121099 Moscow  
Russia  
Tel: +7 (495) 937 8249

[www.citrix.com](http://www.citrix.com)