opentext™ | Cybersecurity

資料表

NetIQ Advanced Authentication

NetIQ Advanced Authentication 讓組織擁有充分的靈活彈性，可調整安全性與使用者體驗以符合所需的驗證層級。您的組織可能已採用了數種安全技術，舉凡各種 ID 及密碼組合、建立存取識別證制度、處理安全回應詞語及 PIN 碼。這些措施對基本存取作業來說都不可或缺。您可透過 NetIQ Advanced Authentication Framework 加上強大的驗證方式 (MFA 或雙因素驗證) 以滿足法規、業界及客戶要求的規範。

主要優點

由 OpenText 提供的 NetIQ Advanced Authentication 可讓您將驗證集中在單一架構下，只要經由單一規則主控台就能進行管理，降低成本又能提升安全性。我們提供廣泛的整合功能及最新的驗證方法和裝置，所以您在整個環境中都能充分自主地針對情境選擇適當的安全性。藉由我們以開放式標準為基礎的解決方案，您在防範安全漏洞時也能避免受限於特定廠商的風險。針對自身需求做出最佳選擇。

驗證彈性講求的不僅是支援哪些驗證方式，支援哪些平台也是一大重點。NetIQ Advanced Authentication 涵蓋最廣泛的平台支援，從 Windows、OS X 和 Linux，到 iOS、Windows Mobile 和 Android 都包含在內。

以上種種特色都意味著 OpenText™ 最大的目標，就是讓您能針對自身環境打造最合適的 NetIQ Advanced Authentication。NetIQ Advanced Authentication 的延展擴充能力能夠應付最大、最複雜的環境，保證能讓大型組織滿意；而它的單純性也能讓小型組織充分受惠。

主要功能

多站點支援
我們支援分布在各地、有多個站點需求的組織。

多用戶支援
如果您的組織有多個部門或是事業體，各自的需求都大不相同的話，我們也能針對各自不同的設定進行支援。

高可用性：備援與負載平衡
我們透過包含內部負載平衡和複製的高可用性設計確保可靠度與效能。

適用於 Active Directory Federation Services (ADFS) 的 NetIQ Advanced Authentication
IT 安全團隊可選擇使用 NetIQ Advanced Authentication 的 ADFS 外掛程式，將存取延伸到更多方法和應用程式整合。

符合 FIPS 140-2 標準
我們將國家標準技術研究所 (NIST) 聯邦資訊處理標準 (FIPS) 140-2 包含在加密中，讓您安心部署。

裝置需求

最低組態
- 2 核心
- 2 GB RAM
- 40 GB 磁碟空間

建議組態
- 4 核心
- 4 GB RAM
- 60 GB 磁碟空間

RADIUS 伺服器
產品隨附 RADIUS 伺服器。目前僅支援 PAP 驗證。

用戶端元件
- Windows Credential Provider、Linux PAM 及 MacOS 驗證外掛程式
- Microsoft Windows 7 (x64/x86) SP1/ Microsoft Windows 8.1 (x64/x86)/ Microsoft Windows 10 (x64/x86)
- Apple MacOS X 10.10.5
- Linux 可外掛驗證模組 (CentOS 7、SUSE Linux Enterprise Desktop 12、SUSE Linux Enterprise Server 12、Red Hat Enterprise Linux Client 7.2 或 Red Hat Enterprise Linux Server 7.2)

智慧型手機應用程式
- Apple iOS 8/ 9
- Google Android 4.2/ 4.3/ 4.4/ 5.1/ 6.0，配備 300 萬像素 (以上) 且具有自動對焦功能的相機
- Windows Phone 8.1/ 10，配備 300 萬像素 (以上) 且具有自動對焦功能的相機

Geo-Fencing
對於使用 IP 的 Geo-Location 技術，您可能已相當熟悉，如今我們更利用全球定位 (GPS) 技術將其提升到全新境界。我們的 Geo-Fencing 讓驗證規則可以根據使用者的特定位置 (例如建築物或校園) 進行設定。

略過雙因素驗證
若您想在存取速度和安全需求間取得平衡，則可在驗證與驗證間設定寬限期間，在此段時間內無需雙因素驗證。不過，使用者仍然必須在一開始時完成完整的驗證要求。另外，您的組織也可以選擇使用由 OpenText™ 提供的 NetIQ Access Manager 風險式驗證引擎，來定義何時必須進行雙因素驗證。

行動工作團隊支援 - 離線登入
在外出差的員工必須進行雙因素驗證才能存取私人資訊，現在他們只要有需要，隨時可以這麼做。意即，即使沒有連線能力，使用者也能夠完成工作。

廣泛支援各種平台
我們專門提供橫跨各種平台 (Windows、OS X、Linux 和行動平台) 的安全防護功能。您可以使用多種驗證方式，例如 iOS、Android 和 Windows Mobile 各自專用的驗證，再搭配 RADIUS、卡片和生物測量。

整合遵循標準的應用
我們的解決方案遵循標準 (HSPD11、PKI12、OAuth、FIDO、OATH、RADIUS、FIPS 140、NFC ISO/IEC 及其他)。我們也支援一些專屬的解決方案，但設計的出發點永遠是為了提供您最高的彈性。

服務台模組
服務台模組所提供的功能可確保優良的端對端客戶體驗 (註冊、重新註冊、記號指派緊急密碼等)。

緊急密碼
如果使用者沒有可用的註冊驗證方法該怎麼辦?在這種情況下，若您的使用者還需要存取權限，服務台可產生緊急密碼來應急。

外部代理
HTTP Proxy 在網際網路和您的驗證伺服器間提供彈性的輪遞。

支援非網域客戶
為自備裝置 (BYOD) 且不屬於企業網域的使用者提供支援。我們不會藉要求網域成員資格等方式，限制您只能將多因素驗證用在企業裝置上。

內部部署、雲端或 SaaS
驗證架構是以可攜式 Docker 容器提供，讓您擁有整合整個環境的彈性，找到最符合您需求的任何格式。Docker 格式可讓您選擇雲端、內部部署或作為由 OpenText 提供的 SaaS 產品。所有這些選項都適用於您的雲端和混合式環境。Docker 平台也讓您能夠運用成熟且功能強大的管理工具組，使其成為符合您組態與維護需求的完美平台。我們的驗證架構也提供「即服務」，讓您以快速、強大的方式在整個環境中整合無密碼驗證。

與我們交流
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity 為所有規模的公司和合作夥伴提供全方位的安全性解決方案。從預防、偵測和回應，到復原、調查和合規，我們的統一端對端平台透過全方位安全性產品組合，來協助客戶建立網路韌性。OpenText Cybersecurity 客戶自我們即時的關聯式威脅情報獲得可據以行動的深入見解，享有可協助管理業務風險的高效率產品、合規體驗以及簡化的安全性。

760-TW0008-007 | O | 04/24 | © 2024 Open Text