NetIQ Advanced Authentication Framework (NAAF)
Micro Focus 的成長之路（創立於1976年）

- **2007**: Liant 公司
  - COBOL and PL/I development

- **2008**: Compuware 测試業務
  - Application Testing

- **2009**: NetManage 公司
  - Connectivity

- **2010**: Borland 公司
  - Application Lifecycle Management & Testing

- **2011**: AccuRev 公司
  - Agile Software Delivery

- **2012**: Progress CORBA 業務
  - Orbix, Orbacus, Artix

- **2013**: Attachmate 集團
  - Novell, NetIQ, SUSE
    - Identity, Access, Security
    - Host Connectivity
    - Collaboration
    - Performance Monitoring
    - Workload Management
    - Cloud Management

- **2014**: Serena 公司
  - Dimensions CM
  - Business Manager
  - Release Control

- **2015**: Authasas 公司
  - Advanced Authentication

- **2016**: HPE Software
  - AcuCorp 公司
    - Acu COBOL
  - AcuCOBOL
Micro Focus International PLC
MCRO : London Stock Quote

Top 3 IT Companies in UK 2015
密碼不再安全，如何加強保護帳密安全？
加強密碼強度

變更密碼
NetIQ Self Service Password Reset

您的密碼已過期，您必須立即設定新密碼。

請變更您的密碼。請保持新密碼的安全性。輸入您的新密碼後，請按一下「變更密碼」按鈕。若您必須寫下新密碼，請務必放在安全的位置。您的新密碼必須符合下列要求：

- 密碼不分大小寫。
- 長度至少必須為6個字元。
- 長度不可超過12個字元。
- 不可包含下列任何值：test password。
- 不可包含您的名稱或使用者名稱的一部分。
- 不可包含常見字或常用字元順序。

已接受新密碼，請按一下「變更密碼」。

新密碼

確認密碼

變更密碼 清除
加強認證強度 (Advanced Authentication)

傳統帳號密碼登入 + Smartphone
Authentication factors

1. **Something you know:**
   - Passwords
   - PIN-codes
   - Questions & Answers

2. **Something you have** (手持裝置)
   - Contactless cards
   - Smartcards
   - USB-tokens
   - OTP-Tokens
   - smartphone
   - Mobile phone (SMS/Text, Voice)
   - **Free NAFF APP for Mobile Device**

3. **Something you are** (生物)
   - Fingerprint
   - Iris
   - Face
   - Voice
   - Signature
What’s the challenge?

Access points

IT-infrastructure Access:
- User devices, networks, access to servers
- Building

Enterprise Application Access:
- ePhI and EMR
- Financial
- Remote
- Kiosks and workstations

Cloud/Web access:
- Web applications
- innerweb information
- Federated access (to or from)

Other
- Execution of transactions
- Signing of transactions
- Business data (storage)

And more.....
The Solution
NetIQ Advanced Authentication Framework

Access points

IT-infrastructure Access:
- User devices, networks, access to servers
- Building

Enterprise Application Access:
- ePhl and EMR
- Financial
- Remote
- Kiosks and workstations

Cloud/Web access:
- Web applications
- innerweb information
- Federated access (to or from)

Other
- Execution of transactions
- Signing of transactions
- Business data (storage)

And more.....

Authentication methods

Smart Cards
- Contact and Contactless Cards, PKI cards

Biometrics
- Fingerprint, Iris, Vein, Voice

Smartphone
- One-Time-Password (OTP), Out-of-Band, LiveEnsure

Radius
- Cryptocard, Phonefactor, SMS-Passcode, etc.

Tokens
- Software tokens, hardware tokens

Knowledge based
- Secret (phrase) questions, Passwords, PINcodes

Other
- Social Login, federated authentication, Thumb drive, Flash drive+PIN

Authentication administration
- Delegation
- PIN caching
- etc.
- **Agent-Based**
  - OS Agent: Windows, Linux, Mac
  - RADIUS Client (Citrix Netscaler, Cisco VPN, Juniper VPN, etc)

- **Proxy-Based (NAM Plug-in)**
  - Web Application, Cloud Service

- **API**
  - REST, Win com, Mobile(IOS, Android)
FIPS 140-2 Inside

Because National Institute of Standards and Technology's (NIST) standards for encryption have been recognized over the world. Federal Information Processing Standard (FIPS) 140-2 is important to any corporation. Advanced Authentication does meet these standards so security conscious businesses as well as organizations operating in regulated industries can deploy with confidence.

Geo-Fencing

Using global positioning (GPS) technology, geo-fencing allows the administrators to define authentication policies based on a user’s specific location, such as a building or campus. The policies can be configured to limit access to only those users in the allowed location(s). This feature differs greatly from typical geo-location using IP address lookup which relies upon
## Primary MFA Competition Comparison

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### On Premises
- Hosted (Authentication As A Service)
  - Password / PIN / Security Questions
  - Token / OATH-TOTP / HOTP
  - Voice Call + PIN
  - Grid One-Time-Password
  - RADIUS Server
  - Short Message Service OTP
  - App Based Out-Of-Band
  - Phone Based NFC
  - E-Mail One-Time-Password
  - Biometric Fingerprint / Finger vein
  - Proximity Card
  - Smart Card
  - Near Field Communications
  - FIDO U2F / YubiKey
  - Fingerprint / Finger vein
  - Live Ensure
  - Flash Drive + PIN
  - Global Positioning

### Integrations
- MS Windows XP/7/8 Gina/CP
- Linux PAM Module
- Apple OSX PAM Module
- Web APIs
- COM APIs
- RADIUS Client
- Symantec VIP

**NetIQ (Novell)**
- 1
- $3
- 3
- 3
- ●
- ●
- ●
- ●
- ●
- ●
- ●

**HXX**
- 1
- $%
- ●
- ●
- ●

**EXX**
- 1
- $%
- ●
- ●
- ●
- ●
- ●
- ●
- ●
- ●
- ●

**SxxxxXXX**
- ●
- ●
- ●
- ●
- ●
- ●
- ●
- ●
- ●
- ●

**Sxxxxxx**
- ●
- ●
- ●
- ●
- ●
- ●
- ●
- 4
- ●
- ●

---

$. Additional Charges  
1. With MSP  
2. Droid Phones with NFC used as proximity cards  
3. NAAF v5.2 / v5.3  
4. Proprietary Drives  
5. SAML Only
## Secondary MFA Competition Comparison

<table>
<thead>
<tr>
<th>On Premises (Hosted Authentication As A Service)</th>
<th>Authentication Methods</th>
<th>Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password / PIN / Security Questions</td>
<td>Grid.OAuth / TOTP / HOTP</td>
<td>RADIUS Server</td>
</tr>
<tr>
<td>Voice Call + PIN</td>
<td>Grid. Once-Time-Password</td>
<td>Short Message Service OTP</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>App-Based One-Time-Password</td>
<td>App-Based One-Time-Password</td>
</tr>
<tr>
<td>App-Based One-Time-Password</td>
<td>Phone Based One-Time-Password</td>
<td>E-Mail One-Time-Password / Finger vein</td>
</tr>
<tr>
<td>Phone Based One-Time-Password</td>
<td>Biometric Fingerprint / Finger vein</td>
<td>Proximity Card</td>
</tr>
<tr>
<td>Proximity Card</td>
<td>Smart Card</td>
<td>Near Field Communications</td>
</tr>
<tr>
<td>Near Field Communications</td>
<td>FIDO U2F / YubiKey</td>
<td>Live Ensure</td>
</tr>
<tr>
<td>Live Ensure</td>
<td>Flash Drive + PIN</td>
<td>Global Positioning</td>
</tr>
</tbody>
</table>

| | | MS: Windows XP/7/8 Gina/CP |
| | | Linux: PAM Module |
| | | Apple: OSX PAM Module |
| | | Device Fingerprinting |
| | | Web APIs |
| | | COM APIs |
| | | RADIUS Client |
| | | Single Sign-On |
| | | Symantec VIP |

### Additional Charges
- 1. With MSP
- 2. Droid Phones with NFC used as proximity cards
- 3. NAAF v5.2 / v5.3
- 4. Proprietary Drives
- 5. SAML Only
Register User smartphone

How it Works

Composition

- The user downloads the NetIQ Authentication Application to their device
- The user navigates to AAF Enrollment Portal and scans the QR code
- The soft token can then be used and it will check back with AAF for validation
Register Biometric Fingerprints
How it Works

Composition
- The user authenticates to workstation PC
- The user goes to AAF Enrollment Portal
- Fingerprint is evaluated and stored in AAF server
- The fingerprint can then be used and it will use AAF server for validation

AAF Client → Scan Fingerprint

AAF Server

Store Minutiae

Use
Integrate with REST API

- NAAF provides REST API, win com API, API for Mobile
Integrate with NetIQ Access Manager

- If there is no internet connection, perform an offline authentication using one-time password (Time-Based).
Integrate with PAM (Privileged Account Manager)
監控存取的路徑

統一管理帳號的建立、變更、撤銷程序

異常存取

統一管理使用者存取的路徑，特權帳號Proxy

即時監控所有帳號活動 + 網路安全
SourceIP
UserID
Time
## Identity-Powered Security 方案總覽
以「人」為中心的資訊安全治理方案

<table>
<thead>
<tr>
<th>方案</th>
<th>產品</th>
</tr>
</thead>
<tbody>
<tr>
<td>加強密碼強度：設定更安全的密碼</td>
<td>NetIQ Self Service Password Reset</td>
</tr>
<tr>
<td>加強認證強度：特定系統採用多因素強認證</td>
<td>NetIQ Advanced Authentication</td>
</tr>
<tr>
<td>統一管理帳號的建立、變更、撤銷程序</td>
<td>NetIQ Identity Manager</td>
</tr>
<tr>
<td>統一管理使用者存取的路徑</td>
<td>NetIQ Access Manager</td>
</tr>
<tr>
<td>加強特權帳號管理與監控</td>
<td>NetIQ Privileged Account Manager</td>
</tr>
<tr>
<td>神盾級自動化端點管理、佈署及安全防禦</td>
<td>Novell ZENworks</td>
</tr>
<tr>
<td>即時監控AD帳號活動 + 檔案存取活動</td>
<td>NetIQ Change Guardian</td>
</tr>
<tr>
<td>即時監控所有帳號活動 + 網路安全 + 端點安全</td>
<td>NetIQ Sentinel (Identity Tracking)</td>
</tr>
</tbody>
</table>
實用範例: Smartphone Authentication

• You need to enter a PIN or use Touch ID
• You have OOB message, click “Accept”
實用範例: Smartphone Authentication

- Message that Authentication was accepted
- User is logged in
- Close “Tab” to logout
Risk Based Authentication (Integrate with NAM)

Resource or Application:
- Financials
- HR
- Salesforce
- Travel Site
- Café Menu

Risk Engine
- External Parameters
- IP Address
- Geolocation
- HTTP Headers
- User Cookies
- User Profile
- Device ID
- User History

Calculated Level of Risk:
- Low risk
- Medium Risk
- High Risk

Decision:
- Allow Access
- Confirm Step-up
- Deny Access

Allowed Resources or Applications:
- Financials
- HR
- Salesforce
- Travel Site
- Café Menu