



## SafeNet身份认证管理器

### 产品简介

#### 优势

- 将安全访问扩展到云环境：安全访问、单点登录及自动为用户配置Office 365 和 SaaS应用。
- 将安全访问扩展到移动终端：针对iOS 设备采用凭据配置及身份认证管理，确保只有配有受信任设备的员工才能访问企业资源。
- 基于上下文的身份认证实现细粒度控制：使用可配置的策略规则，在用户每次登陆访问在线资源时，根据需要的认证级别提供细粒度身份认证。
- 应对不同的风险水平：支持广泛的身份认证方法，帮助组织应对各类风险状况。
- 扩展灵活性：可扩展身份认证基础设施，将OTP和CBA解决方案以及先进的安全应用均纳入其中。
- 降低支持成本：自动化流程、OTA无线激活和安装软件令牌及直观自助服务工具，确保为最终用户提供广泛支持并降低帮助台成本。
- 保持合规：全面的审核和报告功能，保证遵守隐私法规。

为您组织的身份认证基础设施提供一个灵活、可扩展、可伸缩的管理平台。

#### 满足您不断变化的身份认证需求

SafeNet 身份认证管理器 (SAM) 是一种综合的身份认证服务器，帮助组织实施可面向未来的强身份认证战略，确保使用单一身份认证后端平台就能在本地和远程安全访问公司的众多资源。

SafeNet 身份认证管理器提供OTP、基于证书和软件身份认证解决方案，以及基于上下文和级进式的身份认证，使组织能够应对当前的和不断变化的安全访问需求。

#### 方便实用的基于上下文的身份认证管理

SafeNet 身份认证管理器的基于上下文的身份认证功能，使组织能够依靠低调的强身份认证实现方便、高性价比的安全远程访问，同时保证可随时按需增加更加强大的安全防护措施的灵活性和敏捷性。

凭借级进式 (Step-up) 身份认证功能，当用户不能满足 IT 管理员预定义的策略时，SafeNet 身份认证管理器使得要求用户提供额外的认证因素变得更简单。

#### 将强身份认证扩展到云计算

随着企业迁移到云计算环境和SaaS应用，他们面临着确保安全和方便地访问核心应用程序和不再驻留在企业网络内的高度机密资源的挑战。

SafeNet 身份认证管理器通过向需要安全访问Office 365 和 SaaS应用，如GoogleApps 和 Salesforce.com (SFDC) 的企业用户提供无缝的和始终如一的强身份认证及单点登录 (SSO) 体验来应对这一挑战。

#### 移动设备的强身份认证和凭据管理

企业员工越来越多地使用非IT发布的消费类设备来访问敏感企业和客户数据。这些设备使企业面临严重的数据泄露及未经授权访问的安全漏洞，IT部门都在努力对此类设备强制实施安全策略。

通过向移动设备用户提供凭据生命周期管理和OTA无线证书配置，SafeNet 身份认证管理器可以确保只有使用受信任设备且经过身份认证的用户才可以访问公司信息和应用程序。

## 支持的SafeNet身份认证器

- eToken PRO
- eToken PRO Anywhere
- eToken PRO Smart Card
- SafeNet eToken 7300
- SafeNet eToken 5100
- SafeNet eToken 5200
- SafeNet eToken 4100
- SafeNet eToken 3400
- eToken NG-OTP
- eToken PASS
- MobilePASS
- eToken Virtual

## 支持的操作系统

- SAM 服务器及管理：Windows Server 2008/R2 ( 32位和64位 ) , Windows Server 2012
- 客户端：Windows Vista, Windows 7, Windows 8, Windows Server 2008 / R2 ( 32位和64位 ) , Windows Server 2012, Mac OS
- 移动设备：BlackBerry, iOS, Windows Phone, J2ME, Android

## 用户资源库:

- Microsoft Active Directory
- ADAM
- Microsoft SQL Server
- Open LDAP
- Novell eDirectory

## 特性:

### 支持多种认证方式和外形系数

- 支持基于内容的身份认证
- 支持级进式的身份认证
- 支持基于证书、一次性密码OTP、软件和带外OOB身份认证
- 提供多种外形系数, 包括: 钥匙链令牌, USB 令牌, 智能卡, 软件令牌, 手机令牌

### Secure access to multiple resources支持多种安全访问资源

- 通过SAML 2.0 支持云端 (SaaS) 应用程序, 如: Office 365
- VPNs
- OWA和其他基于 Web 的门户网站
- 虚拟桌面环境, 如: Citrix, VMware 和AWS
- 本地网络登录 (支持在线或离线模式)

### 支持移动设备安全

- 从任何终端设备使用任何身份验证方法都可有安全访问
- 凭据配置和管理iOS设备

### 原住民身份联盟

- 支持使用SAML2.0联合登录
- SaaS 应用程序的自动用户注册和配置

### 全面的管理功能:

#### 报告和合规性

- 为整个身份验证的生态系统提供单一审计
- 职责分离和基于角色的授权
- 报告与审核跟踪

### 完整的生命周期管理

- 自助服务门户, 允许用户自助注册和令牌管理
- 证书生命周期管理
- 身份认证器分配、登记和更新基于预定义策略
- 身份认证器吊销、临时禁用和替换
- 临时令牌启用

### 灵活地扩展

- 跨域管理
- 支持多林活动目录Active Directory
- 支持OTP和基于证书的本地网络连接和离线模式访问



联系我们: 400 600 9103

有关所有办事处地址和联系信息, 请访问 [www.safeploy.com/contact](http://www.safeploy.com/contact)

SafePlay徽标是安策科技的政策商标,

SafeNet 和 SafeNet 徽标是 Gemalto 的注册商标。所有其他产品名称都为各自所有者的商标。(CN)

—02-18-15

SafeNet Authentication Manager 产品简介

