

IBM Tivoli Access Manager for Enterprise Single Sign-On

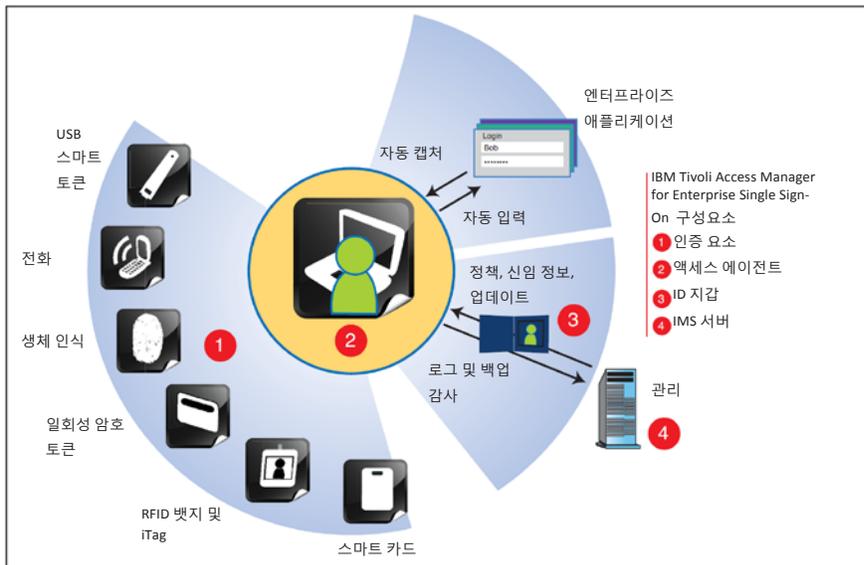
중점 사항

- 암호 재설정 요청의 발생 건수를 줄여 업무 지원 센터의 암호 관련 비용 절감
- 즉시 사용 가능한 다양하고도 강력한 인증 요소를 갖춘 개방형 인증 장치 인터페이스와 강력한 암호를 통해 보안 강화 및 규제 충족
- 중앙 감사 및 보고 기능으로 개인 정보 보호 및 보안 규제 준수 촉진
- 사인-온을 자동화하고 단일 암호로 모든 애플리케이션에 액세스하여 생산성을 높이고, 최종 사용자의 환경을 단순화

모든 유형의 애플리케이션에 적용할 수 있는 검증된 싱글 사인온 솔루션으로 암호 관련 고민이 해결됩니다.

매일 시도해야 하는 로그온의 복잡도와 회수가 증가함에 따라 직원들의 불만이 쌓이고 생산력이 저하됩니다. 대부분의 조직이 직원으로 하여금 5~20자리의 암호를 기억하고, 30일마다 이를 변경하도록 요청하고 있습니다. 암호를 입력하고 변경하며 변경된 암호를 잊지 않도록 메모해 놓고 결국 잊어버릴 경우 재설정하느라 소비하는 시간은 곧 IT 업무 지원 센터 운영의 생산성 및 비용적 손실을 의미합니다.

시장을 선도하는 엔터프라이즈 싱글 사인온 솔루션인 IBM Tivoli® Access Manager for Enterprise Single Sign-On을 사용할 경우, 단 한 차례의 인증만



IBM Tivoli Access Manager for Enterprise Single Sign-On에 기존 인프라의 변경 없이 싱글 사인온, 강력한 인증, 세션 관리, 애플리케이션 화면 자동 탐색 및 감사 추적을 결합

거치고 나면 소프트웨어에서 다음과 같은 해당 직원의 암호 관련 모든 이벤트를 검색하고 자동화합니다.

- 로그인
- 암호 선택
- 암호 변경
- 암호 재설정
- 생산 작업을 즉시 시작할 수 있는 애플리케이션 화면으로 자동 탐색
- 로그오프

Tivoli Access Manager for Enterprise Single Sign-On은 조직의 비용 절감, 보안 강화, 생산성 개선, 정부 규제에 대한 준수 등의 해결을 지원합니다. 이 솔루션은 사용자의 모든 Microsoft® Windows®, Web, Java™, 메인프레임 및 텔레타이프 애플리케이션에 싱글 사인온을 제공하며 Windows 데스크탑, 랩탑, 공유 키오스크, Citrix 서버, Microsoft 터미널 서버 및 웹 포털 등 모든 주요 네트워크 액세스 포인트에서 사용 가능합니다. 이렇듯 완전한 엔드포인트 적용 범위 덕분에 사용자는 장소에 상관없이, 심지어 인터넷 카페의 브라우저를 통해 액세스할 경우에도 엔터프라이즈 네트워크에 단일 암호를 사용해 사인온하고, 모든 애플리케이션에 싱글 사인온으로 액세스할 수 있습니다.

암호 관리 비용 절감

Tivoli Access Manager for Enterprise Single Sign-On을 통해 업무 지원 센터, 규제 준수 및 관리에 소모되는 비용을 절감할 수 있습니다. 업무 지원 센터에 들어오는 요청 중 많게는 80%가 암호 재설정과 관련된 것입니다. 대규모 조직에서는 해당 비용으로 연간 수백만 달러를 지출하기도 합니다. Tivoli Access Manager for Enterprise Single Sign-On을 사용하면 직원이 암호를 잊어버릴 경우 간단한 질의응답 프로세스를 통해 이를 재설정할 수 있습니다.

사용자 액세스를 감사 및 추적하고 필요한 규제 준수 보고서를 작성하여 규제 준수 비용도 줄일 수 있습니다. 사용자 ID 및 암호를 관리하는 한편 사용자에게 셀프 서비스 기능을 제공함으로써 관리 비용 역시 절감 가능합니다.

암호 동작 개선을 통한 보안 강화

사용자가 여러 개의 사용자 ID와 암호를 소유한 경우, 안전하지 않은 장소에 이러한 정보를 적어놓거나, 추측하기 쉬운 암호를 사용하거나, 암호를 동료와 공유하는 사례를 쉽게 찾아 볼 수 있습니다. Tivoli Access Manager for Enterprise Single Sign-On을 사용하면 단 하나의 암호만 기억하면 됩니다.

Tivoli Access Manager for Enterprise Single Sign-On은 암호 변경을 검색하고, 각 애플리케이션에 대한 강력한 암호를 자동 생성하도록 구성 가능합니다. 소프트웨어에서 이 강력한 암호를 통해 싱글 사인온을 기억하고 활성화하므로 사용자가 암호를 직접 기억하거나 관리할 필요가 없으며, 따라서 사용자 생산성이 유지되고 보안이 제공됩니다. 암호와 관련된 데이터를 그 위치에 관계없이 보호하기 위해 현존하는 암호화 중 가장 강력한 유형에 해당하는 AES (Advanced Encryption Standard) 알고리즘을 사용합니다.

강력한 인증으로 정보 보호

수많은 조직에서 중요 정보에 대한 액세스를 보호하고, 정부 규제를 준수하기 위해 암호 이상의 강력한 인증 방법을 모색하고 있습니다. Tivoli Access Manager for Enterprise Single Sign-On에서는 USB 스마트 토큰, 스마트 카드, 능동적 근접식 카드, 수동적 근접식 뱃지, 일회성 암호 토큰 및 지문 생체 인식 장치 등의 다양하고도 강력한 인증자를 지원함은 물론 사무실 뱃지, 사진 뱃지 및 휴대 전화와 같은 기존 식별 장치도 인증에 사용할 수 있습니다.

사용자가 이미 알고 있으며 보유하고 있는 장치를 활용하여 구현을 가속화하고, 총 소유 비용을 절감할 수 있습니다.

Tivoli Access Manager for Enterprise Single Sign-On은 유연성을 더하기 위해 개방형 인증 장치 인터페이스를 제공하며, 그에 따라 PKCS#11 또는 MS-CAPI 호환이 가능한 스마트 카드 및 사무실 출입 뱃지 또는 사진 뱃지 등의 일련 ID 장치와 통합이 용이합니다.

키오스크 및 공유 워크스테이션에 새로운 수준의 보안 추가

신속한 사용자 전환 및 세션 관리는 제조, 의료, 물류 창고, 소매 및 교육 등 여러 산업의 필수 요소입니다. 조직에서 공유 워크스테이션 및 키오스크의 설치를 확대함에 따라 수많은 사용자가 장소의 구매 없이 개인 PC를 이용하지 않고도 정보에 로밍하여 액세스 할 수 있게 되었습니다. 하지만 사용자가 로그오프 하지 않은 채 공유 키오스크에서 이동할 경우 기밀 정보가 권한이 없는 액세스에 노출될 가능성이 있어 심각한 보안 위협이 발생합니다.

보안을 강화하고, 고유의 사용자 로그온을 실행하며, 규제를 준수하려는 노력으로 인해 사용자는 워크스테이션 밖으로 벗어나지 못하게 되며, 결국 생산성이 떨어지는 결과가 초래됩니다.

조직은 Tivoli Access Manager for Enterprise Single Sign-On의 포괄적인 세션 관리와 신속한 사용자 전환 기능을 활용하여 사용자 편의를 증대하고 보안을 개선하여 다양한 사용자 그룹의 액세스 요구를 충족할 수 있습니다. 여러 사용자가 한 대의 컴퓨터를 동시에 공유할 수 있으며, 로그아웃 하거나 자리를 지켜야 하는 번거로움 없이도 사용자 전환이 가능합니다. 언제나 자신의 데스크탑을 사용하기 원하는 사용자라면 소프트웨어의 데스크탑 로밍 지원을 사용하면 됩니다. 또한 개인 데스크탑을 유지하는 동시에 동료와 워크스테이션을 공유할 수도 있습니다.

사용자가 로그아웃 하지 않은 채 자리를 떠날 경우를 대비해 구성 가능 화면 잠금, 애플리케이션 로그아웃 정책, 모든 애플리케이션의 단계적 로그오프 등의 비활성 시간 종료 정책을 실행하도록 Tivoli Access Manager for Enterprise Single Sign-On을 구성할 수 있습니다.

감사 추적 및 준수 보고 단순화

정부 규제 준수를 해결하기 위해 Tivoli Access Manager for Enterprise Single Sign-On은 전체 사용자의 로그온 활동을 투명하게 기록하고, 중앙에서 이를 IMS™ (Integrated Management System) 서버로 보고합니다. 또한 추적에 대한 사용자 정의가 가능하여 애플리케이션 전체가 아닌 활동에 한해 추적 및 모니터링 할 수 있습니다. 그 결과물인 통합 사용자 중심 로그를 통해 관리자를 올바른 애플리케이션 로그로 인도하는 메타 정보를 제공하여 필요에 따라 보다 상세한 분석이 가능합니다. Tivoli Common Reporting과의 통합으로 규제 보고 요구에 부합하는 유연한 보고 기능을 제공합니다.

설치 및 관리 단순화

Tivoli Access Manager for Enterprise Single Sign-On은 마법사 중심의 그래픽 관리 웹 콘솔을 제공하여 설치 및 관리를 단순화합니다. 관리자는 콘솔의 마우스로 이용 가능한 마법사를 통해 구성, 설치 및 관리 작업을 진행할 수 있습니다.

Tivoli Access Manager for Enterprise Single Sign-On은 여러 유명 애플리케이션에 사전 구성 탑재되어 있으며, 그 밖의 수많은 애플리케이션의 경우 액세스 프로파일의 손쉬운 무료 다운로드를 지원하고 있습니다.

또한 관리자는 복잡한 스크립트 또는 고가의 커넥터를 개발하거나, 대상 애플리케이션 또는 시스템의 변경 없이 간단한 마법사 인터페이스만으로 새 애플리케이션의 액세스 프로파일을 자동 생성할 수 있습니다. 보다 복잡한 애플리케이션의 경우 시각적 프로파일링, 즉 끌어서 놓는 간단한 그래픽 접근법으로 자동화 및 사인온 구성을 지원합니다.

본 소프트웨어는 중앙에 설치되도록 설계되었습니다. 설치 프로세스에 직원이 개입할 필요가 없이 네트워크 관리자가 중앙에서 IBM Tivoli Configuration Manager 또는 기타 소프트웨어 배포 솔루션을 사용해 클라이언트 측 소프트웨어를 설치할 수 있습니다.

소프트웨어가 시작 및 실행되면 관리자가 관리 콘솔을 사용해 사용자를 개별적으로 또는 그룹 별로 관리할 수 있습니다. 중앙 콘솔을 통해 관리자는 암호 정책, 시스템 규칙,

사용자 인터페이스 특성, 재인증 매개변수 및 기타 옵션을 설정할 수 있습니다.

기존 IT 인프라 및 디렉토리 자원 활용

Tivoli Access Manager for Enterprise Single Sign-On은 작업 시 조직의 기존 IT 인프라를 아예 또는 거의 변경할 필요가 없도록 설계되었습니다. 작업 시 디렉토리 구조에 구애를 받지 않으므로 설치에 앞서 많은 비용을 요하는 디렉토리 통합 프로젝트가 필요하지 않습니다. 일부 경쟁사의 싱글 사인온 상품과 달리, 디렉토리 스키마 확장 또는 디렉토리 데이터 복제가 불필요합니다.

이 솔루션은 사용자 신임 정보, 시스템 설정 및 정책을 기업 데이터베이스에 중앙 저장하는 한편 ID 데이터와 관련하여 Active Directory, NT Domain Controllers, Sun One LDAP, IBM Tivoli Directory Server 및 Novell eDirectory 등의 기업 디렉토리와 연동됩니다.

또한 이 솔루션은 Microsoft Internet Explorer 및 Mozilla Firefox 브라우저에

호환 가능하므로 두 브라우저 중 하나 또는 모두를 사용하는 사용자에게 편리함과 비용 절감의 효과를 선사합니다.

최종 사용자 및 권한 ID의 중앙 관리와 액세스 단순화

관리자는 일반적으로 직원을 대신하여 각 애플리케이션, 시스템 또는 플랫폼의 계정과 신임 정보를 생성하여 이메일 또는 서면으로 직원에게 이를 통보합니다. 이러한 신임 정보의 수동 생성 및 보급은 생산성 저하는 물론 애플리케이션 신임 정보의 직원 처리로 인해 보안 침해를 유발할 수 있습니다.

Tivoli Access Manager for Enterprise Single Sign-On은 동급 최강 사용자 프로비저닝 기술 및 자가 솔루션과 통합하여 포괄적인 엔드 투 엔드 ID수명 주기 관리를 제공합니다. Tivoli Identity Manager와 같은 ID 관리 솔루션에서 프로비저닝 명령을 받아 들이고, 직원의 ID 지갑에 무작위 생성한 애플리케이션 신임 정보를 사전 입력할 수 있습니다.

이렇듯 프로비저닝 솔루션과의 강력한 통합으로 프로비저닝 시스템을 통해 액세스 권한이나 암호가 변경될 때마다

Tivoli Access Manager for Enterprise Single Sign-On 사용자 정보가 동기화되어 최신 애플리케이션 신임 정보의 사용이 보장됩니다. 마찬가지로 사용자가 디프로비저닝될 경우 이 강력한 통합으로 Tivoli Access Manager for Enterprise Single Sign-On을 통한 액세스의 자동 거부를 보장합니다.

Tivoli Identity Manager 및 Tivoli Access Manager for Enterprise Single Sign-On을 통합하여 사전 정의한 사용자 그룹 간에 계정 공유가 가능하고, 그룹 내 사용자 개개인에게 지정된 공유 계정에 대한 싱글 사인온을 제공하며, 이는 계정 암호가 업데이트되는 순간에도 적용됩니다. 이들 제품은 공유 계정 풀의 강력한 체크인 및 체크아웃을 실행하도록 구성할 수 있어 권한 ID 관리의 신뢰성을 보장합니다.

IBM Tivoli Access Manager for e-business 및 IBM Tivoli Federated Identity Manager 구현 개선

현재 많은 고객이 Tivoli Access Manager for e-business 및 Tivoli Federated Identity Manager의 웹 및 연합 액세스 관리 혜택을 누리고 있습니다. Tivoli Access Manager for Enterprise Single Sign-On은 이러한 환경과의 통합이 용이하여 클라이언트 중심의 전반적인 기능을 전달합니다.

이러한 통합 솔루션 스위트를 통해 내부, 외부 및 조직 간 싱글 사인온이 가능하며 다른 상품에서는 불가능한 포괄적인 엔드 투 엔드 싱글 사인온 솔루션을 제공합니다.

Tivoli Access Manager for Enterprise Single Sign-On의 주요 구성 요소

인증 요소: 유연하고도 비용 효율이 높은 이중 인증을 위해 개방형 인증 장치 인터페이스와 iTag—벤티 및 기타 개인 물건에 부착 가능한 RFID를 포함한 스마트 레이블 등의 다양하고도 강력한 인증 요소를 지원합니다.

액세스 에이전트 및 플러그인: 사용자 대신 싱글 사인온 및 사인오프, 인증 관리 및 세션 관리를 담당하는 클라이언트 소프트웨어입니다. JScript 및 VBScript 플러그인으로 액세스 에이전트의 작동을 사용자 정의할 수 있습니다.

ID 지갑: 사용자 신임 정보를 보관하는 암호화된 개인 저장소입니다. ID 지갑은 액세스 포인트로 이동하여 로그인 신임 정보, 인증서, 암호화 키 및 사용자 정책 등 사용자의 개인 ID 프로파일을 저장합니다.

IMS(Integrated Management System) 서버: 사용자 및 정책에 대한 중앙 관리를 제공합니다. 정책은 전부 중앙에서 정의된 후 액세스 에이전트를 통해 실행됩니다. IMS 서버 또한 신임 정보, 손실 관리, 감사 정보 및 규제 준수 보고에 대한 포괄적인 백업을 제공합니다.

추가 정보

사용자 및 IT 관리자의 암호 관리를 단순화하는 Tivoli Access Manager for Enterprise Single Sign-On과 관련한 자세한 내용은 IBM 마케팅 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 해당 사이트(ibm.com/tivoli/security)를 방문하여 참조 바랍니다.

IBM Tivoli 소프트웨어

IBM Tivoli 소프트웨어는 기업이 IT 자원, 작업 및 프로세스를 효율적이고도 효과적으로 관리하여 끊임 없이 변화하는 비즈니스 요구사항을 충족하고, 유연성과 응답성을 겸비한 IT 서비스 관리를 전달함과 동시에 비용을 절감하도록 돕습니다. Tivoli 소프트웨어 포트폴리오의 범위는 보안, 규제 준수, 저장소, 성능, 가용성, 구성, 운영 및 IT 수명 주기 관리에 이르기까지 다양하며 세계 수준의 IBM 서비스, 지원 및 연구로 이를 뒷받침합니다.



Tivoli Access Manager for Enterprise Single Sign-On 개요

클라이언트 에이전트 요구사항:

- Windows XP SP2, Vista, 2003 Server, 2008 Server
- 600MHz Intel® Pentium® 기반 프로세서 및 256MB RAM
- 디스크 공간: 최소 200MB 여유 하드 디스크 공간
- Microsoft Internet Explorer 5.0 또는 이상 버전(128비트 암호화 포함), Firefox 3.x
- Microsoft Installer(MSI) 패키지를 통한 설치의 경우 Microsoft Windows Installer 필요

관리 콘솔 및 서버 요구사항:

- IMS 서버의 경우 Windows 2003 또는 2008 Server 필요
- AccessAdmin의 경우 Microsoft Internet Explorer 6.0 또는 이상 버전(128 비트 암호화 포함) 필요
- 1.2GHz Pentium 호환 프로세서 및 1GB RAM
- 디스크 공간: 최소 3GB 여유 하드 디스크 공간
- 디렉토리: Active Directory, NT Domain Controllers, Sun One LDAP, Tivoli Directory, Server, Novell eDirectory, 또는 기타 LDAP
- 데이터베이스: DB2® 9.5 또는 9.7, Microsoft SQL 2000 또는 2005 Server, Oracle 9i 또는 10g

인증:

- FIPS 140-2
- Common Criteria EAL 4+ 평가 진행 중 (이 인증은 체계적인 설계, 테스트 및 검토를 거쳐 인증을 입증할 수 있는 선정된 소수의 제품에 한해 수여됩니다.)

고객은 법적 요구사항에 대한 준수 여부를 확인해야 합니다. 고객의 영업에 영향을 줄 수 있는 모든 관련 법률 및 규정과 이러한 법률을 준수하는 데 필요한 모든 조치를 식별하고 해석하기 위해 적절한 법률 고문의 자문을 구하는 것은 전적으로 고객의 책임입니다. IBM은 법률 자문을 제공하지 않으며 IBM의 서비스나 제품을 통해 관련 법률이나 규정에 대한 고객의 준수 여부가 확인된다고 진술하거나 보증하지 않습니다.

© Copyright IBM Corporation 2009

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
November 2009
All Rights Reserved

IBM, IBM 로고, ibm.com 및 Tivoli는 미국 또는 기타 국가에서 사용되는 International Business Machines Corporation의 상표 또는 등록상표입니다. 이와 함께 기타 IBM 상표가 기재된 용어가 상표 기호(® 또는 ™)와 함께 이 정보에 처음 표시된 경우, 이와 같은 기호는 이 정보를 발행할 때 미국에서 IBM이 소유한 등록상표 또는 일반 법적 상표입니다. 또한 이러한 상표는 기타 국가에서 등록상표 또는 일반 법적 상표입니다. 현재 IBM 상표 목록은 웹 '저작권 및 상표 정보' (ibm.com/legal/copytrade.shtml)에 있습니다.

Intel 및 Pentium은 미국 또는 기타 국가에서 사용되는 Intel Corporation 또는 그 계열사의 상표 또는 등록상표입니다.

Java는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, Inc.의 상표입니다.

Microsoft 및 Windows는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

기타 회사, 제품 및 서비스 이름은 타사의 상표 또는 서비스표입니다.

여기서 IBM 제품 또는 서비스를 언급하는 것이 IBM이 영업하는 모든 국가에서 이들 제품 또는 서비스를 사용할 수 있다는 것을 의미하지는 않습니다.

제품 데이터의 정확성은 해당 데이터의 최초 공개일 현재로 이미 검토된 바 있습니다. 제품 데이터는 별도의 통지 없이 변경될 수 있습니다. IBM이 제시하는 장래 방향 및 계획에 대한 모든 진술은 특별한 통지없이 변경 또는 철회될 수 있으며 단지 목표 및 대상을 제시하는 것입니다.

이 책에 제공된 정보는 명시적이거나 묵시적인 일체의 보증 없이 "현상태대로" 배포됩니다. IBM은 상품성, 특정 목적에의 적합성 또는 타인의 권리 침해에 대한 어떠한 보증도 제공하지 않습니다. IBM 제품에 대한 보증은 제품의 준거 계약(예: IBM 기본 계약, 보증 제한 설명서, 국제 프로그램 라이선스 계약 등) 조항에 의거하여 제공됩니다.



Recyclable, please recycle.