(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0045372
(43) 공개일자 2017년04월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/53 (2013.01) *G06F 21/00* (2006.01)
G06F 21/41 (2013.01) *G06F 21/62* (2013.01)
G06F 9/50 (2006.01) *H04L 12/24* (2006.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
G06F 21/53 (2013.01)
G06F 21/00 (2013.01)
(21) 출원번호 10-2017-7010314(분할)
(22) 출원일자(국제) 2013년10월10일
심사청구일자 없음
(62) 원출원 특허 10-2015-7031152
원출원일자(국제) 2013년10월10일
심사청구일자 2015년10월29일
(85) 번역문제출일자 2017년04월14일
(86) 국제출원번호 PCT/US2013/064319
(87) 국제공개번호 WO 2014/158228
국제공개일자 2014년10월02일
(30) 우선권주장
61/806,577 2013년03월29일 미국(US)
(뒷면에 계속)

(71) 출원인
사이트릭스 시스템스, 인크.
미국 플로리다 33309, 포트 라우더데일, 851 더블류. 사이프레스 크릭 로드
(72) 발명자
쿠레쉬, 와히드
미국, 플로리다 33309, 포트 라우더데일, 851 웨스트 사이프레스 크릭 로드, 씨/오 사이트릭스 시스템스, 인크.
(74) 대리인
남호현

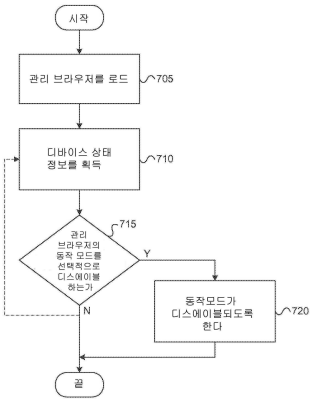
전체 청구항 수 : 총 23 항

(54) 발명의 명칭 **관리 브라우저 제공**

(57) 요 약

관리 브라우저를 제공하기 위한 방법들, 시스템들, 컴퓨터-판독가능 매체 및 장치들이 제시된다. 다양한 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저(managed browser)를 로딩할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책(policy)들이 관리 브라우저에 적용되는 관리 모드 및 이러한 정책들이 적용되지 않을 수 있고 그리고/또는 브라우저가 컴퓨팅 디바이스상에서 실행되는 적어도 하나의 디바이스 관리 에이전트에 의해 관리되지 않을 수 있는 비관리 모드를 제공하도록 구성될 수 있다. 디바이스 상태 정보 및/또는 하나 이상의 정책들에 기초하여, 관리 브라우저는 관리 모드와 비관리 모드 사이에서 전환될 수 있으며, 관리 브라우저는 이러한 상태 정보 및/또는 하나 이상의 정책들에 기초하여 기업 자원들에 대한 액세스를 선택적으로 제공하는 것을 포함할 수 있는 다양한 기능들을 제공할 수 있다.

대 표 도 - 도7



(52) CPC특허분류
G06F 21/41 (2013.01)
G06F 21/6218 (2013.01)
G06F 9/5005 (2013.01)
H04L 41/0816 (2013.01)
H04L 41/50 (2013.01)
H04L 63/0815 (2013.01)
H04L 63/20 (2013.01)
H04L 65/403 (2013.01)
G06F 2221/2143 (2013.01)

(30) 우선권주장
61/866,229 2013년08월15일 미국(US)
14/040,831 2013년09월30일 미국(US)

명 세 서

청구범위

청구항 1

컴퓨팅 디바이스에 의해 관리 브라우저(managed browser)를 로딩하는 단계 – 상기 관리 브라우저는 하나 이상의 정책(policy)들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드(managed mode)를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 –;

상기 컴퓨팅 디바이스에 의해, 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하는 단계;

상기 컴퓨팅 디바이스에 의해, 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하는 단계; 및

상기 컴퓨팅 디바이스에 의해, 상기 획득된 기업 데이터를 보안 문서 컨테이너에 저장하는 단계를 포함하고,

상기 관리 브라우저는, 상기 관리 브라우저가 더 이상 적어도 하나의 디바이스 관리자에 의해 관리되지 않으며 상기 관리 브라우저상에서 정책들이 시행되지 않는 비관리 모드(unmanaged mode)를 제공하도록 또한 구성된 것인, 방법.

청구항 2

제 1항에 있어서,

상기 컴퓨팅 디바이스에 의해, 상기 관리 브라우저가 상기 비관리 모드로 작동할 때 상기 획득된 기업 데이터에 대한 액세스를 선택적으로 차단하는 단계를 더 포함하는, 방법.

청구항 3

제 1항에 있어서,

상기 컴퓨팅 디바이스에 의해, 상기 관리 브라우저가 적어도 하나의 관리 모드로 작동할 때에만 상기 관리 브라우저를 통해 상기 보안 문서 컨테이너에 대한 액세스를 제공하는 단계를 더 포함하는, 방법.

청구항 4

제 1항에 있어서,

상기 컴퓨팅 디바이스에 의해, 상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하는 단계를 더 포함하는, 방법.

청구항 5

제 4항에 있어서, 상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하는 단계는, 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 획득된 기업 데이터를 삭제하는 것을 포함하는 것인, 방법.

청구항 6

제 4항에 있어서, 상기 데이터는 상기 관리 브라우저가 닫혀 있을 때 상기 보안 문서 컨테이너로부터 선택적으로 삭제되는 것인, 방법.

청구항 7

제 4항에 있어서,

상기 데이터는 상기 하나 이상의 정책들에 기초하여 상기 보안 문서 컨테이너로부터 선택적으로 삭제되는 것이고,

상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하는 단계는, 다른 데이터는 상기 보안 문서 컨테이너에 남겨 두는 한편, 특정 기간 동안 저장되었던 데이터를 삭제하는 것을 포함하는 것인, 방법.

청구항 8

적어도 하나의 프로세서; 및

컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하고;

상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하며;

상기 획득된 기업 데이터를 보안 문서 컨테이너에 저장하도록 하고,

상기 관리 브라우저는, 상기 관리 브라우저가 더 이상 적어도 하나의 디바이스 관리자에 의해 관리되지 않으며 상기 관리 브라우저상에서 정책들이 시행되지 않는 비관리 모드(unmanaged mode)를 제공하도록 또한 구성된 것인, 컴퓨팅 디바이스.

청구항 9

제 8항에 있어서,

상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성된 것이고,

상기 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하는 것은, 하나 이상의 암호화된 로컬 캐시들에 상기 적어도 하나의 기업 자원으로부터 획득된 데이터를 캐싱하는 것을 포함하는 것인, 컴퓨팅 디바이스.

청구항 10

제 8항에 있어서, 상기 메모리는 추가적인 컴퓨터-판독가능 명령들을 저장하며, 상기 추가적인 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 또한,

상기 관리 브라우저가 적어도 하나의 관리 모드로 작동할 때에만 상기 관리 브라우저를 통해 상기 보안 문서 컨테이너에 저장되어 있는 상기 획득된 기업 데이터에 대한 액세스를 제공하도록 하고,

상기 획득된 기업 데이터에 대한 액세스를 제공하는 것은, 싱글 사인온(single sign-on; SSO) 크레덴셜에 기초하여 하나 이상의 정책들 중 적어도 하나의 정책을 시행하는 것을 포함하는 것이고,

상기 하나 이상의 정책들 중 적어도 하나의 시행된 정책은 상기 획득된 기업 데이터에 대한 액세스를 제한하도록 구성된 것인, 컴퓨팅 디바이스.

청구항 11

제 8항에 있어서, 상기 메모리는 추가적인 컴퓨터-판독가능 명령들을 저장하며, 상기 추가적인 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 또한,

상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하도록 하는, 컴퓨팅 디바이스.

청구항 12

제 11항에 있어서,

상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하는 것은, 상기 요청에 기초하여 상기 하나 이상의

기업 자원들로부터 획득된 기업 데이터를 삭제하는 것을 포함하는 것인, 컴퓨팅 디바이스.

청구항 13

제 11항에 있어서, 상기 데이터는 상기 관리 브라우저가 닫혀 있을 때 상기 보안 문서 컨테이너로부터 선택적으로 삭제되는 것인, 컴퓨팅 디바이스.

청구항 14

제 11항에 있어서,

상기 데이터는 상기 하나 이상의 정책들에 기초하여 상기 보안 문서 컨테이너로부터 선택적으로 삭제되는 것이고,

상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하는 것은, 다른 데이터는 상기 보안 문서 컨테이너에 남겨 두는 한편, 특정 세션과 관련되어 저장되었던 데이터를 삭제하는 것을 포함하는 것인, 컴퓨팅 디바이스.

청구항 15

명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체로서,

상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하고;

상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하며;

상기 획득된 기업 데이터를 보안 문서 컨테이너에 저장하도록 하고,

상기 관리 브라우저는, 상기 관리 브라우저가 더 이상 적어도 하나의 디바이스 관리자에 의해 관리되지 않으며 상기 관리 브라우저상에서 정책들이 시행되지 않는 비관리 모드(unmanaged mode)를 제공하도록 또한 구성된 것인, 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 16

제 15항에 있어서,

상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성된 것이고,

상기 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하는 것은, 상기 하나 이상의 정책들의 준수에 기초하여 상기 적어도 하나의 기업 자원으로부터 획득된 데이터에 대한 액세스를 제공하는 것을 포함하는 것인, 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 17

제 15항에 있어서, 상기 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체는 추가적인 명령들을 저장하며, 상기 추가적인 명령들은, 실행될 때, 상기 컴퓨팅 디바이스로 하여금 또한,

상기 관리 브라우저가 적어도 하나의 관리 모드로 작동할 때에만 상기 관리 브라우저를 통해 상기 보안 문서 컨테이너에 대한 액세스를 제공하도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 18

제 15항에 있어서, 상기 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체는 추가적인 명령들을 저장하며, 상기 추가적인 명령들은, 실행될 때, 상기 컴퓨팅 디바이스로 하여금 또한,

상기 보안 문서 컨테이너로부터 데이터를 선택적으로 삭제하도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 19

제 18항에 있어서,

상기 관리 브라우저가 관리 모드로 작동할 때 상기 관리 브라우저에 적용되는 적어도 하나의 정책에 기초하여 상기 보안 문서 컨테이너로부터 데이터가 선택적으로 삭제되는 것인, 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 20

제 18항에 있어서,

상기 데이터는 상기 관리 브라우저가 닫혀 있을 때 상기 보안 문서 컨테이너로부터 선택적으로 삭제되는 것인, 하나 이상의 비-일시적 컴퓨터-판독가능 저장 매체.

청구항 21

제 1항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은, 상기 관리 브라우저로 하여금, 상기 컴퓨팅 디바이스와 연관된 디바이스 상태 정보에 기초하여 상기 적어도 하나의 관리 모드로부터 상기 비관리 모드로 전환하게끔 하도록 구성된 하나 이상의 규칙들을 포함하는 것인, 방법.

청구항 22

제 21항에 있어서, 상기 관리 브라우저는 업데이트된 디바이스 상태 정보에 기초하여 상기 비관리 모드로부터 다시 상기 적어도 하나의 관리 모드로 전환하도록 또한 구성된 것인, 방법.

청구항 23

제 21항에 있어서, 상기 컴퓨팅 디바이스와 연관된 상기 디바이스 상태 정보는, 상기 컴퓨팅 디바이스 상의 하나 이상의 애플리케이션들을 식별하는 정보; 상기 컴퓨팅 디바이스의 위치를 식별하는 정보; 및 상기 컴퓨팅 디바이스가 연결된 적어도 하나의 네트워크를 식별하는 정보 중 적어도 하나를 포함하는 것인, 방법.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 "PROVIDING A MANAGED BROWSER"라는 명칭으로 2013년 9월 30일에 출원된 미국 특허출원 일련번호 제14/040,831호의 우선권을 주장하며, 이 출원은 그 전체가 인용에 의해 본원에 통합된다. 게다가, 본 출원은 "PROVIDING A SECURE BROWSER"란 명칭으로 2013년 8월 15일에 출원된 미국 가특허출원 일련번호 제61/866,229호의 우선권을 주장하며, 이 가출원은 그 전체가 인용에 의해 본원에 통합된다. 본 출원은 또한 "SYSTEMS AND METHODS FOR ENTERPRISE MOBILITY MANAGEMENT"라는 명칭으로 2013년 3월 29일에 출원된 미국 가특허출원 일련번호 제61/806,577호의 우선권을 주장하며, 이 가출원은 그 전체가 인용에 의해 본원에 통합된다.

배 경 기 술

[0002] [0002] 본 개시내용의 양상들은 컴퓨터 하드웨어 및 소프트웨어에 관한 것이다. 특히, 본 개시내용의 하나 이상의 양상들은 일반적으로 관리 브라우저(managed browser)를 제공하기 위한 컴퓨터 하드웨어 및 소프트웨어에 관한 것이다.

[0003] [0003] 점점더, 기업들 및 다른 단체들은 스마트폰들, 태블릿 컴퓨터들, 및 다른 모바일 컴퓨팅 디바이스들과 같은 모바일 디바이스들을 자신들의 종업원 및 제휴자들에게 제공하고 그리고/또는 그렇지 않은 경우에 이러한 모바일 디바이스들을 자신들의 종업원 및 제휴자들이 사용할 수 있게 한다. 이들 디바이스들이 계속해서 인기가 상승하고 점점 더 많은 수의 기능들을 제공함에 따라, 많은 단체들은 이들 디바이스들이 어떻게 사용될 수 있는지, 이들 디바이스들이 어떤 자원들에 액세스할 수 있는지, 그리고 이들 디바이스들상에서 실행되는 애플리케이션들이 다른 자원들과 어떻게 상호작용할 수 있는지에 대해 확실히 제어하기를 원할 수 있다.

발명의 내용

[0004] [0004] 개시내용의 다양한 양상들은 모바일 디바이스가 어떻게 사용될 수 있는지, 모바일 디바이스들이 어떤 자

원들에 액세스할 수 있는지, 그리고 이들 디바이스들상에서 실행되는 애플리케이션들 및 다른 소프트웨어가 다른 자원들과 어떻게 상호작용할 수 있는지를 제어할 수 있는 더 효율적이고, 더 효과적이며, 더 기능적이며 그리고 더 편리한 방식들 제공한다. 특히, 이하에서 더 상세히 논의되는 하나 이상의 실시예들에서, 관리 브라우저는 이들 및/또는 다른 장점들 중 하나 이상의 장점을 제공하는 다수의 상이한 방식들로 전개되고, 구현되며 그리고/또는 사용될 수 있다.

[0005] [0005] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신할 수 있다. 이후, 컴퓨팅 디바이스는 관리 브라우저로부터 하나 이상의 기업 자원들까지 적어도 하나의 애플리케이션 터널을 생성할 수 있다. 이후, 컴퓨팅 디바이스는 적어도 하나의 애플리케이션 터널을 통해 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 수 있다.

[0006] [0006] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 디바이스 클라우드를 개시하기 위한 연결을 적어도 하나의 다른 컴퓨팅 디바이스에 설정할 수 있다. 이후, 컴퓨팅 디바이스는 디바이스 클라우드에 걸쳐 관리 브라우저의 세션을 확장시킬 수 있다.

[0007] [0007] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 디바이스 상태 정보를 획득할 수 있다. 이후, 컴퓨팅 디바이스는 디바이스 상태 정보에 기초하여, 관리 브라우저의 하나 이상의 동작 모드들을 선택적으로 디스에이블해야 하는지의 여부를 결정할 수 있다. 관리 브라우저의 적어도 하나의 동작 모드를 선택적으로 디스에이블하는 것을 결정하는 것에 응답하여, 컴퓨팅 디바이스는 적어도 하나의 동작 모드가 디스에이블되도록 할 수 있다.

[0008] [0008] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 하나 이상의 정책들을 수신할 수 있다. 이후, 컴퓨팅 디바이스는 관리 브라우저에 하나 이상의 정책들을 적용할 수 있다.

[0009] [0009] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신할 수 있다. 이후, 컴퓨팅 디바이스는 요청에 기초하여 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 수 있다. 이후, 컴퓨팅 디바이스는 보안 문서 컨테이너에, 획득된 기업 데이터를 저장할 수 있다.

[0010] [0010] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 적어도 하나의 사용자 계정과 연관되는 싱글 사인-온(SSO) 크리덴셜을 수신할 수 있다. 이후, 컴퓨팅 디바이스는 SSO 크리덴셜에 기초하여 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 수 있다. 이후, 컴퓨팅 디바이스는 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공할 수 있다.

[0011] [0011] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 관리 브라우저를 통해 애플리케이션 스토어에 액세스하기 위한 요청을 수신할 수 있다. 이후, 컴퓨팅 디바이스는 요청에 기초하여 애플리케이션 스토어로부터 기업 데이터를 획득할 수 있다.

[0012] [0012] 일부 실시예들에서, 컴퓨팅 디바이스는 관리 브라우저를 로드할 수 있다. 후속하여, 컴퓨팅 디바이스는 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신할 수 있다. 이후, 컴퓨팅 디바이스는 요청에 기초하여 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 수 있다. 이후, 컴퓨팅 디바이스는 하나 이상의 정책들에 기초하여, 획득된 기업 데이터를 제어할 수 있다.

[0013] [0013] 이들 특징들은 많은 다른 특징들과 함께 이하에서 더 상세히 논의된다.

도면의 간단한 설명

[0014] [0014] 본 개시내용은 예로서 예시되며 유사한 참조부호들이 유사한 엘리먼트들을 표시하는 첨부 도면들로 제한되지 않는다.

[0015] [0015] 도 1은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 사용될 수 있는 예시적인 컴퓨터 시스템 아키텍처를 도시한다.

[0016] [0016] 도 2는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 사용될 수 있는 예시적인 원격-액세스 시스템 아키텍처를 도시한다.

[0017] [0017] 도 3은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 사용될 수 있는 예시적인 기업 모빌리티

관리 시스템을 도시한다.

[0018] 도 4는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 사용될 수 있는 또 다른 예시적인 기업 모빌리티 관리 시스템을 도시한다.

[0019] 도 5는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라, 관리 브라우저로부터 하나 이상의 기업 자원들까지 애플리케이션 터널을 생성하는 방법을 예시하는 흐름도를 도시한다.

[0020] 도 6은 본원에 개시된 하나 이상의 예시적인 양상들에 따라 디바이스 클라우드에 걸쳐 관리 브라우저 세션을 연장하는 방법을 예시하는 흐름도를 도시한다.

[0021] 도 7은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저 동작 모드를 선택적으로 디스에이블하는 방법을 예시하는 흐름도를 도시한다.

[0022] 도 8은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저에 하나 이상의 모바일 디바이스 관리 정책들을 적용하는 방법을 예시하는 흐름도를 도시한다.

[0023] 도 9는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 통해 보안 문서 컨테이너에 액세스를 제공하는 방법을 예시하는 흐름도를 도시한다.

[0024] 도 10은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 싱글 사인-온 크리덴셜에 기초하여 기업 데이터를 획득하고 관리 브라우저를 통해 데이터에 대한 액세스를 제공하는 방법을 예시하는 흐름도를 도시한다.

[0025] 도 11은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 통해 애플리케이션 스토어에 액세스를 제공하는 방법을 예시하는 흐름도를 도시한다.

[0026] 도 12는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 기업 데이터를 획득하여 관리 브라우저를 사용하여 제어하는 방법을 예시하는 흐름도를 도시한다.

[0027] 도 13은 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저에 대한 하나 이상의 정책들을 관리하는 방법을 예시하는 흐름도를 도시한다.

[0028] 도 14는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 통해 애플리케이션 스토어에 액세스를 제공하는 다른 방법을 예시하는 흐름도를 도시한다.

[0029] 도 15는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 관리 브라우저내에 관리 실행 환경을 제공하는 방법을 예시하는 흐름도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0015] [0030] 다양한 실시예들의 이하의 설명에서는 실시예의 일부분을 형성하며, 개시내용의 다양한 양상들이 실시될 수 있는 예시적인 다양한 실시예들로 도시되는 앞서 식별된 첨부 도면들을 참조한다. 본원에서 논의된 범위로부터 벗어나지 않고, 다른 실시예들이 활용될 수 있고 구성 및 기능이 수정될 수 있다. 다양한 양상들은 다른 실시예들을 가능하게 하며 다양한 상이한 방식들로 실시되거나 또는 수행될 수 있다. 게다가, 본원에서 사용되는 어법 및 전문 용어는 설명 목적이며 제한하는 것으로 의도되지 않는다. 오히려, 본원에서 사용되는 문구들 및 용어들은 그들의 가장 넓은 해석 및 의미가 부여되어야 한다. "포함하는" 및 "구성하는" 및 이의 변형들의 사용은 이후에 리스트되는 항목들 및 이의 균등물들 뿐만아니라 추가 항목들 및 이의 균등물들을 포함하는 것으로 의미된다.

[0016] [0031] 앞서 언급한 바와같이, 관리 브라우저를 제공하는 것과 관련한 특정 실시예들이 본원에서 논의된다. 그러나, 이들 개념들을 더 상세히 논의하기 전에, 개시내용의 다양한 양상들을 구현하는데 그리고/또는 그렇지 않은 경우에 개시내용의 다양한 양상들을 제공하는데 사용될 수 있는 컴퓨팅 아키텍처 및 기업 모빌리티 관리 아키텍처의 여러 예들이 도 1-4를 참조로 하여 먼저 논의될 것이다.

[0017] [0032] 컴퓨팅 아키텍처

[0018] [0033] 컴퓨터 소프트웨어, 하드웨어 및 네트워크들은 특히 스탠드 얼론(standalone), 네트워크화, 원격-액세스(원격 데이크탑으로도 알려짐), 가상화 및/또는 클라우드-기반 환경들을 비롯하여 다양한 상이한 시스템 환경들에서 활용될 수 있다. 도 1은 스탠드 얼론 및/또는 네트워크화 환경에서, 본원에서 설명된 하나 이상의 예시적

인 양상들을 구현하기 위하여 사용될 수 있는 시스템 아키텍처 및/또는 데이터 프로세싱 디바이스의 일례를 예시한다. 다양한 네트워크 노드들(103, 105, 107 및 109)은 광역 통신망(WAN)(101), 예를들어 인터넷을 통해 상호 연결될 수 있다. 사설 인트라넷들, 기업 네트워크들, 근거리 통신망(LAN)들, 도시권 통신망(MAN)들, 무선 네트워크들, 개인 네트워크(PAN) 등을 포함하는 다른 네트워크들이 또한 또는 대안적으로 사용될 수 있다. 네트워크(101)는 예시적 목적이며, 더 적은 수의 컴퓨터 네트워크들로 또는 추가 네트워크들로 대체될 수 있다. LAN은 임의의 공지된 LAN 토폴로지 중 하나 이상을 가질 수 있으며, 이더넷과 같은 다양한 상이한 프로토콜들 중 하나 이상을 사용할 수 있다. 디바이스들(103, 105, 107, 109) 및 다른 디바이스들(도시안됨)은 트위스트 페어 와이어들, 동축 케이블, 광섬유들, 라디오 파들 또는 다른 통신 매체를 통해 네트워크들 중 하나 이상의 네트워크에 연결될 수 있다.

[0019] [0034] 본원에서 사용되고 도면들에 도시된 바와같은 용어 "네트워크"는 원격 저장 디바이스들이 하나 이상의 통신 경로들을 통해 함께 커플링되는 시스템들 뿐만아니라 가끔씩 저장 능력을 가지는 이러한 시스템들에 커플링될 수 있는 스탠드-얼론 디바이스들을 지칭한다. 결과적으로, 용어 "네트워크"는 "물리적 네트워크" 뿐만아니라 "콘텐츠 네트워크"를 포함하며, "콘텐츠 네트워크"는 모든 물리적 네트워크들에 걸쳐 상주하는 데이터로 구성되며, 단일 엔티티로 여겨질 수 있다.

[0020] [0035] 컴포넌트들은 데이터 서버(103), 웹 서버(105) 및 클라이언트 컴퓨터들(107, 109)을 포함할 수 있다. 데이터 서버(103)는 본원에서 설명된 하나 이상의 예시적인 양상들을 수행하기 위한 제어 소프트웨어 및 데이터베이스들의 전체 액세스, 제어 및 관리를 제공한다. 데이터 서버(103)는 웹 서버(105)에 연결될 수 있으며, 웹 서버(105)를 통해 사용자들은 요청된 데이터와 상호작용하여 이 데이터를 획득한다. 대안적으로, 데이터 서버(103)는 그 자체적으로 웹 서버로서 작용할 수 있고 인터넷에 직접 연결될 수 있다. 데이터 서버(103)는 네트워크(101)(예를들어, 인터넷)를 통해, 직접 또는 간접 연결을 통해 또는 일부 다른 네트워크를 통해 웹 서버(105)에 연결될 수 있다. 사용자들은 웹 서버(105)에 의해 호스팅되는 하나 이상의 외부적으로 노출된 웹 사이트들을 통해 데이터 서버(103)에 연결하기 하여 원격 컴퓨터들(107, 109)을 사용하여, 예를들어 웹 브라우저들을 사용하여 데이터 서버(103)와 상호작용할 수 있다. 클라이언트 컴퓨터들(107, 109)은 데이터 서버(103)에 저장된 데이터에 액세스하기 위하여 데이터 서버(103)와 협력하여 사용될 수 있거나 또는 다른 목적들을 위해 사용될 수 있다. 예를들어, 클라이언트 디바이스(107)로부터, 사용자는 기술분야에서 공지된 인터넷 브라우저를 사용하여 또는 컴퓨터 네트워크(예를들어, 인터넷)를 통해 웹 서버(105) 및/또는 데이터 서버(103)와 통신하는 소프트웨어 애플리케이션을 실행함으로써 웹 서버(105)에 액세스할 수 있다.

[0021] [0036] 서버들 및 애플리케이션들은 동일한 물리적 머신들상에 결합될 수 있고, 개별적인 가상 또는 논리 어드레스들을 보유할 수 있거나 또는 개별 물리 머신들상에 상주할 수 있다. 도 1은 사용될 수 있는 네트워크 아키텍처의 단지 하나의 예를 예시하며, 당업자는, 본원에서 추가로 설명되는 바와같이, 사용된 특정 네트워크 아키텍처 및 데이터 프로세싱 디바이스들이 변화될 수 있으며, 이들이 제공하는 기능이 부차적이라는 것을 인식할 것이다. 예를들어, 웹 서버(105) 및 데이터 서버(103)에 의해 제공되는 서비스들은 단일 서버상에서 결합될 수 있다.

[0022] [0037] 각각의 컴포넌트(103, 105, 107, 109)는 임의의 타입의 공지된 컴퓨터, 서버 또는 데이터 프로세싱 디바이스일 수 있다. 데이터 서버(103)는 예를들어 레이트 서버(rate server)(103)의 전체 동작을 제어하는 프로세서(111)를 포함할 수 있다. 데이터 서버(103)는 RAM(113), ROM(115), 네트워크 인터페이스(117), 입력/출력 인터페이스들(119)(예를들어, 키보드, 마우스, 디스플레이, 프린터 등) 및 메모리(121)를 더 포함한다. I/O(119)는 데이터 또는 파일들을 판독하고, 기록하며, 디스플레이하며 그리고/또는 프린트하기 위한 다양한 인터페이스 유닛들 및 드라이브들을 포함할 수 있다. 메모리(121)는 데이터 프로세싱 디바이스(103)의 전체 동작을 제어하기 위한 운영체제 소프트웨어(123), 본원에서 설명된 양상들을 수행하도록 데이터 서버(103)에 명령하기 위한 제어 로직(125), 및 본원에서 설명된 양상들과 함께 사용될 수 있거나 또는 본원에서 설명된 양상들과 함께 사용되지 않을 수 있는 2차 기능, 지원 기능 및/또는 다른 기능을 제공하는 다른 애플리케이션 소프트웨어(127)를 추가로 저장할 수 있다. 제어 로직은 또한 데이터 서버 소프트웨어(125)로서 본원에서 지칭될 수 있다. 데이터 서버 소프트웨어의 기능은 제어 로직으로 코딩된 규칙들에 기초하여 자동적으로 만들어지거나 또는 시스템내에 입력을 제공하는 사용자에 의해 수동적으로 만들어지거나 또는 사용자 입력(예를들어, 질의들, 데이터 업데이트들 등)에 기초한 자동 프로세싱의 조합으로 만들어진 동작들 또는 결정들을 지칭할 수 있다.

[0023] [0038] 제 1 데이터베이스(129) 및 제 2 데이터베이스(131)를 포함하는 메모리(121)는 또한 본원에서 설명된 하나 이상의 양상들의 수행시에 사용되는 데이터를 저장할 수 있다. 일부 실시예들에서, 제 1 데이터베이스는 (예를들어, 개별 테이블, 보고 등으로서) 제 2 데이터베이스를 포함할 수 있다. 즉, 시스템 설계에 따라, 정보

는 단일 데이터베이스에 저장될 수 있거나 또는 상이한 논리적, 가상적 또는 물리적 데이터베이스들로 분리될 수 있다. 디바이스들(105, 107, 109)은 디바이스(103)와 관련하여 설명된 것과 유사한 또는 상이한 아키텍처를 가질 수 있다. 당업자는 본원에서 설명된 데이터 프로세싱 디바이스(103)(또는 디바이스들(105, 107, 109))의 기능이 예를들어 다수의 컴퓨터들에 걸쳐 프로세싱 로드를 분배하기 위하여, 즉 지리적 위치, 사용자 액세스 레벨, 서비스 품질(QoS) 등에 기초하여 트랜잭션(transaction)들을 분리하기 위하여, 다수의 데이터 프로세싱 디바이스들에 걸쳐 확산될 수 있다는 것을 인식할 것이다.

[0024] [0039] 하나 이상의 양상들은 본원에서 설명되는 바와같이 컴퓨터-사용가능 또는 판독가능 데이터 및/또는 컴퓨터-실행가능 명령들로, 예를들어 하나 이상의 컴퓨터들 또는 다른 디바이스들에 의해 실행되는 하나 이상의 프로그램 모듈들로 구현될 수 있다. 일반적으로, 프로그램 모듈들은 컴퓨터 또는 다른 디바이스의 프로세서에 의해 실행될 때 특정 태스크(task)들을 수행하거나 또는 특정 추상 데이터 타입들을 구현하는 루틴들, 프로그램들, 객체들, 컴포넌트들, 데이터 구조들 등을 포함한다. 모듈들은 실행을 위해 나중에 컴파일링되는 소스 코드 프로그래밍 언어로 쓰여질 수 있거나 또는 Javascript 또는 ActionScript와 같은 (그러나, 이에 제한되지 않음) 스크립팅 언어(scripting language)로 쓰여질 수 있다. 컴퓨터 실행가능 명령들은 비휘발성 저장 디바이스와 같은 컴퓨터 판독가능 매체상에 저장될 수 있다. 하드 디스크들, CD-ROM들, 광 저장 디바이스들, 자기 저장 디바이스들 및/또는 이들의 임의의 조합을 포함하는 임의의 적절한 컴퓨터 판독가능 저장 매체가 활용될 수 있다. 더욱이, 본원에서 설명된 바와 같은 데이터 또는 이벤트들을 나타내는 다양한 전송(비-저장) 매체는 금속 와이어들, 광섬유들, 및/또는 무선 전송 매체(예를들어, 에어(air) 및/또는 공간)와 같은 신호-전도 매체(signal-conducting media)를 통해 이동하는 전자기 파들의 형태로 소스와 목적지사이에서 이동될 수 있다. 본원에서 설명된 다양한 양상들은 방법, 데이터 프로세싱 시스템 또는 컴퓨터 프로그램 제품으로서 구현될 수 있다. 따라서, 다양한 기능들은 소프트웨어, 펌웨어 및/또는 하드웨어 또는 하드웨어 균등물들, 예를들어 집적 회로들, 필드 프로그램가능 게이트 어레이(FPGA)들 등으로 전체적으로 또는 부분적으로 구현될 수 있다. 특정 데이터 구조들이 본원에서 설명된 하나 이상의 양상들을 더 효과적으로 구현하기 위하여 사용될 수 있으며, 이러한 데이터 구조들은 본원에서 설명된 컴퓨터 실행가능 명령들 및 컴퓨터-사용가능 데이터의 범위내에 있는 것으로 고려된다.

[0025] [0040] 도 2를 추가로 참조하면, 본원에서 설명된 하나 이상의 양상들은 원격-액세스 환경에서 구현될 수 있다. 도 2는 본원에서 설명된 하나 이상의 예시적인 양상들에 따라 사용될 수 있는 예시적인 컴퓨팅 환경(200)의 범용 컴퓨팅 디바이스(201)를 포함하는 예시적인 시스템 아키텍처를 도시한다. 범용 컴퓨팅 디바이스(201)는 클라이언트 액세스 디바이스들에 가상 머신들을 제공하도록 구성된 단일-서버 또는 멀티-서버 데스크탑 가상화 시스템(예를들어, 원격 액세스 또는 클라우드 시스템)에서 서버(206a)로서 사용될 수 있다. 범용 컴퓨팅 디바이스(201)는 랜덤 액세스 메모리(RAM)(205), 판독-전용 메모리(ROM)(207), 입력/출력(I/O) 모듈(209) 및 메모리(215)를 비롯하여 서버 및 이와 연관된 컴포넌트들의 전체 동작을 제어하기 위한 프로세서(203)를 가질 수 있다.

[0026] [0041] I/O 모듈(209)은 마우스, 키패드, 터치 스크린, 스캐너, 광 판독기, 및/또는 스타일러스(또는 다른 입력 디바이스(들)) - 이를 통해 범용 컴퓨팅 디바이스(201)의 사용자는 입력을 제공할 수 있음 -를 포함할 수 있으며, 또한 오디오 출력을 제공하기 위한 스피커 및 문자, 시청각 및/또는 그래픽 출력을 제공하기 위한 비디오 디스플레이 디바이스 중 하나 이상을 포함할 수 있다. 소프트웨어는 본원에서 설명된 바와 같은 다양한 기능들을 수행하기 위하여 범용 컴퓨팅 디바이스(201)를 특수 목적 컴퓨팅 디바이스로 구성하기 위한 명령들을 프로세서(203)에 제공하도록 메모리(215) 및/또는 다른 스토리지내에 저장될 수 있다. 예를들어, 메모리(215)는 컴퓨팅 디바이스(201), 예를들어 운영체제(217), 애플리케이션 프로그램들(219) 및 연관된 데이터베이스(221)에 의해 사용된 소프트웨어를 저장할 수 있다.

[0027] [0042] 컴퓨팅 디바이스(201)는 단말들(240)(또한 클라이언트 디바이스들로 지칭됨)과 같은 하나 이상의 원격 컴퓨터들에의 연결들을 지원하는 네트워크화 환경에서 동작할 수 있다. 단말들(240)은 범용 컴퓨팅 디바이스(103 또는 201)와 관련하여 앞서 설명된 엘리먼트들 모두 또는 많은 엘리먼트들을 포함하는, 퍼스널 컴퓨터들, 모바일 디바이스들, 랩탑 컴퓨터들, 태블릿들 또는 서버들일 수 있다. 도 2에 도시된 네트워크 컴포넌트들은 근거리 통신망(LAN)(225) 및 광역 통신망(WAN)(229)을 포함하나, 또한 다른 네트워크들을 포함할 수 있다. LAN 네트워킹 환경에서 사용될 때, 컴퓨팅 디바이스(201)는 네트워크 인터페이스 또는 어댑터(223)를 통해 LAN(225)에 연결될 수 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨팅 디바이스(201)는 모뎀(227), 또는 컴퓨터 네트워크(230)(예를들어, 인터넷)와 같이 WAN(229)를 통해 통신들을 설정하기 위한 다른 광역 네트워크 인터페이스를 포함할 수 있다. 도시된 네트워크 연결들이 예시적이며 컴퓨터들 사이에 통신 링크를 설정하는 다른 수단

이 사용될 수 있다는 것이 인식될 것이다. 컴퓨팅 디바이스(201) 및/또는 단말들(240)은 또한 배터리, 스피커, 및 안테나들(도시안됨)과 같은 다양한 다른 컴포넌트들을 포함하는 모바일 단말들(예를들어, 모바일 전화들, 스마트폰들, PDA들, 노트북들 등)일 수 있다.

[0028] [0043] 본원에서 설명된 양상들은 또한 다수의 다른 범용 또는 특수 목적 컴퓨팅 시스템 환경들 또는 구성들로 운용가능할 수 있다. 본원에서 설명된 양상들과 함께 사용하기에 적합할 수 있는 다른 컴퓨팅 시스템들, 환경들 및/또는 구성들의 예들은 퍼스널 컴퓨터들, 서버 컴퓨터들, 핸드-헬드 또는 랩탑 디바이스들, 멀티프로세서 시스템들, 마이크로프로세서-기반 시스템들, 셋톱 박스들, 프로그램가능 가전제품들, 네트워크 PC들, 미니컴퓨터들, 메인프레임 컴퓨터들, 앞의 시스템들 또는 디바이스들 중 임의의 것을 포함하는 분산형 컴퓨팅 환경들 등을 포함하나 이들에 제한되지 않는다.

[0029] [0044] 도 2에 도시된 바와같이, 하나 이상의 클라이언트 디바이스들(240)은 하나 이상의 서버들(206a-206n)(일반적으로 본원에서 "서버(들)(206)"로 지칭됨)과 통신할 수 있다. 일 실시예에서, 컴퓨팅 환경(200)은 서버(들)(206)와 클라이언트 머신(들)(240) 사이에 설치된 네트워크 기기를 포함할 수 있다. 네트워크 기기는 클라이언트/서버 연결들을 관리할 수 있으며, 일부 경우들에서 복수의 백엔드 서버들(206) 사이의 클라이언트 연결들을 로드 밸런싱할 수 있다.

[0030] [0045] 클라이언트 머신(들)(240)은 일부 실시예들에서 단일 클라이언트 머신(240) 또는 클라이언트 머신들(240)의 단일 그룹으로 지칭될 수 있는 반면에, 서버(들)(206)는 단일 서버(206) 또는 서버들(206)의 단일 그룹으로 지칭될 수 있다. 일 실시예에서, 단일 클라이언트 머신(240)은 2개 이상의 서버(206)와 통신하는 반면에, 다른 실시예에서 단일 서버(206)는 2개 이상의 클라이언트 머신(240)과 통신한다. 또 다른 실시예에서, 단일 클라이언트 머신(240)은 단일 서버(206)와 통신한다.

[0031] [0046] 일부 실시예들에서, 클라이언트 머신(240)은 이하의 비-제한적인 항목들, 즉 클라이언트 머신(들); 클라이언트(들); 클라이언트 컴퓨터(들); 클라이언트 디바이스(들); 클라이언트 컴퓨팅 디바이스(들); 로컬 머신; 원격 머신; 클라이언트 노드(들); 엔드포인트(들) 또는 엔드포인트 노드(들) 중 어느 하나에 의해 참조될 수 있다. 일부 실시예들에서, 서버(206)는 이하의 비-제한적인 항목들, 즉 서버(들); 로컬 머신; 원격 머신; 서버 팜(들) 또는 호스트 컴퓨팅 디바이스(들) 중 어느 하나에 의해 참조될 수 있다.

[0032] [0047] 일 실시예에서, 클라이언트 머신(240)은 가상 머신일 수 있다. 가상 머신은 임의의 가상 머신일 수 있는 반면에, 일부 실시예들에서, 가상 머신은 타입 1 또는 타입 2 하이퍼바이저(hypervisor), 예를들어 Citrix Systems, IBM, VMware에 의해 개발된 하이퍼바이저 또는 임의의 다른 하이퍼바이저에 의해 관리되는 임의의 가상 머신일 수 있다. 일부 양상들에서, 가상 머신은 하이퍼바이저에 의해 관리될 수 있는 반면에, 양상들에서 가상 머신은 서버(206)상에서 실행되는 하이퍼바이저 또는 클라이언트(240)상에서 실행되는 하이퍼바이저에 의해 관리될 수 있다.

[0033] [0048] 일부 실시예들은 서버(206)상에서 원격적으로 실행되는 애플리케이션 또는 다른 원격적으로 위치한 머신에 의해 생성되는 애플리케이션 출력을 디스플레이하는 클라이언트 디바이스(240)를 포함한다. 이들 시스템들에서, 클라이언트 디바이스(240)는 애플리케이션 윈도우, 브라우저 또는 다른 출력 윈도우에서 출력을 디스플레이하기 위하여 가상 머신 클라이언트 에이전트 프로그램 또는 애플리케이션을 실행할 수 있다. 일례에서 애플리케이션은 데스크탑인 반면에, 다른 예에서 애플리케이션은 데스크탑을 생성하거나 또는 제시하는 애플리케이션이다. 데스크탑은 로컬 및/또는 원격 애플리케이션들이 통합될 수 있는 운영체제의 인스턴스(instance)에 대한 사용자 인터페이스를 제공하는 그래픽 쉘(graphical shell)을 포함할 수 있다. 본원에서 설명된 바와같은 애플리케이션들은 운영체제(그리고, 또한 선택적으로 데스크탑)의 인스턴스가 로드된 후 실행되는 프로그램들이다.

[0034] [0049] 일부 실시예들에서, 서버(206)는 서버(206)상에서 실행되는 애플리케이션에 의해 생성되는 디스플레이 출력을 제시하기 위하여 클라이언트상에서 실행되는 씬-클라이언트(thin-client) 또는 원격-디스플레이 애플리케이션에 데이터를 송신하기 위하여 원격 프리젠테이션 프로토콜 또는 다른 프로그램을 사용한다. 씬-클라이언트 또는 원격-디스플레이 프로토콜은 프로토콜들의 이하의 비-제한적인 리스트, 즉 Ft. Lauderdale, Florida에 있는 Citrix Systems, Inc.에 의해 개발된 ICA(Independent Computing Architecture) 프로토콜 또는 Redmond, Washington에 있는 Microsoft Corporation에 의해 제조된 RDP(Remote Desktop Protocol) 중 어느 하나일 수 있다.

[0035] [0050] 원격 컴퓨팅 환경은 예를들어 클라우드 컴퓨팅 환경에서 서버들(206a-206n)이 서버 팜(206)으로 논리적

으로 함께 그룹핑되도록 2개 이상의 서버(206a-206n)를 포함할 수 있다. 서버 팜(206)은 지리적으로 분산된 반면에 함께 논리적으로 그룹핑되는 서버들(206) 또는 서로 근접하게 배치되는 반면에 함께 논리적으로 그룹핑되는 서버들(206)을 포함할 수 있다. 일부 실시예들에서, 서버 팜(206) 내의 지리적으로 분산된 서버들(206a-206n)은 WAN(광역), MAN(대도시) 또는 LAN(지역)을 사용하여 통신할 수 있으며, 여기서 상이한 지리적 지역들은 상이한 대륙들; 상이한 대륙 영역들; 상이한 국가들; 상이한 주들; 상이한 도시들; 상이한 캠퍼스들; 상이한 방들; 또는 전술한 지리적 위치들의 임의의 조합으로 특징지워질 수 있다. 일부 실시예들에서 서버 팜(206)은 단일 엔티티로서 관리될 수 있는 반면에, 다른 실시예들에서 서버 팜(206)은 다수의 서버 팜들을 포함할 수 있다.

[0036] [0051] 일부 실시예들에서, 서버 팜은 실질적으로 유사한 타입의 운영체제 플랫폼(예를들어, WINDOWS, UNIX, LINUX, iOS, ANDROID, SYMBIAN 등)을 실행하는 서버들(206)을 포함할 수 있다. 다른 실시예들에서, 서버 팜(206)은 제 1 타입의 운영체제 플랫폼을 실행하는 하나 이상의 서버들의 제 1 그룹 및 제 2 타입의 운영체제 플랫폼을 실행하는 하나 이상의 서버들의 제 2 그룹을 포함할 수 있다.

[0037] [0052] 서버(206)는 필요에 따라 임의의 타입의 서버로서, 예를들어 파일 서버, 애플리케이션 서버, 웹 서버, 프록시 서버, 어플라이언스, 네트워크 어플라이언스, 게이트웨이, 애플리케이션 게이트웨이, 게이트웨이 서버, 가상화 서버, 전개 서버, SSL VPN 서버, 방화벽, 웹 서버, 애플리케이션 서버로서 또는 마스터 애플리케이션 서버, 액티브 디렉토리를 실행하는 서버, 또는 방화벽 기능, 애플리케이션 기능 또는 로드 밸런싱 기능을 제공하는 애플리케이션 가속 프로그램을 실행하는 서버로서 구성될 수 있다. 다른 서버 타입들이 또한 사용될 수 있다.

[0038] [0053] 일부 실시예들은 클라이언트 머신(240)으로부터의 요청들을 수신하며, 제 2 서버(206b)에 요청을 포워드하며 그리고 제 2 서버(206b)로부터의 응답으로 클라이언트 머신(240)에 의해 생성되는 요청에 응답하는 제 1 서버(206a)를 포함한다. 제 1 서버(206a)는 클라이언트 머신(240)이 이용할 수 있는 애플리케이션들의 목록 뿐만아니라 애플리케이션들의 목록내에서 식별되는 애플리케이션을 호스팅하는 애플리케이션 서버(206)와 연관된 어드레스 정보를 획득할 수 있다. 이후, 제 1 서버(206a)는 웹 인터페이스를 사용하여 클라이언트의 요청에 대한 응답을 제시할 수 있으며, 식별된 애플리케이션에 대한 액세스를 클라이언트(240)에 제공하기 위하여 클라이언트(240)와 직접 통신할 수 있다. 하나 이상의 클라이언트들(240) 및/또는 하나 이상의 서버들(206)은 네트워크(230), 예를들어 네트워크(101)를 통해 데이터를 전송할 수 있다.

[0039] [0054] 도 2는 예시적인 데스크탑 가상화 시스템의 고레벨 아키텍처를 도시한다. 도시된 바와같이, 데스크탑 가상화 시스템은 하나 이상의 클라이언트 액세스 디바이스들(240)에 가상 데스크탑들 및/또는 가상 애플리케이션들을 제공하도록 구성된 적어도 하나의 가상화 서버(206)를 포함하는 단일-서버 또는 멀티-서버 시스템 또는 클라우드 시스템일 수 있다. 본원에서 사용되는 바와같이, 데스크탑은 하나 이상의 애플리케이션들이 호스팅되고 그리고/또는 실행되는 그래픽 환경 또는 공간을 지칭한다. 데스크탑은 로컬 및/또는 원격 애플리케이션들이 통합될 수 있는 운영체제의 인스턴스에 대한 사용자 인터페이스를 제공하는 그래픽 쉘을 포함할 수 있다. 애플리케이션들은 운영체제(그리고 선택적으로 또한 데스크탑)의 인스턴스가 로드된 이후에 실행되는 프로그램들을 포함할 수 있다. 운영체제의 각각의 인스턴스는 물리적(예를들어, 디바이스당 하나의 운영체제) 또는 가상적(예를들어, 단일 디바이스상에서 실행되는 OS의 많은 인스턴스들)일 수 있다. 각각의 애플리케이션은 로컬 디바이스상에서 실행될 수 있거나 또는 원격적으로 위치한 디바이스(예를들어 원격 디바이스)상에서 실행될 수 있다.

[0040] [0055] 기업 모빌리티 관리 아키텍처

[0041] [0056] 도 3은 기업 환경, BYOD 환경 또는 다른 모바일 환경들에서 사용하기 위한 기업 모빌리티 기술 아키텍처(300)를 나타낸다. 아키텍처는 (예를들어, 클라이언트(107, 211) 등으로서) 모바일 디바이스(302)의 사용자가 모바일 디바이스(302)로부터의 기업 또는 개인 자원들에 액세스하고 개인 사용용 모바일 디바이스(302)를 사용하도록 한다. 사용자는 사용자에 의해 구매되는 모바일 디바이스(302) 또는 기업에 의해 사용자에게 제공되는 모바일 디바이스(302)를 사용하여 이러한 기업 자원들(304) 또는 기업 서비스들(308)에 액세스할 수 있다. 사용자는 단지 비지니스용 또는 비지니스 및 개인용으로 모바일 디바이스(302)를 활용할 수 있다. 모바일 디바이스는 iOS 운영체제, 안드로이드 운영체제 등을 실행할 수 있다. 기업은 모바일 디바이스(304)를 관리하기 위한 정책들을 구현하는 것을 선택할 수 있다. 이 정책들은 모바일 디바이스가 식별되거나, 보안 또는 보안 검증되거나 또는 기업 자원들에 대해 선택적으로 또는 전체적으로 액세스할 수 있도록 방화벽 또는 게이트웨이를 통해 주입될 수 있다. 정책들은 모바일 디바이스 관리 정책들, 모바일 애플리케이션 관리 정책들, 모바일 데이터 관리 정책들, 또는 모바일 디바이스, 애플리케이션 및 데이터 관리 정책들의 일부 조합일 수 있다. 모바일 디바

이스 관리 정책들의 애플리케이션을 통해 관리되는 모바일 디바이스(304)는 등록 디바이스로서 지칭될 수 있다.

[0042] [0057] 모바일 디바이스의 운영체제는 관리 파티션(managed partition)(310) 및 비관리 파티션(unmanaged partition)(312)으로 분할될 수 있다. 관리 파티션(310)은 관리 파티션상에서 실행되는 애플리케이션들 및 관리 파티션에 저장된 데이터를 보안하도록 정책들이 그에 적용되게 할 수 있다. 관리 파티션상에서 실행되는 애플리케이션들은 보안 애플리케이션들일 수 있다. 보안 애플리케이션들은 이메일 애플리케이션들, 웹 브라우징 애플리케이션들, SaaS(software-as-a-service) 액세스 애플리케이션들, 윈도우즈 애플리케이션 액세스 애플리케이션들 등일 수 있다. 보안 애플리케이션들은 보안 네이티브 애플리케이션들(314), 보안 애플리케이션 론처(318)에 의해 실행되는 보안 원격 애플리케이션들(322), 보안 애플리케이션 론처(318)에 의해 실행되는 가상화 애플리케이션들(326) 등일 수 있다. 보안 네이티브 애플리케이션들(314)은 보안 애플리케이션 래퍼(wrapper)(320)에 의해 래핑될 수 있다. 보안 애플리케이션 래퍼(320)는 보안 네이티브 애플리케이션이 디바이스상에서 실행될 때 모바일 디바이스(302)상에서 실행되는 통합 정책들을 포함할 수 있다. 보안 애플리케이션 래퍼(320)는 보안 네이티브 애플리케이션(314)의 실행시 요청된 태스크를 완료하기 위하여 보안 네이티브 애플리케이션(314)이 요구할 수 있는, 기업에서 호스팅되는 자원들을 모바일 디바이스(302)상에서 실행되는 보안 네이티브 애플리케이션(314)에게 알려주는 메타-데이터를 포함할 수 있다. 보안 애플리케이션 론치(318)에 의해 실행되는 보안 원격 애플리케이션들(322)은 보안 애플리케이션 론치 애플리케이션(318) 내에서 실행될 수 있다. 보안 애플리케이션 론치(318)에 의해 실행되는 가상화 애플리케이션(326)은 모바일 디바이스(302)상의 자원들, 기업 자원들(304) 등을 활용할 수 있다. 보안 애플리케이션 론치(318)에 의해 실행되는 가상화 애플리케이션들(326)에 의해 모바일 디바이스(302)상에서 사용되는 자원들은 사용자 인터랙션 자원들, 프로세싱 자원들 등을 포함할 수 있다. 사용자 인터랙션 자원들은 키보드 입력, 마우스 입력, 카메라 입력, 촉각 입력, 오디오 입력, 시각 입력, 제스처 입력 등을 수집하여 전송하기 위하여 사용될 수 있다. 프로세싱 자원들은 사용자 인터페이스를 제시하고, 기업 자원들(304)로부터 수신된 데이터를 프로세싱하는 것 등을 수행하기 위하여 사용될 수 있다. 보안 애플리케이션 론치(318)에 의해 실행되는 가상화 애플리케이션들(326)에 의해 기업 자원들(304)에서 사용되는 자원들은 사용자 인터페이스 생성 자원들, 프로세싱 자원들 등을 포함할 수 있다. 사용자 인터페이스 생성 자원들은 사용자 인터페이스를 어셈블리하고, 사용자 인터페이스를 수정하며, 사용자 인터페이스를 리프레시하는 것 등을 수행하기 위하여 사용될 수 있다. 프로세싱 자원들은 정보를 생성하고, 정보를 판독하며, 정보를 업데이트하며, 정보를 삭제하는 것 등을 수행하기 위하여 사용될 수 있다. 예를들어, 가상화 애플리케이션은 GUI와 연관된 사용자 인터랙션들을 기록하고, 이들을 서버 애플리케이션에 통신할 수 있으며, 여기서 서버 애플리케이션은 서버상에서 동작하는 애플리케이션에 대한 입력으로서 사용자 인터랙션 데이터를 사용할 것이다. 이러한 어레인지먼트(arrangement)에서, 기업은 서버측상의 애플리케이션 뿐만아니라 애플리케이션과 연관된 데이터, 파일들 등을 유지하는 것을 선택할 수 있다. 기업이 모바일 디바이스상에서 전개하기 위하여 일부 애플리케이션들을 보안함으로써 본원의 원리들에 따라 그 일부 애플리케이션들을 "동원하는(mobilize)" 것을 선택할 수 있는 반면에, 이러한 어레인지먼트는 또한 특정 애플리케이션들을 위해 선택될 수 있다. 예를들어, 일부 애플리케이션들이 모바일 디바이스상에서 사용하기 위하여 보안될 수 있는 반면에, 다른 애플리케이션들은 모바일 디바이스상에서 전개하기 위하여 준비되거나 또는 전용될 수 없으며, 따라서 기업은 가상화 기술들을 통해 준비되지 않은 애플리케이션들에의 모바일 사용자 액세스를 제공하는 것을 선택할 수 있다. 다른 예로서, 기업은 모바일 디바이스에 대한 애플리케이션을 커스터마이징하는 것이 매우 어렵거나 또는 그렇지 않은 경우에 바람직하지 않을 대량 및 복합 데이터 세트들을 가진 대규모 복합 애플리케이션들(예를들어, 자료 자원 계획 애플리케이션들)을 가질 수 있으며, 따라서, 기업은 가상화 기술들을 통해 애플리케이션에의 액세스를 제공하는 것을 선택할 수 있다. 또 다른 예로서, 기업은 심지어 보안된 모바일 환경에서 조차 기업이 너무 민감하게 생각할 수 있는 고보안 데이터(예를들어, 사람 자원 데이터, 고객 데이터, 엔지니어링 데이터)를 유지하는 애플리케이션을 가질 수 있으며, 따라서 기업은 이러한 애플리케이션들 및 데이터에 대한 모바일 액세스를 허용하기 위하여 가상화 기술들을 사용하는 것을 선택할 수 있다. 기업은 서버측에서 동작하는 것이 더 적절한 것으로 여겨지는 애플리케이션들에 대한 액세스를 허용하기 위하여, 가상화 애플리케이션 뿐만아니라 모바일 디바이스상의 완전하게 보안된 그리고 완전하게 기능적인 애플리케이션들을 제공하는 것을 선택할 수 있다. 일 실시예에서, 가상화 애플리케이션은 보안 저장 위치들 중 하나의 위치에 있는 모바일 폰상에 일부 데이터, 파일들 등을 저장할 수 있다. 기업은 예를들어 다른 정보를 허용하지 않으면서 특정 정보가 폰상에 저장되도록 하는 것을 선택할 수 있다.

[0043] [0058] 본원에 설명된 바와같은 가상화 애플리케이션에 따라, 모바일 디바이스는 GUI들을 제시하고 이후 GUI와의 사용자 인터랙션들을 기록하도록 설계되는 가상화 애플리케이션을 가질 수 있다. 애플리케이션은 애플리케이션과의 사용자 인터랙션들로서 서버측 애플리케이션에 의해 사용될 사용자 인터랙션들을 서버에 통신할 수 있

다. 이에 응답하여, 서버측상의 애플리케이션은 새로운 GUI를 모바일 디바이스에 다시 전송할 수 있다. 예를 들어, 새로운 GUI는 정적 페이지, 동적 페이지, 애니메이션 등일 수 있다.

[0044] [0059] 관리 파티션상에서 실행되는 애플리케이션들은 안정화된 애플리케이션들일 수 있다. 안정화 애플리케이션들은 디바이스 관리자(324)에 의해 관리될 수 있다. 디바이스 관리자(324)는 안정된 애플리케이션들을 모니터링하고 문제점들을 검출하여 제거하기 위한 기술들을 활용할 수 있는데, 만일 문제점들을 검출하여 제거하기 위한 이러한 기술들이 활용되지 않았었더라면 불안정한 애플리케이션이 유발되었을 것이다.

[0045] [0060] 보안 애플리케이션들은 모바일 디바이스의 관리 파티션(310)의 보안 데이터 컨테이너(328)에 저장된 데이터에 액세스할 수 있다. 보안 데이터 컨테이너에서 보안된 데이터는 보안 래핑된 애플리케이션들(314), 보안 애플리케이션 론치(318)에 의해 실행되는 애플리케이션들, 보안 애플리케이션 론치(318)에 의해 실행되는 가상화 애플리케이션들(326) 등에 의해 액세스될 수 있다. 보안 데이터 컨테이너(328)에 저장된 데이터는 파일들, 데이터베이스들 등을 포함할 수 있다. 보안 데이터 컨테이너(328)에 저장된 데이터는 보안 애플리케이션들(332) 사이에서 공유되는 특정 보안 애플리케이션(330)에 제한된 데이터 등을 포함할 수 있다. 보안 애플리케이션에 제한된 데이터는 보안 범용 데이터(334) 및 고보안 데이터(338)를 포함할 수 있다. 보안 범용 데이터는 AES 128-비트 암호화 등과 같은 고강화 암호화를 사용할 수 있는 반면에, 고보안 데이터(338)는 AES 254-비트 암호화와 같은 초고강화 암호화를 사용할 수 있다. 보안 데이터 컨테이너(328)에 저장된 데이터는 디바이스 관리자(324)로부터의 커맨드의 수신시에 디바이스로부터 삭제될 수 있다. 보안 애플리케이션들은 듀얼-모드 옵션(340)을 가질 수 있다. 듀얼 모드 옵션(340)은 비보안 모드에서 보안 애플리케이션을 동작하기 위한 옵션을 사용자에게 제시할 수 있다. 비보안 모드에서, 보안 애플리케이션들은 모바일 디바이스(302)의 비관리 파티션(312)상의 비보안 데이터 컨테이너(342)에 저장된 데이터에 액세스할 수 있다. 비보안 데이터 컨테이너에 저장된 데이터는 개인 데이터(344)일 수 있다. 비보안 데이터 컨테이너(342)에 저장된 데이터는 또한 모바일 디바이스(302)의 비관리 파티션(312)상에서 실행되는 비보안 애플리케이션들(348)에 의해 액세스될 수 있다. 비보안 데이터 컨테이너(342)에 저장된 데이터는 보안 데이터 컨테이너(328)에 저장된 데이터가 모바일 디바이스(302)로부터 삭제될 때 모바일 디바이스(302)상에서 유지될 수 있다. 기업은 사용자에 의해 소유되거나 또는 라이센싱되거나 또는 제어되는 개인 데이터, 파일들 및/또는 애플리케이션들(개인 데이터)를 남기거나 또는 그렇지 않은 경우에 유지하면서 기업에 의해 소유되거나 라이센싱되거나 또는 제어되는 선택된 또는 모든 데이터, 파일들 및/또는 애플리케이션들(기업 데이터)을 모바일 디바이스로부터 삭제하는 것을 원할 수 있다. 이러한 옵션은 선택적 지움(selective wipe)으로서 지칭될 수 있다. 본원에서 설명된 양상들에 따라 기업 및 개인 데이터가 배열되는 경우에, 기업은 선택적 지움을 수행할 수 있다.

[0046] [0061] 모바일 디바이스는 기업의 기업 자원들(304) 및 기업 서비스들(308)에, 공중 인터넷(348) 등에 연결할 수 있다. 모바일 디바이스는 가상 사설 네트워크 연결들을 통해 기업 자원들(304) 및 기업 서비스들(308)에 연결할 수 있다. 가상 사설 네트워크 연결들은 특정 애플리케이션들(350), 특정 디바이스들, 모바일 디바이스상의 특정 보안 영역들 등(예를들어, 352)에 특정적일 수 있다. 예를들어, 폰의 보안 영역에 래핑된 애플리케이션들 각각은 애플리케이션 특정 VPN에의 액세스가 가능한 경우에 사용자 또는 디바이스 속성 정보와 함께 애플리케이션과 연관된 속성들에 기초하여 승인될 수 있도록 애플리케이션 특정 VPN를 통해 기업 자원들에 액세스할 수 있다. 가상 사설 네트워크 연결들은 마이크로소프트 교환 트래픽, 마이크로소프트 액티브 디렉토리 트래픽, HTTP 트래픽, HTTPS 트래픽, 애플리케이션 관리 트래픽 등을 전달할 수 있다. 가상 사설 네트워크 연결들은 싱글-사인-온 인증 프로세스들(354)을 지원하고 인에이블할 수 있다. 싱글-사인-온 프로세스들은 사용자로 하여금 인증 크리덴셜들의 단일 세트를 제공하도록 할 수 있으며, 이후 인증 크리덴셜들은 인증 서비스(358)에 의해 검증된다. 이후, 인증 서비스(358)는 사용자가 각각의 개별 기업 자원(304)에 인증 크리덴셜들을 제공하는 것을 필요로 하지 않고 다수의 기업 자원들(304)에 대한 사용자 액세스를 승인할 수 있다.

[0047] [0062] 가상 사설 네트워크 연결들은 액세스 게이트웨이(360)에 의해 설정 및 관리될 수 있다. 액세스 게이트웨이(360)는 모바일 디바이스(302)에 기업 자원들(304)을 전달하는 것을 관리하고, 가속시키며 그리고 개선하는 성능 강화 특징들을 포함할 수 있다. 액세스 게이트웨이는 또한 모바일 디바이스(302)로부터 공중 인터넷(348)으로 트래픽을 재-라우팅할 수 있으며, 따라서 모바일 디바이스(302)가 공중 인터넷(348)상에서 실행되는 공개적으로 이용가능한 비보안 애플리케이션들에 액세스하도록 할 수 있다. 모바일 디바이스는 트랜스포트 네트워크(362)를 통해 액세스 게이트웨이에 연결할 수 있다. 트랜스포트 네트워크(362)는 유선 네트워크, 무선 네트워크, 클라우드 네트워크, 근거리 통신망, 도시권 통신망, 광역 통신망, 공중 네트워크, 사설 네트워크 등일 수 있다.

[0048] [0063] 기업 자원들(304)은 이메일 서버들, 파일 공유 서버들, SaaS 애플리케이션들, 웹 애플리케이션 서버들,

윈도우즈 애플리케이션 서버들 등을 포함할 수 있다. 이메일 서비스들은 교환 서버들, Lotus Notes 서버들 등을 포함할 수 있다. 파일 공유 서버들은 SHAREFILE 서버들, 다른 파일 공유 서비스들 등을 포함할 수 있다. SaaS 애플리케이션들은 Salesforce 등을 포함할 수 있다. 윈도우즈 애플리케이션 서버들은 로컬 윈도우즈 운영 체제 등 상에서 실행되는 것으로 의도된 애플리케이션들을 제공하도록 구축된 일부 애플리케이션 서버를 포함할 수 있다. 기업 자원들(304)은 전제-기반 자원(premise-based resource)들, 클라우드 기반 자원들 등일 수 있다. 기업 자원들(304)은 직접적으로 또는 액세스 게이트웨이(360)를 통해 모바일 디바이스(302)에 의해 액세스될 수 있다. 기업 자원들(304)은 트랜스포트 네트워크(362)를 통해 모바일 디바이스(302)에 의해 액세스될 수 있다. 트랜스포트 네트워크(362)는 유선 네트워크, 무선 네트워크, 클라우드 네트워크, 근거리 통신망, 도시권 통신망, 광역 네트워크, 공중 네트워크, 사설 네트워크 등일 수 있다.

[0049] [0064] 기업 서비스들(308)은 인증 서비스들(358), 위협 검출 서비스(364), 디바이스 관리 서비스들(324), 파일 공유 서비스들(368), 정책 관리자 서비스들(370), 소셜 통합 서비스들(372), 애플리케이션 제어기 서비스(374) 등을 포함할 수 있다. 인증 서비스들(358)은 사용자 인증 서비스들, 디바이스 인증 서비스들, 애플리케이션 인증 서비스들, 데이터 인증 서비스들 등을 포함할 수 있다. 인증 서비스들(358)은 인증서들을 사용할 수 있다. 인증서들은 기업 자원들(304) 등에 의해 모바일 디바이스(302)상에 저장될 수 있다. 모바일 디바이스(302)상에 저장된 인증서들은 모바일 디바이스상의 암호화된 위치에 저장될 수 있으며, 인증서는 인증 시간 등에 사용하기 위해 모바일 디바이스(302)상에 일시적으로 저장될 수 있다. 위협 검출 서비스들(364)은 침입 검출 서비스들, 비허가 액세스 시도 검출 서비스들 등을 포함할 수 있다. 비허가 액세스 시도 검출 서비스들은 디바이스들, 애플리케이션들, 데이터 등에 액세스하기 위한 비허가 시도들을 포함할 수 있다. 디바이스 관리 서비스들(324)은 구성, 프로비저닝(, 보안, 지원 모니터링, 보고 및 해체 서비스들을 포함할 수 있다. 파일 공유 서비스들(368)은 파일 관리 서비스들, 파일 저장 서비스들, 파일 컬래버레이션 서비스들 등을 포함할 수 있다. 정책 관리 서비스들(370)은 디바이스 정책 관리자 서비스들, 애플리케이션 정책 관리자 서비스들, 데이터 정책 관리자 서비스들 등을 포함할 수 있다. 소셜 통합 서비스들(372)은 접촉 통합 서비스들, 컬래버레이션 서비스들, 페이스북, 트위터 및 LinkedIn 등과 같은 소셜 네트워크와의 통합 등을 포함할 수 있다. 애플리케이션 제어기 서비스들(374)은 관리 서비스들, 프로비저닝 서비스들, 전개 서비스들, 할당 서비스들, 철회 서비스들, 래핑 서비스들 등을 포함할 수 있다.

[0050] [0065] 기업 모빌리티 기술 아키텍처(300)는 애플리케이션 스토어(378)를 포함할 수 있다. 애플리케이션 스토어(378)는 비-래핑된 애플리케이션들(380), 사전-래핑된 애플리케이션들(382) 등을 포함할 수 있다. 애플리케이션들은 애플리케이션 제어기(374)로부터 애플리케이션 스토어(378)에 파퓰레티트될 수 있다. 애플리케이션 스토어(378)는 액세스 게이트웨이(360), 공중 네트워크(348) 등을 통해 모바일 디바이스(302)에 의해 액세스될 수 있다. 애플리케이션 스토어는 사용자 인터페이스를 사용할 때 이해하기 쉽고 용이하도록 제공될 수 있다. 애플리케이션 스토어(378)는 소프트웨어 전개 키트(384)에 대한 액세스를 제공할 수 있다. 소프트웨어 전개 키트(384)는 본 상세한 설명에서 이전에 설명된 바와같이 애플리케이션을 래핑함으로써 사용자에 의해 선택된 애플리케이션들을 보안하는 능력을 사용자에게 제공할 수 있다. 이후, 소프트웨어 전개 키트(384)를 사용하여 래핑된 애플리케이션은 애플리케이션 제어기(374)를 사용하여 애플리케이션 스토어(378)에서 파퓰레이트함으로써 모바일 디바이스(302)가 이용가능하게 만들어질 수 있다.

[0051] [0066] 기업 모빌리티 기술 아키텍처(300)는 관리 및 분석 능력을 포함할 수 있다. 관리 및 분석 능력은 자원들이 어떻게 사용되는지, 자원들이 얼마나 자주 사용되는지 등에 관한 정보를 제공할 수 있다. 자원들은 디바이스들, 애플리케이션들, 데이터 등을 포함할 수 있다. 자원들이 어떻게 사용되는지는 어떤 디바이스들이 어떤 애플리케이션들을 다운로드하는지, 어떤 애플리케이션들이 어떤 데이터에 액세스하는지 등을 포함할 수 있다. 자원들이 얼마나 자주 사용되는지는 애플리케이션들이 얼마나 자주 다운로드되었는지, 데이터의 특정 세트가 애플리케이션에 의해 얼마나 많은 횟수로 액세스되었는지 등을 포함할 수 있다.

[0052] [0067] 도 4는 다른 예시적인 기업 모빌리티 관리 시스템(400)이다. 도 3를 참조로 하여 앞서 설명된 모빌리티 관리 시스템(300)의 컴포넌트들의 일부는 간략화를 위하여 생략되었다. 도 4에 도시된 시스템(400)의 아키텍처는 도 3를 참조로 하여 앞서 설명된 시스템(300)의 아키텍처와 많은 점에서 유사하며, 앞서 언급되지 않는 추가 특징들을 포함할 수 있다.

[0053] [0068] 이러한 경우에, 좌측 측면은 앞의 우측 측면에 도시된, Exchange, Sharepoint, PKI 자원들, Kerberos 자원들 및 Certificate Issuance Service와 같은 다양한 기업 자원들(408) 및 서비스들(409)에 액세스하기 위하여 게이트웨이 서버(406)(액세스 게이트웨이 및 애플리케이션 제어기 기능을 가짐)와 상호작용하는 클라이언트 에이전트(404)를 가진 등록 모바일 디바이스(402)(예를들어, 클라이언트(107, 212, 302 등))을 나타낸다.

비록 특별하게 도시되지 않을지라도, 모바일 디바이스(402)는 또한 애플리케이션들의 선택 및 다운로딩을 위해 기업 애플리케이션 스토어(예를들어, StoreFront)와 상호작용할 수 있다. 클라이언트 에이전트(404)는 예를들어 원적 자원들 및/또는 가상화된 자원들과의 통신들을 용이하게 하는, 클라이언트 디바이스상에서 실행되는 소프트웨어 애플리케이션일 수 있다. 게이트웨이 서버(406)는 예를들어 기업 자원들 및/또는 클라우드 자원들에 대한 액세스를 제공하는 서버 또는 다른 자원일 수 있다.

[0054] [0069] 클라이언트 에이전트(404)는 HDX/ICA 디스플레이 원격 프로토콜 또는 임의의 다른 원격 프로토콜을 사용하여 액세스되는, 기업 데이터 센터에서 호스팅되는 윈도우즈 애플리케이션들/데스크탑들에 대한 UI(사용자 인터페이스) 중간상으로서 작용한다. 클라이언트 에이전트(404)는 또한 네이티브 iOS 또는 안드로이드 애플리케이션들과 같은, 모바일 디바이스(402)상의 네이티브 애플리케이션들의 설치 및 관리를 지원한다. 예를들어, 앞의 도면에 도시된 관리 애플리케이션들(410)(메일, 브라우저, 래핑된 애플리케이션)은 디바이스상에서 국부적으로 실행되는 모든 네이티브 애플리케이션들이다. Fort Lauderdale, Florida에 위치한 Citrix Systems Inc.에 의한 MDX(모바일 경험 기술)와 같은 클라이언트 에이전트(404) 및 애플리케이션 관리 프레임워크(다른 애플리케이션 관리 프레임네트워크들이 또한 사용될 수 있음)는 기업 자원들/서비스들(408)에 연결성 및 SSO(싱글 사인온)와 같은 정책 드라이브 관리 능력들 및 특징들을 제공하도록 작용한다. 클라이언트 에이전트(404)는 기업에 대한 1차 사용자 인증, 일반적으로 다른 게이트웨이 서버 컴포넌트들에 대한 SSO를 가진 액세스 게이트웨이(AG)에 대한 1차 사용자 인증을 처리한다. 클라이언트 에이전트(404)는 모바일 디바이스(402)상의 관리 애플리케이션들(410)의 동작을 제어하기 위한 정책들을 게이트웨이 서버(406)로부터 획득한다. 본원에서 사용되는 바와같이, 관리 애플리케이션은 독립적으로 정의되고 통신된 정책 파일들에 기초하여 제어되고 이 정책 파일들에 따라 동작될 수 있는 애플리케이션이다.

[0055] [0070] 네이티브 애플리케이션들(410)과 클라이언트 에이전트(404) 사이의 보안 IPC 링크들(412)은 클라이언트 에이젠트가 각각의 애플리케이션을 "래핑"하는 애플리케이션 관리 프레임워크(414)에 의해 시행될 정책들을 적용하도록 하는 관리 채널을 나타낸다. IPC 채널(412)은 또한 기업 자원들(408)에 대한 연결 및 SSO를 인에이블하는 크리덴셜 및 인증 정보를 클라이언트 에이전트(404)가 공급하도록 한다. 마지막으로, IPC 채널(412)은 애플리케이션 관리 프레임워크(414)가 클라이언트 에이전트(404)에 의해 구현되는 사용자 인터페이스 기능들, 예를들어 온라인 및 오프라인 인증을 인보크하도록 한다.

[0056] [0071] 클라이언트 에이전트(404) 및 게이트웨이 서버(406) 사이의 통신들은 근본적으로 각각의 네이티브 관리 애플리케이션(410)을 래핑하는 애플리케이션 관리 프레임워크(414)로부터 관리 채널을 확장한다. 애플리케이션 관리 프레임워크(414)는 클라이언트 에이전트(404)로부터 정책 정보를 요청하며, 클라이언트 에이전트(404)는 차례로 게이트웨이 서버(406)로부터 정책 정보를 요청한다. 애플리케이션 관리 프레임워크(414)는 인증을 요청하며, 클라이언트 에이전트(404)는 게이트웨이 서버(406)(또한, NetScaler Access Gateway로 알려짐)의 게이트웨이 서비스 부분내로 로그한다. 이하에서 더 완전하게 설명되는 바와같이, 클라이언트 에이전트(404)는 또한 로컬 데이터 볼트(vault)들(416)에 대한 암호화 키들을 유도하기 위한 입력 자료를 생성하거나 또는 PKI 보호 자원들에 직접 인증을 인에이블할 수 있는 클라이언트 인증서들을 제공할 수 있는 게이트웨이 서버(406)에게 서비스들을 지원할 것을 호출할 수 있다.

[0057] [0072] 더 상세히, 애플리케이션 관리 프레임워크(414)는 각각의 관리 애플리케이션(410)을 래핑한다. 이는 명시적 구축 단계를 통해 또는 구축후 프로세싱 단계를 통해 통합될 수 있다. 애플리케이션 관리 프레임워크(414)는 애플리케이션(410)의 제 1 론치시 클라이언트 에이전트(614)와 "페어링"하여, 보안 IPC 채널을 초기화하고 그 애플리케이션에 대한 정책을 획득할 수 있다. 애플리케이션 관리 프레임워크(414)는 국부적으로 적용하는 정책의 관련 부분들, 예를들어 로컬 OS 서비스들이 어떻게 사용될 수 있는지 또는 로컬 OS 서비스들이 애플리케이션(410)과 어떻게 상호작용할 수 있는지를 제한하는 억제 정책들 중 일부 및 클라이언트 에이전트 로그인 종속성들을 시행할 수 있다.

[0058] [0073] 애플리케이션 관리 프레임워크(414)는 인증 및 내부 네트워크 액세스를 용이하게 하기 위하여 보안 IPC 채널(412)을 통해 클라이언트 에이전트(404)에 의해 제공된 서비스들을 사용할 수 있다. 사설 및 공유 데이터 볼트들(416)(컨테이너들)의 키 관리는 또한 관리 애플리케이션들(410)과 클라이언트 에이전트(404) 간의 적절한 인터랙션들에 의해 관리될 수 있다. 볼트들(416)은 온라인 인증 이후에만 이용가능하게 만들어질 수 있거나 또는 정책에 의해 허용되는 경우에 오프라인 인증 이후에 이용가능하게 만들어질 수 있다. 볼트들(416)의 첫번째 사용은 온라인 인증을 요구할 수 있으며, 오프라인 액세스는 온라인 인증이 다시 요구되기 전에 최대 정책 리프레시 기간으로 제한될 수 있다.

[0059] [0074] 내부 자원들에의 네트워크 액세스는 액세스 게이트웨이(406)를 통해 개별 관리 애플리케이션들(410)로부터 직접 발생할 수 있다. 애플리케이션 관리 프레임워크(414)는 각각의 애플리케이션(410)의 절반에서 네트워크 액세스를 조정하는 것을 담당한다. 클라이언트 에이전트(404)는 온라인 인증 이후에 획득된 적절한 시간 제한된 2차 크리덴셜들을 제공함으로써 이들 네트워크 연결들을 용이하게 할 수 있다. 리버스 웹 프록시 연결들 및 엔드-투-엔드 VPN-스타일 터널들(418)과 같은 다수의 네트워크 연결 모드들이 사용될 수 있다.

[0060] [0075] 메일 및 브라우저 관리 애플리케이션들(410)은 특별한 상태를 가지며, 임의적 래핑된 애플리케이션들이 일반적으로 이용가능하지 않을 수 있는 시설들을 사용할 수 있다. 예를들어, 메일 애플리케이션은 전체 AD 로그온을 요구하지 않고 연장된 시간 기간 동안 그 메일 애플리케이션이 Exchange에 액세스하도록 하는 특별한 백그라운드 네트워크 액세스 메커니즘을 사용할 수 있다. 브라우저 애플리케이션은 상이한 종류의 데이터를 분리하기 위하여 다수의 사설 데이터 볼트들을 사용할 수 있다.

[0061] [0076] 이러한 아키텍처는 다양한 다른 보안 특징들의 통합을 지원한다. 예를들어, 일부 경우들에서, 게이트웨이 서버(406)(자신의 게이트웨이 서비스들을 포함함)는 AD 패드워드들을 인증할 필요가 없을 것이다. 일부 상황들에서 AD 패스워드가 일부 사용자들에 대한 인증 인자로서 사용될 수 있는지는 기업의 재량으로 맡겨질 수 있다. 상이한 인증 방법들은 사용자가 온라인인 경우 또는 오프라인인 경우에 (즉, 네트워크에 연결되거나 또는 연결되지 않는 경우에) 사용될 수 있다.

[0062] [0077] 셋업 인증은 게이트웨이 서버(406)가 강한 인증을 요구하는 높게 분류된 데이터에 대해 액세스하도록 허용되는 관리 네이티브 애플리케이션들(410)을 식별할 수 있고 비록 이것이, 재인증이 이전의 약한 로그인 레벨 이후에 사용자에 의해 요구되는 것을 의미할지라도, 적절한 인증을 수행한 이후에만 이들 애플리케이션들에 대한 액세스가 허용되도록 하는 특징이다.

[0063] [0078] 이러한 솔루션의 다른 보안 특징은 모바일 디바이스(402)상의 데이터 볼트들(416)(컨테이너들)의 암호화이다. 볼트들(416)은 파일들, 데이터베이스들, 및 구성들을 포함하는 모든 온-디바이스 데이터가 보호되도록 암호화될 수 있다. 온라인 볼트들의 경우에 키들이 서버(게이트웨이 서버(406))에 저장될 수 있으며, 오프-라인 볼트들의 경우에 키들의 로컬 복사가 사용자 패스워드에 의해 보호될 수 있다. 데이터가 보안 컨테이너(416)에서 디바이스(402)상에 국부적으로 저장될 때, AES 256 암호화 알고리즘이 최소로 활용되는 것이 바람직하다.

[0064] [0079] 다른 보안 컨테이너 특징들이 또한 구현될 수 있다. 예를들어, 애플리케이션(410)내에서 발생하는 모든 보안 이벤트들이 로깅되어 백엔드에 보고되는 로깅 특징이 포함될 수 있다. 데이터 지움이 지원될 수 있으며, 예를들어 애플리케이션(410)이 탬퍼링을 검출하면, 연관된 암호화 키들은 랜덤 데이터로 쓰여질 수 있으며, 따라서 사용자 데이터가 파괴된 파일 시스템상에는 힌트가 남겨지지 않는다. 스크린샷 보호는 임의의 데이터가 스크린샷들에 저장되는 것을 애플리케이션이 방지할 수 있는 다른 특징이다. 예를들어, 키 윈도우의 은폐된 특성은 YES로 세팅될 수 있다. 이는 스크린상에 현재 디스플레이되고 있는 모든 콘텐츠가 은폐되도록 할 수 있으며, 따라서 임의의 콘텐츠가 정상적으로 상주할 블랭크 스크린샷을 초래한다.

[0065] [0080] 로컬 데이터 전달은 예를들어 임의의 데이터가 애플리케이션 컨테이너 외부로 국부적으로 전달되는 것을 방지함으로써, 예를들어 임의의 데이터를 복사하거나 또는 이를 외부 애플리케이션에 송신함으로써 방지될 수 있다. 키보드 캐시 특징은 민감한 텍스트 필드들에 대한 자동보정 기능을 디스에이블하도록 동작할 수 있다. SSL 인증 검증은 동작가능할 수 있으며, 따라서 애플리케이션은 그것이 키체인에 저장되는 대신에 서버 SSL 인증서를 상세하게 검증한다. 암호화 키 생성 특징은 (오프라인 액세스가 요구되는 경우에) 디바이스상의 데이터를 암호화하기 위하여 사용되는 키가 사용자에 의해 공급되는 패스프레이즈를 사용하여 생성되도록 사용될 수 있다. 이는 오프라인 액세스가 요구되지 않는 경우에 서버측에서 랜덤하게 생성되어 저장되는 다른 키들과 XOR 연산될 수 있다. 키 유도 함수들은 사용자 패스워드로부터 생성된 키들이 키의 암호 해시를 생성하는 것보다 오히려 KDF들(키 유도 함수들, 특히 PBKDF2)을 사용하도록 동작할 수 있다. 후자는 강한 힘 또는 디렉토리 공격들에 취약한 키를 만든다.

[0066] [0081] 추가로, 하나 이상의 초기화 벡터들이 암호화 방법들에서 사용될 수 있다. 초기화 벡터는 동일한 암호화된 데이터의 다수의 복사본들이 상이한 암호 텍스트 출력을 초래하도록 할 것이며, 따라서 리플레이 및 암호 해독 공격들이 방지된다. 이는 또한 데이터를 암호화하기 위하여 사용되는 특정 초기화 벡터가 알려지지 않은 경우에 암호화 키가 도난당했을지라도 공격자가 임의의 데이터를 암호해독하는 것을 방지할 것이다. 추가로, 인증 및 이후 암호해독이 사용될 수 있으며, 여기서 사용자가 애플리케이션 내에서 인증된 이후에만 애플리케이션 데이터가 암호해독된다. 다른 특징은 필요할 때만 (디스크가 아니라) 메모리에서 유지될 수 있는, 메모리내

의 민감 데이터와 관련될 수 있다. 예를들어, 로그인 크리덴션들은 로그인 크리덴셜들은 로그인 이후에 메모리로부터 지워질 수 있으며, 목적-C 인스턴스 변수들 내의 다른 데이터가 저장되지 않는데, 왜냐하면 이들 데이터는 용이하게 참조될 수 있기 때문이다. 대신에, 메모리는 이들을 위해 수동으로 할당될 수 있다.

[0067] [0082] 인액티비티 타임아웃(inactivity timeout)이 구현될 수 있으며, 여기서 인액티비티의 정책-정의된 기간 이후에 사용자 세션이 종료된다.

[0068] [0083] 애플리케이션 관리 프레임워크(414)로부터의 데이터 누출은 다른 방식들로 방지될 수 있다. 예를들어, 애플리케이션(410)이 배경으로 될 때, 메모리는 미리 결정된(구성가능) 시간 기간 이후에 클리어될 수 있다. 배경화 될 때, 전경화 프로세스(foregrounding process)를 고정시키기 위하여 애플리케이션의 마지막으로 디스플레이된 스크린에서 스탭샵이 취해질 수 있다. 스크린샵은 비밀 데이터를 포함할 수 있고 따라서 클리어되어야 한다.

[0069] [0084] 다른 보안 특징은 하나 이상의 애플리케이션들에 액세스하기 위해 AD(active directory)(422) 패스워드를 사용하지 않고 OTP(one time password)(420)의 사용과 관련된다. 일부 경우들에서, 일부 사용자들은 그들의 AD 패스워드를 알지못하며(또는 그들의 AD 패스워드를 알도록 허용되지 않으며) 따라서 이들 사용자들은 OTP(420)를 사용하여, 예를들어 SecurID와 같은 하드웨어 OTP 시스템을 사용함으로써 인증할 수 있다(OTP들은 또한 Entrust 또는 Gemalto와 같은 상이한 벤더들에 의해 제공될 수 있다). 일부 경우들에서, 사용자가 사용자 ID로 인증한 이후에, 텍스트가 OTP(420)와 함께 사용자에게 송신된다. 일부 경우들에서, 이는 프롬프트가 단일 필드인 경우에 단지 온라인 사용을 위해서만 구현될 수 있다.

[0070] [0085] 오프라인 패스워드는 기업 정책을 통해 오프라인 사용이 허용되는 이들 애플리케이션들(410)에 대한 오프라인 인증을 위하여 구현될 수 있다. 예를들어, 기업은 기업 애플리케이션 스토어가 이러한 방식으로 액세스되는 것을 원할 수 있다. 이러한 경우에, 클라이언트 에이전트(404)는 사용자가 고객 오프라인 패스워드를 세팅할 것을 요구할 수 있으며, AD 패스워드가 사용되지 않는다. 게이트웨이 서버(406)는 표준 윈도우즈 서버 패스워드 복잡성 요건들이 수정될 수 있을 지라도 이 요건들에 의해 기술되는 것과 같은 최소 길이, 캐릭터 클래스 구성(character class composition) 및 패스워드들의 수명에 대한 패스워드 표준들을 제어하고 시행하기 위한 정책들을 제공할 수 있다.

[0071] [0086] 다른 특징은 (애플리케이션 관리 프레임워크 마이크로 VPN 특징을 통해 PKI 보호 웹 자원들에 액세스하기 위한) 2차 크리덴셜들로서 특정 애플리케이션들(410)에 대한 클라이언트측 인증서를 인에이블하는 것과 관련된다. 예를들어, 기업 이메일 애플리케이션과 같은 애플리케이션은 이러한 인증서를 활용할 수 있다. 이러한 경우에, ActiveSync 프로토콜를 사용한 인증서-기반 인증이 지원될 수 있으며, 여기서 클라이언트 에이전트(404)로부터의 인증서는 게이트웨이 서버(406)에 의해 리트리브되고 키체인으로 사용될 수 있다. 각각의 관리 애플리케이션은 게이트웨이 서버(406)에서 정의되는 라벨에 의해 식별되는 하나의 연관된 클라이언트 인증서를 가질 수 있다.

[0072] [0087] 게이트웨이 서버(406)는 관련된 관리 애플리케이션들이 내부 PKI 보호 자원들을 인증하도록 클라이언트 인증서들을 발행하는 것을 지원하기 위하여 기업 특수 목적 웹 서비스와 상호작용할 수 있다.

[0073] [0088] 클라이언트 에이전트(404) 및 애플리케이션 관리 프레임워크(414)는 내부 PKI 보호 네트워크 자원들을 인증하기 위한 클라이언트 인증서들을 획득하여 사용하는 것을 지원하도록 시행될 수 있다. 예를들어 보안 및/또는 분리 요건들의 다양한 레벨들을 매칭시키기 위하여 2개 이상의 인증서가 지원될 수 있다. 인증서들은 메일 및 브라우저 관리 애플리케이션들에 의해, 궁극적으로 임의적 래핑된 애플리케이션들에 의해 사용될 수 있다(애플리케이션 관리 프레임워크가 HTTPS 요청들을 중재하는 것이 타당한 웹 서비스 스타일 통신 패턴들을 이들 애플리케이션들이 사용하는 경우에).

[0074] [0089] iOS상에서의 애플리케이션 관리 프레임워크 클라이언트 인증서 지원은 각각의 사용 기간 동안 각각의 관리 애플리케이션에서 PKCS 12 BLOB (Binary Large Object)를 iOS 키체인에 들여놓는 것에 의존할 수 있다. 애플리케이션 관리 프레임워크 클라이언트 인증서 지원은 사설 인-메모리 키 스토리지(private in-memory key storage)를 가진 HTTPS 구현을 사용할 수 있다. 클라이언트 인증서는 iOS 키체인에서 결코 제시되지 않을 것이며 그리고 강하게 보호되는 "온라인-전용" 데이터 값을 잠재적으로 제외하고 지속되지 않을 것이다.

[0075] [0090] 상호 SSL은 또한 모바일 디바이스(402)가 기업에게 인증될 것을 요구함으로써 추가 보안을 제공하도록 구현될 수 있으며, 이와 반대의 경우도 마찬가지다. 게이트웨이 서버(406)에 인증하기 위한 가상 스마트 카드들이 또한 구현될 수 있다.

[0076] [0091] 제한된 그리고 전체 Kerberos 지원은 추가 특징들일 수 있다. 전체 지원 특징은 AD 패스워드 또는 트러스티드 클라이언트 인증서를 사용하여 AD(422)에 대해 전체 Kerberos 로그인을 수행하고 HTTP 교섭 인증 난제들에 응답하기 위하여 Kerberos 서비스 티켓들을 획득하는 능력과 관련된다. 제한된 지원 특징은 AFEE에서의 강제 위임(constrained delegation)과 관련되며, 여기서 AFEE는 Kerberos 프로토콜 전환을 인보크하는 것을 지원하며, 따라서 이는 HTTP 교섭 인증 난제들에 응답하여 (강제 위임 대상인) Kerberos 서비스 티켓들을 획득하여 사용할 수 있다. 이러한 메커니즘은 리버스 웹 프록시(CVPN으로도 지칭됨) 모드에서 그리고 HTTP(HTTPS가 아님) 연결들이 VPN 및 마이크로 VPN 모드에서 프록시될 때 작동한다.

[0077] [0092] 다른 특징은 애플리케이션 컨테이너 로킹 및 지움과 관련되며, 이는 자일-브레이크(jail-break) 또는 루팅 검출시 자동적으로 발생하며 관리 콘솔로부터 푸시 커맨드로서 발생할 수 있으며 그리고 애플리케이션(410)이 실행되지 않을 때 조차 원격 지움 기능을 포함할 수 있다.

[0078] [0093] 기업 애플리케이션 스토어 및 애플리케이션 제어기의 멀티-사이트 아키텍처 또는 구성이 지원될 수 있으며, 이는 사용자들로 하여금 실패의 경우에 여러 상이한 위치들 중 하나의 위치로부터 서비스받도록 한다.

[0079] [0094] 일부 경우들에서, 관리 애플리케이션들(410)은 API(예를들어, OpenSSL)를 통해 인증서 및 개인 키에 액세스하도록 허용될 수 있다. 기업의 트러스티드 관리 애플리케이션들(410)은 애플리케이션의 클라이언트 인증서 및 개인 키를 사용하여 특정 공개 키 동작들을 수행하도록 허용될 수 있다. 예를들어, 애플리케이션이 브라우저와 같이 동작하며 인증서 액세스가 요구되지 않을 때, 애플리케이션이 "나는 누구인가"에 대한 인증서를 판독할 때, 애플리케이션이 보안 세션 토큰을 구축하기 위하여 인증서를 사용할 때, 그리고 애플리케이션이 중요한 데이터에 대한 디지털 서명(예를들어, 트랜잭션 로그) 또는 일시적 데이터 암호화를 위해 개인 키들을 사용할 때, 다양한 사용의 경우들이 식별되어 처리될 수 있다.

[0080] [0095] 관리 브라우저 특징들

[0081] [0096] 개시내용의 다양한 양상들을 제공하고 그리고/또는 구현할 때 사용될 수 있는 기업 모빌리티 관리 아키텍처 및 컴퓨팅 아키텍처의 여러 예들이 논의되었을지라도, 다수의 실시예들이 지금 더 상세히 논의될 것이다. 특히, 앞서 도입된 바와같이, 개시내용의 일부 양상들은 일반적으로 관리 브라우저를 제공하는 것과 관련된다. 이하의 설명에서, 관리 브라우저가 하나 이상의 실시예에 따라 어떻게 제공될 수 있는지를 예시하는 다양한 예들이 논의될 것이다.

[0082] [0097] 도 5는 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 관리 브라우저로부터 하나 이상의 기업 자원들까지 애플리케이션 터널을 생성하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 5에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 5에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 메모리와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0083] [0098] 도 5에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(505)에서 시작할 수 있다. 예를들어, 단계(505)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트폰 또는 다른 타입의 모바일 디바이스)는 (예를들어, 관리 브라우저를 열고 그리고/또는 그렇지 않은 경우에 관리 브라우저의 실행을 개시함으로써) 관리 브라우저를 로드할 수 있다. 하나 이상의 실시예들에서, 관리 브라우저는 하나 이상의 기업 보안 특징들(예를들어, 모바일 디바이스 관리 특징들, 모바일 애플리케이션 관리 특징들, 정책 포착 및 시행 특징들 등)을 제공하도록 구성되는 웹 브라우저일 수 있다. 부가적으로 또는 대안적으로, 관리 브라우저는 브라우저내에서 실행되도록 구성될 수 있는 모바일 디바이스 애플리케이션들과 함께 사용하기 위한 다양한 기업 보안 특징들을 확장시킬 수 있다. 예를들어, 기업은 기업 보안 위험들을 감소시키기 위하여 자신들의 종업원들 일부 또는 모두 및/또는 다른 사용자들이 BYOD(bring-your-own-device) 방식으로 그들의 개별 모바일 디바이스들상에 관리 브라우저을 설치하고 사용할 것을 요구할 수 있다. 게다가, 관리 브라우저는 예를들어 가상 사설 네트워크(VPN)에 연결하지 않고 모바일 디바이스 사용자들이 기업 인트라넷 및/또는 다른 기업 자원들에 액세스하도록 하기 위하여 사용될 수 있다. 예를들어, 관리 브라우저는 기업 인트라넷 및/또는 다른 기업 자원들에 대해 이러한 액세스를 인에이블하도록, 이하에서 더 상세히 논의되는 것과 같은 애플리케이션 터널링 기능들을 구현하고 그리고/또는 제공할 수 있다.

[0084] [0099] 하나 이상의 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 부가적으로 또는 대안적으로 구성될 수 있다. 예를들어, 기업 자원(예를들어, 기업 네트워크에 연결되고 그리고/또는 그렇지 않은 경우에 기업 네트워크의 부분인 서버 또는 데이터베이스)로부

터 데이터를 획득하도록 구성되는 것에 추가하여, 관리 브라우저는 (예를들어, 하나 이상의 암호화 프로토콜들을 사용하여 암호화될 수 있는 하나 이상의 로컬 캐시들에) 획득된 데이터를 보안적으로 캐싱하도록 추가로 구성될 수 있다. 부가적으로 또는 대안적으로, 관리 브라우저는 (예를들어, 하나 이상의 인증 크리덴셜들의 검증에 기초하여, 하나 이상의 모바일 디바이스 관리 및/또는 모바일 애플리케이션 관리 정책들에 따라 그리고/또는 이러한 정책들의 시행 등에 기초하여, 획득된 데이터에 대한 액세스를 제어하고 제공함으로써) 획득된 데이터의 보안 브라우징을 제공하도록 추가로 구성될 수 있다.

[0085] [00100] 하나 이상의 실시예들에서, 관리 브라우저는 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드에서 제공하도록 구성될 수 있다. 하나 이상의 정책들은 예를들어 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 예를들어, 하나 이상의 정책들은 관리 브라우저를 사용하여 액세스될 수 있는 정보의 타입들, 관리 브라우저를 사용하여 액세스될 수 있는 자원들(예를들어, 기업 자원들, 네트워크 자원들 등), 관리 브라우저를 사용하여 정보에 액세스될 수 있는 사용자들, 관리 브라우저가 특정 타입들의 정보에 액세스하기 위하여 사용될 수 있는 시간들, 관리 브라우저가 특정 타입들의 정보에 액세스하기 위하여 사용될 수 있는 위치들 및/또는 다른 제한들을 부과할 수 있는 다른 요소들을 선택적으로 제한할 수 있다. 일부 어레인지먼트들에서, 하나 이상의 정책들 중 적어도 하나의 정책은 이하에서 논의되는 바와같이 관리 브라우저의 애플리케이션 터널링 기능들을 제한하고 그리고/또는 그렇지 않은 경우에 제한할 수 있다. 부가적으로 또는 대안적으로, 관리 브라우저는 (예를들어, 관리 모드에서 브라우저에 적용될 수 있는) 하나 이상의 정책들이 관리 브라우저에 적용되지 않을 수 있는 적어도 하나의 비관리 모드를 제공하도록 구성될 수 있으며, 따라서 관리 브라우저는 하나 이상의 정책들에 의해 부과될 수 있는 제한들 없이 동작할 수 있다.

[0086] [00101] 단계(510)에서, 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청이 수신될 수 있다. 예를들어, 단계(510)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신할 수 있다. 이러한 요청은 예를들어 (예를들어, 사용자가 링크를 선택하고 그리고/또는 그렇지 않은 경우에 관리 브라우저를 사용하여 네트워크 자원에 대한 액세스를 요청하는 것에 기초하여) 관리 브라우저를 통해 컴퓨팅 디바이스에 의해 수신되는 사용자 입력에 기초하고 그리고/또는 이러한 사용자 입력에 대응할 수 있다.

[0087] [00102] 단계(515)에서, 적어도 하나의 애플리케이션 터널이 관리 브라우저로부터 하나 이상의 기업 자원들까지 생성될 수 있다. 예를들어, 단계(515)에서, 컴퓨팅 디바이스는 기업 서버들로, 및/또는 예를들어 관리 브라우저가 기업 서버들 및/또는 다른 기업 자원들로부터의 기업 데이터에 보안적으로 액세스하여 획득할 수 있도록 하는 다른 기업 자원들로의 하나 이상의 VPN-스타일 터널들을 생성하고 그리고/또는 그렇지 않은 경우에 설정할 수 있다. 하나 이상의 어레인지먼트들에서, 애플리케이션 터널링은 하나의 네트워크 프로토콜(예를들어, 전달 프로토콜)이 상이한 네트워크 프로토콜을 캡슐화하는 기술들을 포함할 수 있다. 애플리케이션 터널링을 사용함으로써, 보안 경고가 언트러스티드 네트워크(untrusted network)를 통해 제공될 수 있다.

[0088] [00103] 일부 실시예들에서, 적어도 하나의 애플리케이션 터널을 생성하는 것은 관리 브라우저로부터 제 1 기업 자원까지 제 1 애플리케이션 터널을 생성하는 것 및 관리 브라우저로부터 제 2 기업 자원까지 제 2 애플리케이션 터널을 생성하는 것을 포함할 수 있으며, 여기서 제 2 기업 자원은 제 1 기업 자원과 상이하다. 예를들어, (예를들어, 단계(515)에서) 하나 이상의 애플리케이션 터널들을 생성할 때, 컴퓨팅 디바이스는 관리 브라우저에 의해 액세스될 수 있는 각각의 기업 자원에 대하여 상이한 개별 애플리케이션 터널을 생성할 수 있다. 일부의 경우들에서, 제 1 기업 자원은 제 1 보안 레벨을 가질 수 있으며, 제 2 기업 자원은 제 1 보안 레벨과 상이한 제 2 보안 레벨을 가질 수 있다. 예를들어, 제 2 기업 자원은 제 1 기업 자원 보다 높은 보안 레벨을 가질 수 있으며, 추가 인증 크리덴셜들 및/또는 더 보안적인 액세스 프로토콜들 및/또는 암호화 방법들은 (예를들어, 제 1 기업 자원에 액세스하는 것과 비교하여) 제 2 기업 자원에 액세스하는 데 필요할 수 있다.

[0089] [00104] 일부 실시예들에서, 적어도 하나의 애플리케이션 터널은 관리 브라우저에 적용될 수 있는 하나 이상의 정책들에 기초하여 (예를들어, 단계(515)에서) 생성될 수 있다. 예를들어, 적어도 하나의 애플리케이션 터널을 생성할 때, 관리 브라우저 및/또는 관리 브라우저가 실행중인 컴퓨팅 디바이스는 관리 브라우저에 적용될 수 있고 그리고/또는 애플리케이션 터널들을 생성하고 그리고/또는 사용할 관리 브라우저의 능력을 선택적으로 제한하고 그리고/또는 그렇지 않은 경우에 제약할 수 있는 하나 이상의 정책들에 따라 적어도 하나의 애플리케이션 터널을 생성할 수 있다. 예를들어, 하나 이상의 정책들 중 적어도 하나의 정책은 애플리케이션 터널을 사용하여 액세스될 수 있는 정보의 타입들, 애플리케이션 터널을 사용하여 액세스될 수 있는 자원들, 애플리케이션 터널을 사용하여 정보에 액세스될 수 있는 사용자들, 관리 브라우저가 애플리케이션 터널을 생성할 수 있는 기간들, 관리 브라우저가 애플리케이션 터널을 생성할 수 있는 위치들, 및/또는 다른 제한들을 부과할 수 있는 다른

요소들을 선택적으로 제한할 수 있다.

[0090] [00105] 단계(520)에서, 하나 이상의 기업 자원들로부터의 기업 데이터는 적어도 하나의 애플리케이션 터널을 통해 획득될 수 있다. 예를들어, 단계(520)에서, 컴퓨팅 디바이스는 단계(515)에서 생성된 애플리케이션 터널(들)을 통해 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 수 있다. 기업 데이터를 획득하는 것에 추가하여, 컴퓨팅 디바이스는 또한 (예를들어, 획득된 기업 데이터의 일부 또는 모두가 관리 브라우저에서 디스플레이되도록 함으로써) 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공할 수 있다.

[0091] [00106] 일부 실시예들에서, 하나 이상의 정책들이 관리 브라우저에 적용될 수 있다. 게다가, 하나 이상의 정책들은 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성될 수 있다. 예를들어, 하나 이상의 정책들은 관리 브라우저의 특정 기능(들)이 선택적으로 디스에이블되어야 하는 특정 환경들을 정의할 수 있으며, 컴퓨팅 디바이스는 (예를들어, 이하에서 논의되는 디바이스 상태 정보에 기초하여) 이들 환경들을 검출하고 그리고/또는 그렇지 않은 경우에 식별할 수 있으며, 이후 하나 이상의 정책들에 따라 기능(들)을 디스에이블할 수 있다. 일부 경우들에서 정책에 의해 제한될 수 있는 관리 브라우저의 기능들의 일부 예들은 잘라 붙이기(cut-and-paste) 기능들, 인스턴트 메시징 기능들, 및 비디오 채트(video chat) 기능들을 포함한다. 이들 기능들이 일부 경우들에서 제한될 수 있는 기능들의 예들로서 본원에서 리스트되는 반면에, 다른 기능들이 다른 경우들에서 유사하게 제한될 수 있다.

[0092] [00107] 일부 실시예들에서, 하나 이상의 정책들은 관리 브라우저에 적용될 수 있으며, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터의 사용을 제한하도록 구성될 수 있다. 예를들어, 하나 이상의 정책들은 특정 환경들을 정의할 수 있는데, 이 특정 환경들에서, 기업 데이터(예를들어, 단계(520)에서 컴퓨팅 디바이스 및/또는 관리 브라우저에 의해 애플리케이션 터널(들)을 통해 획득된 기업 데이터)는 특정 방식들로만 사용될 수 있으며, 컴퓨팅 디바이스는 (예를들어, 이하에서 논의되는 디바이스 상태 정보에 기초하여) 이들 환경들을 검출하고 그리고/또는 그렇지 않은 경우에 식별할 수 있으며, 이후 데이터가 하나 이상의 정책들에 따라 사용될 수 있는 방식(들)을 제한하고 그리고/또는 그렇지 않은 경우에 제어한다. 예를들어, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터가 (예를들어, 관리 브라우저로부터 다른 애플리케이션으로) 복사되고 붙여질 수 있는 환경들을 제한하도록 구성될 수 있다. 다른 예로서, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터가 (예를들어, 관리 브라우저 및/또는 컴퓨팅 디바이스에 의해) 세이브되거나 또는 프린트될 수 있는 환경들을 제한하도록 구성될 수 있다.

[0093] [00108] 일부 실시예들에서, 하나 이상의 정책들 중 적어도 하나의 정책은 디바이스 상태 정보에 의존할 수 있다. 예를들어, (예를들어, 하나 이상의 정책들에 의해 부과되는,) 관리 브라우저의 기능(들)에 대한 제한(들) 및/또는 기업 데이터가 (예를들어, 하나 이상의 정책들에 의해 부가적으로 또는 대안적으로 부과되는,) 관리 브라우저에 의해 사용될 수 있는 방식(들)에 대한 제한(들)은 컴퓨팅 디바이스의 현재 상태를 표시하는 상태 정보에 의존할 수 있다. 이러한 상태 정보는 예를들어 (예를들어, 배경 애플리케이션, 서비스 또는 프로세스로서) 컴퓨팅 디바이스상에서 실행되도록 구성되며 예를들어 (앞서 논의된) 클라이언트 에이전트(404)의 하나 이상의 양상들을 통합할 수 있는 모바일 자원 관리(MRM) 에이전트에 의해 수집되고 그리고/또는 모니터링될 수 있다. MRM 에이전트는 예를들어 모바일 디바이스 관리(MDM) 기능들, 모바일 애플리케이션 관리(MAM) 기능들 및/또는 다른 기능들 제공할 수 있고 그리고/또는 이들을 제공하도록 구성될 수 있다. 예를들어, MRM 에이전트는 디바이스-레벨 상태 정보, 예를들어 디바이스상에 저장되고 디바이스 상에서 실행되는 애플리케이션들 및/또는 운영 체제들을 표시하는 상태 정보, 디바이스가 이용할 수 있고 그리고/또는 디바이스에 의해 사용되는 네트워크 연결들을 표시하는 상태 정보, 및/또는 (예를들어, 지리적 좌표들 측면에서, "집" 또는 "직장"과 같은 의미상 라벨들 측면 등에서) 디바이스가 위치하고 그리고/또는 디바이스가 사용되는 현재 위치를 표시하는 상태 정보를 수집하고 그리고/또는 모니터링하도록 구성될 수 있다. 일부 경우들에서, 이들 타입들의 상태 정보가 (예를들어, MRM 에이전트에 의해, 컴퓨팅 디바이스상의 하나 이상의 다른 애플리케이션들 또는 서비스들 또는 프로세스들 등에 의해) 수집되고 그리고/또는 모니터링될 수 있는 상태 정보의 타입들의 예들로서 여기에서 리스트되는 반면에, 다른 경우들에서 추가적인 그리고/또는 대안적인 타입들의 상태 정보가 유사하게 수집되고 그리고/또는 모니터링될 수 있다. 게다가, 이러한 상태 정보의 일부 및/또는 모두는 앞서 논의된 정책들과 같은, 관리 브라우저상의 정책들을 적용하고 그리고/또는 시행할 때 (예를들어, 컴퓨팅 디바이스에 의해 그리고/또는 관리 브라우저에 의해) 사용될 수 있다.

[0094] [00109] 도 6은 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 디바이스 클라우드에 걸쳐 관리 브라우저 세션을 확장하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 6에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다.

다른 실시예들에서, 도 6에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 메모리와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0095] [00110] 도 6에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(605)에서 시작할 수 있다. 예를들어, 단계(605)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0096] [00111] 단계(610)에서, 적어도 하나의 다른 컴퓨팅 디바이스에의 연결은 디바이스 클라우드를 개시하도록 설정될 수 있다. 예를들어, 단계(610)에서, 컴퓨팅 디바이스는 디바이스 클라우드를 개시하기 위한 네트워크 연결을 하나 이상의 다른 컴퓨팅 디바이스들에 설정할 수 있다. 하나 이상의 어레인지먼트들에서, 디바이스 클라우드는 예를들어 서로 결합하여 사용될 2개 이상의 컴퓨팅 디바이스들이 단일 기능 또는 태스크를 수행하도록 할 수 있다. 통상적인 경우들에서, 디바이스들은 동일한 사용자에 의해 사용될 수 있으며 그리고/또는 이들 둘다는 서로의 근처에 (예를들어, 서로의 미리 결정된 거리내에) 그리고/또는 사용자 근처에 (예를들어, 사용자의 미리 결정된 거리내에) 위치할 수 있다. 일부 경우들에서, 디바이스 클라우드는 사용자의 디바이스들 중 하나의 디바이스에 의해 지원되는 것이 아니라 사용자의 디바이스들 중 다른 디바이스에 의해 지원되는 기능을 제공하기 위하여 사용될 수 있다. 예를들어, 랩탑 컴퓨터의 사용자는 다른 사람과 화상 회의를 수행하기를 원할 수 있으나 랩탑 컴퓨터는 카메라를 포함하지 않을 수 있다. 그러나, 만일 사용자가 또한 카메라를 포함하는 스마트 폰(또는 다른 컴퓨팅 디바이스)을 가지면, 디바이스 클라우드는 2개의 디바이스들에 의해 제공된 기능들을 동적으로 링크하기 위하여 사용될 수 있으며, 따라서 이들은 화상회의를 제공할 때 사용될 수 있다. 특히, 이러한 예에서, 디바이스 클라우드는 사용자의 스마트 폰이 화상회의를 위한 비디오 입력 디바이스로서 사용될 수 있는 반면에 (예를들어, 관리 브라우저내에서 실행될 수 있는 화상회의 플러그-인, 애플릿, 웹 애플리케이션 등에 의해 용이하게 될 수 있음) 사용자의 랩탑 컴퓨터가 화상회의를 수행할 때 (예를들어, 다른 사람의 디바이스(들)에 연결을 설정하고, 텍스트-기반 채트 기능들을 등을 제공할 때) 수반될 수 있는 다른 기능들을 수행하기 위하여 사용될 수 있도록 설정될 수 있다. 일부 실시예들에서 하나 이상의 디바이스들의 기능을 확장시키기 위하여 디바이스 클라우드가 사용될 수 있는 일부 방식들을 이러한 예가 예시할지라도, 다른 실시예들에서, 이러한 디바이스 클라우드는 다양한 디바이스들의 추가 기능 및/또는 대안 기능을 확장시키기 위하여 다른 방식들로 사용될 수 있다.

[0097] [00112] 단계(615)에서, 관리 브라우저의 세션은 디스플레이 클라우드에 걸쳐 확장될 수 있다. 예를들어, 단계(615)에서, 컴퓨팅 디바이스는 디바이스 클라우드(예를들어, 단계(610)에서 생성된 디바이스 클라우드)에 걸쳐 관리 브라우저의 세션(예를들어, 컴퓨팅 디바이스의 사용자가 상호작용하는 관리 브라우저의 현재의 세션)을 확장할 수 있다. 하나 이상의 어레인지먼트들에서, 디바이스 클라우드에 걸쳐 관리 브라우저의 세션을 확장하는 것은 적어도 하나의 다른 관리 브라우저가 적어도 하나의 다른 컴퓨팅 디바이스상에 로드되도록 하는 것 및 적어도 하나의 다른 관리 브라우저와 세션 데이터를 공유하는 것을 포함할 수 있다. 예를들어, 디바이스 클라우드에 걸쳐 관리 브라우저의 세션을 확장할 때, 컴퓨팅 디바이스는 초기에 관리 브라우저의 인스턴스(들)가 디바이스 클라우드에 참여하는 다른 디바이스(들)상에 로드되도록 할 수 있다. 후속하여, 컴퓨팅 디바이스는 디바이스 클라우드에 참여하는 다른 디바이스(들)상에서 실행중인 관리 브라우저의 인스턴스(들)와 세션 데이터를 공유할 수 있다. 이러한 세션 데이터를 공유할 때, 컴퓨팅 디바이스는 예를들어 기업 데이터 및/또는 비-기업 데이터를 포함할 수 있는, 컴퓨팅 디바이스상의 관리 브라우저에 의해 현재 사용되고 그리고/또는 디스플레이되고 있는 정보의 일부 또는 모두를 송신할 수 있다. 부가적으로 또는 대안적으로, 디바이스 클라우드에 참여하는 다른 디바이스(들)상에서 실행중인 관리 브라우저의 인스턴스(들)와 세션 데이터를 공유할 때, 컴퓨팅 디바이스는 컴퓨팅 디바이스상의 관리 브라우저에 의해 후속하여 디스플레이되고 그리고/또는 그렇지 않은 경우에 사용될 수 있는 정보를 수신할 수 있다.

[0098] [00113] 일부 실시예들에서, 하나 이상의 정책들이 관리 브라우저에 적용될 수 있으며, 하나 이상의 정책들은 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성될 수 있다. 예를들어, 컴퓨팅 디바이스 및/또는 (MRM 에이전트와 같이) 컴퓨팅 디바이스상에서 실행되는 소프트웨어는 앞서 논의된 바와같이 관리 브라우저의 기능(들)을 제한하도록 구성되는 하나 이상의 정책들을 관리 브라우저에 적용할 수 있다.

[0099] [00114] 일부 실시예들에서, 하나 이상의 정책들은 관리 브라우저에 적용될 수 있으며, 하나 이상의 정책들은 디바이스 클라우드를 제한하도록 구성될 수 있다. 예를들어, 일부의 경우들에서, 컴퓨팅 디바이스 및/또는 (MRM 에이전트와 같이) 컴퓨팅 디바이스상에서 실행되는 소프트웨어는 디바이스 클라우드(예를들어, 단계(610)에서 생성된 디바이스 클라우드)의 다양한 양상들을 제한하도록 구성되는 관리 브라우저에 하나 이상의 정책들을 적용할 수 있다. 하나 이상의 정책들이 디바이스 클라우드를 제한하도록 구성되는 일부 경우들에서, 하나 이상의 정책들 중 적어도 하나의 정책은 적어도 하나의 다른 컴퓨팅 디바이스에 적어도 하나의 역할(role)을 할당하도록 구성될 수 있다. 예를들어, 하나 이상의 정책들이 디바이스 클라우드를 제한하도록 구성되는 경우들에서, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 소프트웨어는 디바이스 클라우드에 참여중인 다른 컴퓨팅 디바이스(들)에 디바이스 클라우드의 특정 역할(들)을 할당하도록 구성되는 적어도 하나의 정책을 정의하고, 적용하고 그리고/또는 시행할 수 있다. 예를들어, 화상회의를 수반한, 앞서 논의된 예에서, 모바일 디바이스 관리 정책들은 디바이스 클라우드와 관련된 스마트 폰에 비디오 캡처링 역할을 할당할 수 있으며, 모바일 디바이스 관리 정책들은 디바이스 클라우드와 관련된 랩탑 컴퓨터에 연결 유지 역할을 할당할 수 있다.

[0100] [00115] 일부 실시예들에서, 적어도 하나의 다른 컴퓨팅 디바이스에의 연결은 관리 브라우저에 적용될 수 있는 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여 설정될 수 있다. 예를들어, 적어도 하나의 다른 컴퓨팅 디바이스에 연결을 설정할 때, 관리 브라우저 및/또는 관리 브라우저가 실행중인 컴퓨팅 디바이스는 관리 브라우저에 적용될 수 있는 하나 이상의 정책들에 따라 적어도 하나의 다른 컴퓨팅 디바이스에 연결되고 그리고/또는 이 다른 컴퓨팅 디바이스와 데이터를 교환할 수 있다. 예를들어, 하나 이상의 정책들은 디바이스 클라우드를 개시하기 위한 관리 브라우저의 능력이 선택적으로 인에이블되고, 선택적으로 디스에이블되며 그리고/또는 그렇지 않은 경우에 제한될 수 있는 특정 환경들을 정의할 수 있다. 예를들어, 하나 이상의 정책들 중 적어도 하나의 정책은 다른 컴퓨팅 디바이스(들)와 교환될 수 있는 정보의 타입들, 다른 컴퓨팅 디바이스(들)와 교환되는 정보에 액세스할 수 있는 사용자들, 관리 브라우저가 다른 컴퓨팅 디바이스(들)와 정보를 교환할 수 있는 시간들, 관리 브라우저가 다른 컴퓨팅 디바이스(들)와 정보를 교환할 수 있는 위치들 및/또는 다른 제한들을 부과할 수 있는 다른 요소들을 선택적으로 제한할 수 있다. 이들 제한들의 일부 및/또는 모두는 컴퓨팅 디바이스가 적어도 하나의 다른 컴퓨팅 디바이스에의 연결을 설정하고 그리고/또는 그렇지 않은 경우에 디바이스 클라우드가 개시될 수 있는 환경들을 컴퓨팅 디바이스가 제한할 수 있는 환경들을 제한할 수 있다.

[0101] [00116] 일부 실시예들에서, 적어도 하나의 다른 컴퓨팅 디바이스에 연결을 설정하는 것은 적어도 하나의 다른 컴퓨팅 디바이스와 연관된 상태 정보를 평가하는 것 및 평가된 상태 정보에 기초하여 적어도 하나의 다른 컴퓨팅 디바이스가 디바이스 클라우드에 참여하도록 하는 것을 결정하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(610)에서) 적어도 하나의 다른 컴퓨팅 디바이스에 연결을 설정할 때, 컴퓨팅 디바이스는 적어도 하나의 다른 컴퓨팅 디바이스와 연관된 상태 정보를 획득하고 그리고/또는 평가할 수 있다. 이러한 상태 정보는 예를들어 적어도 하나의 다른 컴퓨팅 디바이스의 현재의 디바이스 상태의 다양한 양상들, 예를들어 적어도 하나의 다른 컴퓨팅 디바이스상에서 설치될 수 있고 그리고/또는 이러한 다른 컴퓨팅 디바이스상에서 실행되는 애플리케이션들, 적어도 하나의 다른 컴퓨팅 디바이스가 연결되는 네트워크들, 적어도 하나의 다른 컴퓨팅 디바이스의 위치 및/또는 다른 고려사항들을 기술할 수 있다. 이후, 컴퓨팅 디바이스는 이러한 상태 정보에 기초하여, 적어도 하나의 다른 컴퓨팅 디바이스가 디바이스 클라우드에 참여해야 하는지의 여부를 결정할 수 있다. 이러한 결정은 예를들어 하나 이상의 정책들에 기초할 수 있다. 예를들어, 하나 이상의 정책들은, 디바이스가 특정 위치에 있는지 또는 있지 않는지, 디바이스상에 설치되고 그리고/또는 디바이스상에서 실행되는 특정 애플리케이션들을 가지는지 또는 가지지 않는지, 하나 이상의 특정 네트워크들에 연결되는지 또는 연결되지 않는지 등을 적어도 하나의 다른 컴퓨팅 디바이스와 연관된 상태 정보가 표시하는 경우에, 적어도 하나의 다른 컴퓨팅 디바이스가 디바이스 클라우드에 참여하도록 컴퓨팅 디바이스가 허용할 수 있음을 표시할 수 있다.

[0102] [00117] 도 7은 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 관리 브라우저의 동작 모드를 선택적으로 디스에이블하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 7에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 7에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 매체와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0103] [00118] 도 7에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(705)에서 시작할 수 있다. 예를들어, 단계(705)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상

의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0104] [00119] 하나 이상의 실시예들에서, 관리 브라우저는 관리 모드 및 비관리 모드를 가진 듀얼-모드 애플리케이션일 수 있다. 게다가, 관리 브라우저의 관리 모드는 기업 데이터에 액세스하도록 구성될 수 있으며, 관리 브라우저의 비관리 모드는 기업 데이터에 액세스하는 것을 제공하도록 구성될 수 있다. 예를들어, 관리 모드에서, 관리 브라우저는 특정 콘텐츠 필터들을 적용할 수 있고, 특정 다운링크들을 제한할 수 있으며, 그리고/또는 특정 플러그-인들을 차단할 수 있는 반면에, 비관리 모드에서 관리 브라우저는 이러한 셔터들을 적용하지 않을 수 있고, 이러한 다운링크들을 제한하지 않을 수 있으며 그리고/또는 이러한 플러그-인들을 차단하지 않을 수 있다. 일부 경우들에서, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 다른 소프트웨어(예를들어, MRM 에이전트)는 이하에서 논의되는 바와같이 관리 브라우저의 관리 모드를 선택적으로 디스에이블할 수 있으며, 따라서 관리 브라우저는 단지 (예를들어, 관리 브라우저의 관리 모드가 컴퓨팅 디바이스에 의해 및/또는 컴퓨팅 디바이스상에서 실행되는 다른 적절한 소프트웨어에 의해 재-인에이블될 때까지) 비관리 모드에서 실행할 수 있고 그리고/또는 이러한 비관리 모드에서 실행하는 것을 계속할 수 있다.

[0105] [00120] 단계(710)에서, 디바이스 상태 정보가 획득될 수 있다. 예를들어, 단계(710)에서, 컴퓨팅 디바이스는 컴퓨팅 디바이스의 현재의 상태를 표시하는 상태 정보를 획득할 수 있다. 일부 경우들에서, 이러한 상태 정보는 앞의 예들에서 논의된 MRM 에이전트와 같은, 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트에 의해 획득될 수 있다.

[0106] [00121] 일부 실시예들에서, 디바이스 상태 정보는 컴퓨팅 디바이스상에서 존재하는 하나 이상의 애플리케이션들을 식별하는 정보를 포함할 수 있다. 예를들어, (예를들어, 단계(710)에서) 디바이스 상태 정보를 획득할 때, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트는 애플리케이션(들)이 어떤 컴퓨팅 디바이스상에 저장되는지, 어떤 컴퓨팅 디바이스상에 설치되는지, 어떤 컴퓨팅 디바이스상에서 이전에 실행되었는지 및/또는 어떤 컴퓨팅 디바이스상에서 현재 실행되고 있는지를 결정하기 위하여 (예를들어, 컴퓨팅 디바이스에 연결될 수 있고 그리고/또는 그렇지 않은 경우에 컴퓨팅 디바이스에 액세스할 수 있는) 하나 이상의 저장 디바이스들 및/또는 (예를들어 컴퓨팅 디바이스에 의해 유지될 수 있는) 설치 로그들을 검사할 수 있다.

[0107] [00122] 일부 실시예들에서, 디바이스 상태 정보는 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보를 포함할 수 있다. 예를들어, (예를들어, 단계(710)에서) 디바이스 상태 정보를 획득할 때, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트는 컴퓨팅 디바이스가 어떤 네트워크(들)에 액세스하고 그리고/또는 어떤 네트워크(들)의 범위내에서 액세스하는지, 컴퓨팅 디바이스가 어떤 네트워크(들)에 이전에 연결되었는지, 그리고/또는 컴퓨팅 디바이스가 어떤 네트워크(들)에 현재 연결되고 있는지를 결정하기 위하여 (예를들어, 컴퓨팅 디바이스에 연결될 수 있고 그리고/또는 그렇지 않은 경우에 컴퓨팅 디바이스에 사용할 수 있는) 하나 이상의 네트워크 인터페이스들 및/또는 다른 네트워크 디바이스들 및/또는 (예를들어 컴퓨팅 디바이스에 의해 유지될 수 있는) 하나 이상의 연결 로그들을 검사할 수 있다.

[0108] [00123] 일부 실시예들에서, 디바이스 상태 정보는 컴퓨팅 디바이스의 현재 위치를 식별하는 정보를 포함할 수 있다. 예를들어, (예를들어, 단계(710)에서) 디바이스 상태 정보를 획득할 때, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트는 하나 이상의 다른 컴포넌트들(예를들어, GPS 수신기, 다른 포지셔닝 컴포넌트들 등) 및/또는 디바이스들을 결정할 수 있고 그리고/또는 이들이 컴퓨팅 디바이스의 현재 위치를 결정하도록 할 수 있다. 일부 경우들에서, 위치 정보는 컴퓨팅 디바이스의 현재 위치를 표시하는 지리적 좌표들을 포함할 수 있다. 일부 경우들에서, 위치 정보는 하나 이상의 사용자-특정 랜드마크들(예를들어, "집" 또는 "직장")에 대한 컴퓨팅 디바이스의 현재 위치를 표시하는 의미상 라벨들을 포함할 수 있다. 이러한 위치의 일부 및/또는 모두는 예를들어 하나 이상의 위치-기반 모바일 디바이스 관리 정책들을 적용하고 그리고/또는 시행할 때 컴퓨팅 디바이스상에서 실행되는 MRM 및/또는 컴퓨팅 디바이스에 의해 사용될 수 있다.

[0109] [00124] 단계(715)에서는 관리 브라우저의 하나 이상의 동작 모드들을 선택적으로 디스에이블해야 하는지의 여부가 디바이스 상태 정보에 기초하여 결정될 수 있다. 예를들어, 단계(715)에서, 컴퓨팅 디바이스는 관리 브라우저의 하나 이상의 동작 모드들을 선택적으로 디스에이블해야 하는지의 여부를 단계(710)에서 획득된 디바이스 상태 정보에 기초하여 결정할 수 있다. 앞서 논의된 바와같이, 일부 경우들에서, 관리 브라우저는 관리 모드 및 비관리 모드를 가지는 듀얼-모드 애플리케이션일 수 있다. 따라서, 일부 경우들에서, 단계(715)에서, 컴퓨

팅 디바이스는 단계(710)에서 획득된 디바이스 상태 정보에 기초하여 관리 브라우저의 관리 모드를 선택적으로 디스에이블해야 하는지의 여부를 결정할 수 있다. 예를들어, 컴퓨팅 디바이스는 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보, 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보, 및/또는 컴퓨팅 디바이스의 현재 위치를 식별하는 정보에 기초하여, 관리 브라우저의 관리 모드를 선택적으로 디스에이블해야 하는지의 여부를 결정할 수 있다. 일부 경우들에서, 컴퓨팅 디바이스는 관리 브라우저의 모드(예를들어, 관리 브라우저의 관리 모드)를 선택적으로 디스에이블해야 하는지의 여부를 결정할 때 디바이스 상태 정보와 결합하여 하나 이상의 정책들을 부가적으로 또는 대안적으로 평가할 수 있다.

[0110] [00125] 만일 관리 브라우저의 하나 이상의 동작 모드들을 디스에이블하지 않는 것이 단계(715)에서 결정되면, 방법은 종료될 수 있다. 부가적으로 또는 대안적으로, 방법은 (예를들어, 업데이트된 디바이스 상태 정보를 획득하기 위하여 그리고/또는 관리 브라우저의 하나 이상의 동작 모드들을 선택적으로 디스에이블해야 하는지의 여부를 결정하도록 업데이트된 디바이스 상태 정보를 재평가하기 위하여) 단계들(710 및 715)이 주기적으로 반복될 수 있도록 루프에서 계속될 수 있다.

[0111] [00126] 다른 한편으로, 관리 브라우저의 적어도 하나의 동작 모드를 선택적으로 디스에이블하는 것이 단계(715)에서 결정되면, 단계(720)에서, 관리 브라우저의 적어도 하나의 동작 모두가 디스에이블될 수 있다. 예를들어, 단계(720)에서, 컴퓨팅 디바이스는 관리 브라우저의 적어도 하나의 동작 모드(예를들어, 단계(715)에서 디스에이블하도록 결정된 모드(들))을 디스에이블할 수 있으며 그리고/또는 관리 브라우저의 적어도 하나의 동작 모드가 디스에이블되도록 할 수 있다. 관리 브라우저가 관리 모드 및 비관리 모드를 가진 듀얼-모드 애플리케이션인 경우들에서, 관리 모드는 예를들어 단계(720)에서 컴퓨팅 디바이스에 의해 디스에이블될 수 있다(그리고/또는 컴퓨팅 디바이스에 의해 디스에이블되도록 초래될 수 있다).

[0112] [00127] 일부 실시예들에서, 적어도 하나의 관리 모드가 디스에이블되도록 하는 것은 관리 브라우저가 적어도 하나의 관리 모드와 상이한 제 2 모드로 들어가도록 하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(720)에서) 관리 브라우저의 관리 모드의 관리 모드를 디스에이블하고 그리고/또는 그렇지 않은 경우에 관리 브라우저의 관리 모드가 디스에이블되도록 할 때, 컴퓨팅 디바이스는 (예를들어, 상이한 정책들이 관리 브라우저에 적용되기 때문에) 관리 브라우저가 이전에 동작중이었던 관리 모드와 상이한 제 2 모드에 관리 브라우저가 들어가도록 할 수 있다. 일부 경우들에서, 제 2 모드는 (예를들어, 상이한 정책들이 관리 브라우저에 적용되기 때문에) 관리 브라우저가 이전에 동작중이었던 관리 모드와 단순히 상이한 다른 관리 모드일 수 있다. 다시 말해서, 일부 경우들에서, 제 2 모드는 하나 이상의 정책들의 제 2 세트가 관리 브라우저에 적용되는 관리 모드일 수 있으며, 여기서 하나 이상의 정책들의 제 2 세트는 적어도 하나의 관리 모드에서 관리 브라우저에 적용되는 하나 이상의 정책들과 상이한 적어도 하나의 정책을 포함한다.

[0113] [00128] 다른 경우들에서, (예를들어, 적어도 하나의 관리 모드가 디스에이블된 이후에 관리 브라우저가 들어갈 수 있는) 제 2 모드는 관리 브라우저가 더이상 적어도 하나의 디바이스 관리자에 의해 관리되지 않는 비관리 모드일 수 있다. 예를들어, (예를들어, 단계(720)에서) 관리 브라우저의 관리 모드를 디스에이블하고 그리고/또는 그렇지 않은 경우에 관리 브라우저의 관리 모드가 디스에이블되도록 할 때, 컴퓨팅 디바이스는 관리 브라우저가 적어도 하나의 디바이스 관리자에 의해 관리되지 않을 수 있는, 앞서 논의된 비관리 모드와 같은 비관리 모드로 관리 브라우저가 들어가도록 할 수 있다. 이러한 디바이스 관리자는 예를들어 디바이스상에서 실행중이고 그리고 관리 브라우저 및/또는 다른 애플리케이션들, 서비스들 및/또는 디바이스의 기능들에 대하여 하나 이상의 정책들을 적용하고 그리고/또는 시행하도록 구성되는 모바일 자원 관리 에이전트일 수 있다.

[0114] [00129] 일부 실시예들에서, 하나 이상의 자원들에의 액세스는 비관리 모드에서 차단될 수 있다. 예를들어, 비관리 모드로 들어간 이후에, 관리 브라우저 및/또는 컴퓨팅 디바이스는 특정 기업 자원들과 같은 특정 자원들에 대한 액세스를 차단할 수 있다. 이러한 차단은 예를들어 관리 브라우저를 사용하여 달리 액세스될 수 있는 기업 정보의 보안을 보장하기 위하여 정책 시행, 모니터링 및/또는 다른 보안 특징들이 적용되지 않고 그리고/또는 이용가능하지 않는 비관리 모드에서 관리 브라우저가 동작하는 동안 관리 브라우저의 사용자가 기업 자원들 및/또는 다른 특정 자원들에 액세스하는 것을 막을 수 있다. 원격 기업 자원들의 원격적으로 저장된 정보에 대한 액세스를 차단하는 것에 추가하여, 관리 브라우저 및/또는 컴퓨팅 디바이스는 또한, 비관리 모드에서, 디바이스상에 국부적으로 캐싱될 수 있는 특정 정보에 대한 액세스를 차단할 수 있다. 예를들어, 비관리 모드 동안, 이러한 차단은 관리 브라우저가 기업 자원들로부터 원래 획득되었던 국부적으로 캐싱된 데이터, 예를들어 국부적으로 캐싱된 기업 애플리케이션 스토어 정보 및/또는 다른 국부적으로 캐싱된 기업 정보에 액세스하는 것을 막을 수 있다.

[0115] [00130] 일부 실시예들에서, 관리 브라우저는 업데이트된 디바이스 상태 정보에 기초하여, 비관리 모드로부터 다시 적어도 하나의 관리 모드로 전환하도록 구성될 수 있다. 예를들어, 비관리 모드로 들어간 이후에, 관리 브라우저 및/또는 컴퓨팅 디바이스는 (예를들어, 하나 이상의 정책들이 관리 브라우저에 적용될 수 있고, 관리 브라우저가 디바이스 관리자에 의해 관리될 수 있는 등이 이루어지는) 관리 모드로 관리 브라우저가 다시 들어갈 수 있는지의 여부를 결정하기 위하여 현재의 디바이스 상태 정보를 모니터링하고 주기적으로 재평가하도록 구성될 수 있다. 만일 예를들어 관리 브라우저 및/또는 컴퓨팅 디바이스가, 특정 환경들이 만족됨을 예를들어 상태 정보에 기초하여 결정하면, 컴퓨팅 디바이스는 관리 브라우저가 관리 모드로 다시 전환되도록 할 수 있다. 일부 경우들에서, 관리 브라우저가 관리 모드로 다시 들어갈 수 있는지의 여부를 결정할 때, 컴퓨팅 디바이스 및/또는 관리 브라우저는 예를들어 하나 이상의 정책들을 고려하여 현재의 디바이스 상태 정보를 평가할 수 있으며, 이 하나 이상의 정책들은 관리 브라우저를 제 1 위치에서 비관리 모드로 전환하는 것을 결정할 때 평가된 하나 이상의 정책들을 포함할 수 있다.

[0116] [00131] 도 8은 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 하나 이상의 모바일 디바이스 관리 정책들을 관리 브라우저에 적용하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 8에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 8에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 매체와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0117] [00132] 도 8에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(805)에서 시작할 수 있다. 예를들어, 단계(805)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0118] [00133] 단계(810)에서, 하나 이상의 정책들이 수신될 수 있다. 예를들어, 단계(810)에서, 컴퓨팅 디바이스는 하나 이상의 정책들을 수신할 수 있다. 하나 이상의 정책들은 예를들어 디바이스 상태 정보(예를들어, 컴퓨팅 디바이스에 의해 그리고/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트에 의해 획득되고 그리고/또는 모니터링되는 디바이스 상태 정보)를 사용하여 평가될 수 있는 환경들의 상이한 세트들에 기초하여, 허용된, 금지된 그리고/또는 제한된 기능들을 정의하는 모바일 디바이스 관리 정책들일 수 있다. 따라서, 정책들은 관리 브라우저의 다양한 기능들을 포함하는 다양한 기능들에 대해 디바이스-상태-기반 동작 제한들을 시행할 때 사용될 수 있다.

[0119] [00134] 일부 실시예들에서, 하나 이상의 정책들은 정책 서버로부터 수신될 수 있다. 예를들어, 정책들을 수신할 때, 컴퓨팅 디바이스는, 단계(810)에서, 정책 서버에 연결될 수 있고 그리고/또는 정책 서버로부터의 다수의 정책들을 수신할 수 있다. 정책 서버는 예를들어 기업 네트워크 인프라스트럭처의 부분일 수 있으며 그리고 (예를들어, 단계(810)에서 컴퓨팅 디바이스에 의해) 수신되는 정책들에 따라 관리 브라우저에 의해 액세스될 수 있는 하나 이상의 기업 자원들에 연결되고 그리고/또는 이 하나 이상의 기업 자원들에 포함될 수 있다.

[0120] [00135] 단계(815)에서, 하나 이상의 정책들은 관리 브라우저에 적용될 수 있다. 예를들어, 단계(815)에서, 컴퓨팅 디바이스는 관리 브라우저에 (예를들어, 단계(810)에서 수신되는) 하나 이상의 정책들을 적용할 수 있으며, 따라서 관리 브라우저의 특정 기능들은 (예를들어, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트에 의해 획득되고 그리고/또는 모니터링되는 디바이스 상태 정보에 기초하여) 선택적으로 인에이블되고 그리고/또는 디스에이블될 수 있다.

[0121] [00136] 일부 실시예들에서, 하나 이상의 정책들은 컴퓨팅 디바이스의 사용자와 연관된 식별 정보에 기초하여 관리 브라우저에 적용될 수 있다. 예를들어, (예를들어, 단계(815)에서) 하나 이상의 정책들을 관리 브라우저에 적용할 때, 컴퓨팅 디바이스는 컴퓨팅 디바이스의 현재의 사용자와 연관된 식별 정보를 요청하고 그리고/또는 획득할 수 있다. 이러한 식별 정보는 예를들어 사용자의 로그인 정보 및/또는 다른 식별 크리덴셜들을 제공하도록 사용자에게 프롬프트하도록 구성되는 하나 이상의 인증 프롬프트들을 통해 획득될 수 있다. 식별 정보에 기초하여 관리 브라우저에 정책들을 적용함으로써, 관리 브라우저 및/또는 컴퓨팅 디바이스의 현재 사용자에 대하여 (예를들어, 관리 브라우저에 적용되는 하나 이상의 정책들에 의해) 선택적으로 인에이블되고, 디스에이

블되며 그리고/또는 제한되는 특정 기능들은 그들의 아이덴티티를 고려하여 현재의 사용자에게 더 특별하게 맞추어질 수 있다.

[0122] [00137] 일부 실시예들에서, 하나 이상의 정책들은 컴퓨팅 디바이스의 사용자와 연관된 역할 정보에 기초하여 관리 브라우저에 적용될 수 있다. 예를들어, (예를들어, 단계(815)에서) 관리 브라우저에 하나 이상의 정책들을 적용할 때, 컴퓨팅 디바이스는 컴퓨팅 디바이스의 현재 사용자와 연관된 식별 정보 및/또는 역할 정보를 요청하고 그리고/또는 획득할 수 있다. 역할 정보는 예를들어 기업내의 현재 사용자의 역할(들)(예를들어, 세일, 엔지니어링, 법적 요건, 계정, 경영진 등)을 특정할 수 있다. 일부 경우들에서, 컴퓨팅 디바이스는 예를들어 컴퓨팅 디바이스의 현재 사용자에 대한 식별 정보에 기초하여 (예를들어, 하나 이상의 데이터베이스들, 디렉토리들 및/또는 기업 자원들에서 사용자에 대한 역할 정보에 액세스하고 그리고/또는 이 역할 정보를 룩업하기 위하여 식별 정보를 사용함으로써) 컴퓨팅 디바이스의 현재 사용자에 대한 역할 정보를 결정할 수 있다. 역할 정보에 기초하여 관리 브라우저에 정책들을 적용함으로써, 컴퓨팅 디바이스 및/또는 관리 브라우저의 현재 사용자에 대하여 (예를들어, 관리 브라우저에 적용되고 있는 하나 이상의 정책들에 의해) 선택적으로 인에이블되고, 디스에이블되며 그리고/또는 제한되는 특정 기능들은 기업 내의 그들의 역할(들)을 고려하여 현재 사용자의 요구들 및/또는 액세스 레벨에 더 특별하게 맞추져질 수 있다.

[0123] [00138] 예를들어, 병원과 같은 헬스케어 기업의 맥락에서 역할 정보에 기초하여 관리 브라우저에 하나 이상의 정책들을 적용할 때, 컴퓨팅 디바이스는 (예를들어, 컴퓨팅 디바이스의 현재 사용자에 대한 식별 정보를 획득하고 그리고/또는 분석함으로써) 컴퓨팅 디바이스의 현재 사용자가 의사인지 또는 간호사인지를 결정할 수 있다. 만일 컴퓨팅 디바이스의 현재 사용자가 의사라고 컴퓨팅 디바이스가 결정하면 컴퓨팅 디바이스는 관리 브라우저에 정책들의 제 1 세트를 적용할 수 있으며, 만일 컴퓨팅 디바이스의 현재 사용자가 간호사라고 컴퓨팅 디바이스가 결정하면 컴퓨팅 디바이스는 정책들의 제 1 세트와 상이한 정책들의 제 2 세트를 관리 브라우저에 적용할 수 있다. 특히, 정책들의 제 2 세트는 예를들어 헬드케어 기업의 간호사의 역할과 헬드케어 기업의 의사의 역할 사이의 차이들에 기초하여 정책들의 제 1 세트에 비해 관리 브라우저의 추가적인 그리고/또는 대안적인 기능들을 선택적으로 인에이블하고, 디스에이블하며 그리고/또는 제한할 수 있다. 예를들어, 관리 브라우저에 적용되는 정책들의 결과로서, 의사는 예를들어 간호사가 액세스하지 못할 수 있는 특정 자원들에 액세스하기 위하여 컴퓨팅 디바이스상의 관리 브라우저를 사용하는 것이 가능하게 할수 있다.

[0124] [00139] 다른 예로서, 로펌과 같은 법률 기업의 맥락에서 역할 정보에 기초하여 관리 브라우저에 하나 이상의 정책들을 적용할 때, 컴퓨팅 디바이스는 컴퓨팅 디바이스의 현재 사용자가 로펌에 의해 처리하고 있는 특정 경우들 및/또는 다른 사건들로부터 스크리닝되었던 전문가들의 그룹내의 다른 전문가인지 또는 변호사인지의 여부를 결정할 수 있다. 컴퓨팅 디바이스의 현재 사용자가 스크리닝된 전문가들의 그룹내에 있다고 컴퓨팅 디바이스가 결정하면 컴퓨팅 디바이스는 관리 브라우저에 정책들의 제 1 세트를 적용할 수 있으며, 만일 컴퓨팅 디바이스의 현재 사용자가 스크리닝된 전문가들의 그룹내에 있지 않다고 컴퓨팅 디바이스가 결정하면 컴퓨팅 디바이스는 정책들의 제 1 세트와 상이한 정책들의 제 2 세트를 관리 브라우저에 적용할 수 있다. 특히, 정책들의 제 2 세트는 예를들어 법률 기업의 특정 전문가의 역할들 사이의 차이들에 기초하여 정책들의 제 1 세트에 비해 관리 브라우저의 추가적인 그리고/또는 대안적인 기능들을 선택적으로 인에이블하고, 디스에이블하며 그리고/또는 제한할 수 있다. 예를들어, 관리 브라우저에 적용되는 정책들의 결과로서, 특정 변호사들은 로펌내의 다른 변호사들이 액세스하지 못할 수 있는 특정 자원들에 액세스하기 위하여 컴퓨팅 디바이스상의 관리 브라우저를 사용하는 것이 가능하게 할수 있다.

[0125] [00140] 일부 실시예들에서, 관리 브라우저에 하나 이상의 정책들을 적용하는 것은 관리 브라우저를 통해 액세스할 수 있는 하나 이상의 기업 자원들에 대한 액세스를 제어하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(815)에서) 관리 브라우저에 하나 이상의 정책들을 적용할 때, 컴퓨팅 디바이스는 관리 브라우저를 사용하여 액세스될 수 있는 기업 자원(들)에 대한 액세스를 제어할 수 있다. 특히, 하나 이상의 정책들 중 적어도 하나의 정책은 예를들어 특정 기업 자원(들), 예를들어 특정 데이터베이스들, 서버들 및/또는 다른 기업 자원들(예를들어, 기업 인프라스트럭처에 연결되고 그리고/또는 기업 인프라스트럭처의 부분일 수 있음)에 대한 액세스를 선택적으로 인에이블하고, 디스에이블하며 그리고/또는 제한할 수 있다. 부가적으로 또는 대안적으로, 이러한 정책은 예를들어 (예를들어, 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보, 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보, 및/또는 컴퓨팅 디바이스의 현재 위치를 식별하는 정보를 포함할 수 있는) 디바이스 상태 정보에 의존할 수 있으며, 따라서 특정 기업 자원(들)에 대한 액세스는 컴퓨팅 디바이스의 현재 상태에 기초하여 제어될 수 있다.

[0126] [00141] 일부 실시예들에서, 관리 브라우저에 하나 이상의 정책들을 적용하는 것은 관리 브라우저를 통해 하나

이상의 기업 자원들로부터 획득된 정보의 사용을 제어하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(815)에서) 관리 브라우저에 하나 이상의 정책들을 적용할 때, 컴퓨팅 디바이스는 기업 자원들(들)로부터 획득되는 정보, 예를들어 관리 브라우저를 사용하여 기업 자원(들)으로부터 획득된 정보가 (예를들어, 관리 브라우저에 의해 및/또는 컴퓨팅 디바이스상의 다른 애플리케이션들, 서비스들 및/또는 프로세스들에 의해) 어떻게 사용될 수 있는지를 제어할 수 있다. 특히, 하나 이상의 정책들 중 적어도 하나의 정책은 예를들어 기업 자원들(들)로부터 획득된 정보를 세이브하는 능력, 기업 자원(들)으로부터 획득된 정보를 프린트하는 능력, 기업 자원(들)으로부터 획득된 정보를 절단하고, 복사하며 그리고/또는 붙이는 능력, 기업 자원(들)으로부터 획득된 정보를 편집하는 능력 및/또는 기업 자원(들)으로부터 획득된 정보와 상호작용하고 그리고/또는 이러한 정보를 사용하는 다른 능력들을 선택적으로 허용하고, 금지하며 그리고/또는 그렇지 않은 경우에 제한할 수 있다. 부가적으로 또는 대안적으로, 이러한 정책은 예를들어 (예를들어, 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보, 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보, 및/또는 컴퓨팅 디바이스의 현재 위치를 식별하는 정보를 포함할 수 있는) 디바이스 상태 정보에 의존할 수 있으며, 따라서 기업 자원(들)으로부터 획득된 특정 정보의 사용은 컴퓨팅 디바이스의 현재 상태에 기초하여 제어될 수 있다.

[0127] [00142] 도 9는 본원에서 논의되는 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 통해 보안 문서 컨테이너에 액세스를 제공하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 9에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 9에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 매체와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0128] [00143] 도 9에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(905)에서 시작할 수 있다. 예를들어, 단계(905)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0129] [00144] 단계(910)에서, 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청이 수신될 수 있다. 예를들어, 단계(910)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신할 수 있다. 이러한 요청은 예를들어 (예를들어, 사용자가 링크를 선택하고 그리고/또는 그렇지 않은 경우에 관리 브라우저를 사용하여 네트워크 자원에 대한 액세스를 요청하는 것에 기초하여) 관리 브라우저를 통해 컴퓨팅 디바이스에 의해 수신되는 사용자 입력에 기초하고 그리고/또는 이러한 사용자 입력에 대응할 수 있다.

[0130] [00145] 단계(915)에서, 하나 이상의 기업 자원들로부터의 기업 데이터는 요청에 기초하여 획득될 수 있다. 예를들어, 단계(915)에서, 컴퓨팅 디바이스는 단계(910)에서 수신된 요청에 기초하여 하나 이상의 기업 자원들에 연결하고, 이 하나 이상의 기업 자원들로부터 정보를 요청하고 이후 수신하고 그리고/또는 그렇지 않은 경우에 획득할 수 있다.

[0131] [00146] 단계(920)에서, 획득된 기업 데이터는 보안 문서 컨테이너에 저장될 수 있다. 예를들어, 단계(920)에서, 컴퓨팅 디바이스는 단계(915)에 포함된 기업 데이터는 보안 문서 컨터이너에 저장할 수 있다. 하나 이상의 어레인지먼트들에서, 보안 문서 컨테이너는 하나 이상의 기업 자원들로부터 컴퓨팅 디바이스에 의해 수신된 기업 데이터를 보안적으로 저장하도록 구성되는, 컴퓨팅 디바이스상의 데이터 저장소일 수 있다. 부가적으로 또는 대안적으로, 하나 이상의 모바일 디바이스 관리 정책은 특정 환경들을 정의할 수 있으며, 이 특정 환경들에서, 보안 문서 컨테이너에 대한 액세스는 제한되고, 수정되고 그리고/또는 그렇지 않은 경우에 제어될 수 있으며, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트는 디바이스 상태 정보에 기초하여 이들 환경들을 검출할 수 있으며, 이후 정책들에 따라 보안 문서 컨테이너들에 대한 액세스를 제한하고, 수정하며 그리고/또는 그렇지 않은 경우에 제어할 수 있다. 다른 경우들에서, (예를들어, 보안 문서 컨테이너에 대한 액세스가 아닌) 보안 문서 컨테이너의 다른 양상들은 하나 이상의 모바일 디바이스 관리 정책들에 의해 유사하게 제어될 수 있다.

[0132] [00147] 단계(925)에서,보안 문서 컨테이너에 대한 액세스는 관리 브라우저를 통해 제공될 수 있다. 예를들어, 단계(925)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해 보안 문서 컨테이너에 대한 액세스를 제공할 수 있다. 관리 브라우저를 통해 보안 문서 컨테이너에 대한 액세스를 제공할 때, 컴퓨팅 디바이스는 예를들어 관리 브라우저가 하나 이상의 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있으며, 이 하나 이상의 사용자 인터페이스들은 보안 문서 컨테이너에 저장된 기업 데이터 및/또는 다른 정보가 보여지고, 편집되고 그리고/또는 그렇지 않은 경우에 액세스되도록 구성된다. 예를들어, 단계(925)에서, 컴퓨팅 디바이스는 관리 브라우저가 하나 이상의 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있으며, 이 하나 이상의 사용자 인터페이스들은, 컴퓨팅 디바이스의 사용자로 하여금, 보안 문서 컨테이너에 저장된 정보를 브라우징하고, 보안 문서 컨테이너에 저장된 특정 파일들 및/또는 다른 정보를 보고, 보안 문서 컨테이너에 저장된 정보를 편집하며, 보안 문서 컨테이너에 저장된 정보를 삭제하며, 그리고/또는 그렇지 않은 경우에 보안 문서 컨테이너에 저장되는 정보와 상호작용하고 그리고/또는 이 정보에 액세스하도록 한다.

[0133] [00148] 단계(930)에서, 데이터는 보안 문서 컨테이너로부터 선택적으로 지워질 수 있다. 예를들어, 단계(930)에서, 컴퓨팅 디바이스는 보안 문서 컨테이너로부터의 정보를 선택적으로 지우고 그리고/또는 그렇지 않은 경우에 삭제할 수 있다. 하나 이상의 어레인지먼트에서, 컴퓨팅 디바이스는 디바이스 상태 정보, 하나 이상의 정책들, 및/또는 컴퓨팅 디바이스에 의해 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트에 의해 평가되고 그리고/또는 검출될 수 있는 다른 요인들 및/또는 환경들에 기초하여 보안 문서 컨테이너로부터의 데이터를 선택적으로 지울 수 있다. 일부 경우들에서, 컴퓨팅 디바이스는 보안 문서 컨테이너에 저장될 수 있는 다른 기업 데이터를 포함하는 다른 데이터와 같은 다른 데이터를 남기면서, 단계(915)에서 획득된 기업 데이터와 같은, 보안 문서 컨테이너로부터의 일부 데이터를 지울 수 있다. 다른 경우들에서, 컴퓨팅 디바이스는 다른 데이터(예를들어, 상이한 시간 기간 동안 수신되고 그리고/또는 저장된 데이터)를 남기면서 특정 시간 기간 동안(예를들어, 마지막 4기간 내에) 수신되고 그리고/또는 저장된 보안 문서 컨테이너로부터 데이터를 지울 수 있다. 또 다른 경우에서, 컴퓨팅 디바이스는 다른 데이터(예를들어, 관리 브라우저의 다른 세션(들) 및/또는 다른 애플리케이션들과 연관된 데이터)를 남기면서, 관리 브라우저 및/또는 관리 브라우저의 특정 세션과 관련하여 수신되고 그리고/또는 저장된 보안 문서 컨테이너로부터 데이터를 지울 수 있다.

[0134] [00149] 일부 실시예들에서, 보안 문서 컨테이너로부터 데이터를 선택적으로 지우는 것은 요청에 기초하여 하나 이상의 기업 자원들로부터 획득된 기업 데이터를 삭제하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(930)에서) 보안 문서 컨테이너로부터 데이터를 선택적으로 지울때, 컴퓨팅 디바이스는 단계(915)에서 기업 자원(들)으로부터 획득된 기업 데이터를 삭제할 수 있다. 이러한 기업 데이터를 삭제할 때, 컴퓨팅 디바이스는 예를들어 보안 문서 컨테이너에 저장될 수 있는 (예를들어, 다른 브라우징 세션(들) 동안 획득될 수 있고, 다른 애플리케이션(들)과 연관될 수 있는 등의) 다른 데이터를 남기고 그리고/또는 그렇지 않은 경우에 보존하면서, 기업 데이터가 획득되었던 특정 브라우징 세션(들) 동안 획득된 기업 데이터 뿐만아니라 이들 브라우징 세션(들) 동안 획득되었을 수 있는 임의의 다른 정보를 삭제할 수 있다.

[0135] [00150] 일부 실시예들에서, 데이터는 관리 브라우저가 닫힐 때 보안 문서 컨테이너로부터 선택적으로 지워질 수 있다. 예를들어, 일부 경우들에서, 컴퓨팅 디바이스는 관리 브라우저가 닫히는 것에 응답하여 그리고/또는 그렇지 않은 경우에 이에 기초하여 (예를들어, 컴퓨팅 디바이스의 사용자가 관리 브라우저를 닫을 때, 컴퓨팅 디바이스들의 사용자가 관리 브라우저의 탭을 닫고 그리고/또는 그렇지 않은 경우에 관리 브라우저의 특정 세션을 닫을 때, 관리 브라우저가 닫혀지거나 또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트와 같은, 컴퓨팅 디바이스상의 다른 애플리케이션, 서비스 또는 프로세스에 의해 닫혀지게 초래될 때 등) 보안 문서 컨테이너로부터 데이터를 선택적으로 지울 수 있다.

[0136] [00151] 일부 실시예들에서, 데이터는 하나 이상의 정책들에 기초하여 보안 문서 컨테이너로부터 선택적으로 지워질 수 있다. 예를들어, 일부 경우들에서, 컴퓨팅 디바이스는 하나 이상의 모바일 디바이스 관리 정책들에 기초하여 보안 문서 컨테이너로부터 데이터를 선택적으로 지울 수 있다. 예를들어, 하나 이상의 모바일 디바이스 관리 정책들은 특정 환경들을 정의할 수 있으며, 이 특정 환경들에서, 특정 타입(들)의 데이터는 보안 문서 컨테이너로부터 선택적으로 지워질 수 있으며, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트는 디바이스 상태 정보에 기초하여 이들 환경들을 검출하고 후속하여 정책들에 따라 보안 문서 컨테이너로부터 데이터를 지울 수 있다. 예를들어, 디바이스 상태 정보(예를들어, 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보, 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보, 및/또는 컴퓨팅 디바이스의 현재 위치를 식별하는 정보를 포함할 수 있음)에 기초하여, 컴퓨팅 디

바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트는 (예를들어, 단계(915)에서) 관리 브라우저를 사용하여 하나 이상의 기업 자원들로부터 획득되었고 그리고 후속하여 (예를들어, 단계(920)에서) 보안 문서 컨테이너에 저장된 기업 데이터를 보안 문서 컨테이너로부터 선택적으로 지울 수 있다.

[0137] [00152] 일부 실시예들에서, 데이터는 관리 브라우저가 관리 모드에서 동작중일 때 관리 브라우저에 적용되는 하나 이상의 정책들에 기초하여 보안 문서 컨테이너로부터 선택적으로 지워질 수 있다. 예를들어, 일부 경우들에서, 컴퓨팅 디바이스는 관리 모드에서 관리 브라우저에 적용되는 하나 이상의 정책들에 기초하여 보안 문서 컨테이너로부터 데이터를 선택적으로 지울 수 있으며, 적어도 하나의 이러한 정책은 특정 환경들을 정의할 수 있으며, 이 특정 환경들에서 (예를들어, 관리 브라우저를 사용하여 획득된) 특정 데이터가 보안 문서 컨테이너로부터 선택적으로 삭제되어야 한다. 추가로, 이들 특정 환경들은, 앞서 논의된 예들에서 처럼, 디바이스 상태 정보에 기초하여 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트에 의해 검출될 수 있다.

[0138] [00153] 도 10은 본원에서 논의된 하나 이상의 예시적인 양상들에 따라, 싱글 사인-온 크리덴셜에 기초하여 기업 데이터를 획득하고 관리 브라우저를 통해 데이터에 대한 액세스를 제공하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 10에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스 (예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 10에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 매체와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0139] [00154] 도 10에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(1005)에서 시작할 수 있다. 예를들어, 단계(1005)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0140] [00155] 단계(1010)에서, 적어도 하나의 사용자 계정과 연관되는 싱글 사인-온(SSO:single sign-on) 크리덴셜이 수신될 수 있다. 예를들어, 단계(1010)에서, 컴퓨팅 디바이스는 싱글 사인-온 크리덴셜을 수신할 수 있으며, 싱글 사인-온 크리덴셜은 (예를들어, 컴퓨팅 디바이스 및/또는 다른 자원들, 예를들어 기업 자원들 및/또는 다른 네트워크 자원들에 액세스하고 그리고/또는 이를 사용할 때 활용될 수 있는) 특정 사용자 계정 및/또는 컴퓨팅 디바이스의 특정 사용자에 링크되고 그리고/또는 그렇지 않은 경우에 이와 연관될 수 있다. 하나 이상의 어레인지먼트들에서, 싱글 사인-온 크리덴셜은 적어도 2개의 상이한 기업 자원들(예를들어, 다양한 기업 웹사이트들, 데이터베이스들, 서버들, 다른 자원들 등)에 액세스할 때 사용되도록 구성되는 인증 크리덴셜일 수 있다. 부가적으로 또는 대안적으로, 싱글 사인-온 크리덴셜은 사용자가 컴퓨팅 디바이스상의 사용자 계정에 로그인하고, 컴퓨팅 디바이스상의 애플리케이션에 로그인하며, 컴퓨팅 디바이스를 통해 액세스되는 웹사이트에 로그인하며, 컴퓨팅 디바이스상에 제시되는 인증 프롬프트와 상호작용하며 그리고/또는 다른 방식들을 수행할 때 수신될 수 있다. 일부 경우들에서, 싱글 사인-온 크리덴셜은 예를들어 하나 이상의 기업 자원들 및/또는 관리 브라우저를 사용하는 다른 자원들 또는 정보에 액세스하는 요청 또는 시도와 관련하여 관리 브라우저를 통해 수신될 수 있다.

[0141] [00156] 단계(1015)에서, 하나 이상의 기업 자원들로부터의 기업 데이터는 SSO 크리덴셜에 기초하여 획득될 수 있다. 예를들어, 단계(1015)에서, 컴퓨팅 디바이스는 단계(1010)에서 수신된 SSO 크리덴셜을 사용하여 하나 이상의 기업 자원들에 연결하고 후속하여 이 하나 이상의 기업 자원들로부터 정보를 수신하고 그리고/또는 그렇지 않으면 획득할 수 있다. 일부 경우들에서, SSO 크리덴셜은 예를들어 기업 자원들에 대해 인증하고, 기업 자원들로부터 권리-제어 정보를 요청하고 그리고/또는 그렇지 않으면 기업 자원들로부터 기업 데이터를 수신하는데 사용될 수 있다. 예를들어, 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 때, 컴퓨팅 디바이스는 특정 기업 자원에의 연결을 개시할 수 있는데, 이는 관리 브라우저가 인증 정보를 제공할 것을 회답 요구한다. 이러한 회답 요구에 응답하여, 관리 브라우저는 기업 자원에 대해 인증하고 그리고/또는 기업 자원으로부터 정보를 획득하기 위하여 기업 자원에 (예를들어, 단계(1010)에서 수신된) SSO 크리덴셜을 제공할 수 있다.

[0142] [00157] 단계(1020)에서, 획득인 기업 데이터에 대한 액세스는 관리 브라우저를 통해 제공될 수 있다. 예를들

어, 단계(1020)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해 단계(1015)에서 획득된 기업 데이터에 대한 액세스를 제공할 수 있다. 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공할 때, 컴퓨팅 디바이스는 예를들어 관리 브라우저가 하나 이상의 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있는데, 이 하나 이상의 사용자 인터페이스들은 기업 데이터가 보여지고, 편집되고 그리고/또는 그렇지 않은 경우에 액세스되도록 구성된다. 예를들어, 단계(920)에서, 컴퓨팅 디바이스는 관리 브라우저가 하나 이상의 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있으며, 이 하나 이상의 사용자 인터페이스들은, 컴퓨팅 디바이스의 사용자로 하여금, 획득된 기업 데이터를 브라우징하고, 획득된 기업 데이터를 보고, 획득된 보안 데이터를 편집하며, 획득된 기업 데이터를 삭제하며, 그리고/또는 그렇지 않은 경우에 획득된 기업 데이터와 상호작용하고 그리고/또는 이 정보에 액세스하도록 한다.

[0143] [00158] 일부 실시예들에서, SSO 크리덴셜에 기초하여 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 때, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 관리 브라우저는, 하나 이상의 정책들 및/또는 디바이스 상태 정보에 기초하여, 사용자의 개입 없이 SSO 크리덴셜을 사용하여 (예를들어, 하나 이상의 기업 자원들에 의해 제시될 수 있는) 하나 이상의 인증 회답 요구에 응답할 수 있다. 예를들어, 이러한 인증 회답요구는 하나 이상의 정책들 및/또는 디바이스 상태 정보에 기초하여 SSO 크리덴셜을 사용하는 관리 브라우저 및/또는 컴퓨팅 디바이스에 의해 자동적으로 어드레싱될 수 있다. 더욱이, 이러한 방식으로 자동적으로 어드레싱될 수 있는 특정 인증 회답요구들 및/또는 인증 회답요구들의 타입들은 (예를들어, 앞서 논의된 예들에서 처럼, 디바이스 상태 정보에 의해 표시될 수 있는) 디바이스의 현재 콘텍스트 및/또는 하나 이상의 정책들에 따라 변경될 수 있다.

[0144] [00159] 따라서, 하나 이상의 실시예들에서, (예를들어, 단계(1015)에서) SSO 크리덴셜에 기초하여 하나 이상의 기업 자원들로부터 기업 데이터를 획득하는 것은 하나 이상의 기업 자원들 중 적어도 하나의 기업 자원으로부터 인증 회답요구를 수신하는 것; 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 인증 회답요구에 응답하여 적어도 하나의 기업 자원에 SSO 크리덴셜을 제공해야 하는지의 여부를 결정하는 것; 및 인증 회답요구에 응답하여 적어도 하나의 기업 자원에 SSO 크리덴셜을 제공하는 것을 결정하는 것에 기초하여, 적어도 하나의 기업 자원에 SSO 크리덴셜을 제공하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(1015)에서) SSO 크리덴셜을 사용하여 하나 이상의 기업 자원들로부터 기업 데이터를 획득할 때, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행되는 관리 브라우저는 (관리 브라우저가 예를들어 액세스를 시도할 수 있는) 기업 자원으로부터 인증 회답요구를 수신할 수 있다. 예를들어, 이러한 인증 회답요구는 통상적으로 대응 자원에 액세스하기 위하여 하나 이상의 인증 크리덴셜들을 제공할 것을 사용자에게 요구할 수 있다.

[0145] [00160] 인증 회답요구를 수신한 이후에, 컴퓨팅 디바이스 및/또는 컴퓨팅 디바이스상에서 실행하는 관리 브라우저는, 하나 이상의 정책들에 기초하여, 인증 회답요구에 응답하여 기업 자원에 SSO 크리덴셜을 제공해야 하는지의 여부를 결정할 수 있다. 예를들어, 컴퓨팅 디바이스 및/또는 관리 브라우저는 SSO 크리덴셜을 사용하여 관리 브라우저가 이러한 인증 회답요구에 자동적으로 응답할 수 있는 특정 환경들을 정의하는 하나 이상의 정책들에 기초하여 이러한 결정을 수행할 수 있다. 더욱이, 컴퓨팅 디바이스 및/또는 관리 브라우저는 이러한 디바이스 상태 정보가 앞서 논의된 예들로 평가될 수 있는 방법과 유사하게 디바이스 상태 정보에 기초하여 이들 환경들을 평가할 수 있다. 만일 컴퓨팅 디바이스 및/또는 관리 브라우저가, 하나 이상의 정책들 및/또는 디바이스 상태 정보를 고려하여, SSO 크리덴셜이 인증 회답요구에 응답하여 기업 자원에 제공될 수 있음을 결정하면, 컴퓨팅 디바이스 및/또는 관리 브라우저는 SSO 크리덴셜을 기업 자원에 제공할 수 있다. 예를들어, 컴퓨팅 디바이스 및/또는 관리 브라우저는 인증 회답요구에 자동적으로 응답하기 위하여 (예를들어, 단계(1010)에서 수신될 수 있었던) SSO 크리덴셜을 기업 자원에 송신할 수 있으며, 이는 차례로 컴퓨팅 디바이스 및/또는 관리 브라우저가 기업 자원으로부터의 그리고/또는 기업 자원에 의해 저장된 정보에 액세스하도록 할 수 있다. 게다가, 컴퓨팅 디바이스 및/또는 관리 브라우저는 사용자 개입 없이 SSO 크리덴셜을 이러한 방식으로 송신할 수 있다. 예를들어, 컴퓨팅 디바이스 및/또는 관리 브라우저는 임의의 인증 크리덴셜들을 제공하도록 사용자에게 프롬프트하지 않고 그리고/또는 심지어 SSO 크리덴셜이 기업 자원에 제공되고 있음을 사용자에게 통지하지 않고 SSO 크리덴셜을 송신할 수 있다. 대안적으로, 만일 컴퓨팅 디바이스 및/또는 관리 브라우저가, 하나 이상의 정책들 및/또는 디바이스 상태 정보를 고려하여, SSO 크리덴셜이 인증 회답요구에 응답하여 기업 자원에 제공될 수 없다는 것을 결정하면, 컴퓨팅 디바이스 및/또는 관리 브라우저는 (예를들어, 인증 회답요구에 응답할 때 컴퓨팅 디바이스 및/또는 관리 브라우저에 의해 나중에 사용될 수 있는) 하나 이상의 인증 크리덴셜들을 제공하도록 사용자에게 프롬프트할 수 있다. 따라서, 하나 이상의 실시예들에서, 인증 회답요구에 응답하여 적어도 하나의 기업 자원에 SSO 크리덴셜을 제공하지 않는 것을 결정하는 것에 기초하여, 컴퓨팅 디바이스 및/또는 컴퓨팅 디

바이스상에서 실행되는 관리 브라우저는 컴퓨팅 디바이스의 사용자로부터 적어도 하나의 인증 크리덴셜을 수신하도록 구성되는 인증 프롬프트를 생성할 수 있다.

[0146] [00161] 일부 실시예들에서, 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공하는 것은 SSO 크리덴셜에 기초하여 하나 이상의 정책들을 시행하는 것을 포함할 수 있다. 예를들어, 획득된 기업 데이터에 대한 액세스를 제공하고 그리고/또는 SSO 크리덴셜에 기초하여 정책들을 시행할 때, 컴퓨팅 디바이스는 (예를들어, SSO 크리덴셜에 기초하여 정책 서버 및/또는 다른 기업 자원들로부터 하나 이상의 정책들을 다운로드하고, 수신하며 그리고/또는 그렇지 않은 경우에 획득함으로써) SSO 크리덴셜에 기초하여 하나 이상의 정책들을 획득하고, (예를들어, SSO 크리덴셜과 연관될 수 있는 식별 정보를 고려하여, 컴퓨팅 디바이스의 현재 사용자에게 적용가능하고 그리고/또는 컴퓨팅 디바이스의 현저 사용자에게 적절한 정책들을 선택적으로 활성화하고, 비활성화하며 그리도/또는 시행함으로써) SSO 크리덴셜에 기초하여, 적용가능 정책들을 선택하며, 그리고/또는 (예를들어, SSO 크리덴셜, 하나 이상의 정책들 및/또는 디바이스 상태 정보를 고려하여, 사용자의 아이덴티티 및/또는 역할에 적용가능하고 그리고/또는 이에 적절할 수 있는 관리 브라우저에 대해 동작 제한들을 시행함으로써) 정책들에 따라 관리 브라우저에 대해 하나 이상의 동작 제한들을 부과할 수 있다.

[0147] [00162] 하나 이상의 정책들이 SSO 크리덴셜에 기초하여 시행되는 일부 실시예들에서, 하나 이상의 정책들은 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 예를들어, 하나 이상의 정책들은 특정 사용자들에 대해 관리 브라우저의 특정 기능(들)이 선택적으로 디스에이블될 특정 환경들을 정의할 수 있으며, 컴퓨팅 디바이스는 (예를들어, 디바이스 상태 정보에 기초하여) 이들 환경들을 검출하고 그리고/또는 그렇지 않은 경우에 식별할 수 있으며, 후속하여 하나 이상의 정책들에 따라 그리고 단계(1010)에서 수신된 SSO 크리덴셜에 기초하여 기능(들)을 디스에이블할 수 있다. 앞서 논의된 바와같이, 일부 경우들에서 정책에 의해 제한될 수 있는 관리 브라우저의 기능들의 일부 예들은 잘라 붙이기 기능들, 인스턴트 메시징 기능들, 및 비디오 채트 기능들을 포함한다. 게다가, 이들 기능들이 일부 경우들에서 제한될 수 있는 기능들의 예들로서 여기에서 리스트되는 반면에, 다른 기능들은 다른 경우들에서 유사하게 제한될 수 있다.

[0148] [00163] 하나 이상의 정책들이 SSO 크리덴셜에 기초하여 시행되는 일부 실시예들에서, 하나 이상의 정책들은 획득된 기업 데이터에 액세스하는 것을 제한하도록 구성될 수 있다. 예를들어, 하나 이상의 정책들은 특정 환경들을 정의할 수 있으며, 이 특정 환경들에서, 기업 데이터(예를들어, 단계(1015)에서 획득된 기업 데이터)는 단지 특정 방식들로 액세스되고 그리고/또는 사용될 수 있으며, 컴퓨팅 디바이스는 (예를들어, 디바이스 상태 정보에 기초하여) 이들 환경들을 검출하고 그리고/또는 그렇지 않은 경우에 식별할 수 있으며, 후속하여 하나 이상의 정책들에 따라 그리고 단계(1010)에서 수신된 SSO 크리덴셜에 기초하여 데이터가 액세스되고 그리고/또는 사용될 수 있는 방식(들)을 제한하고 그리고/또는 그렇지 않은 경우에 식별할 수 있다. 예를들어, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터가 (예를들어, 관리 브라우저로부터 다른 애플리케이션으로) 복사되고 붙여질 수 있는 환경들을 제한하도록 구성될 수 있다. 다른 예로서, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터가 (예를들어, 관리 브라우저 및/또는 컴퓨팅 디바이스에 의해) 세이브되거나 또는 프린트될 수 있는 환경들을 제한하도록 구성될 수 있다.

[0149] [00164] 하나 이상의 정책들이 SSO 크리덴셜에 기초하여 시행되는 일부 실시예들에서, 하나 이상의 정책들 중 적어도 하나의 정책의 시행은 디바이스 상태 정보에 의존할 수 있다. 예를들어, (예를들어, 하나 이상의 정책들에 의해 부과되는) 관리 브라우저의 기능(들)에 대한 제한(들) 및/또는 기업 데이터가 (예를들어, 하나 이상의 정책들에 의해 부가적으로 또는 대안적으로 부과되는 바와같이) 관리 브라우저에 의해 사용될 수 있는 방식(들)에 대한 제한(들)은 컴퓨팅 디바이스의 현재 상태를 표시하는 상태 정보에 의존할 수 있다. 이러한 상태 정보는, 앞서 논의된 예들에서 처럼, 예를들어 (예를들어, 배경 애플리케이션, 서비스 또는 프로세스로서) 컴퓨팅 디바이스상에서 실행되도록 구성된 MRM 에이전트에 의해 수집되고 그리고/또는 모니터링될 수 있다. 예를들어, MRM 에이전트는 디바이스-레벨 상태 정보, 예를들어 디바이스상에 저장되고 그리고/또는 디바이스상에서 실행되는 애플리케이션들 및/또는 운영체제들을 표시하는 상태 정보, 디바이스가 이용할 수 있고 그리고/또는 디바이스에 의해 사용되는 네트워크 연결들을 표시하는 상태 정보, 및/또는 디바이스가 위치하며 그리고/또는 사용되고 있는 현재 위치를 표시하는 상태 정보를 수집하고 그리고/또는 모니터링하도록 구성될 수 있다. 게다가, 이러한 상태 정보의 일부 및/또는 모두는 (예를들어, 앞서 논의된 바와같이, 단계(1010)에서 수신될 수 있는) SSO 크리덴셜과 결합하여, 앞서 논의된 정책들과 같은, 관리 브라우저상의 정책들을 적용하고 그리고/또는 시행할 때 (예를들어, 컴퓨팅 디바이스에 의해 그리고/또는 관리 브라우저에 의해) 사용될 수 있다.

[0150] [00165] 도 11은 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 통해 애플리케이션 스토어에 액세스를 제공하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 11에 예시된 방

법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 11에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 메모리와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0151] [00166] 도 11에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(1105)에서 시작할 수 있다. 예를들어, 단계(1105)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0152] [00167] 단계(1110)에서, 관리 브라우저를 통해 애플리케이션 스토어에 액세스하기 위한 요청이 수신될 수 있다. 예를들어, 단계(1110)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해 애플리케이션 스토어에 액세스하기 위한 요청을 수신할 수 있다. 이러한 요청은 예를들어 (예를들어, 사용자가 링크를 선택하고 그리고/또는 그렇지 않은 경우에 관리 브라우저를 사용하여 애플리케이션 스토어에 대한 액세스를 요청하는 것에 기초하여) 관리 브라우저를 통해 컴퓨팅 디바이스에 의해 수신되는 사용자 입력에 기초하고 그리고/또는 이러한 사용자 입력에 대응할 수 있다. 예를들어, 관리 브라우저는 아이콘 또는 툴바를 포함할 수 있으며, 아이콘 또는 툴바는 애플리케이션 스토어가 아이콘 또는 툴바의 선택시 관리 브라우저내에서 디스플레이되도록 구성될 수 있다. 부가적으로 또는 대안적으로, 관리 브라우저에 적용되는 특정 정책은 콘텍스트(예를들어, 디바이스상에서 실행될 수 있는 브라우저 및/또는 다양한 다른 프로그램들의 상태), 사용자 계정 정보 및/또는 사용자 역할 정보와 같은 하나 이상의 요인들에 기초하여 정확한 애플리케이션 스토어로 브라우저를 동적으로 보낼 수 있다.

[0153] [00168] 하나 이상의 어레인지먼트들에서, (예를들어, 단계(1110)에서 액세스되도록 요청되는) 애플리케이션 스토어는 하나 이상의 모바일 컴퓨팅 디바이스들에 기업 애플리케이션들을 제공하도록 구성되는 기업 애플리케이션 스토어일 수 있다. 다양한 디바이스들에 기업 애플리케이션들을 제공하도록 구성되는 것에 추가하여, 기업 애플리케이션 스토어는 또한 하나 이상의 모바일 디바이스 관리 정책들 및/또는 정책 업데이트들을 다양한 디바이스들에 제공하도록 구성될 수 있다. 예를들어, 애플리케이션 스토어는 하나 이상의 모바일 컴퓨팅 디바이스들 및/또는 다른 사용자 디바이스들에 의해 다운로드될 수 있고 이러한 사용자 디바이스들상에서 본래 후속하여 실행될 수 있는 하나 이상의 애플리케이션들을 제공하도록 구성될 수 있다. 애플리케이션 스토어는 또한 하나 이상의 웹 애플리케이션들 및/또는 하나 이상의 가상화 애플리케이션들에 액세스하기 위하여 사용될 수 있는 정보를 제공할 수 있다. 예를들어, 애플리케이션 스토어는 이러한 웹 애플리케이션 또는 가상화 애플리케이션을 실행하거나 그리고/또는 그렇지 않은 경우에 이를 제공하도록 구성되는 서버의 위치를 결정하고 그리고/또는 이 서버에 연결하기 위하여 관리 브라우저에 의해 사용될 수 있는 포인터 및/또는 위치 정보를 제공할 수 있다. 일부 경우들에서, 포인트 및/또는 위치 정보는 또한 웹 애플리케이션 또는 가상화 애플리케이션을 실행하도록 관리 브라우저에 의해 컴퓨팅 디바이스상의 상이한 애플리케이션으로 전달될 수 있다.

[0154] [00169] 단계(1115)에서, 애플리케이션 스토어로부터의 기업 데이터는 요청에 기초하여 획득될 수 있다. 예를들어, 단계(1115)에서, 컴퓨팅 디바이스는 단계(1110)에서 수신된 요청에 기초하여 애플리케이션 스토어에 연결하고, 이 애플리케이션 스토어로부터 정보를 요청하고, 후속하여 이를 수신하고 그리고/또는 그렇지 않은 경우에 획득할 수 있다.

[0155] [00170] 단계(1120)에서, 획득된 기업 데이터의 적어도 일부분은 관리 브라우저를 통해 제시될 수 있다. 예를들어, 단계(1120)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해, 단계(1115)에서 애플리케이션 스토어로부터 획득된 기업 데이터의 적어도 일부분을 제시할 수 있다. 관리 브라우저를 통해 기업 데이터를 제기할 때, 컴퓨팅 디바이스는 예를들어 관리 브라우저가 하나 이상의 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있으며, 하나 이상의 사용자 인터페이스들은 애플리케이션 스토어로부터 획득된 기업 데이터가 보여지고, 상호 작용하고 그리고/또는 그렇지 않은 경우에 액세스되도록 구성된다. 예를들어, 단계(1120)에서, 컴퓨팅 디바이스는 관리 브라우저가 하나 이상의 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있으며, 하나 이상의 사용자 인터페이스들은 사용자가 애플리케이션 스토어에서 이용가능한 애플리케이션들 및/또는 다른 콘텐츠를 보도록 하고, 이러한 애플리케이션들 및/또는 다른 콘텐츠를 선택 및/또는 다운로드하도록 하고, 그리고/또는 그렇지 않은 경우에 애플리케이션

스토어 데이터와 상호작용하도록 한다.

[0156] [00171] 일부 실시예들에서, 획득된 기업 데이터의 적어도 일부분을 제시하는 것은 애플리케이션 다운로드 인터페이스가 관리 브라우저를 통해 제공되도록 하는 것을 포함할 수 있다. 예를들어, 애플리케이션 스토어로부터 획득된 기업 데이터의 적어도 일부분을 제시할 때, 컴퓨팅 디바이스는 애플리케이션 다운로드 인터페이스를 디스플레이할 수 있고 그리고/또는 관리 브라우저가 애플리케이션 다운로드 인터페이스를 디스플레이하고 그리고/또는 그렇지 않은 경우에 제시하도록 할 수 있다. 애플리케이션 다운로드 인터페이스는 예를들어 애플리케이션 스토어를 통해 다운로드하기 위하여 이용가능할 수 있는 하나 이상의 애플리케이션들에 대한 정보를 포함할 수 있고 그리고/또는 이용가능한 애플리케이션(들)을 다운로드하기 위하여 선택할 수 있는 하나 이상의 링크들 및/또는 다른 제어들을 포함할 수 있다.

[0157] [00172] 일부 실시예들에서, 획득된 기업 데이터의 적어도 일부분을 제시하는 것은 애플리케이션 스토어로부터의 적어도 하나의 애플리케이션에 액세스를 제공하는 것을 포함할 수 있으며, 여기서 적어도 하나의 애플리케이션은 단지 관리 브라우저를 통해 액세스가능하다. 예를들어, 애플리케이션 스토어로부터 획득된 기업 데이터의 적어도 일부분을 제시할 때, 컴퓨팅 디바이스는 애플리케이션 스토어가 (예를들어, 통상적인 그리고/또는 비-관리 브라우저가 아니라) 관리 브라우저에 의해 액세스될 때만 (예를들어, 액세스, 다운로드 등을 위해) 단지 이용가능한 애플리케이션 스토어의 애플리케이션에 액세스를 제공할 수 있다. 일부 경우들에서, (예를들어, 애플리케이션 스토어에서 이용가능할 수 있고 그리고/또는 애플리케이션 스토어로부터 획득되었을 수도 있는) 특정 애플리케이션과 연관된 특정 타입들의 정보는 단지 사용자 디바이스가 관리 브라우저를 통해 애플리케이션 스토어에 액세스할 때 사용자 디바이스에 제공될 수 있다. 예를들어, 기업 템플레이트들, 특정 데이터 세트들, 동료 리뷰들, 애플리케이션이 사용되었던 특정 프로젝트들에 대한 정보, 애플리케이션을 다운로드했던 다른 사용자들 및/또는 종업원들의 리스트들 및/또는 특정 애플리케이션과 연관된 다른 타입들의 정보에 대한 액세스는 단지 관리 브라우저를 통해 제공될 수 있다. 이러한 정보는 예를들어 기업 특정적인 것으로 고려될 수 있으며, 따라서 정보에 대한 액세스는 관리 브라우저의 사용을 통해 제한될 수 있다.

[0158] [00173] 일부 실시예들에서, 획득된 기업 데이터의 적어도 일부분을 제시하는 것은 적어도 하나의 애플리케이션의 가상화 세션이 관리 브라우저를 통해 제공되도록 하는 것을 포함할 수 있다. 예를들어, 애플리케이션 스토어로부터 획득된 기업 데이터의 적어도 일부분을 제시할 때, 컴퓨팅 디바이스는 애플리케이션의 가상화 세션이 관리 브라우저를 통해 제공되도록 할 수 있다. 예를들어, 컴퓨팅 디바이스는 관리 브라우저가 애플리케이션의 하나 이상의 가상화 사용자 인터페이스들을 디스플레이하고 그리고/또는 그렇지 않은 경우에 제공하도록 할 수 있으며, 이들은 애플리케이션 스토어 및/또는 하나 이상의 기업 자원들로부터 획득되고 그리고/또는 애플리케이션 스토어 및/또는 하나 이상의 기업 자원들에 의해 원격적으로 실행될 수 있다.

[0159] [00174] 일부 실시예들에서, 관리 브라우저는 디바이스 상태 정보를 모니터링하고 디바이스 상태 정보에 기초하여 하나 이상의 정책들을 시행하도록 추가로 구성될 수 있다. 예를들어, 애플리케이션 스토어로부터 획득된 기업 데이터를 제시하도록 구성된 것에 추가하여, 관리 브라우저는 디바이스 상태 정보를 모니터링하고, (예를들어, 관리 브라우저 그 자체에 대해 그리고/또는 디바이스상에서 실행될 수 있는 하나 이상의 다른 애플리케이션들에 대해) 하나 이상의 정책들을 시행하도록 추가로 구성될 수 있다. 예를들어, 관리 브라우저는 앞서 논의된 MRM 에이전트로서 동작하고 그리고/또는 이 MRM 에이전트와 유사한 기능들을 제공하도록 구성될 수 있으며, 따라서 관리 브라우저는 기업 자원들에 보안적으로 액세스할 수 있는 브라우저로서 뿐만아니라 디바이스 상태 정보를 모니터링하고 상태 정보에 기초하여 다양한 애플리케이션들 및/또는 디바이스의 다른 기능들에 대하여 정책들을 시행할 수 있는 모바일 자원 관리 에이전트로서 컴퓨팅 디바이스상에서 동작할 수 있다.

[0160] [00175] 도 12는 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 사용하여 기업 데이터를 획득하여 제어하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 12에 예시된 방법 및 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 12에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 매체와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0161] [00176] 도 12에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(1205)에서 시작할 수 있다. 예를들어, 단계(1205)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의

정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0162] [00177] 단계(1210)에서, 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청이 수신될 수 있다. 예를들어, 단계(1210)에서, 컴퓨팅 디바이스는 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신할 수 있다. 이러한 요청은 예를들어 (예를들어, 사용자가 링크를 선택하고 그리고/또는 그렇지 않은 경우에 관리 브라우저를 사용하여 네트워크 자원에 대한 액세스를 요청하는 것에 기초하여) 관리 브라우저를 통해 컴퓨팅 디바이스에 의해 수신되는 사용자 입력에 기초하고 그리고/또는 이러한 사용자 입력에 대응할 수 있다.

[0163] [00178] 단계(1215)에서, 하나 이상의 기업 자원들로부터의 기업 데이터는 요청에 기초하여 획득될 수 있다. 예를들어, 단계(1215)에서, 컴퓨팅 디바이스는 단계(1210)에서 수신된 요청에 기초하여 하나 이상의 기업 자원들에 연결하고, 이 하나 이상의 기업 자원들로부터 정보를 요청하고 이후 수신하고 그리고/또는 그렇지 않은 경우에 획득할 수 있다.

[0164] [00179] 단계(1220)에서, 획득된 기업 데이터는 하나 이상의 정책들에 기초하여 제어될 수 있다. 예를들어, 단계(1220)에서, 컴퓨팅 디바이스는 하나 이상의 모바일 디바이스 관리 정책들을 사용하여 단계(1215)에서 획득된 기업 데이터를 제어할 수 있다. 하나 이상의 모바일 디바이스 관리 정책들은 예를들어 특징 기능들(예를들어, 관리 브라우저의 특정 기능들, 획득된 기업 데이터를 수반하는 특정 기능들 등)이 허용되고, 금지되며 그리고/또는 그렇지 않은 경우에 제한될 수 있는 특정 환경들을 정의할 수 있다. 부가적으로 또는 대안적으로, 컴퓨팅 디바이스는 디바이스 상태 정보에 기초하여 이들 환경들을 평가하고 이후에 하나 이상의 정책들에 따라 기업 데이터를 제어하도록 구성될 수 있다. 일부 경우들에서, 획득된 기업 데이터는 관리 모드에서 관리 브라우저에 적용될 수 있는 정책들의 동일한 세트(예를들어, 정책들의 제 1세트)를 사용하여 제어될 수 있다. 다른 경우들에서, 획득된 기업 데이터는 관리 모드에서 관리 브라우저에 적용될 수 있는 정책들의 상이한 세트(예를들어, 정책들의 제 1 세트와 상이한 정책들의 제 2 세트)를 사용하여 제어될 수 있다.

[0165] [00180] 일부 실시예들에서, (예를들어, 단계(1220)에서) 기업 데이터를 제어하는데 사용되는 정책들은 하나 이상의 특정 산업들, 예를들어 헬스케어, 금융, 법률, 공학 등에 특정적일 수 있으며 그리고/또는 이들에 대하여 그룹핑될 수 있다. 이러한 방식으로 정책들을 그룹핑하고 그리고/또는 그렇지 않으면 구현함으로써, 산업-특정 정책들의 화합 그룹은 산업-특정 브라우저를 생성하기 위하여 관리 브라우저에 적용될 수 있다. 예를들어, 헬드케어-관련 정책들의 화합 그룹은 예를들어, 정책들이 규제 및/또는 사적 관심을 만족하는 특정 기능을 차단하도록 동작할 수 있는 "헬스케이 브라우저"를 생성하기 위하여 관리 브라우저에 적용될 수 있다.

[0166] [00181] 일부 실시예들에서, (예를들어, 단계(1220)에서) 기업 데이터를 제어할 때 사용되는 정책들은 로깅 기능들 및/또는 다른 모니터링 기능들이 선택적으로 적용되고 그리고/또는 실행되도록 하는 하나 이상의 정책들을 포함할 수 있다. 이러한 로깅 기능들 및/또는 다른 모니터링 기능들은 관리 브라우저들에 및/또는 컴퓨팅 디바이스상에서 실행되는 하나 이상의 다른 애플리케이션들 및/또는 서비스들에 적용될 수 있다. 예를들어, 하나 이상의 정책들은 특정 시간들 동안, 특정 위치들에서 그리고/또는 디바이스의 현재의 콘텍스트에 기초하여 네트워크 트래픽을 모니터링하고 그리고/또는 선택적으로 필터링할 수 있다. 부가적으로 또는 대안적으로, 하나 이상의 정책들은 사용자 역할 정보, (예를들어, 디바이스 성능 및/또는 네트워크 성능을 포함할 수 있는) 성능 정보, 및/또는 하나 이상의 다른 요인들에 기초하여 필터 네트워크 트래픽을 모니터링하고 그리고/또는 선택적으로 필터링할 수 있다.

[0167] [00182] 일부 실시예들에서, 획득된 기업 데이터를 제어하는 것은 모바일 자원 관리(MRM) 에이전트, 예를들어 컴퓨팅 디바이스상의 적어도 하나의 다른 애플리케이션에 적어도 하나의 정책을 적용하도록 구성되는 모바일 자원 관리(MRM) 에이전트를 사용하여 관리 브라우저를 제어하는 것을 포함한다. 예를들어, (예를들어, 관리 브라우저에 정책들을 적용하고 그리고/또는 시행함으로써) 관리 브라우저를 제어하도록 구성되는 것에 추가하여, 컴퓨팅 디바이스상에서 실행될 수 있는 MRM 에이전트는 컴퓨팅 디바이스상에 저장되고 그리고/또는 컴퓨팅 디바이스상에서 실행중인 다른 애플리케이션들에 다양한 모바일 디바이스 관리 정책들을 적용하도록 추가로 구성될 수 있다. 이러한 MRM 에이전트는 예를들어 클라이언트 에이전트(404)의 하나 이상의 양상들(앞서 논의됨)을 통합할 수 있다.

[0168] [00183] 일부 실시예들에서, 하나 이상의 정책들 중 적어도 하나의 정책은 디바이스 상태 정보에 기초하여 관리 브라우저의 하나 이상의 기능들을 선택적으로 디스에이블하도록 구성될 수 있다. 일부 경우들에서 이러한 정책

에 의해 선택적으로 디스에이블될 수 있는 관리 브라우저의 기능들의 일부 예들은 잘라 붙이기 기능들, 인스턴트 메시징 기능들 및 비디오 채트 기능들을 포함한다. 이들 기능들이 일부 경우들에서 선택적으로 디스에이블될 수 있는 기능들의 예들로서 여기에서 리스트되는 반면에, 다른 기능들은 다른 경우들에서 유사하게 디스에이블될 수 있다. 더욱이, 하나 이상의 정책들을 평가할 때 사용될 수 있는 디바이스 상태 정보는 앞서 논의된 예들에서 처럼 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보, 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보, 및/또는 컴퓨팅 디바이스의 현재 위치를 식별하는 정보를 포함할 수 있다.

[0169] [00184] 일부 실시예들에서, 하나 이상의 정책들에 기초하여, 획득된 기업 데이터를 제어하는 것은 획득된 기업 데이터에 대한 액세스를 제거하는 것을 포함할 수 있다. 더욱이, 일부 경우들에서, 획득된 기업 데이터에 대한 액세스를 제어하는 것은 획득된 기업 데이터의 사용을 제어하는 것을 포함할 수 있다. 예를들어, 하나 이상의 정책들은 특정 환경들을 정의할 수 있으며, 이러한 특정 환경들에서, 기업 데이터(예를들어, 단계(1215)에서 획득된 관리 브라우저를 사용되는 기업 데이터)는 단지 특정 방식들로 액세스 및/또는 사용될 수 있으며, 컴퓨팅 디바이스는 (예를들어, 디바이스 상태 정보에 기초하여) 이들 환경들을 검출하고 그리고/또는 그렇지 않은 경우에 식별할 수 있으며, 이후 데이터가 하나 이상의 정책들에 따라 액세스 및/또는 사용될 수 있는 방식(들)을 제한하고 그리고/또는 그렇지 않은 경우에 제어한다. 예를들어, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터가 (예를들어, 관리 브라우저로부터 다른 애플리케이션으로) 복사되고 붙여질 수 있는 환경들을 제한하도록 구성될 수 있다. 다른 예로서, 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터가 (예를들어, 관리 브라우저 및/또는 컴퓨팅 디바이스에 의해) 세이브되거나 또는 프린트될 수 있는 환경들을 제한하도록 구성될 수 있다.

[0170] [00185] 일부 실시예들에서, 관리 브라우저는 정책 관리 서버로부터 MRM 에이전트에 대한 하나 이상의 정책 업데이트들을 수신하도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 브라우저는 (예를들어, 관리 브라우저, 다른 애플리케이션들, 및/또는 컴퓨팅 디바이스의 다른 양상들에 적용될 새로운 및/또는 업데이트된 정책들을 포함할 수 있는) 하나 이상의 정책 업데이트들을 수신할 수 있다. 이러한 정책 업데이트들은 예를들어 정책 관리 서버로부터 수신될 수 있으며, 이러한 정책 업데이트를 수신한 이후에, 관리 브라우저는 MRM 에이전트에 정책 업데이트 및 이의 연관된 정보를 제공할 수 있다(이후 MRM 에이전트는 예를들어 새로운 및/또는 업데이트된 정책들을 수신하여 적절하게 적용할 수 있다).

[0171] [00186] 일부 실시예들에서, 획득된 기업 데이터를 제어하는 것은 관리 브라우저가 비관리 모드에서 동작중일 때 획득된 기업 데이터에 대한 액세스를 선택적으로 차단하는 것을 포함할 수 있다. 예를들어, (예를들어, 단계(1215)에서) 하나 이상의 기업 자원들로부터 기업 데이터를 획득한 이후에, 관리 브라우저 및/또는 관리 브라우저가 실행중인 컴퓨팅 디바이스는 관리 브라우저가 비관리 모드(앞의 예에서 논의된 바와같이, 비관리 모드에서는 예를들어 하나 이상의 정책들이 브라우저에 적용되지 않을 수 있다)에서 동작중일 때 획득된 기업 데이터에 대한 액세스를 선택적으로 차단할 수 있다. 다시 말해서, 관리 브라우저 및/또는 관리 브라우저가 실행중인 컴퓨팅 디바이스는 관리 브라우저가 관리 모드에서 실행중인 동안 컴퓨팅 디바이스의 사용자가 단지 관리 브라우저를 사용하여, 획득된 기업 데이터에 액세스할 수 있는 반면에 관리 브라우저가 관리 모드에서 실행중이지 않는 동안 (예를들어, 관리 브라우저가 비관리 모드에서 실행중일 때) 컴퓨팅 디바이스의 사용자가 관리 브라우저를 통해 획득된 기업 데이터에 액세스하는 것이 차단될 수 있도록 구성될 수 있다.

[0172] [00187] 도 13는 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 관리 브라우저에 대한 하나 이상의 정책들을 관리하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 13에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 13에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 매체와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0173] [00178] 도 13에서 알 수 있는 바와같이, 방법은 하나 이상의 사용자 컴퓨팅 디바이스들상의 관리 브라우저에 적용될 적어도 하나의 정책이 수신될 수 있는 단계(1305)에서 시작할 수 있다. 예를들어, 이러한 정책은 (예를들어, 범용 컴퓨팅 디바이스(201)의 하나 이상의 양상들을 통합할 수 있고 그리고/또는 기업 조직 및/또는 다양한 사용자에게 정책 관리 기능들을 제공하도록 구성될 수 있는) 서버 컴퓨팅 디바이스에 의해 수신될 수 있다. 게다가, 정책은 관리 사용자 및/또는 이러한 사용자에 의해 동작되고 있는 컴퓨팅 디바이스로부터 서버 컴퓨팅 디바이스에 의해 수신될 수 있으며, 이 사용자는 다양한 사용자 컴퓨팅 디바이스들상의 관리 브라우저(들)에 적용될 하나 이상의 새로운 및/또는 업데이트 정책들을 정의할 수 있다. 앞서 논의된 예들에서 처럼, 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되고 하나 이상의 정책들이 관리 브라우저의 하나

이상의 기능들을 제한하도록 구성될 수 있는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0174] [00189] 단계(1310)에서, 적어도 하나의 정책 업데이트는 적어도 하나의 정책에 기초하여 하나 이상의 사용자 컴퓨팅 디바이스들 중 적어도 하나의 사용자 컴퓨팅 디바이스에 제공될 수 있다. 예를들어, 단계(1315)에서, 서버 컴퓨팅 디바이스는 단계(1305)에서 수신된 정책에 기초하여 사용자 컴퓨팅 디바이스에 정책 업데이트를 제공할 수 있다. 사용자 컴퓨팅 디바이스에 정책 업데이트를 제공할 때, 서버 컴퓨팅 디바이스는 예를들어 사용자 컴퓨팅 디바이스에 연결되어, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신되었을 수도 있는 새로운 및/또는 업데이트 정책에 대한 정보를 사용자 컴퓨팅 디바이스에 푸시(push)하고 그리고/또는 그렇지 않은 경우에 송신할 수 있다.

[0175] [00190] 하나 이상의 어레인지먼트들에서, 적어도 하나의 정책 업데이트는 적어도 하나의 사용자 컴퓨팅 디바이스가 적어도 하나의 사용자 컴퓨팅 디바이스의 관리 브라우저에 적어도 하나의 수신된 정책을 적용하도록 구성될 수 있다. 예를들어, (예를들어, 단계(1310)에서 서버 컴퓨팅 디바이스에 의해 사용자 컴퓨팅 디바이스로 제공될 수 있는) 정책 업데이트는 사용자 컴퓨팅 디바이스가 사용자 컴퓨팅 디바이스상의 관리 브라우저에 (예를들어, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신될 수 있는) 정책을 적용하도록 구성될 수 있다. 이러한 관리 브라우저는 예를들어 서버 컴퓨팅 디바이스로부터 정책 업데이트를 수신하는 사용자 컴퓨팅 디바이스(예를들어, 단계(1310)) 상에서 실행되고, 이 사용자 컴퓨팅 디바이스상에 저장되며 그리고/또는 그렇지 않은 경우에 존재할 수 있다. 일부 어레인지먼트들에서, (예를들어, 서버 컴퓨팅 디바이스에 의해 단계(1305)에서 수신되고, 이후 단계(1310)에서 정책 업데이트를 통해 사용자 컴퓨팅 디바이스에게 제공되고 이 사용자 컴퓨팅 디바이스에 의해 수신될 수 있는) 정책은 관리 브라우저 및/또는 관리 브라우저를 실행하는 사용자 컴퓨팅 디바이스에 대해 시행될 수 있는 하나 이상의 특정 규칙들을 정의할 수 있다. 이러한 규칙들은 예를들어 (예를들어, 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 등을 포함할 수 있는) 디바이스 상태 정보의 측면에서 정의되고 그리고/또는 이 디바이스 상태 정보에 기초하여 평가될 수 있는 특정 환경들에서 시행될 수 있다.

[0176] [00191] 일부 실시예들에서, 적어도 하나의 수신된 정책은 하나 이상의 콘텐츠 필터링 규칙들을 포함할 수 있다. 예를들어, 일부 경우들에서, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신되는 정책은 하나 이상의 콘텐츠 필터링 규칙들을 포함할 수 있다. 이러한 콘텐츠 필터링 규칙은 예를들어 특정 기업 자원들을 포함할 수 있는 특정 네트워크 자원들에 액세스하는 관리 브라우저의 능력을 제어할 수 있다. 예를들어, 콘텐츠 필터링 규칙은 (예를들어, 앞서 논의된 바와같이, 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 등을 포함할 수 있는) 디바이스 상태 정보 및/또는 다른 특정 기준에 기초하여, 관리 브라우저에 의한, 특정 타입들의 콘텐츠에 대한 액세스를 선택적으로 차단하고 그리고/또는 선택적으로 허용할 수 있다.

[0177] [00192] 일부 실시예들에서, 적어도 하나의 수신된 정책은 하나 이상의 캐싱 규칙들을 포함할 수 있다. 예를들어, 일부 경우들에서, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신된 정책은 하나 이상의 콘텐츠 캐싱 규칙들을 포함할 수 있다. 이러한 콘텐츠 캐싱 규칙은 예를들어 하나 이상의 기업 자원들로부터 수신된 특정 타입들의 콘텐츠, 다른 네트워크 자원들로부터 수신된 특정 타입들의 콘텐츠(예를들어, 웹 콘텐츠, 쿠키(cookies) 등) 및/또는 다른 타입들의 정보를 포함할 수 있는 특정 타입들의 콘텐츠를 캐싱하는 관리자 브라우저의 능력을 제어할 수 있다. 예를들어, 콘텐츠 캐싱 규칙은 (예를들어, 앞서 논의된 바와같이, 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 등을 포함할 수 있는) 디바이스 상태 정보 및/또는 다른 특정 기준에 기초하여 관리 브라우저에 의한, 특정 타입들의 콘텐츠의 캐싱을 선택적으로 차단하고 그리고/또는 선택적으로 허용할 수 있다.

[0178] [00193] 일부 실시예들에서, 적어도 하나의 수신된 정책은 플러그-인 규칙(plug-in rule)들을 포함할 수 있다. 예를들어, 일부 경우들에서, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신된 정책은 하나 이상의 플러그-

인 관리 규칙들을 포함할 수 있다. 이러한 플러그-인 관리는 (예를들어 다양한 타입들의 애플리케이션들, 확장자들, 애플릿들, 스크립트들 및/또는 다른 타입들의 플러그-인들)을 포함할 수 있는) 특정 플러그-인들에 액세스하고, 이 특정 플러그-인들을 실행하고 그리고/또는 그렇지 않은 경우에 사용하는 관리 브라우저의 능력을 제어할 수 있다. 예를들어, 플러그-인 관리 규칙은 (예를들어, 앞서 논의된 바와같이, 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 등을 포함할 수 있는) 디바이스 상태 정보 및/또는 다른 특정 기준에 기초하여 관리 브라우저에 의한, 하나 이상의 특정 플러그-인들의 액세스, 실행 및/또는 사용을 선택적으로 차단하고 그리고/또는 선택적으로 인에이블할 수 있다.

[0179] [00194] 일부 실시예들에서, 적어도 하나의 수신된 정책은 하나 이상의 크리덴셜 관리 규칙들을 포함할 수 있다. 예를들어, 일부 경우들에서, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신되는 정책은 하나 이상의 크리덴셜 관리 규칙들을 포함할 수 있다. 예를들어, 이러한 크리덴셜 관리 규칙은 예를들어 하나 이상의 자원들에 액세스할 때 하나 이상의 싱글 사인-온(SSO) 크리덴셜들을 포함할 수 있는 특정 크리덴셜들을 사용하는 관리 브라우저의 능력을 제어할 수 있다. 예를들어, 크리덴셜 관리 규칙은 (예를들어, 앞서 논의된 바와같이, 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 등을 포함할 수 있는) 디바이스 상태 정보 및/또는 다른 특정 기준에 기초하여 관리 브라우저에 의한, 하나 이상의 특정 크리덴셜들의 액세스 및/또는 사용을 선택적으로 차단하고 그리고/또는 인에이블할 수 있다.

[0180] [00195] 일부 실시예들에서, 적어도 하나의 수신된 정책은 디바이스 상태 정보에 기초하여 적어도 하나의 사용자 컴퓨팅 디바이스에 의해 시행되도록 구성될 수 있다. 예를들어, 일부 경우들에서, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신되는 정책은 사용자 컴퓨팅 디바이스와 연관된 디바이스 상태 정보에 기초하여 사용자 컴퓨팅 디바이스에 의해 시행되도록 구성될 수 있다. 이러한 정책은 예를들어 사용자 컴퓨팅 디바이스와 연관된 상태 정보에 기초하여 하나 이상의 특정 기능들이 실행되도록 그리고/또는 하나 이상의 다른 특정 기능들이 실행되는 것을 막도록 할 수 있다. 앞서 논의된 바와같이, 이러한 상태 정보는 예를들어 (예를들어, 관리 브라우저 외의) 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보, 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보, 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 및/또는 다른 정보를 포함할 수 있다.

[0181] [00196] 일부 실시예들에서, 적어도 하나의 수신된 정책은 관리 브라우저가 하나 이상의 기준에 기초하여 비관리 모드로 전환하도록 구성되는 하나 이상의 규칙들을 포함할 수 있다. 예를들어, 일부 경우들에서, 단계(1305)에서 서버 컴퓨팅 디바이스에 의해 수신되는 정책은 사용자 컴퓨팅 디바이스상의 관리 브라우저가 하나 이상의 기준에 기초하여 관리 모드로부터 비관리 모드로 전환하도록 구성되는 하나 이상의 규칙들을 포함할 수 있다. 하나 이상의 기준들은 예를들어 사용자 컴퓨팅 디바이스와 연관된 디바이스 상태 정보에 기초할 수 있고 그리고/또는 이러한 디바이스 상태 정보를 포함할 수 있다. 앞서 논의된 바와같이, 이러한 상태 정보는 예를들어 (예를들어, 관리 브라우저 외의) 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보, 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보, 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 및/또는 다른 정보를 포함할 수 있다.

[0182] [00197] 도 14는 본원에서 논의된 하나 이상의 예시적인 양상들에 따라 관리 브라우저를 통해 애플리케이션 스토어에 액세스를 제공하는 다른 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 14에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 14에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 메모리와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0183] [00198] 도 14에서 알 수 있는 바와같이, 방법은 애플리케이션 스토어의 제 1 부분에 액세스하기 위하여 사용자 컴퓨팅 디바이스상의 관리 브라우저로부터의 요청이 애플리케이션 스토어에서 수신될 수 있는 단계(1405)에서 시작할 수 있다. 예를들어, 단계(1405)에서, 애플리케이션 스토어를 제공할 수 있고 그리고/또는 기업 애플리케이션 스토어를 제공하도록 구성되는 서버 컴퓨팅 디바이스와 같은 애플리케이션 스토어로 구성될 수 있는 컴퓨팅 디바이스는 애플리케이션 스토어의 특정 부분, 예를들어 특정 애플리케이션들 및/또는 특정 타입들의 애플

리케이션들과 연관된 애플리케이션 스토어의 부분에 액세스하기 위한 요청을 사용자 컴퓨팅 디바이스상의 관리 브라우저로부터 수신할 수 있다.

[0184] [00199] 단계(1410)에서는 하나 이상의 정책들이 관리 브라우저에 적용되는 관리 모드에서 관리 브라우저가 동작중인지의 여부가 애플리케이션 스토어에 의해 결정될 수 있으며, 여기서 하나 이상의 정책들은 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성된다. 예를들어, 단계(1410)에서, 컴퓨팅 디바이스는 사용자 컴퓨팅 디바이스상에서 실행되는 관리 브라우저가 관리 모드에서 실행중인지의 여부를 결정할 수 있다. 예를들어, 사용자 컴퓨팅 디바이스상의 관리 브라우저는 앞의 예들에서 논의된 관리 브라우저의 관리 모드(들)와 유사하게 관리 모드를 제공하고 그리고/또는 가질 수 있으며, 예를들어 관리 모드에서, 하나 이상의 정책들이 관리 브라우저에 적용된다. 게다가, 애플리케이션 스토어는 자신의 현재의 동작 모드를 결정하기 위하여, 관리 브라우저에 질의하고 그리고/또는 그렇지 않은 경우에 이 관리 브라우저와 정보(예를들어, 사용자 컴퓨팅 디바이스와 연관된 디바이스 상태 정보를 포함할 수 있음)를 교환함으로써, 관리 브라우저가 관리 모드에서 동작중인지의 여부를 결정할 수 있다.

[0185] [00200] 만일 단계(1410)에서 관리 브라우저가 관리 모드에서 동작중임이 결정되면, 단계(1415)에서, 애플리케이션 스토어는 관리 브라우저가 애플리케이션 스토어의 제 1 부분에 액세스하도록 할 수 있다. 예를들어, 단계(1415)에서, 컴퓨팅 디바이스는 애플리케이션 스토어의 제 1 부분에 대한 액세스를 관리 브라우저에 제공할 수 있다 (이는 예를들어 애플리케이션의 제 1 부분과 연관된 정보, 예를들어 특정 애플리케이션들 및/또는 특정 타입들의 애플리케이션들과 연관된 정보를 관리 브라우저에 제공하는 것을 포함할 수 있다). 이러한 방식으로, 사용자 컴퓨팅 디바이스상의 관리 브라우저는 자신이 관리 모드에서 실행중인 동안 애플리케이션 스토어의 특정 부분들, 예를들어 본 예에서는 애플리케이션 스토어의 제 1 부분에 액세스할 수 있으며, 이하에서 예시된 바와 같이, 관리 브라우저는 자신이 관리 모드에서 실행중이지 않을 때 (예를들어, 브라우저가 비관리 모드에서 실행중일 때) 애플리케이션 스토어의 특정 부분들에 액세스하는 것이 가능하지 않을 수 있다.

[0186] [00201] 따라서, 만일 단계(1410)에서 관리 브라우저가 관리 모드에서 동작중이 아니라는 것이 결정되면, 단계(1420)에서, 애플리케이션 스토어는 관리 브라우저가 애플리케이션 스토어의 제 1 부분에 액세스하는 것을 막을 수 있다. 예를들어, 단계(1420)에서, 컴퓨팅 디바이스는 관리 브라우저(및/또는 관리 브라우저가 실행중인 사용자 컴퓨팅 디바이스)가 애플리케이션 스토어의 제 1 부분에 액세스하고 그리고/또는 그렇지 않은 경우에 이 애플리케이션 스토어의 제 1 부분으로부터 정보를 획득하는 것을 막고 그리고/또는 차단할 수 있다.

[0187] [00202] 부가적으로 또는 대안적으로, 단계(1425)에서, 애플리케이션 스토어는 애플리케이션 스토어의 제 1 부분과 상이한 애플리케이션 스토어의 제 2 부분에 대한 액세스를 관리 브라우저에 제공할 수 있다. 예를들어, (단계(1410)에서) 관리 브라우저가 관리 모드에서 동작중이지 않음을 결정한 이후에, 단계(1425)에서, 애플리케이션 스토어는 애플리케이션 스토어의 상이한 부분(예를들어, 관리 브라우저 및/또는 관리 브라우저의 사용자에 의해 원래 요청되었을 수도 있는 부분과 상이한 부분)에 대한 액세스를 관리 브라우저에 제공할 수 있다.

[0188] [00203] 부가적으로 또는 대안적으로, 단계(1430)에서, 애플리케이션 스토어는 관리 브라우저에 커맨드를 송신할 수 있으며, 커맨드는 관리 브라우저가 관리 모드로 들어가도록 구성될 수 있다. 예를들어, (예를들어, 단계(1410)에서) 관리 브라우저가 관리 모드에서 동작중이지 않는다고 결정한 이후에, 단계(1430)에서 애플리케이션 스토어는 관리 브라우저에 이러한 커맨드를 송신할 수 있다. 이러한 커맨드를 송신할 때, 애플리케이션 스토어를 제공하는 컴퓨팅 디바이스는 예를들어 관리 브라우저가 실행중인 사용자 컴퓨팅 디바이스에 데이터를 송신하고 그리고/또는 이 사용자 컴퓨팅 디바이스와 데이터를 교환할 수 있다. 게다가, 비록 애플리케이션 스토어가 이러한 커맨드를 송신할 수 있을지라도, 사용자 컴퓨팅 디바이스상의 관리 브라우저는, 예를들어 사용자 컴퓨팅 디바이스에 대한 하나 이상의 정책들 및/또는 현재 디바이스 상태 정보가, 관리 브라우저가 관리 모드로 들어가는 것을 막는 경우에, 관리 모드로 들어가지 않을 수 있다.

[0189] [00204] 따라서, 단계(1435)에서, 애플리케이션 스토어는 관리 브라우저에 커맨드를 송신한 이후에 관리 브라우저가 관리 모드에서 동작중인지의 여부를 재평가할 수 있다. 예를들어, 단계(1435)에서, 애플리케이션 스토어는 다시 사용자 컴퓨팅 디바이스 및/또는 사용자 컴퓨팅 디바이스상에서 실행되는 관리 브라우저에 질의하며 그리고/또는 그렇지 않은 경우에 이와 데이터를 교환할 수 있다 (이는 사용자 컴퓨팅 디바이스로부터 디바이스 상태 정보를 획득하고 그리고/또는 분석하는 것을 포함할 수 있다).

[0190] [00205] 만일 단계(1435)에서 재평가한 이후에 관리 브라우저가 관리 모드에서 동작중임이 결정되면, 단계(1440)에서, 애플리케이션 스토어는 관리 브라우저가 애플리케이션 스토어의 제 1 부분에 액세스하도록 할 수 있다. 예를들어, 단계(1440)에서, 컴퓨팅 디바이스는 애플리케이션 스토어가 단계(1415)에서 이러한 액세스를

제공할 수 있는 방법과 유사하게, 애플리케이션 스토어의 제 1 부분에 대한 액세스를 관리 브라우저에 제공할 수 있다. 대안적으로, 만일 단계(1435)에서의 재평가 이후에 관리 브라우저가 아직 관리 모드에서 동작중이지 않다고 결정되면, 단계(1445)에서, 애플리케이션 스토어는 통지를 생성하고 그리고/또는 이 통지를 관리 브라우저에 송신할 수 있으며, 이러한 통지는 관리 브라우저가 관리 모드에서 실행되지 않는 동안 애플리케이션 스토어의 제 1 부분에 대한 액세스가 제공될 수 없음을 표시할 수 있다. 예를들어, 단계(1445)에서, 애플리케이션 스토어는, 관리 브라우저의 사용자가 관리 브라우저를 관리 모드로 수동으로 전환하고 그리고/또는 하나 이상의 정책들에 따라 디바이스 상태 정보를 변경할 수 있는 다른 동작들을 취할 수 있다는 기대하에, 관리 브라우저가 관리 모드로 들어가도록 이러한 통지를 관리 브라우저에 송신할 수 있다. 이러한 동작들은 예를들어 관리 브라우저 외에 사용자 컴퓨팅 디바이스상에 있을 수 있는 특정 애플리케이션들을 닫고 그리고/또는 제거하는 것, 디바이스가 현재 위치하고 있는 위치와 상이한 다른 위치로 사용자 컴퓨팅 디바이스를 이동시키는 것 및/또는 디바이스가 현재 연결될 수 있는 현재 네트워크(들)과 다른 하나 이상의 네트워크들에 사용자 컴퓨팅 디바이스를 연결하는 것을 포함할 수 있다.

[0191] [00206] 도 15는 본원에서 논의되는 하나 이상의 예시적인 양상들에 따라 관리 브라우저내에 관리 실행 환경을 제공하는 방법을 예시하는 흐름도를 도시한다. 하나 이상의 실시예들에서, 도 14에 예시된 방법 및/또는 이의 하나 이상의 단계들은 컴퓨팅 디바이스(예를들어, 범용 컴퓨팅 디바이스(201))에 의해 수행될 수 있다. 다른 실시예들에서, 도 14에 예시된 방법 및/또는 이의 하나 이상의 단계들은 비-일시적 컴퓨터-판독가능 메모리와 같은 컴퓨터-판독가능 매체에 저장되는 컴퓨터-실행가능 명령들로 구현될 수 있다.

[0192] [00207] 도 15에서 알 수 있는 바와같이, 방법은 관리 브라우저가 로드될 수 있는 단계(1505)에서 시작할 수 있다. 예를들어, 단계(1505)에서, 컴퓨팅 디바이스(예를들어, 모바일 컴퓨팅 디바이스, 예를들어 랩탑 컴퓨터, 태블릿 컴퓨터, 스마트 폰 또는 다른 타입의 모바일 디바이스)는 이러한 관리 브라우저가 단계(505)에서 로드될 수 있는 방법(앞서 논의됨)과 유사하게 관리 브라우저를 로드할 수 있다. 관리 브라우저는 예를들어 하나 이상의 정책들이 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성될 수 있으며, 하나 이상의 정책들은 앞서 논의된 바와같이 관리 브라우저의 하나 이상의 기능들을 제한하도록 구성될 수 있다. 부가적으로, 일부 실시예들에서, 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성될 수 있다.

[0193] [00208] 단계(1510)에서, 관리 실행 환경은 관리 브라우저내에 제공될 수 있다. 관리 실행 환경은 하나 이상의 웹 애플리케이션들의 실행을 용이하게 하기 위하여 구성될 수 있으며, 관리 실행 환경은 하나 이상의 정책들 중 적어도 하나의 정책을 하나 이상의 웹 애플리케이션들에 적용하도록 추가로 구성될 수 있다. 예를들어, 단계(1510)에서, 컴퓨팅 디바이스는 관리 브라우저내에 관리 실행 환경을 제공할 수 있다. 관리 실행 환경은 예를들어 하나 이상의 웹 애플리케이션들이 실행될 수 있는 쉘로서 동작할 수 있다. 관리 실행 환경에서 실행될 수 있는 웹 애플리케이션들은 예를들어 다양한 상이한 프로그래밍 언어들 (이는 예를들어 관리 실행 환경에서 실행 시간에 컴퓨팅 디바이스에 의해 실행될 때 해석될 수 있음)로 쓰여질 수 있고 그리고/또는 그렇지 않은 경우에 이 다양한 상이한 프로그래밍 언어들을 활용할 수 있다. 부가적으로 또는 대안적으로, 하나 이상의 정책들이 관리 실행 환경내에서 실행되는 웹 애플리케이션들에 적용될 수 있으며, 하나 이상의 정책들은 컴퓨팅 디바이스, 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트, 관리 브라우저 및/또는 관리 실행 환경 그 자체에 의해 정의되고 그리고/또는 이에 의해 부과될 수 있다. 관리 실행 환경내에서 웹 애플리케이션들에 적용되는 정책들은 앞의 예들에서 논의된 정책들과 유사할 수 있으며, 예를들어 디바이스 상태 정보(이는 예를들어 관리 실행 환경을 제공하는 컴퓨팅 디바이스에 대한 디바이스 상태 정보를 포함할 수 있음)에 기초하여 시행될 수 있으며 그리고/또는 그렇지 않은 경우에 디바이스 상태 정보에 의존할 수 있다.

[0194] [00209] 일부 실시예들에서, 관리 실행 환경은 적어도 하나의 HTML5 (HyperText 마크업 언어 5) 애플리케이션의 실행을 용이하게 하도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경내에서 실행될 수 있는 하나 이상의 웹 애플리케이션들 중 적어도 하나의 웹 애플리케이션은 예를들어 HTML5 마크업 언어로 코딩되는 HTML5 애플리케이션일 수 있다.

[0195] [00210] 일부 실시예들에서, 하나 이상의 정책들 중 적어도 하나의 정책은 정책 관리 서버로부터 수신될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경에서 웹 애플리케이션에 적용될 수 있는 하나 이상의 정책들은 정책 관리 서버로부터 수신될 수 있다. 이러한 정책 관리 서버는 예를들어 관리 브라우저내의 관리 실행 환경에서 실행될 수 있는 다양한 웹 애플리케이션들에 적용될 새로운 및/또는 업데이트된 정책들을 제공하기 위하여, 컴퓨팅 디바이스상의 관리 실행 환경과 및/또는 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트 및/또는

관리 브라우저와 직접 통신할 수 있다.

[0196] [00211] 일부 실시예들에서, 적어도 하나의 정책(이는 예를들어 관리 실행 환경내의 하나 이상의 웹 애플리케이션들에 적용될 수 있음)은 하나 이상의 웹 애플리케이션들이 적어도 하나의 로컬 저장 자원에 액세스하는 것을 막도록 구성될 수 있다. 예를들어, 관리 실행 환경에 의해 적용될 수 있는 하나 이상의 정책들에 기초하여 그리고/또는 디바이스 상태 정보(이는, 예를들어 앞서 논의된 예들에서 처럼, 특정 정책들이 시행되는 방법에 영향을 미침)에 기초하여, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 웹 애플리케이션들이 컴퓨팅 디바이스상의 하나 이상의 로컬 자원들에 데이터를 저장하는 것을 막을 수 있다. 부가적으로 또는 대안적으로, 관리 실행 환경에 의해 적용될 수 있는 하나 이상의 정책들에 기초하여 그리고/또는 디바이스 상태 정보에 기초하여, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 웹 애플리케이션들이 국부적으로 저장된 데이터(이는 예를들어 컴퓨팅 디바이스상의 하나 이상의 로컬 자원들에 저장될 수 있음)에 액세스하는 것을 막을 수 있다.

[0197] [00212] 일부 실시예들에서, 적어도 하나의 정책(이는 예를들어 관리 실행 환경내의 하나 이상의 웹 애플리케이션들에 적용될 수 있음)은 하나 이상의 웹 애플리케이션들이 적어도 하나의 로컬 스토리지에 선택적으로 액세스하도록 구성될 수 있다. 예를들어, 관리 실행 환경에 의해 적용될 수 있는 하나 이상의 정책들에 기초하여 그리고/또는 디바이스 상태 정보(이는, 예를들어 앞서 논의된 예들에서 처럼, 특정 정책들이 시행되는 방법에 영향을 미침)에 기초하여, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 특정 웹 애플리케이션들이 컴퓨팅 디바이스상의 하나 이상의 로컬 자원들의 데이터에 액세스하는 것을 허용할 수 있다. 부가적으로 또는 대안적으로, 관리 실행 환경에 의해 적용될 수 있는 하나 이상의 정책들에 기초하여 그리고/또는 디바이스 상태 정보에 기초하여, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 특정 웹 애플리케이션들이 컴퓨팅 디바이스상의 하나 이상의 로컬 자원들에 데이터를 저장하고 그리고/또는 이 하나 이상의 로컬 자원들의 데이터를 수정하는 것을 허용할 수 있다. 일부 경우들에서, 이러한 정책은 하나 이상의 웹 애플리케이션들이 로컬 저장 자원들과 상호작용중인 경우들에서 (예를들어, 로컬 자원들로부터 액세스되고 있고 그리고/또는 로컬 자원들에 저장되고 있는 데이터를 암호화하기 위한) 하나 이상의 암호화 기능들을 활용할 것을 하나 이상의 웹 애플리케이션들에 부가적으로 또는 대안적으로 요구할 수 있다.

[0198] [00213] 일부 실시예들에서, 관리 실행 환경은 컴퓨팅 디바이스상의 정책 관리 에이전트를 하나 이상의 웹 애플리케이션들에 노출시키도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 컴퓨팅 디바이스상에서 실행중인 정책 관리 에이전트(이는 예를들어 앞의 예들에서 논의된 바와같은 MRM 에이전트들일 수 있음)를 관리 실행 환경에서 실행될 수 있는 하나 이상의 웹 애플리케이션들에 노출시킬 수 있다. 이러한 방식으로 정책 관리 에이전트를 웹 애플리케이션들에 노출시킴으로써, 관리 실행 환경은 정책 관리 기능들, 보안 키 관리 기능들 및/또는 다른 기능들을 관리 실행 환경 및/또는 관리 실행 환경의 웹 애플리케이션으로 확장시키는 것이 가능할 수 있다.

[0199] [00214] 일부 실시예들에서, 관리 실행 환경은 하나 이상의 기능들을 애플리케이션 프로그래밍 인터페이스를 통해 하나 이상의 웹 애플리케이션들에 노출시키도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 하나 이상의 기능들을 하나 이상의 인터페이스들을 통해 하나 이상의 웹 애플리케이션들에 노출시킬 수 있으며, 하나 이상의 인터페이스들은 이러한 웹 애플리케이션이 다른 웹 애플리케이션들에 의해 제공될 수 있는 것보다 고레벨의 기능들을 제공하도록 할 수 있다. 예를들어, 노출된 기능들은 관리 실행 환경의 웹 애플리케이션이, 암호화 기능들, 보안 터널링 기능들, 보안 데이터 저장 기능들, 정책 관리 기능들 및/또는 예를들어 컴퓨팅 디바이스상에서 실행되는 MRM 에이전트와 같이 컴퓨팅 디바이스상에 실행되는 다른 애플리케이션들 및/또는 서비스들에 의해 제공될 수 있는 다른 기능들을 활용하도록 할 수 있다.

[0200] [00215] 일부 실시예들에서, 관리 실행 환경은 하나 이상의 웹 애플리케이션들에 대한 인증 서비스를 제공하도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경 및/또는 관리 브라우저내에 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경에서 하나 이상의 웹 애플리케이션들에 대한 인증 서비스를 제공할 수 있다. 이러한 인증 서비스를 제공할 때, 관리 실행 환경 및/또는 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 예를들어 웹 애플리케이션에 대한 멀티-팩터 인증 프로세스(multi-factor authentication process)들을 처리할 수 있으며, 이 멀티-팩터 인증 프로세스들은 크리덴셜들을 획득하는 것, 키들을 유지하는 것 및/또는 특정 환경들에서 다양한 핸드셰이크(handshake)들을 용이하게 하기 위한 크리덴셜들 및/또는 키들을 제공하는 것

을 포함할 수 있다. 일부 경우들에서, 이러한 멀티-팩트 인증 프로세스들을 처리함으로써, 관리 실행 환경 및/또는 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 특정 웹 애플리케이션 내의 하나 이상의 특정 기능들의 실행을 인에이블하고 그리고/또는 웹 애플리케이션 그 자체의 실행을 인에이블할 수 있다.

[0201] [00216] 일부 실시예들에서, 관리 실행 환경은 하나 이상의 웹 애플리케이션들에 정책들의 디폴트 세트를 적용하도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경 및/또는 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 특정 웹 애플리케이션들에 정책들의 디폴트 세트 또는 "정책 번들(policy bundle)을 적용할 수 있다. 정책들의 디폴트 세트는 예를들어 정책 관리 서버로부터 수신되고 그리고/또는 이 정책 관리 서버에 의해 주기적으로 업데이트될 수 있다. 게다가, 정책들의 디폴트 세트는 정책들의 상이한 세트 및/또는 맞춤 세트가 웹 애플리케이션에 대하여 정의되지 않으면 관리 실행 환경의 특정 웹 애플리케이션에 적용될 수 있다.

[0202] [00217] 일부 실시예들에서, 관리 실행 환경은 하나 이상의 웹 애플리케이션들에 적용되는 정책들의 세트를 동적으로 업데이트하도록 구성될 수 있다. 예를들어, 일부 경우들에서, 관리 실행 환경 및/또는 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 디바이스의 현재 사용 콘텍스트에 기초하여 관리 실행 환경의 동작을 실시간으로 변경시키기 위하여, 디바이스 상태 정보 및/또는 사용자 정보(이는 예를들어 사용자 역할 정보를 포함할 수 있음)에 기초하여 관리 실행 환경의 특정 웹 애플리케이션에 적용되는 정책들을 동적으로 업데이트하고 그리고/또는 그렇지 않은 경우에 재빠르게 수정할 수 있다. 예를들어, 디바이스 상태 정보(이는 예를들어 다른 애플리케이션들이 사용자 컴퓨팅 디바이스상에서 어떻게 실행되고 있는지, 어떻게 설치되어 있는지 그리고/또는 그렇지 않은 경우에 어떻게 존재하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어디에 위치하는지에 대한 정보; 사용자 컴퓨팅 디바이스가 어떤 네트워크들에 연결되어 있는지에 대한 정보 등을 포함할 수 있음)에 기초하여, 관리 실행 환경 및/또는 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 웹 애플리케이션들에 적용될 수 있는 하나 이상의 정책들을 선택적으로 인에이블하고 그리고/또는 선택적으로 디스에이블할 수 있다. 다른 예로서, 사용자 정보의 변경(이는 예를들어, 사용자가 계정들을 전환한 결과로서 및/또는 다른 사용자가 디바이스에 로그인한 결과로서 발생할 수 있음)에 기초하여, 관리 실행 환경 및/또는 관리 실행 환경을 제공하는 컴퓨팅 디바이스는 관리 실행 환경의 하나 이상의 웹 애플리케이션들에 적용될 수 있는 하나 이상의 정책들을 선택적으로 인에이블하고 그리고/또는 선택적으로 디스에이블할 수 있다. 이러한 방식으로, 관리 실행 환경은 관리 실행 환경내에 존재하고 그리고/또는 관리 실행 환경에서 실행되고 있는 웹 애플리케이션들에 대해 상이한 제어 레벨들이 부과될 것을 요구할 수 있는 변화하는 상태들에 동적으로 적응될 수 있다.

[0203] [00218] 앞서 예시된 바와같이, 개시내용의 다양한 양상들은 모바일 컴퓨팅 디바이스상의 관리 브라우저를 제공하는 것에 관한 것이다. 그러나, 다른 실시예들에서는 본원에서 논의된 개념들이 임의의 다른 타입의 컴퓨팅 디바이스(예를들어, 데스크탑 컴퓨터, 서버, 콘솔, 셋톱 박스 등)에서 구현될 수 있다. 따라서, 비록 요지가 구성적 특징들 및/또는 방법적 동작들에 특정한 언어로 설명되었을지라도, 첨부된 청구항들에서 정의된 요지가 반드시 앞서 설명된 특정 특징들 또는 동작들로 제한되는 것이 아니라는 것이 이해되어야 한다. 오히려, 앞서 설명된 특정 특징들 및 동작들은 하기의 청구항들의 일부 예시적인 구현들로서 설명된다.

[0204] 샘플 실시예들

[0205] 개시내용의 샘플 실시예들은 하기를 포함한다:

[0206] 1. 방법으로서,

[0207] 컴퓨팅 디바이스에 의해 관리 브라우저(managed browser)를 로딩하는 단계 - 상기 관리 브라우저는 하나 이상의 정책(policy)들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0208] 디바이스 클라우드를 개시하기 위한 연결을 상기 컴퓨팅 디바이스에 의해 적어도 하나의 다른 컴퓨팅 디바이스에 설정하는 단계; 및

[0209] 상기 컴퓨팅 디바이스에 의해, 상기 관리 브라우저의 세션을 상기 디바이스 클라우드에 걸쳐 확장하는 단계를 포함하며;

[0210] 상기 관리 브라우저의 세션을 확장하는 단계는,

[0211] 적어도 하나의 다른 관리 브라우저가 상기 적어도 하나의 다른 컴퓨팅 디바이스상에 로딩되는 것을 야기하는 단계, 및

[0212] 상기 적어도 하나의 다른 관리 브라우저와 세션 데이터를 공유하는 단계를 포함하는, 방법.

[0213] 2. 제 1항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원(enterprise resource)으로부터 획득된 데이터의 보안 브라우징(browsing) 및 캐싱(caching)을 제공하도록 구성되는, 방법.

[0214] 3. 제 1항에 있어서, 상기 디바이스 클라우드는 단일 기능을 수행하기 위하여 2개 이상의 컴퓨팅 디바이스들이 서로 결합하여 사용되도록 하는, 방법.

[0215] 4. 제 1항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 상기 디바이스 클라우드를 제한하도록 구성되는, 방법.

[0216] 5. 제 4항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 적어도 하나의 역할(role)을 상기 적어도 하나의 다른 컴퓨팅 디바이스에 할당하도록 구성되는, 방법.

[0217] 6. 제 1항에 있어서, 상기 적어도 하나의 다른 컴퓨팅 디바이스에의 연결은 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여 설정되는, 방법.

[0218] 7. 제 6항에 있어서, 상기 적어도 하나의 정책은 상기 디바이스 클라우드를 개시하는 상기 관리 브라우저의 능력을 제한하는, 방법.

[0219] 8. 제 1항에 있어서, 상기 적어도 하나의 다른 컴퓨팅 디바이스에의 연결을 설정하는 단계는,

[0220] 상기 적어도 하나의 다른 컴퓨팅 디바이스와 연관된 상태 정보를 평가하는 단계; 및

[0221] 평가된 상태 정보에 기초하여, 상기 적어도 하나의 다른 컴퓨팅 디바이스가 상기 디바이스 클라우드에 참여하도록 허용하는 것을 결정하는 단계를 포함하는, 방법.

[0222] 9. 컴퓨팅 디바이스로서,

[0223] 적어도 하나의 프로세서; 및

[0224] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0225] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0226] 관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0227] 디바이스 클라우드를 개시하기 위한 연결을 적어도 하나의 다른 컴퓨팅 디바이스에 설정하며; 그리고

[0228] 상기 관리 브라우저의 세션을 상기 디바이스 클라우드에 걸쳐 확장하도록 하며;

[0229] 상기 관리 브라우저의 세션을 확장하는 것은,

[0230] 적어도 하나의 다른 관리 브라우저가 상기 적어도 하나의 다른 컴퓨팅 디바이스상에 로딩되는 것을 야기하는 것, 및

[0231] 상기 적어도 하나의 다른 관리 브라우저와 세션 데이터를 공유하는 것을 포함하는, 컴퓨팅 디바이스.

[0232] 10. 제 9항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 컴퓨팅 디바이스.

[0233] 11. 제 9항에 있어서, 상기 디바이스 클라우드는 단일 기능을 수행하기 위하여 2개 이상의 컴퓨팅 디바이스들이 서로 결합하여 사용되도록 하는, 컴퓨팅 디바이스.

[0234] 12. 제 9항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 상기 디바이스 클라우드를 제한하도록 구성되는, 컴퓨팅 디바이스.

[0235] 13. 제 12항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 적어도 하나의 역할을 상기 적어도 하나의 다른 컴퓨팅 디바이스에 할당하도록 구성되는, 컴퓨팅 디바이스.

[0236] 14. 제 9항에 있어서, 상기 적어도 하나의 다른 컴퓨팅 디바이스에의 연결은 상기 하나 이상의 정책들 중 적어

도 하나의 정책에 기초하여 설정되는, 컴퓨팅 디바이스.

[0237] 15. 제 14항에 있어서, 상기 적어도 하나의 정책은 상기 디바이스 클라우드를 개시하는 상기 관리 브라우저의 능력을 제한하는, 컴퓨팅 디바이스.

[0238] 16. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0239] 상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

[0240] 관리 브라우저를 로딩하고 – 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 –;

[0241] 디바이스 클라우드를 개시하기 위한 연결을 적어도 하나의 다른 컴퓨팅 디바이스에 설정하며; 그리고

[0242] 상기 관리 브라우저의 세션을 상기 디바이스 클라우드에 걸쳐 확장하도록 하며;

[0243] 상기 관리 브라우저의 세션을 확장하는 것은,

[0244] 적어도 하나의 다른 관리 브라우저가 상기 적어도 하나의 다른 컴퓨팅 디바이스상에 로딩되는 것을 야기하는 것, 및

[0245] 상기 적어도 하나의 다른 관리 브라우저와 세션 데이터를 공유하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0246] 17. 제 16항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0247] 18. 제 16항에 있어서, 상기 디바이스 클라우드는 단일 기능을 수행하기 위하여 2개 이상의 컴퓨팅 디바이스들이 서로 결합하여 사용되도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0248] 19. 제 16항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 상기 디바이스 클라우드를 제한하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0249] 20. 제 19항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 적어도 하나의 역할을 상기 적어도 하나의 다른 컴퓨팅 디바이스에 할당하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0250] 샘플 실시예들

[0251] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0252] 1. 방법으로서,

[0253] 컴퓨팅 디바이스에 의해 관리 브라우저를 로딩하는 단계 – 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 –;

[0254] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 상기 컴퓨팅 디바이스에 의해 수신하는 단계;

[0255] 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 상기 관리 브라우저로부터 상기 하나 이상의 기업 자원들까지 적어도 하나의 애플리케이션 터널을 상기 컴퓨팅 디바이스에 의해 생성하는 단계; 및

[0256] 상기 적어도 하나의 애플리케이션 터널을 통해 상기 하나 이상의 기업 자원들로부터의 기업 데이터를 상기 컴퓨팅 디바이스에 의해 획득하는 단계를 포함하는, 방법.

[0257] 2. 제 1항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 방법.

[0258] 3. 제 1항에 있어서, 상기 적어도 하나의 애플리케이션 터널을 생성하는 단계는,

[0259] 상기 관리 브라우저로부터 제 1 기업 자원까지 제 1 애플리케이션 터널을 생성하는 단계; 및

[0260] 상기 관리 브라우저로부터 제 2 기업 자원까지 제 2 애플리케이션 터널을 생성하는 단계를 포함하며,

[0261] 상기 제 2 기업 자원은 상기 제 1 기업 자원과 상이한, 방법.

[0262] 4. 제 3항에 있어서, 상기 제 1 기업 자원은 제 1 보안 레벨을 가지며, 상기 제 2 기업 자원은 상기 제 1 보안 레벨과 상이한 제 2 보안 레벨을 가지는, 방법.

[0263] 5. 제 1항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 애플리케이션 터널을 생성하기 위한 상기 관리 브라우저의 능력을 선택적으로 제한하도록 구성되는, 방법.

[0264] 6. 제 1항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터의 사용을 제한하도록 구성되는, 방법.

[0265] 7. 제 6항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 디바이스 상태 정보에 의존하는, 방법.

[0266] 8. 컴퓨팅 디바이스로서,

[0267] 적어도 하나의 프로세서; 및

[0268] 컴퓨터-판독 명령들을 저장한 메모리를 포함하며;

[0269] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0270] 관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0271] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하며;

[0272] 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 상기 관리 브라우저로부터 상기 하나 이상의 기업 자원들까지 적어도 하나의 애플리케이션 터널을 생성하며; 그리고

[0273] 상기 적어도 하나의 애플리케이션 터널을 통해 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하도록 하는, 컴퓨팅 디바이스.

[0274] 9. 제 8항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 컴퓨팅 디바이스.

[0275] 10. 제 8항에 있어서, 상기 적어도 하나의 애플리케이션 터널을 생성하는 것은,

[0276] 상기 관리 브라우저로부터 제 1 기업 자원까지 제 1 애플리케이션 터널을 생성하는 것; 및

[0277] 상기 관리 브라우저로부터 제 2 기업 자원까지 제 2 애플리케이션 터널을 생성하는 것을 포함하며,

[0278] 상기 제 2 기업 자원은 상기 제 2 기업 자원과 상이한, 컴퓨팅 디바이스.

[0279] 11. 제 10항에 있어서, 상기 제 1 기업 자원은 제 1 보안 레벨을 가지며, 상기 제 2 기업 자원은 상기 제 1 보안 레벨과 상이한 제 2 보안 레벨을 가지는, 컴퓨팅 디바이스.

[0280] 12. 제 8항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 애플리케이션 터널을 생성하기 위한 상기 관리 브라우저의 능력을 선택적으로 제한하도록 구성되는, 컴퓨팅 디바이스.

[0281] 13. 제 8항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터의 사용을 제한하도록 구성되는, 컴퓨팅 디바이스.

[0282] 14. 제 6항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 디바이스 상태 정보에 의존하는, 컴퓨팅 디바이스.

[0283] 15. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0284] 상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

[0285] 관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0286] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하며;

[0287] 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 상기 관리 브라우저로부터 상기 하나 이상의 기업 자원들까지 적어도 하나의 애플리케이션 터널을 생성하며; 그리고

[0288] 상기 적어도 하나의 애플리케이션 터널을 통해 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0289] 16. 제 15항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0290] 17. 제 15항에 있어서, 상기 적어도 하나의 애플리케이션 터널을 생성하는 것은,

[0291] 상기 관리 브라우저로부터 제 1 기업 자원까지 제 1 애플리케이션 터널을 생성하는 것; 및

[0292] 상기 관리 브라우저로부터 제 2 기업 자원까지 제 2 애플리케이션 터널을 생성하는 것을 포함하며,

[0293] 상기 제 2 기업 자원은 상기 제 1 기업 자원과 상이한, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0294] 18. 제 17항에 있어서, 상기 제 1 기업 자원은 제 1 보안 레벨을 가지며, 상기 제 2 기업 자원은 상기 제 1 보안 레벨과 상이한 제 2 보안 레벨을 가지는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0295] 19. 제 15항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 애플리케이션 터널을 생성하기 위한 상기 관리 브라우저의 능력을 선택적으로 제한하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0296] 20. 제 15항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터의 사용을 제한하도록 구성되는, 컴퓨팅 디바이스.

[0297] 샘플 실시예들

[0298] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0299] 1. 방법으로서,

[0300] 적어도 하나의 서버 컴퓨팅 디바이스에 의해, 하나 이상의 사용자 컴퓨팅 디바이스들 상의 관리 브라우저에 적용될 적어도 하나의 정책을 수신하는 단계 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성됨 -; 및

[0301] 적어도 하나의 수신된 정책에 기초하여 상기 하나 이상의 사용자 컴퓨팅 디바이스들 중 적어도 하나의 사용자 컴퓨팅 디바이스에 적어도 하나의 정책 업데이트를, 상기 적어도 하나의 서버 컴퓨팅 디바이스에 의해 제공하는 단계를 포함하는, 방법.

[0302] 2. 제 1항에 있어서, 상기 적어도 하나의 정책 업데이트는 상기 적어도 하나의 사용자 컴퓨팅 디바이스가 상기 적어도 하나의 사용자 컴퓨팅 디바이스상의 관리 브라우저에 상기 적어도 하나의 수신된 정책을 적용하도록 구성되는, 방법.

[0303] 3. 제 1항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 콘텐츠 필터링 규칙들을 포함하는, 방법.

[0304] 4. 제 1항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 캐싱 규칙들을 포함하는, 방법.

[0305] 5. 제 1항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 플러그인 규칙들을 포함하는, 방법.

[0306] 6. 제 1항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 크리덴셜 관리 규칙들을 포함하는, 방법.

[0307] 7. 제 1항에 있어서, 상기 적어도 하나의 수신된 정책은 디바이스 상태 정보에 기초하여 상기 적어도 하나의 사용자 컴퓨팅 디바이스에 의해 시행되도록 구성되는, 방법.

[0308] 8. 제 1항에 있어서, 상기 적어도 하나의 수신된 정책은 상기 관리 브라우저가 하나 이상의 기준에 기초하여 비-관리 모드로 전환되도록 구성되는 하나 이상의 규칙들을 포함하는, 방법.

[0309] 9. 컴퓨팅 디바이스로서,

[0310] 적어도 하나의 프로세서; 및

[0311] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0312] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0313] 하나 이상의 사용자 컴퓨팅 디바이스들 상의 관리 브라우저에 적용될 적어도 하나의 정책을 수신하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성됨 -; 그리고

[0314] 적어도 하나의 수신된 정책에 기초하여 상기 하나 이상의 사용자 컴퓨팅 디바이스들 중 적어도 하나의 사용자 컴퓨팅 디바이스에 적어도 하나의 정책 업데이트를 제공하도록 하는, 컴퓨팅 디바이스.

[0315] 10. 제 9항에 있어서, 상기 적어도 하나의 정책 업데이트는 상기 적어도 하나의 사용자 컴퓨팅 디바이스가 상기 적어도 하나의 사용자 컴퓨팅 디바이스상의 관리 브라우저에 상기 적어도 하나의 수신된 정책을 적용하도록 구성되는, 컴퓨팅 디바이스.

[0316] 11. 제 9항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 콘텐츠 필터링 규칙들을 포함하는, 컴퓨팅 디바이스.

[0317] 12. 제 9항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 캐싱 규칙들을 포함하는, 컴퓨팅 디바이스.

[0318] 13. 제 9항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 플러그인 규칙들을 포함하는, 컴퓨팅 디바이스.

[0319] 14. 제 9항에 있어서, 상기 적어도 하나의 수신된 정책은 하나 이상의 크리덴셜 관리 규칙들을 포함하는, 컴퓨팅 디바이스.

[0320] 15. 제 9항에 있어서, 상기 적어도 하나의 수신된 정책은 디바이스 상태 정보에 기초하여 상기 적어도 하나의 사용자 컴퓨팅 디바이스에 의해 시행되도록 구성되는, 컴퓨팅 디바이스.

[0321] 16. 제 9항에 있어서, 상기 적어도 하나의 수신된 정책은 상기 관리 브라우저가 하나 이상의 기준에 기초하여 비관리 모드로 전환되도록 구성되는 하나 이상의 규칙들을 포함하는, 컴퓨팅 디바이스.

[0322] 17. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0323] 상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

[0324] 하나 이상의 사용자 컴퓨팅 디바이스들 상의 관리 브라우저에 적용될 적어도 하나의 정책을 수신하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성됨 -; 그리고

[0325] 적어도 하나의 수신된 정책에 기초하여 상기 하나 이상의 사용자 컴퓨팅 디바이스들 중 적어도 하나의 사용자 컴퓨팅 디바이스에 적어도 하나의 정책 업데이트를 제공하도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0326] 18. 제 17항에 있어서, 상기 적어도 하나의 정책 업데이트는 상기 적어도 하나의 사용자 컴퓨팅 디바이스가 상기 적어도 하나의 사용자 컴퓨팅 디바이스상의 관리 브라우저에 상기 적어도 하나의 수신된 정책을 적용하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0327] 19. 제 17항에 있어서, 상기 적어도 하나의 수신된 정책은 디바이스 상태 정보에 기초하여 상기 적어도 하나의 사용자 컴퓨팅 디바이스에 의해 시행되도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0328] 20. 제 17항에 있어서, 상기 적어도 하나의 수신된 정책은 상기 관리 브라우저가 하나 이상의 기준에 기초하여 비관리 모드로 전환되도록 구성되는 하나 이상의 규칙들을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0329] 샘플 실시예들

[0330] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0331] 1. 방법으로서,

[0332] 컴퓨팅 디바이스에 의해 관리 브라우저를 로딩하는 단계 - 상기 관리 브라우저는 하나 이상의 정책들이 상기

관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0333] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들을 액세스하기 위한 요청을 상기 컴퓨팅 디바이스에 의해 수신하는 단계;

[0334] 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터의 기업 데이터를 상기 컴퓨팅 디바이스에 의해 획득하는 단계; 및

[0335] 획득된 기업 데이터를 상기 컴퓨팅 디바이스에 의해 보안 문서 컨테이너에 저장하는 단계를 포함하는, 방법.

[0336] 2. 제 1항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 방법.

[0337] 3. 제 1항에 있어서, 상기 관리 브라우저를 통해 상기 보안 문서 컨테이너에 대한 액세스를 상기 컴퓨팅 디바이스에 의해 제공하는 단계를 더 포함하는, 방법.

[0338] 4. 제 1항에 있어서, 상기 보안 문서 컨테이너로부터의 데이터를 상기 컴퓨팅 디바이스에 의해 선택적으로 지우는 단계를 더 포함하는, 방법.

[0339] 5. 제 4항에 있어서, 상기 보안 문서 컨테이너로부터의 데이터를 선택적으로 지우는 단계는 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 획득된 상기 기업 데이터를 제거하는 단계를 포함하는, 방법.

[0340] 6. 제 4항에 있어서, 상기 데이터는 상기 관리 브라우저가 닫혀질 때 상기 보안 문서 컨테이너로부터 선택적으로 지워지는, 방법.

[0341] 7. 제 4항에 있어서, 상기 데이터는 상기 하나 이상의 정책들에 기초하여 상기 보안 문서 컨테이너로부터 선택적으로 지워지는, 방법.

[0342] 8. 컴퓨팅 디바이스로서,

[0343] 적어도 하나의 프로세서; 및

[0344] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0345] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0346] 관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0347] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들을 액세스하기 위한 요청을 수신하며;

[0348] 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하며; 그리고

[0349] 획득된 기업 데이터를 보안 문서 컨테이너에 저장하도록 하는, 컴퓨팅 디바이스.

[0350] 9. 제 8항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 컴퓨팅 디바이스.

[0351] 10. 제 8항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 관리 브라우저를 통해 상기 보안 문서 컨테이너에 대한 액세스를 제공하도록 하는, 컴퓨팅 디바이스.

[0352] 11. 제 8항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 보안 문서 컨테이너로부터의 데이터를 지우도록 하는, 컴퓨팅 디바이스.

[0353] 12. 제 11항에 있어서, 상기 보안 문서 컨테이너로부터의 데이터를 선택적으로 지우는 것은 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 획득된 상기 기업 데이터를 제거하는 것을 포함하는, 컴퓨팅 디바이스.

[0354] 13. 제 11항에 있어서, 상기 데이터는 상기 관리 브라우저가 닫혀질 때 상기 보안 문서 컨테이너로부터 선택적

으로 지워지는, 컴퓨팅 디바이스.

[0355] 14. 제 11항에 있어서, 상기 데이터는 상기 하나 이상의 정책들에 기초하여 상기 보안 문서 컨테이너로부터 선택적으로 지워지는, 컴퓨팅 디바이스.

[0356] 15. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0357] 상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

[0358] 관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0359] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하며;

[0360] 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 기업 데이터를 획득하며; 그리고

[0361] 획득된 기업 데이터를 보안 문서 컨테이너에 저장하도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0362] 16. 제 15항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0363] 17. 제 15항에 있어서, 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 관리 브라우저를 통해 상기 보안 문서 컨테이너에 대한 액세스를 제공하도록 하는 추가 명령들이 저장된, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0364] 18. 제 15항에 있어서, 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 보안 문서 컨테이너로부터의 데이터를 선택적으로 지우도록 하는 추가 명령들이 저장된, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0365] 19. 제 18항에 있어서, 상기 보안 문서 컨테이너로부터의 데이터를 선택적으로 지우는 것은 상기 요청에 기초하여 상기 하나 이상의 기업 자원들로부터 획득된 상기 기업 데이터를 제거하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0366] 20. 제 18항에 있어서, 상기 데이터는 상기 관리 브라우저가 닫혀질 때 상기 보안 문서 컨테이너로부터 선택적으로 지워지는, 컴퓨팅 디바이스.

[0367] 샘플 실시예들

[0368] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0369] 1. 방법으로서,

[0370] 컴퓨팅 디바이스에 의해 관리 브라우저를 로딩하는 단계 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0371] 적어도 하나의 사용자 계정과 연관된 싱글 사인-온(SSO) 크리덴셜을 상기 컴퓨팅 디바이스에 의해 수신하는 단계;

[0372] 상기 SSO 크리덴셜에 기초하여, 하나 이상의 기업 자원들로부터의 기업 데이터를 상기 컴퓨팅 디바이스에 의해 획득하는 단계; 및

[0373] 상기 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 상기 컴퓨팅 디바이스에 의해 제공하는 단계를 포함하며;

[0374] 상기 SSO 크리덴셜에 기초하여 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하는 상기 단계는,

[0375] 상기 하나 이상의 기업 자원들 중 적어도 하나의 기업 자원으로부터 인증 회답요구를 수신하는 단계;

[0376] 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공해야 하는지의 여부를 결정하는 단계; 및

[0377] 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하는 것을 결정하는 것에 기초하여, 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하는 단계를 포함하는, 방법.

[0378] 2. 제 1항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 방법.

[0379] 3. 제 1항에 있어서, 상기 SSO 크리덴셜은 적어도 2개의 상이한 기업 자원들에 액세스할 때 사용되도록 구성되는 인증 크리덴셜인, 방법.

[0380] 4. 제 1항에 있어서, 상기 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공하는 상기 단계는 상기 SSO 크리덴셜에 기초하여 상기 하나 이상의 정책들 중 적어도 하나의 정책을 시행하는 단계를 포함하는, 방법.

[0381] 5. 제 1항에 있어서, 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하지 않을 것을 결정하는 것에 기초하여, 상기 컴퓨팅 디바이스의 사용자로부터 적어도 하나의 인증 크리덴셜을 수신하도록 구성된 인증 프롬프트를 상기 컴퓨팅 디바이스에 의해 생성하는 단계를 더 포함하는, 방법.

[0382] 6. 제 4항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터에 대한 액세스를 제한하도록 구성되는, 방법.

[0383] 7. 제 4항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책의 시행은 디바이스 상태 정보에 의존하는, 방법.

[0384] 9. 컴퓨팅 디바이스로서,

[0385] 적어도 하나의 프로세서; 및

[0386] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0387] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0388] 관리 브라우저를 로딩하고 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0389] 적어도 하나의 사용자 계정과 연관된 싱글 사인-온(SSO) 크리덴셜을 수신하며;

[0390] 상기 SSO 크리덴셜에 기초하여, 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하며; 그리고

[0391] 상기 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공하도록 하며;

[0392] 상기 SSO 크리덴셜에 기초하여 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하는 것은,

[0393] 상기 하나 이상의 기업 자원들 중 적어도 하나의 기업 자원으로부터 인증 회답요구를 수신하는 것;

[0394] 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공해야 하는지의 여부를 결정하는 것; 및

[0395] 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하는 것을 결정하는 것에 기초하여, 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하는 것을 포함하는, 컴퓨팅 디바이스.

[0396] 9. 제 8항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 컴퓨팅 디바이스.

[0397] 10. 제 8항에 있어서, 상기 SSO 크리덴셜은 적어도 2개의 상이한 기업 자원들에 액세스할 때 사용되도록 구성되는 인증 크리덴셜인, 컴퓨팅 디바이스.

[0398] 11. 제 8항에 있어서, 상기 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공하는 것은 상기 SSO 크리덴셜에 기초하여 상기 하나 이상의 정책들 중 적어도 하나의 정책을 시행하는 것을 포함하는, 컴퓨팅 디바이스.

[0399] 12. 제 8항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하지 않을 것을 결정하는 것에 기

초하여, 상기 컴퓨팅 디바이스의 사용자로부터 적어도 하나의 인증 크리덴셜을 수신하도록 구성된 인증 프롬프트를 생성하도록 하는, 컴퓨팅 디바이스.

[0400] 13. 제 11항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터에 대한 액세스를 제한하도록 구성되는, 컴퓨팅 디바이스.

[0401] 14. 제 11항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책의 시행은 디바이스 상태 정보에 의존하는, 컴퓨팅 디바이스.

[0402] 15. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0403] 상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

[0404] 관리 브라우저를 로딩하고 – 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 –;

[0405] 적어도 하나의 사용자 계정과 연관된 싱글 사인-온(SSO) 크리덴셜을 수신하며;

[0406] 상기 SSO 크리덴셜에 기초하여, 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하며; 그리고

[0407] 상기 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공하도록 하며;

[0408] 상기 SSO 크리덴셜에 기초하여 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하는 것은,

[0409] 상기 하나 이상의 기업 자원들 중 적어도 하나의 기업 자원으로부터 인증 회답요구를 수신하는 것;

[0410] 상기 하나 이상의 정책들 중 적어도 하나의 정책에 기초하여, 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공해야 하는지의 여부를 결정하는 것; 및

[0411] 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하는 것을 결정하는 것에 기초하여, 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0412] 16. 제 15항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0413] 17. 제 15항에 있어서, 상기 SSO 크리덴셜은 적어도 2개의 상이한 기업 자원들에 액세스할 때 사용되도록 구성되는 인증 크리덴셜인, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0414] 18. 제 15항에 있어서, 상기 관리 브라우저를 통해, 획득된 기업 데이터에 대한 액세스를 제공하는 것은 상기 SSO 크리덴셜에 기초하여 상기 하나 이상의 정책들 중 적어도 하나의 정책을 시행하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0415] 19. 제 18항에 있어서, 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 인증 회답요구에 응답하여 상기 적어도 하나의 기업 자원에 상기 SSO 크리덴셜을 제공하지 않을 것을 결정하는 것에 기초하여, 상기 컴퓨팅 디바이스의 사용자로부터 적어도 하나의 인증 크리덴셜을 수신하도록 구성된 인증 프롬프트를 상기 컴퓨팅 디바이스에 의해 생성하도록 하는 추가 명령들이 저장되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0416] 20. 제 18항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 획득된 기업 데이터에 대한 액세스를 제한하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0417] 샘플 실시예들

[0418] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0419] 1. 방법으로서,

[0420] 상기 애플리케이션 스토어의 제 1 부분에 액세스하기 위한 요청을 사용자 컴퓨팅 디바이스상의 관리 브라우저로부터 애플리케이션 스토어에서 수신하는 단계;

[0421] 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 관리 모드에서 상기 관리 브라우저가 동작중인지의 여부를 상기 애플리케이션 스토어에 의해 결정하는 단계 – 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어

도 하나의 기능을 제한하도록 구성됨 -; 및

[0422] 상기 관리 브라우저가 상기 관리 모드에서 동작중임을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하도록 허용하는 단계를 포함하는, 방법.

[0423] 2. 제 1항에 있어서, 상기 관리 브라우저가 상기 관리 모드에서 동작중이 아님을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하는 것을 막는 단계를 더 포함하는, 방법.

[0424] 3. 제 2항에 있어서, 상기 제 1 부분과 상이한, 상기 애플리케이션 스토어의 제 2부분에 대한 액세스를 상기 애플리케이션 스토어에 의해 상기 관리 브라우저에 제공하는 단계를 더 포함하는, 방법.

[0425] 4. 제 1항에 있어서,

[0426] 상기 관리 브라우저가 상기 관리 모드에서 동작중이 아님을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저에 커맨드를 송신하는 단계를 더 포함하며, 상기 커맨드는 상기 관리 브라우저가 상기 관리 모드로 들어가도록 구성되는, 방법.

[0427] 5. 제 4항에 있어서, 상기 커맨드를 상기 관리 브라우저에 송신한 이후에 상기 관리 브라우저가 상기 관리 모드에서 동작중인지의 여부를 상기 애플리케이션 스토어에 의해 재평가하는 단계를 더 포함하는, 방법.

[0428] 6. 제 5항에 있어서, 상기 재평가 이후에, 상기 관리 브라우저가 상기 관리 모드에서 동작중임을 결정한 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하도록 허용하는 단계를 더 포함하는, 방법.

[0429] 7. 제 5항에 있어서, 상기 재평가 이후에, 상기 관리 브라우저가 상기 관리 모드에서 동작중임이 아님을 결정한 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저에 통지를 송신하는 단계를 더 포함하는, 방법.

[0430] 8. 컴퓨팅 디바이스로서,

[0431] 적어도 하나의 프로세서; 및

[0432] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0433] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0434] 상기 애플리케이션 스토어의 제 1 부분에 액세스하기 위한 요청을 사용자 컴퓨팅 디바이스상의 관리 브라우저로부터, 상기 컴퓨팅 디바이스에 의해 제공된 애플리케이션 스토어에서 수신하며;

[0435] 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 관리 모드에서 상기 관리 브라우저가 동작중인지의 여부를 상기 애플리케이션 스토어에 의해 결정하며 - 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -; 그리고

[0436] 상기 관리 브라우저가 상기 관리 모드에서 동작중임을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하게 허용하도록 하는, 컴퓨팅 디바이스.

[0437] 9. 제 8항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 관리 브라우저가 상기 관리 모드에서 동작중이 아님을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하는 것을 막도록 하는, 컴퓨팅 디바이스.

[0438] 10. 제 9항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 제 1 부분과 상이한, 상기 애플리케이션 스토어의 제 2부분에 대한 액세스를 상기 애플리케이션 스토어에 의해 상기 관리 브라우저에 제공하도록 하는, 컴퓨팅 디바이스.

[0439] 11. 제 8항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명

령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 관리 브라우저가 상기 관리 모드에서 동작중이 아님을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저에 커맨드를 송신하도록 하며, 상기 커맨드는 상기 관리 브라우저가 상기 관리 모드로 들어가도록 구성되는, 컴퓨팅 디바이스.

[0440] 12. 제 11항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 커맨드를 상기 관리 브라우저에 송신한 이후에 상기 관리 브라우저가 상기 관리 모드에서 동작중인지의 여부를 상기 애플리케이션 스토어에 의해 재평가하도록 하는, 컴퓨팅 디바이스.

[0441] 13. 제 12항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 재평가 이후에, 상기 관리 브라우저가 상기 관리 모드에서 동작중임을 결정한 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하게 허용하도록 하는, 컴퓨팅 디바이스.

[0442] 14. 제 12항에 있어서, 상기 메모리는 추가 컴퓨터-판독가능 명령들을 저장하며, 상기 추가 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 재평가 이후에, 상기 관리 브라우저가 상기 관리 모드에서 동작중임이 아님을 결정한 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저에 통지를 송신하도록 하는, 컴퓨팅 디바이스.

[0443] 15. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0444] 상기 명령들은, 실행될 때, 컴퓨팅 디바이스로 하여금,

[0445] 상기 애플리케이션 스토어의 제 1 부분에 액세스하기 위한 요청을 사용자 컴퓨팅 디바이스상의 관리 브라우저로부터, 상기 컴퓨팅 디바이스에 의해 제공된 애플리케이션 스토어에서 수신하며;

[0446] 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 관리 모드에서 상기 관리 브라우저가 동작중인지의 여부를 상기 애플리케이션 스토어에 의해 결정하며 – 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 –; 그리고

[0447] 상기 관리 브라우저가 상기 관리 모드에서 동작중임을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하는 것을 허용하도록 하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0448] 16. 제 15항에 있어서, 실행시, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 관리 브라우저가 상기 관리 모드에서 동작중이 아님을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하는 것을 막도록 하는 추가 명령들이 저장된, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0449] 17. 제 16항에 있어서, 실행시, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 제 1 부분과 상이한, 상기 애플리케이션 스토어의 제 2부분에 대한 액세스를 상기 애플리케이션 스토어에 의해 상기 관리 브라우저에 제공하도록 하는 추가 명령들이 저장된, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0450] 18. 제 15항에 있어서, 실행시, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 관리 브라우저가 상기 관리 모드에서 동작중이 아님을 결정하는 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저에 커맨드를 송신하도록 하는 추가 명령들이 저장되며, 상기 커맨드는 상기 관리 브라우저가 상기 관리 모드로 들어가도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0451] 19. 제 18항에 있어서, 실행시, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 커맨드를 상기 관리 브라우저에 송신한 이후에 상기 관리 브라우저가 상기 관리 모드에서 동작중인지의 여부를 상기 애플리케이션 스토어에 의해 재평가하도록 하는 추가 명령들이 저장된, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0452] 20. 제 19항에 있어서, 실행시, 상기 컴퓨팅 디바이스로 하여금 추가로, 상기 재평가 이후에, 상기 관리 브라우저가 상기 관리 모드에서 동작중임을 결정한 것에 기초하여, 상기 애플리케이션 스토어에 의해, 상기 관리 브라우저가 상기 애플리케이션 스토어의 제 1 부분에 액세스하게 허용하도록 하는 추가 명령들이 저장된, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0453] 샘플 실시예들

[0454] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0455] 1. 방법으로서,

[0456] 컴퓨팅 디바이스에 의해 관리 브라우저를 로딩하는 단계 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0457] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 상기 컴퓨팅 디바이스에 의해 수신하는 단계;

[0458] 상기 요청에 기초하여, 상기 하나 이상의 기업 자원들로부터의 기업 데이터를 상기 컴퓨팅 디바이스에 의해 획득하는 단계; 및

[0459] 하나 이상의 정책들에 기초하여, 획득된 기업 데이터를 상기 컴퓨팅 디바이스에 의해 제어하는 단계를 포함하며;

[0460] 상기 획득된 기업 데이터를 제어하는 단계는 상기 컴퓨팅 디바이스상의 적어도 하나의 다른 애플리케이션에 적어도 하나의 정책을 적용하도록 구성되는 모바일 자원 관리(MRM) 에이전트를 사용하여 상기 관리 브라우저를 제어하는 단계를 포함하는, 방법.

[0461] 2. 제 1항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 방법.

[0462] 3. 제 1항에 있어서, 상기 관리 브라우저는 정책 관리 서버로부터 상기 MRM 에이전트에 대한 하나 이상의 정책 업데이트들을 수신하도록 구성되는, 방법.

[0463] 4. 제 1항에 있어서, 상기 획득된 기업 데이터를 제어하는 단계는 상기 관리 브라우저가 비관리 모드에서 동작중일 때 상기 획득된 기업 데이터에 대한 액세스를 선택적으로 차단하는 단계를 포함하는, 방법.

[0464] 5. 제 1항에 있어서, 상기 디바이스 상태 정보는 상기 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보; 상기 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보; 및 상기 컴퓨팅 디바이스의 현재 위치를 식별하는 정보 중 적어도 하나를 포함하는, 방법.

[0465] 6. 제 1항에 있어서, 상기 획득된 기업 데이터를 제어하는 단계는 상기 획득된 기업 데이터에 대한 액세스를 제어하는 단계를 포함하는, 방법.

[0466] 7. 제 6항에 있어서, 상기 획득된 기업 데이터에 대한 액세스를 제어하는 단계는 상기 획득된 기업 데이터의 사용을 제어하는 단계를 포함하는, 방법.

[0467] 8. 컴퓨팅 디바이스로서,

[0468] 적어도 하나의 프로세서; 및

[0469] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0470] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0471] 관리 브라우저를 로딩하며 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0472] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하며;

[0473] 상기 요청에 기초하여, 상기 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하며; 그리고

[0474] 하나 이상의 정책들에 기초하여, 획득된 기업 데이터를 제어하도록 하며;

[0475] 상기 획득된 기업 데이터를 제어하는 것은 상기 컴퓨팅 디바이스상의 적어도 하나의 다른 애플리케이션에 적어도 하나의 정책을 적용하도록 구성되는 모바일 자원 관리(MRM) 에이전트를 사용하여 상기 관리 브라우저를 제어

하는 것을 포함하는, 컴퓨팅 디바이스.

[0476] 9. 제 8항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 컴퓨팅 디바이스.

[0477] 10. 제 8항에 있어서, 상기 관리 브라우저는 정책 관리 서버로부터 상기 MRM 에이전트에 대한 하나 이상의 정책 업데이트들을 수신하도록 구성되는, 컴퓨팅 디바이스.

[0478] 11. 제 8항에 있어서, 상기 획득된 기업 데이터를 제어하는 것은 상기 관리 브라우저가 비관리 모드에서 동작중일 때 상기 획득된 기업 데이터에 대한 액세스를 선택적으로 차단하는 것을 포함하는, 컴퓨팅 디바이스.

[0479] 12. 제 8항에 있어서, 상기 디바이스 상태 정보는 상기 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보; 상기 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보; 및 상기 컴퓨팅 디바이스의 현재 위치를 식별하는 정보 중 적어도 하나를 포함하는, 컴퓨팅 디바이스.

[0480] 13. 제 8항에 있어서, 상기 획득된 기업 데이터를 제어하는 것은 상기 획득된 기업 데이터에 대한 액세스를 제어하는 것을 포함하는, 컴퓨팅 디바이스.

[0481] 14. 제 13항에 있어서, 상기 획득된 기업 데이터에 대한 액세스를 제어하는 것은 상기 획득된 기업 데이터의 사용을 제어하는 것을 포함하는, 컴퓨팅 디바이스.

[0482] 15. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0483] 상기 명령들은, 실행시, 컴퓨팅 디바이스로 하여금,

[0484] 관리 브라우저를 로딩하며 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -;

[0485] 상기 관리 브라우저를 통해 하나 이상의 기업 자원들에 액세스하기 위한 요청을 수신하며;

[0486] 상기 요청에 기초하여, 상기 하나 이상의 기업 자원들로부터의 기업 데이터를 획득하며; 그리고

[0487] 하나 이상의 정책들에 기초하여, 획득된 기업 데이터를 제어하도록 하며;

[0488] 상기 획득된 기업 데이터를 제어하는 것은 상기 컴퓨팅 디바이스상의 적어도 하나의 다른 애플리케이션에 적어도 하나의 정책을 적용하도록 구성되는 모바일 자원 관리(MRM) 에이전트를 사용하여 상기 관리 브라우저를 제어하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0489] 16. 제 15항에 있어서, 상기 관리 브라우저는 적어도 하나의 기업 자원으로부터 획득된 데이터의 보안 브라우징 및 캐싱을 제공하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0490] 17. 제 15항에 있어서, 상기 관리 브라우저는 정책 관리 서버로부터 상기 MRM 에이전트에 대한 하나 이상의 정책 업데이트들을 수신하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0491] 18. 제 15항에 있어서, 상기 획득된 기업 데이터를 제어하는 것은 상기 관리 브라우저가 비관리 모드에서 동작중일 때 상기 획득된 기업 데이터에 대한 액세스를 선택적으로 차단하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0492] 19. 제 15항에 있어서, 상기 디바이스 상태 정보는 상기 컴퓨팅 디바이스상에 존재하는 하나 이상의 애플리케이션들을 식별하는 정보; 상기 컴퓨팅 디바이스에 의해 사용되는 하나 이상의 네트워크 연결들을 식별하는 정보; 및 상기 컴퓨팅 디바이스의 현재 위치를 식별하는 정보 중 적어도 하나를 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0493] 20. 제 15항에 있어서, 상기 획득된 기업 데이터를 제어하는 것은 상기 획득된 기업 데이터에 대한 액세스를 제어하는 것을 포함하는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

[0494] 샘플 실시예들

[0495] 개시내용의 추가 샘플 실시예들은 하기를 포함한다:

[0496] 1. 방법으로서,

[0497] 컴퓨팅 디바이스에 의해 관리 브라우저를 로딩하는 단계 - 상기 관리 브라우저는 하나 이상의 정책들이 상기

관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -; 및

[0498] 상기 컴퓨팅 디바이스에 의해, 상기 관리 브라우저 내에 관리 실행 환경을 제공하는 단계를 포함하며;

[0499] 상기 관리 실행 환경은 하나 이상의 웹 애플리케이션들의 실행을 용이하게 하도록 구성되며; 그리고

[0500] 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 상기 하나 이상의 정책들 중 적어도 하나의 정책을 적용하도록 구성되는, 방법.

[0501] 2. 제 1항에 있어서, 상기 관리 실행 환경은 적어도 하나의 HTML5 애플리케이션의 실행을 용이하게 하도록 구성되는, 방법.

[0502] 3. 제 1항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 정책 관리 서버로부터 수신되는, 방법.

[0503] 4. 제 1항에 있어서, 상기 적어도 하나의 정책은 상기 하나 이상의 웹 애플리케이션들이 적어도 하나의 로컬 저장 자원에 액세스하는 것을 막도록 구성되는, 방법.

[0504] 5. 제 1항에 있어서, 상기 적어도 하나의 정책은 상기 하나 이상의 웹 애플리케이션들이 적어도 하나의 로컬 스토리지에 액세스하는 것을 선택적으로 허용하도록 구성되는, 방법.

[0505] 6. 제 1항에 있어서, 상기 관리 실행 환경은 상기 컴퓨팅 디바이스상의 정책 관리 에이전트를 상기 하나 이상의 웹 애플리케이션들에 노출시키도록 구성되는, 방법.

[0506] 7. 제 1항에 있어서, 상기 관리 실행 환경은 애플리케이션 프로그래밍 인터페이스를 통해 상기 하나 이상의 웹 애플리케이션들에 하나 이상의 기능들을 노출시키도록 구성되는, 방법.

[0507] 8. 제 1항에 있어서, 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 대한 인증 서비스를 제공하도록 구성되는, 방법.

[0508] 9. 제 1항에 있어서, 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 정책들의 디폴트 세트를 적용하도록 구성되는, 방법.

[0509] 10. 제 1항에 있어서, 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 적용된 정책들의 세트를 동적으로 업데이트하도록 구성되는, 방법.

[0510] 11. 컴퓨팅 디바이스로서,

[0511] 적어도 하나의 프로세서; 및

[0512] 컴퓨터-판독가능 명령들을 저장한 메모리를 포함하며;

[0513] 상기 컴퓨터-판독가능 명령들은, 상기 적어도 하나의 프로세서에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

[0514] 관리 브라우저를 로딩하며 - 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 -; 그리고

[0515] 상기 관리 브라우저 내에 관리 실행 환경을 제공하도록 하며;

[0516] 상기 관리 실행 환경은 하나 이상의 웹 애플리케이션들의 실행을 용이하게 하도록 구성되며; 그리고

[0517] 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 상기 하나 이상의 정책들 중 적어도 하나의 정책을 적용하도록 구성되는, 컴퓨팅 디바이스.

[0518] 12. 제 11항에 있어서, 상기 관리 실행 환경은 적어도 하나의 HTML5 애플리케이션의 실행을 용이하게 하도록 구성되는, 컴퓨팅 디바이스.

[0519] 13. 제 11항에 있어서, 상기 하나 이상의 정책들 중 적어도 하나의 정책은 정책 관리 서버로부터 수신되는, 컴퓨팅 디바이스.

[0520] 14. 제 11항에 있어서, 상기 적어도 하나의 정책은 상기 하나 이상의 웹 애플리케이션들이 적어도 하나의 로컬 저장 자원에 액세스하는 것을 막도록 구성되는, 컴퓨팅 디바이스.

[0521] 15. 제 11항에 있어서, 상기 적어도 하나의 정책은 상기 하나 이상의 웹 애플리케이션들이 적어도 하나의 로컬 스토리지에 액세스하는 것을 선택적으로 허용하도록 구성되는, 컴퓨팅 디바이스.

[0522] 16. 제 11항에 있어서, 상기 관리 실행 환경은 상기 컴퓨팅 디바이스상의 정책 관리 에이전트를 상기 하나 이상의 웹 애플리케이션들에 노출시키도록 구성되는, 컴퓨팅 디바이스.

[0523] 17. 제 11항에 있어서, 상기 관리 실행 환경은 애플리케이션 프로그래밍 인터페이스를 통해 상기 하나 이상의 웹 애플리케이션들에 하나 이상의 기능들을 노출시키도록 구성되는, 컴퓨팅 디바이스.

[0524] 18. 제 11항에 있어서, 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 대한 인증 서비스를 제공하도록 구성되는, 컴퓨팅 디바이스.

[0525] 19. 제 11항에 있어서, 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 정책들의 디폴트 세트를 적용하도록 구성되는, 컴퓨팅 디바이스.

[0526] 20. 명령들이 저장된 하나 이상의 비-일시적 컴퓨터-판독가능 매체로서,

[0527] 명령들은, 실행시, 컴퓨팅 디바이스로 하여금,

[0528] 관리 브라우저를 로딩하며 – 상기 관리 브라우저는 하나 이상의 정책들이 상기 관리 브라우저에 적용되는 적어도 하나의 관리 모드를 제공하도록 구성되며, 상기 하나 이상의 정책들은 상기 관리 브라우저의 적어도 하나의 기능을 제한하도록 구성됨 –; 그리고

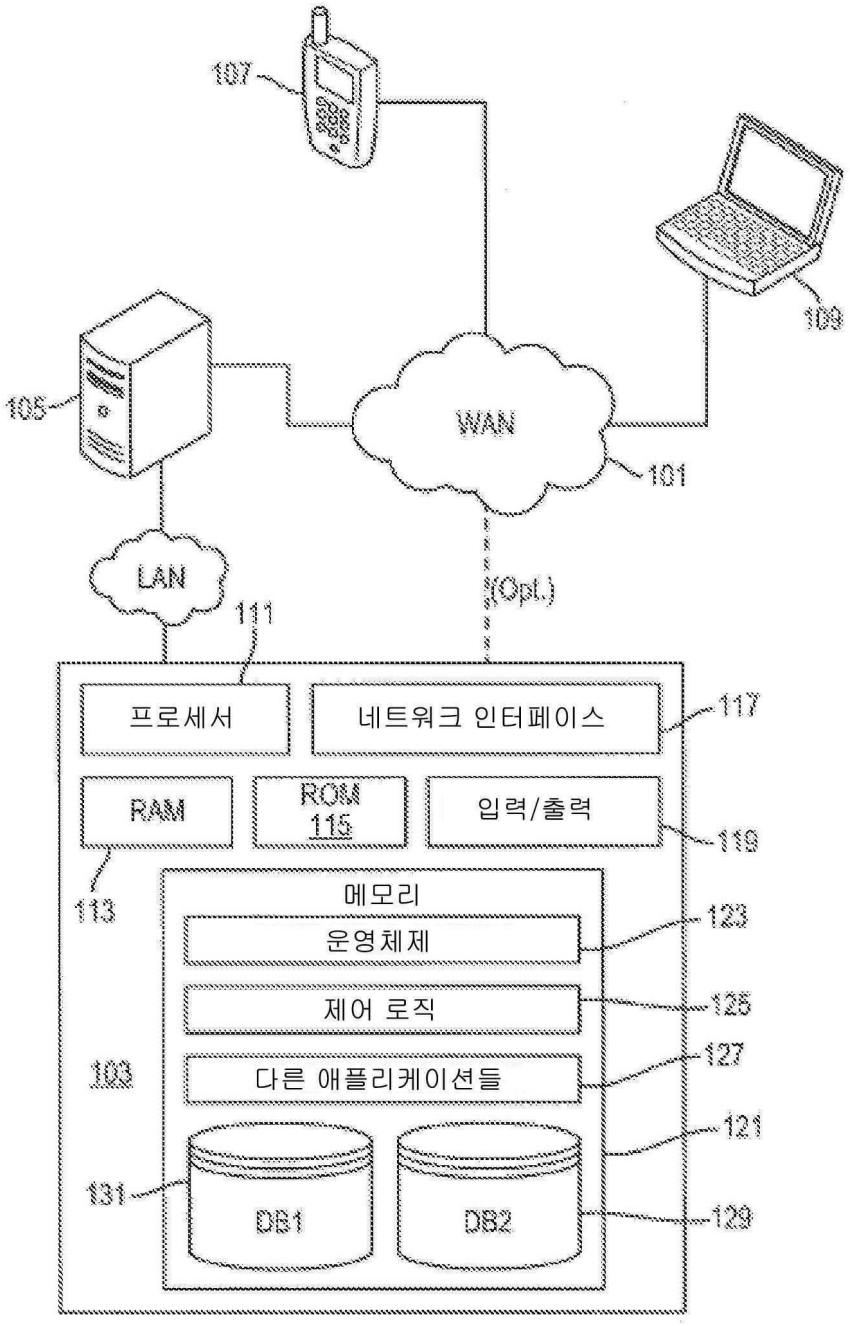
[0529] 상기 관리 브라우저 내에 관리 실행 환경을 제공하도록 하며;

[0530] 상기 관리 실행 환경은 하나 이상의 웹 애플리케이션들의 실행을 용이하게 하도록 구성되며; 그리고

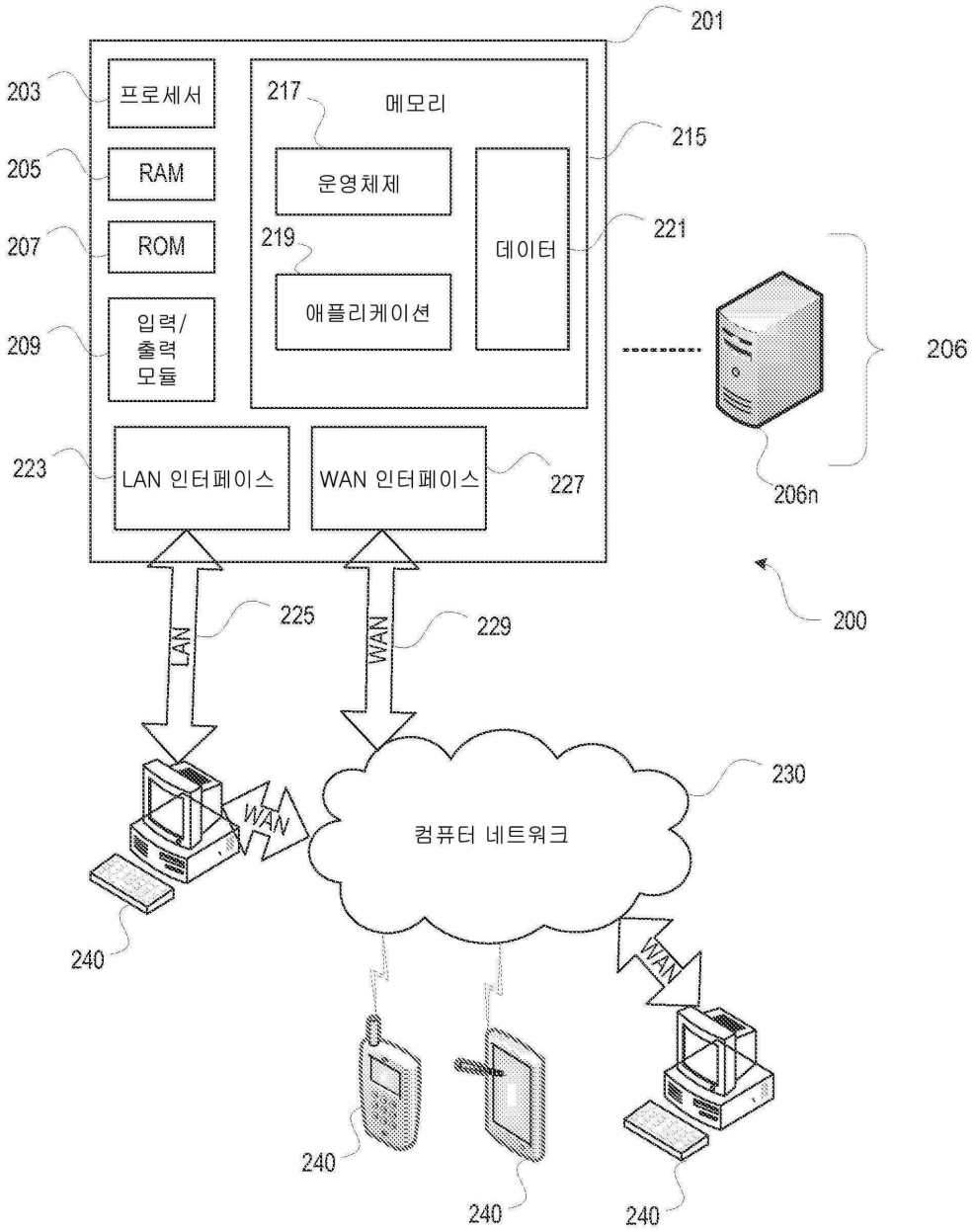
[0531] 상기 관리 실행 환경은 상기 하나 이상의 웹 애플리케이션들에 상기 하나 이상의 정책들 중 적어도 하나의 정책을 적용하도록 구성되는, 하나 이상의 비-일시적 컴퓨터-판독가능 매체.

도면

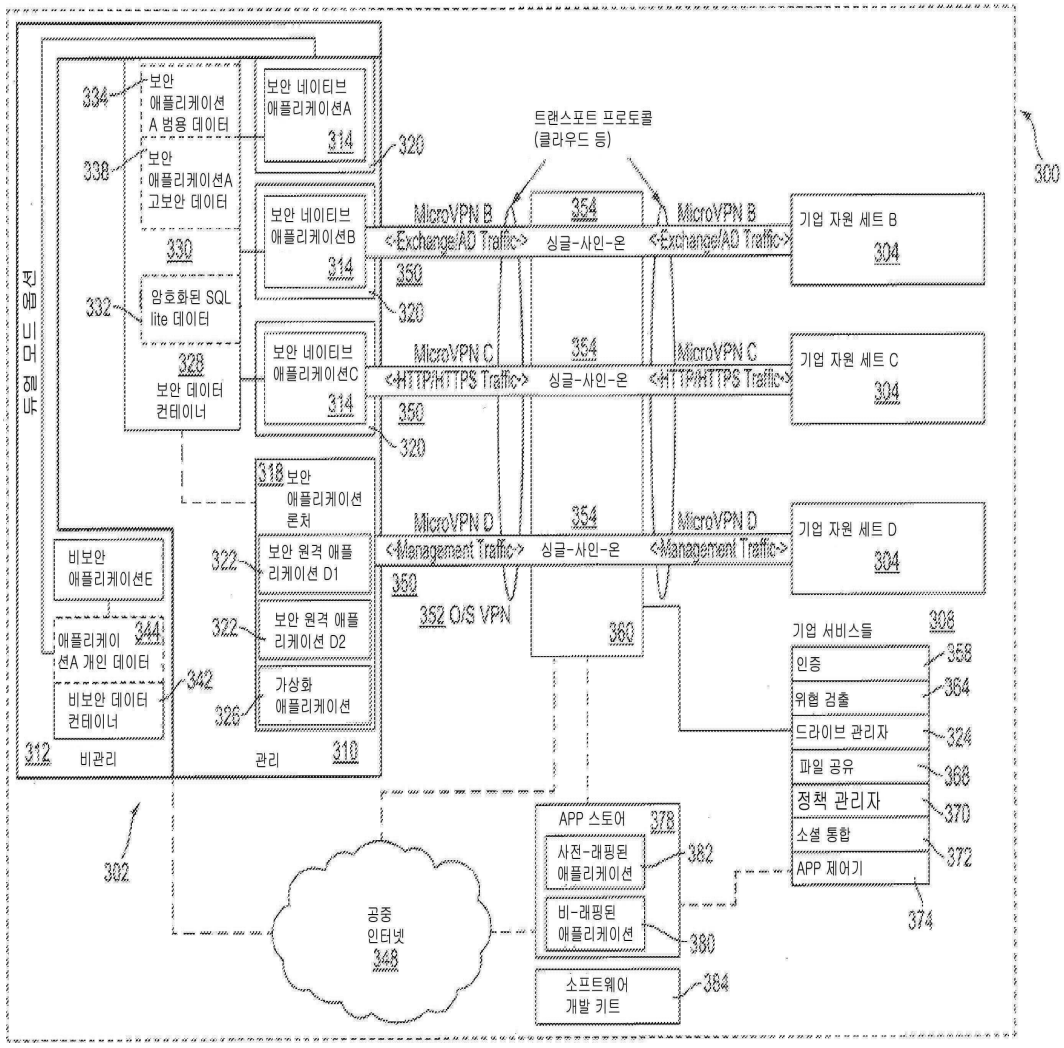
도면1


107
109
105
WAN
101
LAN
111
(Opt.)
프로세서
네트워크 인터페이스
117
RAM
ROM
115
입력/출력
119
113
메모리
운영체제
123
제어 로직
125
103
다른 애플리케이션들
127
121
131
DB1
DB2
129

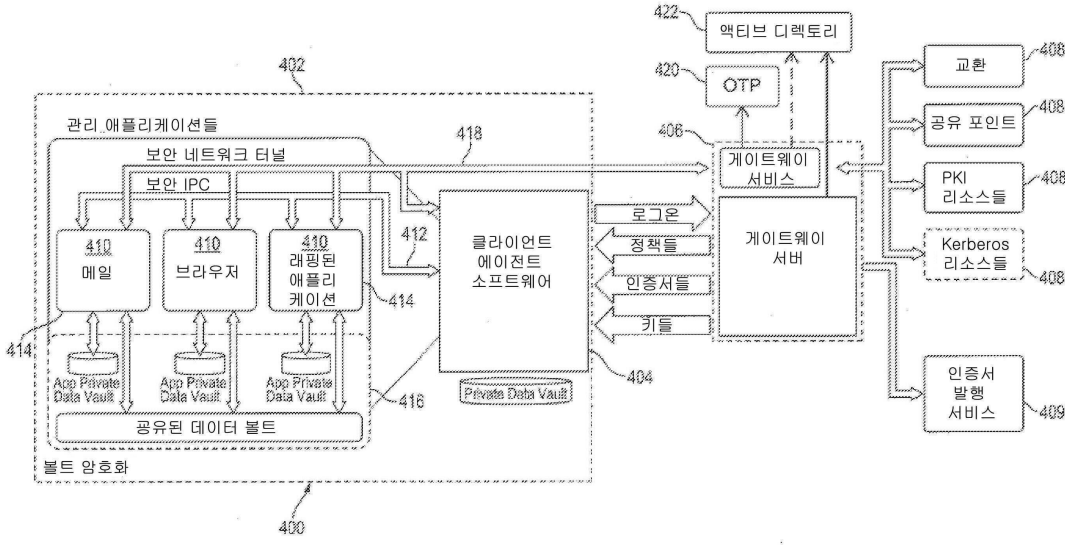
도면2


201
203
프로세서
217
메모리
215
205
RAM
운영체제
207
ROM
219
221
데이터
209
입력/
출력
모듈
애플리케이션
206
206n
223
LAN 인터페이스
WAN 인터페이스
227
200
LAN
225
WAN
229
230
컴퓨터 네트워크
WAN
WAN
240
240
240
240

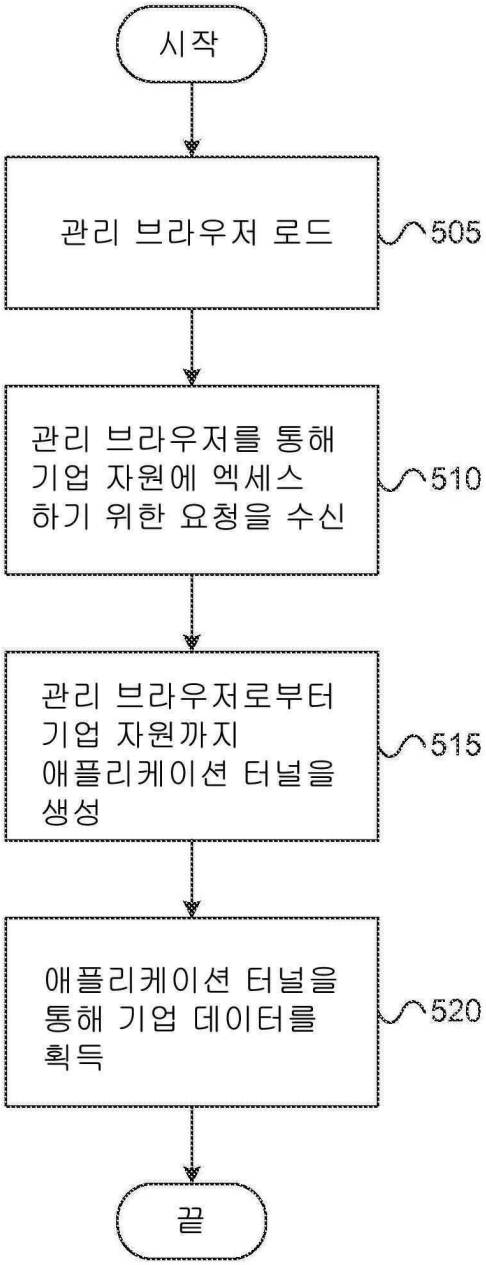
도면3


컨테이너
보안 애플리케이션 A 범용 데이터
334
보안 애플리케이션A 고보안 데이터
338
330
암호화된 SQL lite 데이터
332
328
보안 데이터 컨테이너
보안 네이티브 애플리케이션A
314
320
보안 네이티브 애플리케이션B
314
320
보안 네이티브 애플리케이션C
314
320
318 보안 애플리케이션 론처
보안 원격 애플리케이션 D1
322
보안 원격 애플리케이션 D2
322
가상화 애플리케이션
326
비보안 애플리케이션E
애플리케이션A 개인 데이터
344
342
비보안 데이터 컨테이너
312 비관리
관리 310
302
트랜스포트 프로토콜 (클라우드 등)
300
MicroVPN B
<Exchange/AD Traffic>
354
싱글-사인-온
MicroVPN B
<Exchange/AD Traffic>
기업 자원 세트 B
304
350
320
MicroVPN C
<HTTP/HTTPS Traffic>
354
싱글-사인-온
MicroVPN C
<HTTP/HTTPS Traffic>
기업 자원 세트 C
304
350
320
MicroVPN D
<Management Traffic>
354
싱글-사인-온
MicroVPN D
<Management Traffic>
기업 자원 세트 D
304
350
352 O/S VPN
360
기업 서비스들
308
인증
358
위협 검출
364
드라이브 관리자
324
파일 공유
368
정책 관리자
370
소셜 통합
372
APP 제어기
374
APP 스토어
378
사전-래핑된 애플리케이션
382
비-래핑된 애플리케이션
380
소프트웨어 개발 키트
384
공중 인터넷 348

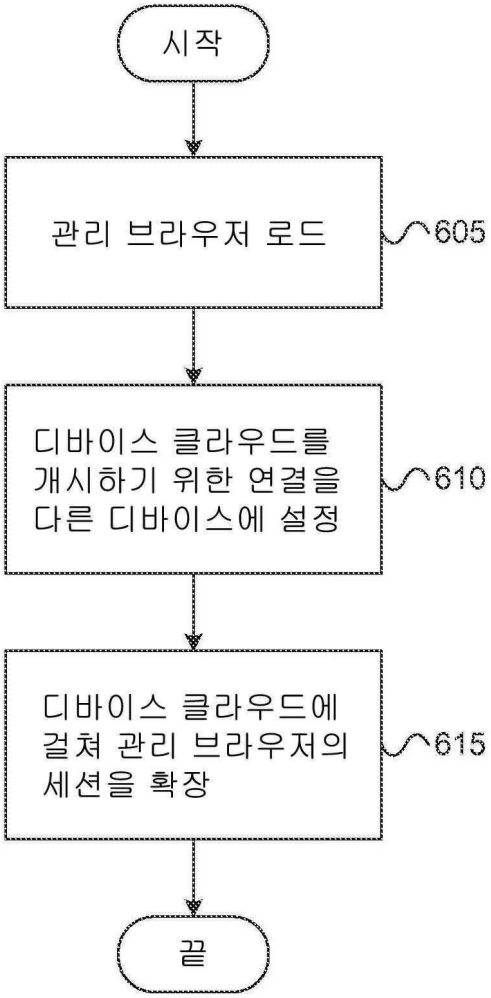
도면4


402
관리 애플리케이션들
보안 네트워크 터널
보안 IPC
418
410 메일
410 브라우저
410 래핑된 애플리케이션
412
414
414
클라이언트 에이전트 소프트웨어
로그온
정책들
인증서들
키들
404
App Private Data Vault
App Private Data Vault
App Private Data Vault
Private Data Vault
416
공유된 데이터 볼트
볼트 암호화
400
422
액티브 디렉토리
420
OTP
406
게이트웨이 서비스
게이트웨이 서버
교환
408
공유 포인트
408
PKI 리소스들
408
Kerberos 리소스들
408
인증서 발행 서비스
409

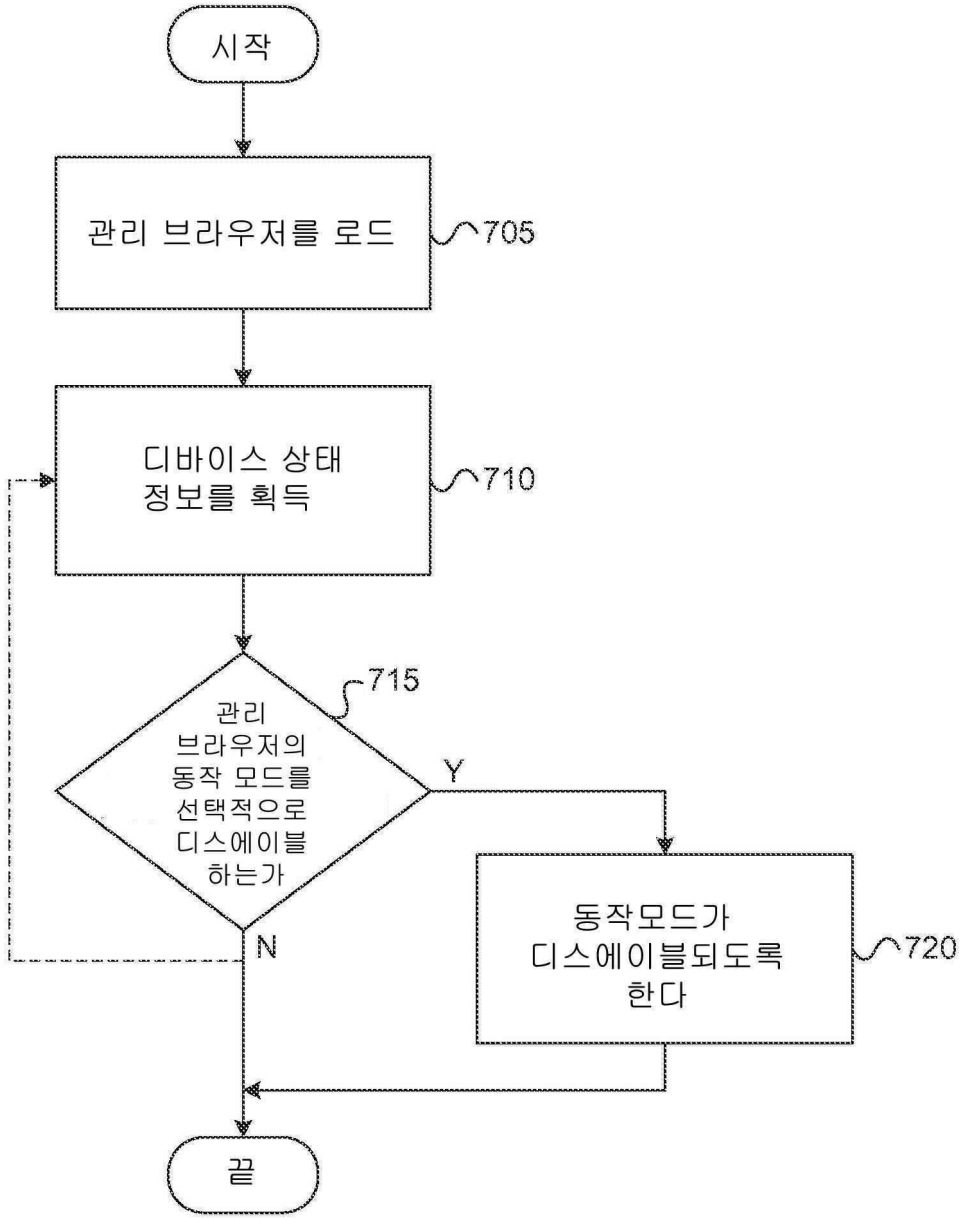
도면5


시작
관리 브라우저 로드
505
관리 브라우저를 통해 기업 자원에 엑세스 하기 위한 요청을 수신
510
관리 브라우저로부터 기업 자원까지 애플리케이션 터널을 생성
515
애플리케이션 터널을 통해 기업 데이터를 획득
520
끝

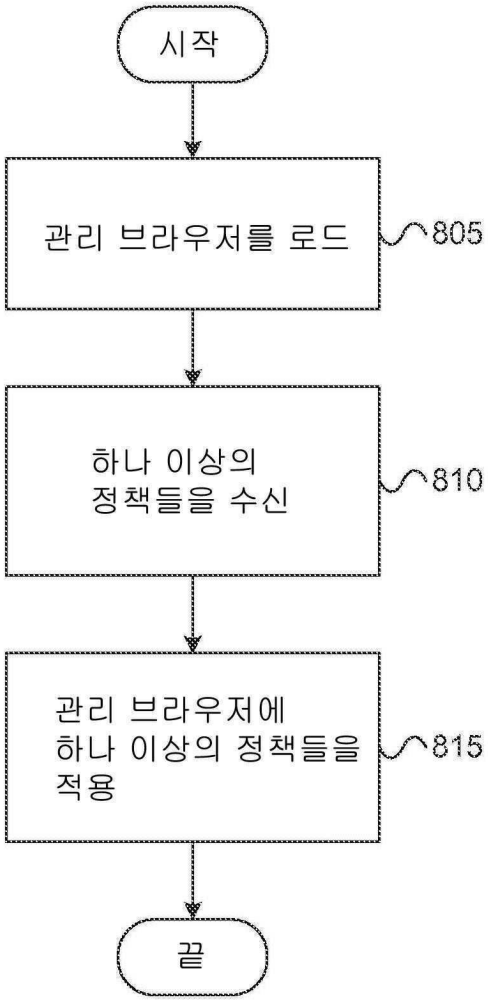
도면6


시작
관리 브라우저 로드
605
디바이스 클라우드를 개시하기 위한 연결을 다른 디바이스에 설정
610
디바이스 클라우드에 걸쳐 관리 브라우저의 세션을 확장
615
끝

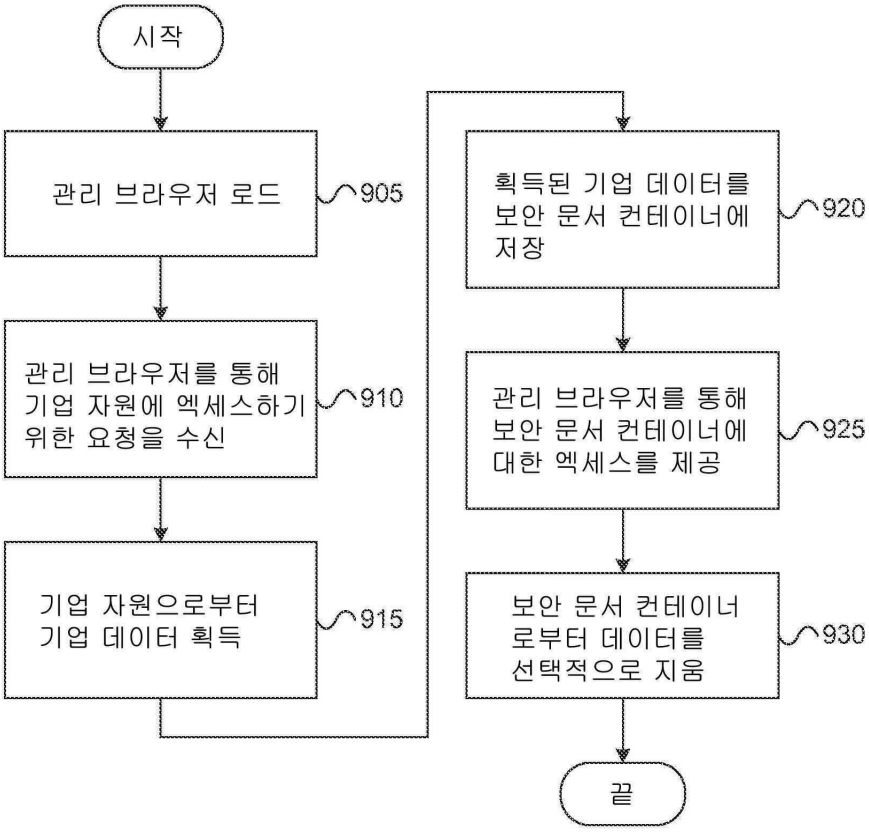
도면7


시작
관리 브라우저를 로드
705
디바이스 상태 정보를 획득
710
715
관리 브라우저의 동작 모드를 선택적으로 디스에이블 하는가
Y
N
동작모드가 디스에이블되도록 한다
720
끝

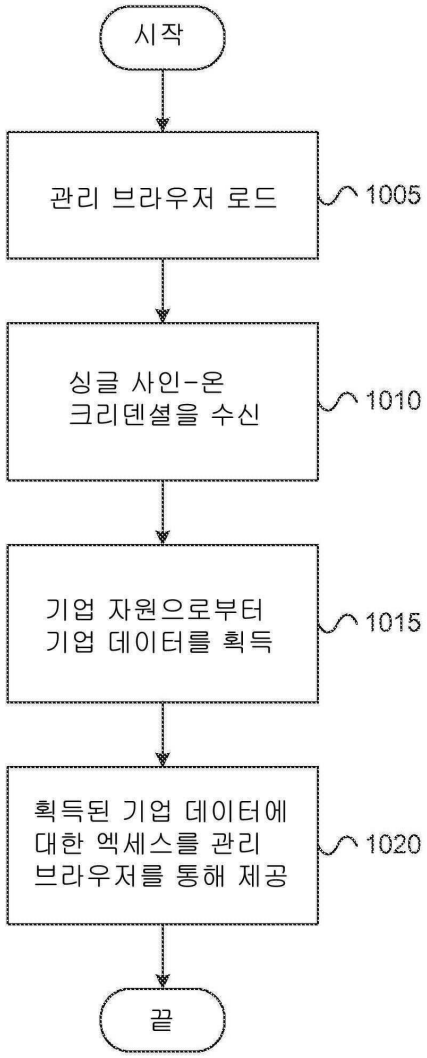
도면8


시작
관리 브라우저를 로드
805
하나 이상의
정책들을 수신
810
관리 브라우저에
하나 이상의 정책들을
적용
815
끝

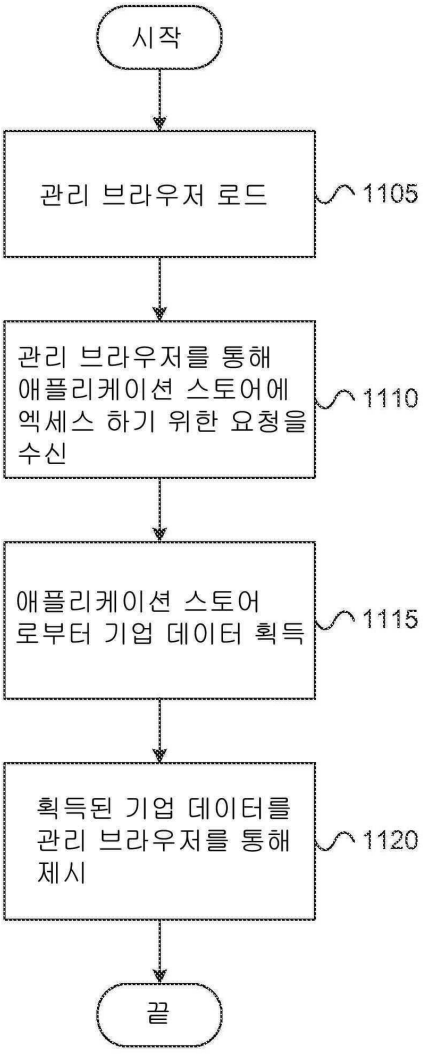
도면9


시작
관리 브라우저 로드
905
관리 브라우저를 통해 기업 자원에 엑세스하기 위한 요청을 수신
910
기업 자원으로부터 기업 데이터 획득
915
획득된 기업 데이터를 보안 문서 컨테이너에 저장
920
관리 브라우저를 통해 보안 문서 컨테이너에 대한 엑세스를 제공
925
보안 문서 컨테이너로부터 데이터를 선택적으로 지움
930
끝

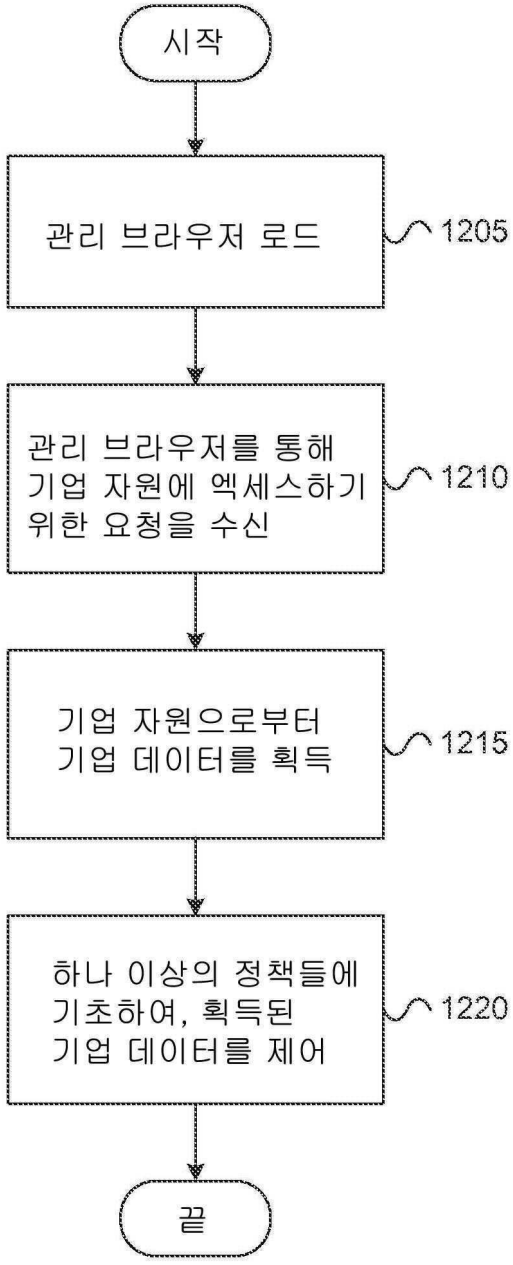
도면10


시작
관리 브라우저 로드
1005
싱글 사인-온
크리덴셜을 수신
1010
기업 자원으로부터
기업 데이터를 획득
1015
획득된 기업 데이터에
대한 엑세스를 관리
브라우저를 통해 제공
1020
끝

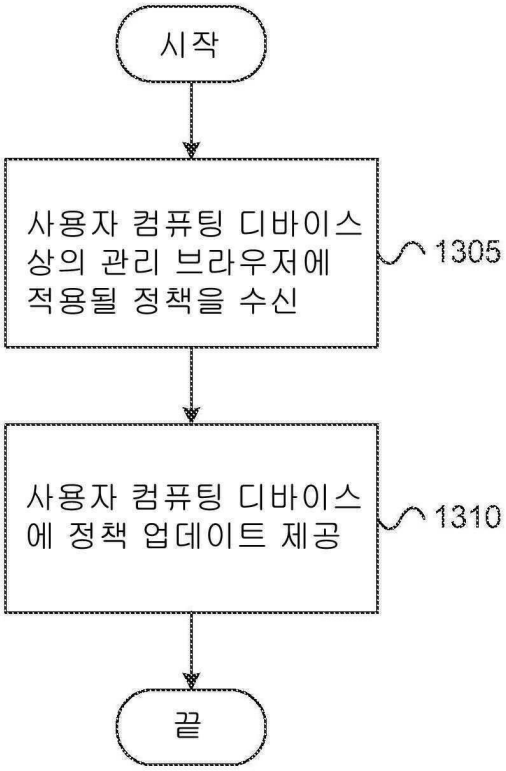
도면11


시작
관리 브라우저 로드
1105
관리 브라우저를 통해 애플리케이션 스토어에 엑세스 하기 위한 요청을 수신
1110
애플리케이션 스토어로부터 기업 데이터 획득
1115
획득된 기업 데이터를 관리 브라우저를 통해 제시
1120
끝

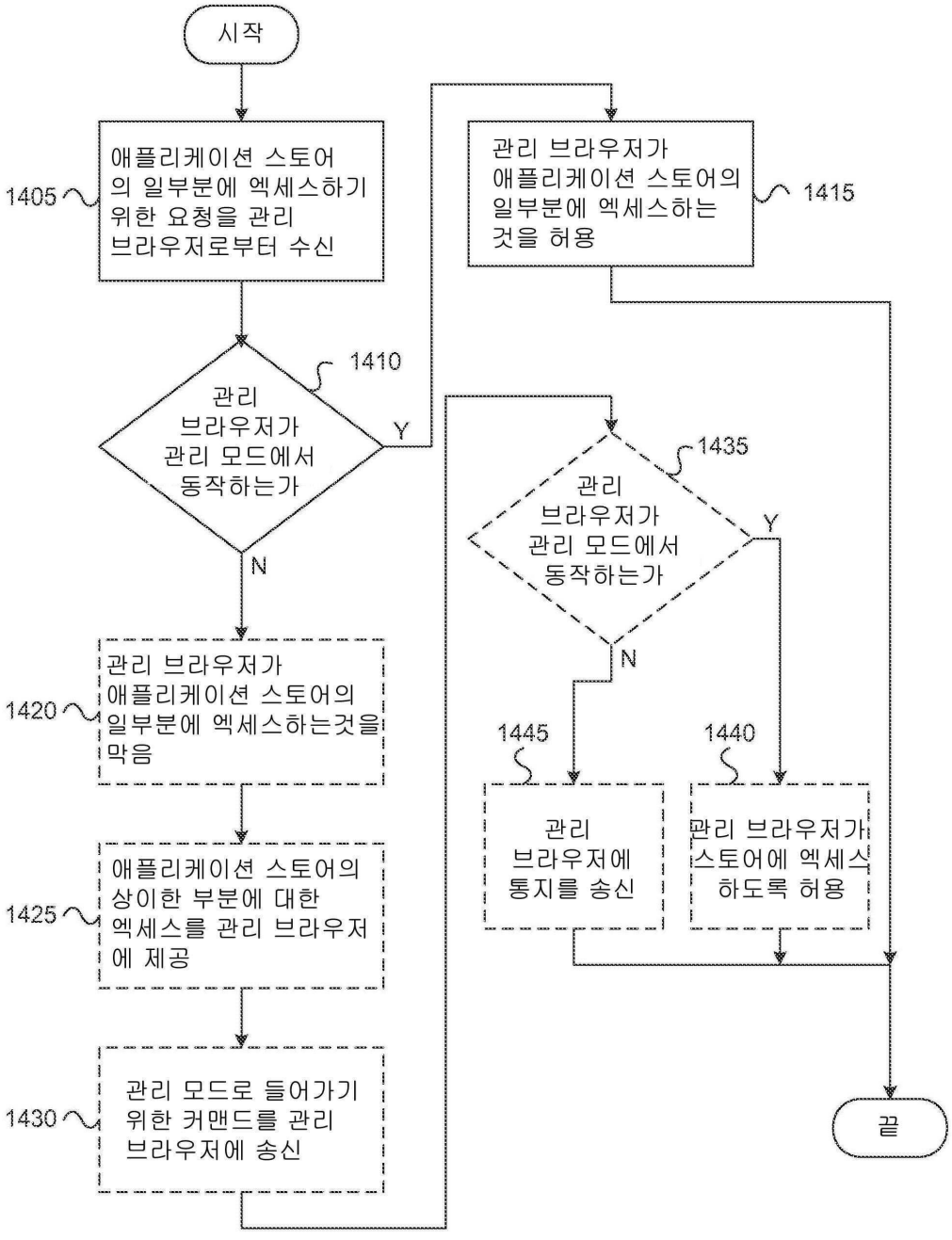
도면12


시작
관리 브라우저 로드
1205
관리 브라우저를 통해 기업 자원에 엑세스하기 위한 요청을 수신
1210
기업 자원으로부터 기업 데이터를 획득
1215
하나 이상의 정책들에 기초하여, 획득된 기업 데이터를 제어
1220
끝

도면13


시작
사용자 컴퓨팅 디바이스 상의 관리 브라우저에 적용될 정책을 수신
1305
사용자 컴퓨팅 디바이스에 정책 업데이트 제공
1310
끝

도면14


시작
애플리케이션 스토어의 일부분에 엑세스하기 위한 요청을 관리 브라우저로부터 수신
1405
관리 브라우저가 애플리케이션 스토어의 일부분에 엑세스하는 것을 허용
1415
관리 브라우저가 관리 모드에서 동작하는가
1410
Y
N
관리 브라우저가 애플리케이션 스토어의 일부분에 엑세스하는것을 막음
1420
애플리케이션 스토어의 상이한 부분에 대한 엑세스를 관리 브라우저에 제공
1425
관리 모드로 들어가기 위한 커맨드를 관리 브라우저에 송신
1430
관리 브라우저가 관리 모드에서 동작하는가
1435
Y
N
관리 브라우저에 통지를 송신
1445
관리 브라우저가 스토어에 엑세스 하도록 허용
1440
끝

도면15