



Windows용 Odyssey 액세스 클라이언트

관리 가이드

**엔터프라이즈 버전
FIPS 버전**

*릴리스 5.0
2009년 2월*

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

부품 번호: 530-028166-01-KO

Copyright Notice

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Copyright © 2008 Juniper Networks, Inc. All rights reserved.
Printed in the USA.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with the instruction manual, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device and may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

U.S. Government Rights

Commercial software and commercial software documentation: This documentation is commercial computer software documentation and the products (whether hardware or software) covered by this documentation are or contain commercial computer software. Government users are subject to the Juniper Networks, Inc. standard end user license agreement and any applicable provisions of the FAR and its supplements. No further rights are granted.

Products (whether hardware or software) covered by, and information contained in, this documentation are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical, biological weapons end uses or end users, whether direct or indirect, are strictly prohibited. Export or re-export to countries subject to U.S. embargo or to entities identified on US export exclusion lists, including, but not limited to, the denied persons and specially designated national lists, is strictly prohibited.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").
2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.
3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
 - a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
 - b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.
 - c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
 - d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 3D-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 3D-day trial period.
 - e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services. The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.
4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.
5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.
7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19; or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>. and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation are and will be in the English language)).

목차

| | |
|---------------------------------------|-----------|
| 서문 | ix |
| 대상 | ix |
| 규칙 | x |
| 설명서 | xi |
| 릴리스 노트 및 제품 설명서 | xii |
| 상황에 맞는 도움말 | xii |
| 기술 지원 요청 | xii |
| 자체 도움말 온라인 도구 및 리소스 | xiii |
| JTAC로 케이스 열기 | xiii |
| 1 장 Odyssey 액세스 클라이언트 관리자 이해 | 1 |
| OAC 네트워크 인증 개요 | 2 |
| OAC 구성 계획 | 3 |
| Odyssey 액세스 클라이언트 관리자 도구 개요 | 5 |
| 연결 설정 | 6 |
| 초기 설정 | 6 |
| 시스템 계정 | 6 |
| 권한 편집기 | 7 |
| 병합 규칙 | 7 |
| 사용자 정의 설치기 | 7 |
| 스크립트 작성기 | 7 |
| PAC 관리자 | 7 |
| 2 장 사용자 계정 구성 | 9 |
| 초기 설정 도구 개요 | 9 |
| 초기 설정을 위한 도구 메뉴 옵션 | 10 |
| 초기 설정을 위한 프로세스 흐름 | 12 |
| 초기 설정 구성 | 13 |
| Windows 로그인 설정 관리 | 14 |
| 기본 Windows 로그인 설정 덮어쓰기 관련 주의 사항 | 14 |
| 로그인 이름 형식 구성 | 15 |
| 사용자 계정의 연결 타이밍 구성 | 17 |
| 구성 설정 테스트 | 17 |
| 시스템 연결 설정 테스트 | 18 |
| 네트워크 어댑터 및 기타 Wi-Fi 지원 프로그램 제어 | 18 |

| | | |
|------------|--|-----------|
| 3 장 | 시스템 계정 구성 | 21 |
| | 시스템 계정 도구 개요..... | 22 |
| | 시스템 계정 설정을 위한 프로세스 흐름..... | 23 |
| | 시스템 계정 연결 활성화..... | 24 |
| | 시스템 계정 설정 구성..... | 24 |
| | 시스템 계정 프로필 옵션..... | 25 |
| 4 장 | 네트워크 연결 실시 시기 및 방법 구성 | 29 |
| | 연결 설정 도구 개요..... | 29 |
| | 연결 설정 구성을 위한 프로세스 흐름..... | 31 |
| | 네트워크 연결 타이밍 정보..... | 32 |
| | 사용자 계정 연결 구성..... | 33 |
| | Windows 로그인 후 데스크톱이 나타나기 전에 연결..... | 33 |
| | Windows 로그인 전에 연결..... | 34 |
| | 시스템 계정 연결 구성..... | 35 |
| | 시스템 계정 연결 설정 구성..... | 36 |
| | 시스템만 연결 구성..... | 36 |
| | 사용자 연결로 전환되는 시스템 연결 구성..... | 36 |
| | GINA를 사용하여 Windows 로그인 전에 연결을 구성..... | 37 |
| | Odyssey GINA 모듈 설치..... | 38 |
| | Odyssey GINA 모듈 제거..... | 38 |
| | 제 3자 GINA 모듈과 Odyssey GINA의 사용..... | 38 |
| | Windows 로그인 시 실행되는 다른 모듈과의 GINA 호환성..... | 38 |
| | 스마트 카드와 GINA 사용..... | 39 |
| 5 장 | 개별 OAC 기능의 권한 설정 | 41 |
| | 권한 설정 개요..... | 41 |
| | 인증 프로토콜..... | 41 |
| | TTLS 내부 인증 프로토콜..... | 42 |
| | TTLS 내부 EAP 프로토콜..... | 42 |
| | PEAP 내부 인증 프로토콜..... | 42 |
| | 프로필 속성..... | 42 |
| | 옵션..... | 42 |
| | 네트워크 속성..... | 42 |
| | Odyssey 제어..... | 42 |
| | 사용자 인터페이스 설정..... | 43 |
| | 사용자 인터페이스—섹션 숨기기..... | 43 |
| | 사용자 인터페이스—섹션 비활성화 및 숨기기..... | 43 |
| | 권한 또는 제약 설정..... | 43 |
| | 권한 편집기 사용 지침..... | 44 |
| 6 장 | 병합 규칙을 사용하여 업데이트 관리 | 47 |
| | 병합 규칙 개요..... | 47 |
| | 병합 규칙 사용 사례..... | 47 |
| | 병합 규칙 설정..... | 48 |
| | 병합 규칙 설정..... | 49 |
| | 프로필을 위한 병합 규칙 설정..... | 49 |
| | 네트워크를 위한 병합 규칙 설정..... | 50 |
| | 개별 네트워크를 위한 병합 규칙 설정..... | 50 |
| | 자동 스캔 목록의 병합 규칙 설정..... | 50 |
| | 인프라넷 컨트롤러의 병합 규칙 설정..... | 51 |

| | | |
|------------|--|-----------|
| | 신뢰의 병합 규칙 설정 | 51 |
| | 기타 탭의 병합 규칙 설정 | 52 |
| 7 장 | 배치 Odyssey 액세스 클라이언트 | 53 |
| | 사용자 정의 설치기 도구 개요 | 53 |
| | 사용자 정의 설치기 도구를 엽니다 | 54 |
| | 배치를 위한 프로세스 흐름 | 55 |
| | 새로운 설치기 파일 만들기 | 56 |
| | 새로운 사용자 정의 설치기 파일 작성을 위한 지침 | 56 |
| | 사용자 정의 업데이트 파일 작성 | 57 |
| | 사용자 계정 설정 업데이트를 위한 프로세스 흐름 | 58 |
| | 사전 구성된 파일 내보내기 | 59 |
| | 자동 설치 옵션 사용 | 60 |
| | 사용자 그룹에 대해 OAC 사전 구성 | 60 |
| | OAC구성 설정 | 60 |
| | 여러 사용자에게 배포할 업데이트 구성 OAC | 61 |
| | 사전 구성된 네트워크 연결의 예외 | 61 |
| | 작업 요약: 시스템 계정에 대한 업데이트 설정 병합 | 62 |
| | 시스템 계정 설정 업데이트를 위한 프로세스 흐름 | 63 |
| | 스크립트를 사용한 OAC 배치 | 64 |
| | 스크립트 작성기 개요 | 64 |
| | 스크립트 생성 | 65 |
| | 스크립트를 사용한 프로필 추가 또는 설정 | 66 |
| | 스크립트를 사용하여 프로필 제거 | 66 |
| | 스크립트를 사용하여 유선 연결을 위한 프로필 활성화 | 66 |
| | 스크립트를 사용한 네트워크 추가 또는 설정 | 67 |
| | 스크립트를 사용하여 구성된 네트워크 제거 | 67 |
| | 스크립트를 사용하여 유선 연결을 위한 네트워크 활성화 | 67 |
| | 스크립트를 사용하여 자동 스캔 목록 추가 또는 설정 | 68 |
| | 스크립트를 사용하여 자동 스캔 목록 제거 | 68 |
| | 스크립트를 사용한 기타 탭의 설정 관리 | 68 |
| | 스크립트를 사용하여 신뢰 트리 추가 또는 설정 | 69 |
| | 스크립트를 사용하여 옵션 설정 대체 | 69 |
| | 스크립트와 SSID를 사용하여 네트워크 제거 | 69 |
| | 스크립트를 사용하여 FIPS 옵션(FE만 해당) 설정 또는 대체 | 70 |
| | 스크립트를 사용하여 증분 업데이트 배치 | 70 |
| | 명령을 사용하여 OAC스크립트 생성 및 로드 | 71 |
| 8 장 | PAC (Protected Access Credentials: 보호 액세스 자격 증명) 관리 | 75 |
| | PAC 관리자 디스플레이 새로고침 | 75 |
| | PAC 삭제 | 75 |
| | PAC 관리자 종료 | 75 |
| 9 장 | 관리 워크플로우 예제 | 77 |
| | TTLS 또는 PEAP용 단일 사인온 | 77 |
| | GINA를 사용하여 Windows 로그인 전에 구성을 구성 | 78 |
| | 사용자 계정 연결 설정 및 OAC GINA 설치 지정 | 78 |
| | Windows 로그인 전에 설정 테스트 | 79 |
| | 색인 | 81 |

서문

이 가이드에서는 Odyssey 액세스 클라이언트 관리자 도구를 사용하여 Odyssey 액세스 클라이언트 (OAC)를 구성 및 업데이트하여 사용자에게 배치하는 방법을 설명합니다. 회사 네트워크에서, OAC는 보호 네트워크로의 인증된 보안 액세스를 제공하기 위해 802.1X 무선 액세스 지점, 802.1X 스위치 및 인프라넷 컨트롤러를 협상합니다. Juniper Networks Steel-Belted Radius와 같은 인증 서버는 각 사용자의 유효성을 검사해야 합니다. Juniper Networks UAC (Unified Access Control) 네트워크에서 사용자의 종점 컴퓨터는 보안 준수 여부를 검사한 후에야 네트워크의 보호 리소스에 액세스하도록 허용됩니다. 802.1X가 활성화된 스위치를 사용한 네트워크에서 스위치는 네트워크 보안 아키텍처의 실행 지점입니다.

이 릴리스는 다음과 같은 두 가지 OAC 라이선스 버전을 지원합니다.

- OAC EE (Enterprise Edition: 엔터프라이즈 버전)
- OAC FIPS (Federal Information Processing Standards: 연방정부 정보처리 표준) 버전(FE)

이 가이드에서는 라이선스 유형을 바탕으로 제품 기능이나 옵션의 차이점을 식별합니다.

Juniper Networks Unified Access Control 보안 솔루션이 포함된 네트워크에 OAC를 배치할 수 있으며 보호된 네트워크 리소스에 대한 인증 액세스를 인프라넷 컨트롤러에서 관리합니다. 인프라넷 컨트롤러가 없고 인증된 액세스를 위해 OAC가 AAA 서버와 직접 협상하는 전통적인 네트워크에도 OAC를 배치할 수 있습니다.

이 가이드는 다음 Juniper Networks 웹 사이트에서 PDF 형식으로 보실 수 있습니다.

<http://www.juniper.net/techpubs/>

대상

이 가이드는 회사 사용자를 위해 보안 유선 및 무선 네트워크 액세스를 관리하는 업무를 맡고 있는 네트워크 관리자를 대상으로 합니다. 특히, OAC 구성 및 사용자에게 배치, EAP 인증 프로토콜 구성, 사용자가 보거나 구성할 수 있는 OAC 기능 구성 등을 담당하는 관리자를 대상으로 합니다.

OAC는 관리자와 개별 사용자가 사용할 수 있는 다양한 구성 옵션과 제어를 제공합니다. 회사 보안 정책 및 Odyssey 액세스 클라이언트 관리자 구성 설정에 따라, 사용자에게 어느 정도의 융통성과 제어를 허용할지를 결정하는 것은 관리자의 몫입니다. OAC 관리를 담당하는 모든 관리자는 OAC 사용 방법과 *Odyssey 액세스 클라이언트 사용자 가이드*에 포함된 정보에 능통해야 합니다. "설명서" (페이지 xi)를 참조하십시오.

이 설명서에 포함된 정보 중 일부는 Juniper Networks UAC (Unified Access Control) 보안 솔루션용 구성 작업과 관련되어 있습니다. OAC를 UAC 네트워크에서 사용하는 경우, 다음 웹 사이트에 있는 *Unified Access Control Administration Guide*를 참조하십시오.

<http://www.juniper.net/techpubs/>

규칙

다음 표는 이 설명서 전체에서 사용되는 규칙을 보여줍니다. 표 1은 공지 아이콘을 정의하고 표 2는 텍스트 규칙을 정의하고 표 3은 CLI 규칙을 정의하며 표 4는 GUI 규칙을 정의합니다.

표 1: 공지 아이콘




| 아이콘 | 의미 | 설명 |
|---|-------|------------------------------------|
|  | 참고 정보 | 중요한 기능이나 지침을 나타냅니다. |
|  | 주의 | 데이터를 잃거나 하드웨어를 손상시킬 위험이 있음을 나타냅니다. |
|  | 경고 | 부상의 위험을 경고합니다. |

표 2: 텍스트 규칙

| 규칙 | 설명 |
|-------------|--|
| 일반 굴림체 | 파일 이름과 디렉터리 이름. |
| <i>이탤릭체</i> | <ul style="list-style-type: none"> ■ 텍스트에 정의된 용어. ■ 사용자가 값을 제공하는 변수 요소. ■ 설명서 제목. |
| + (더하기 기호) | 더하기 기호와 연결된 키 이름은 둘 이상의 키를 동시에 눌러야 함을 나타냅니다. |

표 3: CLI 규칙

| 규칙 | 설명 |
|-------------|---|
| 굵은 글꼴 | 사용자가 입력하는 명령, 명령 이름 및 옵션. |
| 일반 굴림체 | <ul style="list-style-type: none"> ■ 파일 이름과 디렉터리 이름. ■ 코드 및 시스템 출력. |
| <i>이탤릭체</i> | 사용자가 값을 제공하는 변수. |
| [] 대괄호 | 대괄호로 묶인 요소는 선택적 키워드나 변수를 나타냅니다. |
| 파이프 기호 | 파이프 기호로 구분된 요소는 상호 배타적인 키워드나 변수 중 선택함을 나타냅니다. |
| { } 중괄호 | 중괄호로 묶인 요소는 필수 키워드나 변수를 나타냅니다. |

표 4: GUI 규칙

| 규칙 | 설명 |
|-------------|--|
| > (갈매기 표시) | UI의 검색 경로. |
| 굵은 글꼴 | 탭, 버튼, 메뉴 옵션 같이 사용자가 절차 중 선택하는 사용자 인터페이스 요소. |
| <i>이탤릭체</i> | 사용자가 값을 제공하는 변수. |

설명서

표 5는 OAC 및 UAC 설명서 세트와 온라인으로 설명서에 액세스하는 방법을 설명합니다.

표 5: OAC/UAC 설명서 세트

| 제목 | 목적 |
|---|---|
| <i>Odyssey 액세스 클라이언트 퀵 스타트 가이드</i> | 기본 사용자가 OAC를 설치하고 유선 또는 무선 네트워크에 신속하게 연결할 수 있도록 도와줍니다. |
| <i>Odyssey 액세스 클라이언트 사용자 가이드</i> | 기본 및 고급 사용자에게 OAC의 개요를 제공하고 네트워크와 인증 설정 구성에 대한 자세한 설명과 지침을 제공하며 기본적인 문제 해결 방법에 대한 조언을 제공합니다. |
| <i>Odyssey 액세스 클라이언트 관리 가이드</i> | OAC를 계획, 구성하여 여러 사용자에게 배치하는 방법, 사용자 그룹의 요구와 기술 수준에 따라 OAC 옵션에 대한 액세스를 제어하는 방법, 업데이트 관리 방법, 스크립트를 사용하여 업데이트를 배치하는 방법을 설명합니다. |
| <i>Unified Access Control Administration Guide</i> | Juniper Networks Unified Access Control (UAC) 솔루션을 설명하고 구성과 유지 관리 지침을 제공합니다. |
| <i>Unified Access Control Quick Start Guide</i> | 인프라넷 컨트롤러 및 인프라넷 실행기 구성을 위한 기본 작업을 설명합니다. |
| <i>Unified Access Control Client-Side Changes Guide</i> | 설치된 파일과 레지스트리 변경을 포함하여 클라이언트 컴퓨터에서 Odyssey 액세스 클라이언트와 인프라넷 컨트롤러가 수행하는 변경을 설명합니다. |

표 5: OAC/UAC 설명서 세트

| 제목 | 목적 |
|--|--|
| <i>Unified Access Control Custom Sign-in Pages Solutions Guide</i> | 인프라넷 컨트롤러가 사용자와 관리자에게 표시하는 사전 인증 및 로그인 페이지의 모양과 느낌을 개별화하는 방법을 설명합니다. |
| <i>Unified Access Control J.E.D.I. Solutions Guide</i> | 호스트 체커 클라이언트와 서버 API를 통해 솔루션을 작성하고 구현하는 방법을 설명합니다. |
| <i>Unified Access Control Deployment Scenarios Guide</i> | Unified Access Control 솔루션 배포를 위한 권장 사항을 제공합니다. |

릴리스 노트 및 제품 설명서

다음 웹 사이트에서 제품 릴리스 노트, *Odyssey 액세스 클라이언트 쿵 스타트 가이드* 및 *Odyssey 액세스 클라이언트 사용자 가이드*를 보실 수 있습니다.

<http://www.juniper.net/techpubs/>

릴리스 노트는 기능, 변경 사항, 알려진 문제 및 해결된 문제에 대한 최신 정보를 제공합니다. 릴리스 노트의 정보가 설명서 세트에 제공된 정보와 다른 경우, 릴리스 노트를 따르십시오.

상황에 맞는 도움말

Odyssey 액세스 클라이언트 관리자에는 온라인 도움말이 제공되며, Odyssey 액세스 클라이언트 관리자 메뉴 모음의 **도움말 > 도움말 항목**을 통해 액세스할 수 있습니다.

Odyssey 액세스 클라이언트 관리자에 대한 상황에 맞는 도움말을 구하려면 키보드에서 F1을 누르십시오. 표시되는 도움말은 현재 OAC 상황과 관련된 정보를 제공합니다.

기술 지원 요청

기술 제품 지원은 JTAC (Juniper Networks Technical Assistance Center: Juniper Networks 기술 지원 센터)를 통해 받을 수 있습니다. 활성 J-Care 또는 JNASC 지원 계약 고객이거나 보증을 적용 받고 사후 기술 지원이 필요한 경우 도구와 리소스를 온라인으로 액세스하거나 JTAC에 케이스를 열 수 있습니다.

- JTAC 정책—JTAC 절차와 정책의 완전한 이해를 위해 <http://www.juniper.net/customers/support/downloads/710059.pdf>에 있는 *JTAC User Guide*를 검토하십시오.
- 제품 보증—제품 보증 정보를 보려면 <http://www.juniper.net/support/warranty/>를 방문하십시오.
- JTAC 운영 시간—JTAC 센터는 1년 365일 연중 무휴 이용할 수 있습니다.

자체 도움말 온라인 도구 및 리소스

빠르고 쉬운 문제 해결을 위해 Juniper Networks는 다음과 같은 기능을 제공하는 CSC (Customer Support Center: 고객 지원 센터)라는 온라인 자체 서비스 포털을 설계했습니다.

- CSC 서비스 찾기—<http://www.juniper.net/customers/support/>
- 제품 설명서 찾기—<http://www.juniper.net/techpubs/>
- 기술 자료를 사용하여 솔루션과 질문의 답변 찾기—<http://kb.juniper.net/>
- 최신 소프트웨어 버전 다운로드 및 릴리스 노트 검토—
<http://www.juniper.net/customers/csc/software/>
- 기술 게시판에서 관련 하드웨어와 소프트웨어 통지 검색—
<http://www.juniper.net/alerts/>
- Juniper Networks 커뮤니티 포럼 가입 및 참가—
<http://www.juniper.net/company/communities/>
- CSC 케이스 관리자에서 온라인으로 케이스 열기—
<http://www.juniper.net/customers/cm/>
- 제품 일련 번호로 서비스 자격 여부를 확인하려면
<https://tools.juniper.net/SerialNumberEntitlementSearch/>
에서 SNE (Serial Number Entitlement: 일련 번호 권한 부여) 도구를 사용하십시오.

JTAC로 케이스 열기

웹이나 전화를 통해 JTAC로 케이스를 열 수 있습니다.

- <http://www.juniper.net/customers/cm/>의 CSC에서 케이스 관리자 도구를 사용합니다.
- 1-888-314-JTAC로 전화하십시오(미국, 캐나다 및 멕시코의 경우, 무료 전화 1-888-314-5822).

무료 전화 번호가 없는 국가에서 국제 전화 또는 직통 다이얼 옵션을 알아 보려면 <http://www.juniper.net/customers/support/requesting-support/> 페이지를 방문하십시오.

1 장

Odyssey 액세스 클라이언트 관리자 이해

이 항목은 Odyssey 액세스 클라이언트 관리자의 개요로, OAC를 구성 및 업데이트 하여 사용자에게 배치하고, 사용자가 액세스할 수 있는 OAC 기능을 제어하는 데 필요한 도구의 제품군입니다. Odyssey 액세스 클라이언트 관리자는 OAC 관리자 메뉴 모음을 통해 액세스합니다. **도구 > Odyssey 액세스 클라이언트 관리자**를 클릭하십시오.

또한, 보안 네트워크 인증을 위해 필요한 구성 요소 및 프로세스에 대한 설명과, OAC를 구성하여 사용자에게 배치하고자 할 때 고려할 항목이 요약되어 있습니다.

OAC는 802.1X 네트워크 액세스 클라이언트 소프트웨어로, 보안 무선 LAN 액세스에 필요한 EAP (Extensible Authentication Protocols: 확장 가능 인증 프로토콜)에 대한 모든 지원을 제공합니다. Juniper Networks Steel-Belted Radius와 같은 802.1X 호환 RADIUS 서버와 함께 사용하면, OAC는 WLAN 사용자의 인증 및 연결의 보안을 강화하여, 권한이 있는 사용자만 연결할 수 있도록 하며, 로그인 자격 증명의 보안이 위협을 받지 않고, 무선 링크 상에서 데이터 프라이버시가 유지되도록 해줍니다. 또한, OAC는 ID 기반(유선 802.1X) 네트워킹을 배치하는 기업의 클라이언트 역할을 하며, 회사 네트워크, 홈 Wi-Fi 네트워크, 공용 핫스팟 등에 대한 무선 액세스를 제공해 줍니다.

Juniper Networks UAC (Unified Access Control) 솔루션은 사용자 ID와 장치 보안 상태 정보를 네트워크 위치와 조합하여, 각 사용자에게 대한 고유한 액세스 제어 정책을 작성합니다. 이러한 솔루션은 802.1X를 사용하면 레이어 2에서, 오버레이 배치를 사용하면 레이어 3에서 설정할 수 있습니다. UAC는 네트워크 허가 제어에는 802.1X를 사용하고, 리소스 액세스 제어에는 레이어 3을 사용하는 혼합 모드로 제공될 수도 있습니다. 이 솔루션의 중심에는 인프라넷 컨트롤러가 있는데, 이 컨트롤러는 보호된 리소스에 대한 액세스를 허용하기 전에, 사용자 ID와 컴퓨터의 보안 요건 준수 여부를 확인하는 서버입니다. 인프라넷 실행기는 인프라넷 컨트롤러에서 보안 정책을 실행할 수 있도록 해주는 방화벽입니다. 인프라넷 실행기는 인프라넷 컨트롤러와 보호 네트워크 리소스 앞에서 배치됩니다.

OAC 구성 계획

OAC 구성을 계획할 때 다음 질문을 고려하십시오.

- 인증할 대상이 사용자 또는 시스템입니까, 아니면 모두입니까? 여러 사용자를 지원하는 개별 중점을 설정하는 경우, 시스템 인증 사용을 고려해보십시오. 사용하는 방법에 따라, 클라이언트 설정 구성에 필요한 단계의 흐름이 결정됩니다.
- 사용자 데스크톱 인터페이스가 표시되기 전에 클라이언트 시스템이 네트워크에 연결되어야 합니까? 이전에 실행되는 설정 스크립트나 기타 프로세스를 실행해야 하는 경우, 이 기능을 지원하도록 OAC 사용자 계정 설정을 구성할 수 있습니다.
- OAC 구성의 변형이 몇 가지나 필요합니까? 인프라넷 컨트롤러에 구성된 사용자 역할에 따라, OAC를 구성하고 설정을 인프라넷 컨트롤러로 내보내 특정 역할에 이러한 설정을 매핑할 수 있습니다.
- 어떠한 외부 EAP 인증 프로토콜이 필요합니까? UAC 네트워크의 경우에는 TTLS (Tunneled Transport Layer Security: 터널 전송 계층 보안) 또는 PEAP (Protected EAP: 보호된 EAP)를 사용할 수 있으며, 전통적인 네트워크의 경우에는 회사 보안 정책을 확인하거나 네트워크 보안 담당자에게 어떠한 프로토콜이 지원되는지 확인하십시오.
- TTLS 또는 PEAP를 사용하는 경우, 어떠한 내부 인증 프로토콜이 필요합니까? 내부 인증 프로토콜은 TTLS와 같은 터널링 프로토콜에서 제공한 터널 내 통신을 전송 및/또는 수신하는 프로토콜을 말합니다. UAC 네트워크인 경우, JUC (Juniper Networks UAC)를 사용해야 합니다.
- 어떠한 암호화 방법이 사용됩니까? WEP (Wired Equivalent Privacy: 유선 동등 프라이버시), WPA (Wi-Fi Protected Access: Wi-Fi 보호 액세스), WPA2 등, 네트워크에 배치된 액세스 지점과 선택한 연결 모드에 따라 사용 가능한 암호화 방법이 달라집니다. OAC FE (FIPS 버전)를 사용하는 경우, FIPS 모드 선택 여부에 따라 암호화 방법에 특정 제한이 적용됩니다. 네트워크에서 어떠한 방법을 지원하는지 확실치 않은 경우, 네트워크 보안 담당자에게 문의하십시오.
- 사용자가 네트워크 자동 스캔 목록에 액세스하고 업데이트할 수 있도록 허용해야 합니까? 자동 스캔 목록으로 인해, MMA (man-in-the-middle attack: 맨인더미들 공격) 또는 기타 무선 연결을 끌어오도록 설계된 응용 프로그램의 위험이 있을 수 있습니다. 선점 네트워크를 무선 네트워크 구성의 일부로 사용하는 것을 고려해보십시오.
- 무선 네트워크의 경우, 무선 액세스 지점의 SSID (service set identifiers: 서비스 집합 ID)는 무엇이며, 사용자가 이를 브로드캐스트해야 합니까? 무선 네트워크 구성에 사용하는 SSID는 네트워크상의 무선 액세스 지점의 SSID와 일치해야 합니다. SSID가 없으면, OAC에서 무선 네트워크를 감지할 수는 있지만 연결할 수는 없습니다.
- 사용자에게 무선 제거가 유용합니까? 무선 제거를 사용하면 클라이언트에 유선 네트워크 연결이 있는 한 무선 연결이 비활성화됩니다. 일반적으로 유선 연결은 보다 넓은 네트워크 대역폭을 제공하기는 하지만, 무선 연결이 필요한 사용자를 위한 무선 네트워크를 보존합니다.

- 사용자에게 ad hoc 네트워크에 대한 액세스를 허용해야 합니까? ad hoc 네트워크 액세스는 일부 사용자에게는 유용할 수 있지만, 이로 인해 회사 네트워크의 보안 위험이 증대될 수 있습니다.
- 배치 후 구성 설정을 사용자가 수정할 수 있도록 허용해야 합니까? 개별 사용자에게 제공하는 구성 유연성의 정도는 회사 보안 정책과 사용자의 기술적 지식을 반영합니다. 이러한 유연성을 허용함으로써 발생하는 한 가지 장점은 사전 구성된 구성 설정을 변경하지 않고자 하는 많은 사용자에게 대한 제어 및 옵션의 더욱 간단한 집합을 제공할 수 있다는 점입니다. 관리 도구를 사용하면 개별 구성 설정을 숨기고, 비활성화하고, 잠글 수 있습니다.
- 신뢰할 수 있는 서버와 인증서를 사용자가 추가, 제거 또는 수정하도록 허용해야 합니까? Odyssey 액세스 클라이언트 관리자에 표시되지 않도록 신뢰 설정에 대한 액세스를 비활성화함으로써 신뢰 구성 설정을 사용자가 수정하지 못하도록 할 수 있습니다.
- 네트워크에 인프라넷 컨트롤러가 있는 경우, 어떠한 네트워크 프로필 구성 설정을 적용합니까? 사용자가 변경할 수 없도록 이러한 설정을 잠가야 합니까? 각 인프라넷 컨트롤러에는 별도의 프로필이 필요합니다.
- Windows Vista 사용자에게 빠른 사용자 전환 (Fast User Switching)을 허용해야 합니까? 빠른 사용자 전환은 Windows Vista에 활성화되어 있으며, Windows 2000 및 Windows XP에서처럼 도메인 사용자에게 기본적으로 비활성화되어 있지 않습니다.

즉, 주어진 Windows Vista 시스템 상에 모든 동시 사용자 세션에서 네트워크 및 인프라넷 컨트롤러에 대한 현재 데스크톱 연결에 액세스할 수 있음을 의미합니다. 따라서, 한 사용자가 현재 네트워크에 연결되어 있는 경우, 같은 시스템에서 로그인한 다른 사용자들도 같은 네트워크 연결에 액세스할 수 있습니다. 이로 인해 보안 위험이 발생할 수 있습니다. 한 사용자 세션에서 실행되는 백그라운드 프로세스가 다른 세션에 부여된 네트워크 액세스로 함께 전달되어 해당 사용자가 액세스 권한을 가져서는 안 되는 리소스에 액세스할 수 있습니다. Windows Vista 사용자에게는 빠른 사용자 전환을 비활성화하도록 권장합니다.

- 대부분의 사용자에게 대해, OAC 구성을 제한하고 단순화하려면 어떠한 구성이 최적의 구성입니까? 숨겨야 할 옵션 설정과 액세스하지 못하도록 비활성화해야 할 옵션 설정은 무엇입니까?
- 기타 무선 지원 프로그램에 대한 액세스를 허용해야 합니까, 아니면 OAC 사용 실행을 선호합니까? 모든 네트워크 어댑터를 관리하고, 사용자가 OAC를 종료하지 못하도록 OAC를 구성하여, 사용자가 다른 Wi-Fi 지원 프로그램을 사용하지 못하도록 할 수 있습니다.
- 어떠한 방식으로 구성을 배치하고자 합니까?
 - UAC 네트워크에서 사전 구성된 OAC 설정을 만들어 저장하고, ZIP 파일로 저장하여, 인프라넷 컨트롤러에 업로드되도록 할 수 있습니다. 그러면 IC 관리자가 특정 OAC 구성을 특정 역할에 연결하여 사전 구성된 클라이언트를 인프라넷 컨트롤러에서 다운로드할 수 있습니다.
 - 전통적인 네트워크에서는 MSI 파일을 사용하고 스크립트를 업데이트할 수 있습니다.

사용자에 대해 OAC를 구성하기에 앞서 본 가이드와 *Odyssey 액세스 클라이언트 사용자 가이드*를 철저히 검토하여 사용 가능한 옵션에 대해 자세히 파악하십시오.

9 장 "관리 워크플로우 예제"에서는 사용자 단일 로그인 설정과 같이, 일반적인 관리 작업 수행을 위한 워크플로우 시나리오 예제가 제공됩니다.

Odyssey 액세스 클라이언트 관리자 도구 개요

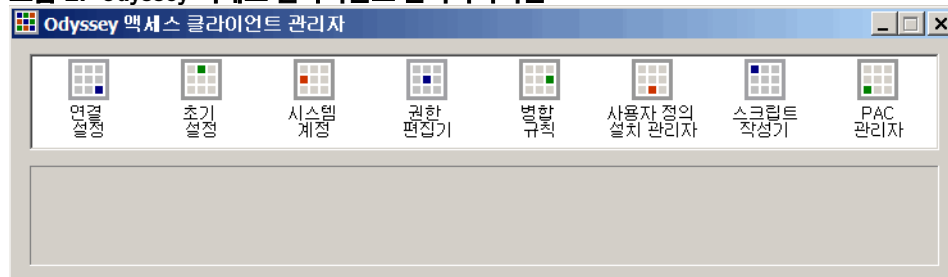
OAC를 사전 구성하고, "푸쉬" 기술 소프트웨어 배치 제품을 사용하여 공통 구성을 여러 사용자에게 배치할 수 있습니다. 이러한 제품은 동시에 여러 사용자에게 소프트웨어를 배포할 때 사용되는 제 3자 제품입니다. 또한, 현재 네트워크 보안 정책을 반영하는 새로운 또는 수정된 구성 설정으로 기존 클라이언트를 업데이트할 수도 있습니다. Odyssey 액세스 클라이언트 관리자 도구를 사용하면 사용자에게 구성된 OAC 클라이언트를 배치하기 전에 개별 OAC 기능을 선택하여 개별 설정을 숨기고, 비활성화하거나 잠글 수 있습니다.

Odyssey 액세스 클라이언트 관리자 도구는 Odyssey 액세스 클라이언트 관리자 관리 인터페이스에 개별 아이콘으로 표시됩니다.

Odyssey 액세스 클라이언트 관리자를 사용하려면, Odyssey 액세스 클라이언트 관리자 메뉴 모음에서 **도구 > Odyssey 액세스 클라이언트 관리자**를 선택합니다. OAC가 설치된 디렉터리에서 `odClientAdministrator.exe` 응용 프로그램을 더블 클릭할 수도 있습니다. 기본 위치는 `C:\Program Files\Juniper Networks\Odyssey Access Client\Odyssey Access Client Manager`입니다.

Odyssey 액세스 클라이언트 관리자를 열면, 페이지 5의 그림 2에 표시된 것처럼 사용 가능한 관리 도구가 아이콘으로 표시됩니다. 도구 중 하나를 열려면 이름 위에 표시된 아이콘을 더블 클릭하십시오.

그림 2: Odyssey 액세스 클라이언트 관리자 아이콘



연결 설정

네트워크 연결이 되는 구체적인 네트워크 연결 시간을 구성하려면 이 도구를 사용합니다. 이러한 연결 설정은 인증이 완료되어 시작 스크립트 실행 등의 프로세스를 수용할 시기를 보다 융통성 있게 제어할 수 있게 해줍니다. 옵션:

- Windows 데스크톱이 나타난 후 네트워크에 연결. 이 연결 유형에는 사용자 로그인 자격 증명이 필요합니다.
- Windows에 로그인한 후 Windows 데스크톱이 나타나기 전에 네트워크에 연결. 이 연결 유형에는 사용자 로그인 자격 증명이 필요합니다.
- Windows 로그인 전에 네트워크에 연결. 이 연결 유형의 경우, OAC GINA (Graphical Identification and Authentication: 그래픽 식별 및 인증) 모듈을 설치해야 합니다. "Windows 로그인 전에 연결" (페이지 34) 및 "Odyssey GINA 모듈 설치" (페이지 38)를 참조하십시오. 이 연결 유형에는 사용자 로그인 자격 증명이 필요합니다.
- Windows 시작 시 시스템 하드웨어 차원에서(사용자 차원이 아니라) 네트워크에 연결. "시스템 계정 연결 구성" (페이지 35)을 참조하십시오.
- GINA를 설치 및 사용. "GINA를 사용하여 Windows 로그인 전에 연결을 구성" (페이지 37)을 참조하십시오.

"연결 설정 구성을 위한 프로세스 흐름" (페이지 31)을 참조하십시오.

초기 설정

사용자 계정 구성을 위해 다음 중 하나 이상의 작업을 수행할 때 이 도구를 사용합니다.

- 사용자 그룹에 대해 OAC 사전 구성. "초기 설정 구성" (페이지 13) 및 "사전 구성된 파일 내보내기" (페이지 59)를 참조하십시오.
- OAC를 배치하기 전에 사용자에게 대해 네트워크 및 인증 프로필을 설정.
- 새로운 사용자 정의 설치기 또는 업데이트 파일을 만들기 전에 사전 구성된 설정을 작성 및 테스트. "시스템 연결 설정 테스트" (페이지 18)을 참조하십시오.
- SIM 카드 및 SIM 카드 PIN 설정 관리. 자세한 내용은 *Odyssey 액세스 클라이언트 사용자 가이드*의 4 장을 참조하십시오.

"초기 설정을 위한 프로세스 흐름" (페이지 12)을 참조하십시오.

시스템 계정

사용자가 아니라 실제 시스템에 대해 인증된 네트워크 연결을 구성할 때 이 도구를 사용합니다. 시스템 계정은 로그인한 사용자가 없을 때 지속적인 네트워크 연결을 제공합니다. "시스템 계정 연결 구성" (페이지 35)을 참조하십시오.

"시스템 계정 설정을 위한 프로세스 흐름" (페이지 23)을 참조하십시오.

권한 편집기

구성에서 OAC 특정 기능을 사용자가 사용 또는 수정할 능력에 대해 사용자 정의된 기능별 제한사항을 적용할 때 이 도구를 사용합니다. 이 도구로 사용자가 변경하지 않기를 원하는 설정을 비활성화하고, Odyssey 액세스 클라이언트 관리자 도구 모음의 보기 메뉴에서 켜도록 선택할 수 있는 일부 기능을 비활성화하는 대신 숨길 수도 있습니다.

병합 규칙

설정 업데이트 파일 또는 새로운 사용자 정의 설치기 파일을 작성하기 위한 규칙을 지정할 때 이 도구를 사용합니다. 병합 규칙에 따라 기존 사용자 구성에 구성 항목을 추가하는 방식이 결정됩니다. 현재 구성을 수정하거나 사용자가 구성을 편집하지 못하도록 하는 규칙을 할당할 수 있습니다. 또한, 이 도구를 사용하여 프로필, 네트워크, 자동 스캔 목록, 인프라넷 컨트롤러 및 기타 설정을 잠가 사용자가 수정할 수 없도록 할 수도 있습니다.

사용자 정의 설치기

Odyssey 액세스 클라이언트 관리자 도구로 구성했던 초기 사용자 또는 시스템 설정에서 사전 구성된 설치기 (MSI) 파일 또는 설정 업데이트 파일을 만들 때 이 도구를 사용합니다. 업그레이드 및 새로운 사용자 설치에 사용자 정의 설치기를 사용합니다. 일단 MSI 파일을 만들고 나면, 다양한 대량 배포 배치 도구를 사용하여 사용자에게 OAC 구성을 배치할 수 있습니다.

또한, 사용자 정의 설치기를 사용하여 기존 시스템 계정(이 경우만 해당) 설정을 업데이트된 구성 설정과 병합할 수도 있습니다.

다음 항목을 참조하십시오.

- "배치를 위한 프로세스 흐름" (페이지 55).
- "사용자 계정 설정 업데이트를 위한 프로세스 흐름" (페이지 58).
- "시스템 계정 설정 업데이트를 위한 프로세스 흐름" (페이지 63).

스크립트 작성기

새로운 설정을 추가하고, 기존 설정을 대체하거나 제거하는 OAC 구성을 업데이트하기 위한 구성 스크립트를 만들 때 이 도구를 사용합니다.

PAC 관리자

EAP-FAST의 PAC (protected access credentials: 보호 액세스 자격 증명)를 관리할 때 이 도구를 사용합니다.

2 장 사용자 계정 구성

하나 이상의 사용자에게 배치할 수 있도록 초기 설정 도구를 사용하여 OAC를 사전 구성합니다. 연결 설정 도구를 사용하여 사용자 계정 연결 타이밍을 구성하기 전에 이러한 설정을 구성합니다. 전용 컴퓨터나 컴퓨터실 시스템을 사용하여 구성 설정을 설정합니다. 사용자 정의 설치기 도구를 사용하여 추후 MSI 설치 파일에 이러한 설정을 저장합니다.

사용자에 대해 OAC를 사전 구성하면, 사용자가 처음으로 OAC를 시작할 때, OAC가 이러한 설정 상태로 열립니다. 사전 구성된 설정이 없는 경우, 네트워크, 프로필 또는 어댑터가 구성되지 않은 Juniper Networks의 기본 구성이 표시됩니다.

초기 설정 도구를 사용하여 사용자 정의 설치기 또는 설정 업데이트 파일의 네트워크 연결을 정의합니다. 이러한 구성 중 하나의 유형에 관한 편집기 도구와 병합 규칙 도구를 고려할 수도 있습니다.

초기 설정 도구에서 선택하는 설정은 권한 편집기 또는 병합 규칙 도구를 사용하여 적용한 규칙에 대한 구성 설정이 됩니다. 마찬가지로, 병합 규칙은 업데이트 파일에 대해 사용자 정의 설치기를 사용하여 배치한 사용자 구성에 적용됩니다. "병합 규칙을 사용하여 업데이트 관리" (페이지 47) 및 "배치를 위한 프로세스 흐름" (페이지 55)을 참조하십시오. 초기 설정 도구는 병합 규칙을 기능에 적용하기 전에 기능을 구성하기 위해 사용할 수 있습니다.

초기 설정 도구 개요

초기 설정 도구는 Odyssey 액세스 클라이언트 관리자와 매우 유사하게 보입니다. 양 보기 모두에서 사이드바가 동일하기 때문에 프로필, 네트워크, 자동 스캔 목록, 신뢰 서버, 어댑터, 인프라넷 컨트롤러 등의 각 설정을 동일한 방식으로 구성할 수 있습니다. 옵션에 약간의 차이가 있긴 하지만, 가장 중요한 차이는 여러 사용자에게 배치하기 위해 사전 구성된 OAC 사본을 만드는 경우, Odyssey 액세스 클라이언트 관리자가 아니라 초기 설정 도구를 사용해야 한다는 점입니다.



참고: FIPS 라이선스가 있는 경우, 파일 메뉴에 FIPS 모드를 설정 및 해제하기 위한 옵션이 표시됩니다.

초기 설정 도구의 도구 메뉴상 옵션은 Odyssey 액세스 클라이언트 관리자 도구 메뉴 상의 옵션과 다릅니다. 초기 설정의 파일 메뉴에는 Odyssey 액세스 클라이언트 관리자에서 사용 가능한 암호 분실 및 임시 신뢰 분실 옵션이 들어 있지 않습니다. 이러한 옵션은 여러 사용자에게 배포된 구성에 대해서는 적용되지 않는 로컬 사용자 옵션입니다.

초기 설정을 위한 도구 메뉴 옵션

초기 설정 도구의 도구 메뉴에는 다음 옵션이 제공됩니다.

- 초기 설정 다시 로드 및 테스트—사용자에게 배치하기 전에 초기 구성을 테스트합니다. "사용자 계정의 연결 타이밍 구성" (페이지 17)을 참조하십시오.
- SIM 카드 관리자—SIM (Subscriber Identity Module: 가입자 ID 모듈 카드) 카드는 일부 모바일 무선 장치에 들어 있으며 네트워크 구독자를 식별하는 데 사용하는 전자 카드입니다. 클라이언트 컴퓨터에 SIM 카드 리더가 있는 경우, OAC 인증에 SIM 카드를 사용할 수 있습니다.

OAC를 이용하며, SIM 카드 하드웨어의 PIN (Personal Identification Number: 개인 식별 번호)를 관리할 수 있습니다. *Odyssey 액세스 클라이언트 사용자 가이드*에 있는 SIM 카드 PIN 설정 관리에 대한 설명을 참조하십시오.

- 로그—`debuglog.log` 파일의 현재 내용을 표시합니다. *Odyssey 액세스 클라이언트 사용자 가이드*의 로그 파일 및 진단 보기에 대한 설명을 참조하십시오.
- 기본설정—시스템 트레이 아이콘, 제어판 아이콘 또는 Odyssey 액세스 클라이언트 관리자 스플래시 화면의 디스플레이를 토글합니다.
- Windows 로그인 설정—기본 구성 이미지를 배치하는 모든 사용자에게 기본 네트워크 연결 타이밍을 덮어쓸 수 있게 해줍니다. *Odyssey 액세스 클라이언트 사용자 가이드*의 Windows 로그인 설정 관리에 대한 설명을 참조하십시오.
- 옵션—다음 카테고리의 설정을 별도의 탭으로 정리하여 보여 줍니다.

■ 보안

- 세션 재개 활성화 설정한 시간보다 오래된 세션에 대한 세션 재개를 제한합니다.
- 자동 재인증 활성화: 정기적인 자동 재인증을 활성화하고 재인증 빈도 수 설정을 설정합니다.
- 서버 임시 신뢰 활성화: 신뢰할 수 있는 서버 대화 상자에서 신뢰되는 아직 구성되지 않은 인증 서버의 네트워크로 인증할 수 있게 해줍니다.
- 스마트 카드 PIN 묻기: 스마트 카드 PIN을 확인합니다.

■ 인터페이스

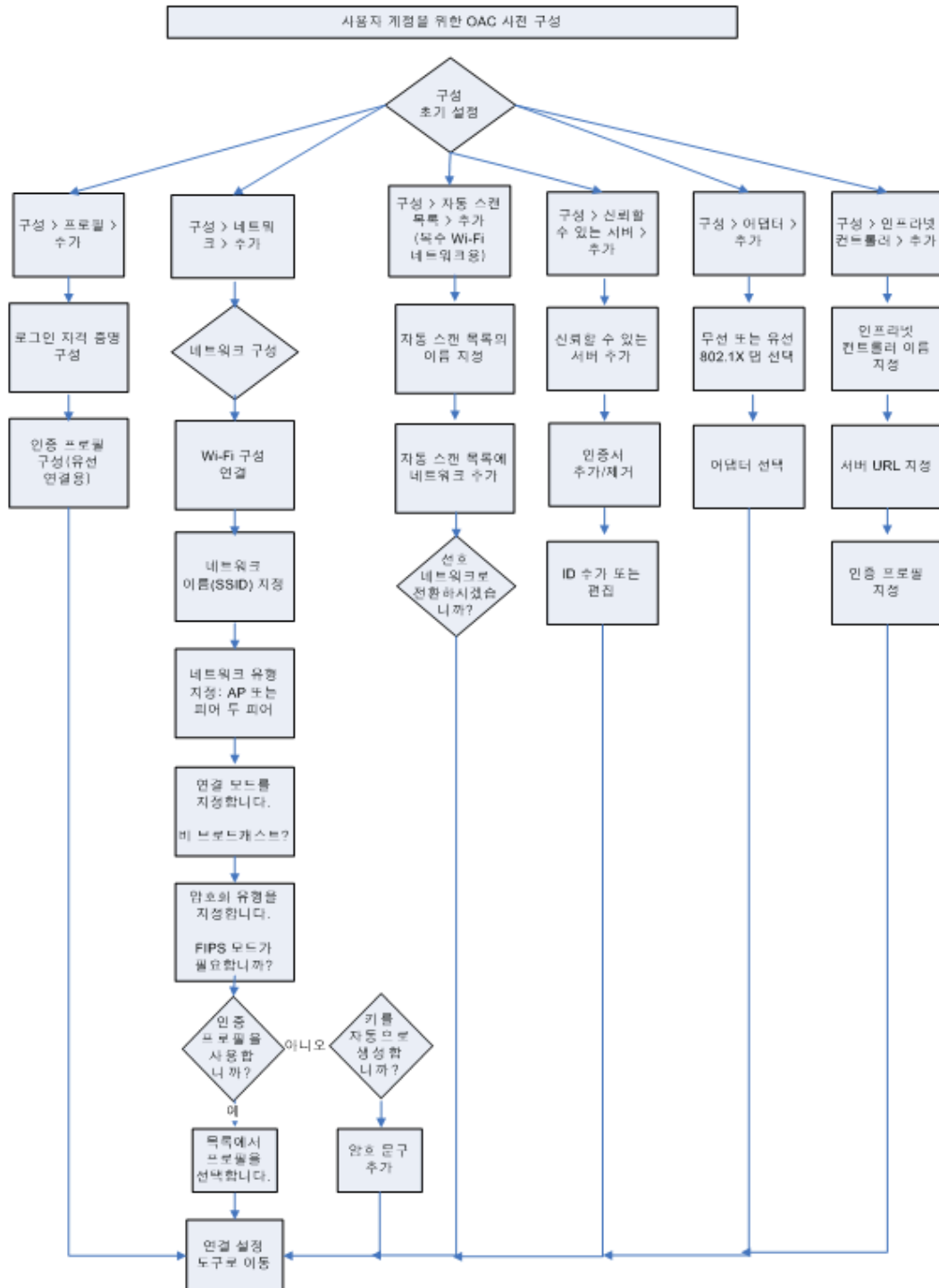
- 무선 제거: 유선 연결이 없는 사용자를 위한 무선 대역폭을 보존하기 위해 사용 가능할 때마다 유선 네트워크 연결을 기본값으로 사용합니다.
- 모든 유선/무선 어댑터 관리: 모든 유선 또는 무선 어댑터에 대해 OAC를 자동으로 구성합니다.

- 선점 네트워크—Wi-Fi 연결 대화 상자에 현재 활성화되어 있는 네트워크나 자동 스캔 목록을 항상 덮어쓰는 선호 네트워크의 자동 스캔 목록을 지정합니다.
- EAP-FAST—OAC에서 EAP-FAST 자격 증명을 확인할 시기를 제어합니다.

- 통지—인증 및 네트워크 연결 상태와 관련된 통지 메시지의 표시를 관리합니다.
- 기본 로그인 이름—작성한 인증 프로필에 표시되는 기본 로그인 이름 프롬프트 형식을 수정할 수 있습니다. 관리자가 이 옵션을 활성화한 경우에만 Odyssey 액세스 클라이언트 관리자에 이러한 옵션이 표시됩니다. 가끔 사용되는 옵션으로, 연결해야 할 네트워크에 기본으로 구성된 형식과 다른 로그인 이름 형식 조건이 있는 경우 이 옵션을 사용하면 로그인 이름 형식을 설정할 수 있습니다.

초기 설정을 위한 프로세스 흐름

그림 3: 초기 설정을 위한 프로세스 흐름



초기 설정 구성

Odyssey 액세스 클라이언트에서 **초기 설정** 도구를 더블 클릭합니다.

Odyssey 액세스 클라이언트 관리자에서 구성한 것과 동일한 방식으로, 초기 설정 도구에서 다음과 같은 기능 집합을 구성합니다. 공통적인 구성 이미지를 배치할 개별 사용자 또는 사용자 그룹에 대해 이 작업을 수행합니다. 다른 사용자 그룹에 다른 설정이 필요하거나 한 그룹에 다른 그룹보다 많은 제한을 적용해야 하는 경우, 하나 이상의 구성 이미지를 만들 수 있습니다.

다음 카테고리의 설정이 초기 설정 도구 사이드바의 구성 아래 표시됩니다.

- 프로필—인증된 액세스를 요구하는 특정 네트워크에 해당하는 인증 설정을 사전 구성합니다. 인증 프로필 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오. (유선 802.1X 연결에는 인증 프로필이 필요).



참고: 사용하는 인증 서버에서 OAC에서 사용 가능한 EAP 인증 방법을 모두 지원하지는 않을 수도 있습니다. 표준 관행은 OAC에서 인증을 설정하기 전에 인증 서버가 허용하는 방법을 미리 파악해 두는 것을 권장합니다.

- 네트워크—여러 사용자에게 배치할 사용자의 기본 네트워크 또는 구성 이미지를 구성합니다. 네트워크 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.
- 자동 스캔 목록—현재 사용자 또는 여러 사용자에게 배치할 구성 이미지를 위한 자동 스캔 목록에 대한 네트워크를 사전 구성하고 정렬합니다. 무선 제거와 같은 자동 스캔 목록 및 기능 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.
- 신뢰할 수 있는 서버—구성 업데이트를 위해 사용할 시스템의 로컬 시스템 인증서 저장소에 있는 신뢰할 수 있는 루트 CA 또는 중개 CA 인증서를 사전 구성합니다. 그 다음 초기 설정 도구에서 사용자를 위한 신뢰할 수 있는 서버를 구성합니다. 신뢰 설정은 개별적으로 구성할 수 있습니다. 신뢰할 수 있는 서버 구성 및 인증서 추가 또는 제거에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

신뢰 구성의 병합 규칙 설정을 관리하려면, "신뢰의 병합 규칙 설정" (페이지 51)을 참조하십시오. 이제, 개별 인증서와 ID 항목에 대해 잠금과 같은 병합 규칙 설정을 관리할 수 있습니다.

- 어댑터—사용자가 가질 수 있는 유선 또는 무선 어댑터를 사전 구성합니다. 사용자가 시스템에 유사한 종류의 어댑터(유선 또는 무선)를 설치한 경우, 자신의 어댑터와 완전히 동일한 어댑터(이름과 모델은 다를 수 있음)를 가질 필요는 없습니다. 네트워크 어댑터 관리에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

- 인프라넷 컨트롤러—사용자에 대해 하나 이상의 인프라넷 컨트롤러를 사전 구성합니다. 사용자에 대해 인프라넷 컨트롤러를 사전 구성하는 경우, 초기 설정 도구의 **사용자는 이 IC에서 연결을 해제할 수 없습니다** 옵션을 사용하면 사용자가 연결을 해제할 수 없도록 특정 인프라넷 컨트롤러로의 사용자 연결을 잠글 수 있습니다. 이 기능은 사용자가 인프라넷 컨트롤러에 연결되어 있는 한, 호스트 체커 정책과 중점 무결성 검사를 유지합니다. 이 옵션은 초기 설정 도구에서만 사용할 수 있습니다.

사용자가 OAC를 처음 실행할 경우, 일반적으로 초기 설정 도구에서 사전 구성된 설정이 표시됩니다. 이러한 구성 설정은 다음에 사용할 수도 있습니다.

- 사용자 정의 설치기
- 설정 업데이트 파일
- 인프라넷 컨트롤러로 내보내기를 위한 사전 구성된 설정



참고: 사용자 정의 설치기나 설정 업데이트 파일을 생성하기 전에 병합 규칙 도구를 사용하여 업데이트되거나 새로운 사용자 구성에 초기 설정 도구 구성을 적용하는 방법을 지정하십시오.

Windows 로그인 설정 관리

네트워크 연결 타이밍의 기본 설정을 덮어쓰도록 **도구 > Windows 로그인 설정**을 선택합니다. 이 옵션은 사전 구성된 GINA 연결 타이밍을 바탕으로 한 구성을 가진 사용자를 지원하고 기본 설정을 덮어쓸 수 있도록 해줍니다. 이렇게 함으로써, 사용자는 OAC에 대해 구성된 기본 연결 이외의 네트워크에 연결할 수 있게 되며 이 경우 로그인 자격 증명은 달라질 수 있습니다. 로그인 타이밍 옵션에 대한 자세한 설명은 "Windows 로그인 전에 연결" (페이지 34)을 참조하십시오.



참고: 로그인 타이밍을 변경하면 다른 시작 프로세스에 영향을 줄 수 있습니다.

네트워크 관리자가 OAC를 어떻게 설정했는지에 따라, Windows 로그인 옵션 중 어느 옵션이라도 기본 네트워크 연결 타이밍으로 구성될 수 있습니다. 또한, 네트워크 관리자가 사용자로 하여금 기본 네트워크 연결 설정을 수정하도록 허용할 수도 있습니다. 이 경우, 기본 네트워크 연결 설정을 덮어쓸 수 있습니다.

예를 들어, 사용자는 캐시된 자격 증명을 사용하여 도메인에 로그인할 수 있고, Windows 로그인 이전에 네트워크 연결이 이루어지도록 구성된 경우, 데스크톱이 표시된 다음 네트워크에 연결하도록 연결 타이밍을 변경할 수 있습니다.

기본 Windows 로그인 설정 덮어쓰기 관련 주의 사항

Odyssey 액세스 클라이언트 관리자의 **도구 > Windows 로그인 설정** 옵션을 사용하면, 사용자가 기본 네트워크 연결 타이밍을 덮어씁니다. 이 옵션은 주로 연결 설정 도구를 사용하여 설정됩니다. 이 설정의 목적은 로그인 시, 연결 요건이 다른 사용자를 수용하는 것입니다. 예를 들어, 여러 사용자에게 배포되는 OAC 구성에 대부분의 회사 사용자에게 사전 구성된 네트워크가 포함되어 있을 수 있습니다. 그러나, 원격 위치의 사용자는 다른 네트워크에 연결해야 할 수도 있고, 로그인 타이밍 조건이 다를 수도 있습니다. 이 옵션을 사용하면 이러한 원격 위치의 사용자가 관리 권한 없이도 기본 로그인 설정을 덮어쓸 수 있습니다. 이 옵션은 자주 사용되지는 않습니다.



참고: 연결 설정 도구의 GINA 탭에서 구성한 네트워크 연결 설정을 사용자가 덮어쓰게 하려는 경우가 아니라면, 초기 설정 도구에서 **Windows 로그인을 위한 기본 설정 덮어쓰기**를 선택하지 마십시오.

기본 로그인 설정을 덮어쓰고 사용자가 OAC GINA 모듈을 사용하는 경우, 사용자는 Windows 로그인 전에 이루어진 네트워크 연결을 구성할 수 있습니다. 사용자가 권한 편집기로 제한하지 않는 한, 구성된 기본 네트워크 연결 설정을 사용자가 덮어쓸 수 있습니다.

사용자는 OAC가 Windows 로그인 전에 연결하도록 설정된 경우, 신뢰할 수 있는 서버 구성을 덮어쓸 수 없습니다. Windows 로그인 연결의 신뢰 설정을 변경하는 유일한 방법은 초기 설정 도구의 신뢰할 수 있는 서버 대화 상자에서 해당 설정을 수정하는 것입니다.

로그인 이름 형식 구성

초기 설정 도구에서 **도구 > 옵션 기본 로그인 이름**을 선택하여 모든 새로운 OAC 사용자에게 대해 기본 로그인을 지정합니다. 지정한 기본 로그인 이름 옵션은 사용자 정의 형식을 지정한 경우 사용자 입력이 필요할 수 있습니다. 이 경우, 사용자 정의 로그인 이름을 확인하는 프롬프트가 표시됩니다. "사용자 정의 로그인 이름 형식 지정" (페이지 16)을 참조하십시오.

선택되는 사용자 기본 로그인 이름이 다음 조건 하에 적용됩니다.

- 기본 로그인 이름은 사용자가 생성한 새로운 Odyssey 액세스 클라이언트 관리자 인증 프로필의 로그인 이름 상자에 자동으로 표시됩니다.
- 여러 사용자에게 배치할 인증 프로필을 사전 구성하는 경우, 로그인 이름 상자를 공백으로 둘 수 있습니다. 프로필을 배치한 사용자가 OAC를 실행할 때, 로그인 이름 상자에 개별 사용자의 Windows 로그인 이름이 채워집니다.
- 사용자 이름이 공백인 프로필이 포함된 OAC 스크립트를 사용자가 가져올 경우, 프로필에 기본 로그인 이름이 자동으로 채워집니다.



참고: 사용자 정의 설치기 또는 설정 업데이트 파일이 사용하는 기본 로그인 이름은 병합 규칙으로 잠그지 않아도 됩니다. 초기 설정 도구에서 지정하는 기본 로그인 이름 옵션이 모든 사용자 정의 설치기 또는 설정 업데이트 파일에서 자동으로 사용됩니다.

옵션 대화 상자에서 로그인 이름 형식을 지정합니다. 다음 항목을 참조하십시오.

- "사용자 정의 로그인 이름 형식 지정" (페이지 16) — 사용자가 OAC를 처음 사용할 때 사용자에게 올바른 로그인 이름 형식을 확인하기 위해 표시할 텍스트를 삽입할 때 이 형식을 사용합니다.
- "도메인이 꾸며진 또는 꾸며지지 않은 로그인 이름 구성" (페이지 16) — 모든 프로필에서 사용할 Windows 로그인 이름 형식을 지정할 때 사용합니다.

사용자 정의 로그인 이름 형식 지정

사용자 인증을 위해 OAC를 처음 실행할 때 사용할 로그인 이름 형식을 사용자에게 표시하는 프롬프트를 구성할 수 있습니다. 사용자가 사용하는 로그인 이름은 다음 프로필에 대해 자동으로 채워집니다.

- 사용자가 생성하는 모든 새로운 인증 프로필.
- 설정 업데이트 파일과 사용자 정의 설치를 통해 사용자에게 배포할 빈 로그인 이름으로 구성할 인증 프로필.

예를 들어, 사용자가 로그인 이름에 대해 다음 형식을 사용하도록 할 수 있습니다.

username@domain

새로운 사용자가 로그인할 때 새로운 사용자에게 로그인 이름을 표시하는 지침 텍스트를 지정하려면 다음 절차를 따르십시오.

1. 초기 설정 도구 모음에서 **도구 > 옵션**을 선택합니다. 옵션 대화 상자가 나타납니다. **기본 로그인 이름** 탭을 선택합니다.
2. 다음 프롬프트를 사용하여 로그인 이름 묻기를 선택합니다.
3. 로그인 이름을 입력하는 방법을 사용자에게 알리기 위한 프롬프트를 입력합니다.
4. **확인**을 클릭합니다.

도메인이 꾸며진 또는 꾸며지지 않은 로그인 이름 구성

도메인이 꾸며진 또는 꾸며지지 않은 Windows 로그인 이름으로 모든 사용자 프로필에 대해 기본 로그인 이름을 지정하려면:

1. 초기 설정 도구에서 **도구 > 옵션**을 선택합니다. 옵션 대화 상자가 나타나면, **기본 로그인 이름** 탭을 선택합니다.
2. 다음 Windows 로그인 이름 형식 중 하나를 선택합니다.
 - **꾸며진 Windows 로그인 이름**—*Domain_name\Logon_Name*이라는 도메인이 꾸며진 기본 Windows 로그인 이름 형식을 사용합니다.
 - **꾸며지지 않은 Windows 로그인 이름**—도메인 이름 꾸미기 없이 Windows 로그인 이름을 사용합니다.
3. **확인**을 클릭합니다.

사용자 계정의 연결 타이밍 구성

시스템 차원의 인증을 사용하고 있지 않은 경우, 사용자는 로그인 자격 증명을 제공하여 네트워크에 연결합니다. 그러나, 인증된 연결이 완료될 시기는 네트워크 인증의 타이밍 옵션에 의해 결정된다는 사실을 유념하십시오. 초기 설정 도구를 사용하여 사용자 계정 구성 설정을 완료한 후에 이러한 설정을 구성합니다.

사용자 네트워크 연결을 구성하려면:

1. **연결 설정** 도구를 더블 클릭합니다.
2. **사용자 계정** 탭을 선택합니다.
3. 선호하는 연결 타이밍 옵션을 선택합니다. 구체적인 지침과 상세 정보는 "네트워크 연결 타이밍 정보" (페이지 32)를 참조하십시오.
4. 설정을 저장하고 연결 설정 도구를 닫습니다.
5. 권한 편집기 도구를 이용하여 제한하거나 잠가야 하는 구성 기능을 비활성화합니다.

구성 설정 테스트

이 항목에서는 배치를 위해 사용자 정의 설치를 생성하기 전에 사용자 또는 시스템 연결의 구성을 테스트하는 방법에 대해 설명합니다.

초기 설정 다시 로드 및 테스트 옵션은 초기 설정 도구에 정의된 구성을 Odyssey 액세스 클라이언트 관리자 로드하고, 네트워크 연결을 시도합니다. 연결에 실패할 경우, 오류 메시지와 로그 파일의 항목을 기준으로 다른 실패한 연결처럼 실패 문제를 해결해 보십시오.

사용자 연결 설정을 테스트하려면 다음 절차를 따르십시오.

1. **초기 설정** 도구를 더블 클릭합니다.
2. 초기 설정 도구에서 **도구 > 초기 설정 다시 로드 및 테스트**를 선택합니다.
3. **확인**을 클릭합니다. 이는 현재 Odyssey 액세스 클라이언트 관리자 설정을 영구적으로 삭제하고 초기 설정 도구의 설정을 Odyssey 액세스 클라이언트 관리자에 로드합니다.
4. Odyssey 액세스 클라이언트 관리자의 Wi-Fi 또는 이더넷 연결 대화 상자에서 모든 연결을 테스트합니다. Odyssey 액세스 클라이언트 관리자에서 하는 모든 수정 사항은 초기 설정 도구에 반영되어 있지 않습니다.
5. 초기 설정 도구로 돌아가 필요에 따라 연결 문제를 해결하고 재검사하십시오.

시스템 연결 설정 테스트

테스트하고자 하는 네트워크 연결은 연결 설정 도구의 시스템 계정 탭에 구성된 연결 유형에 대해 구성 및 설정되어 있어야 합니다.

시스템 연결 설정을 테스트하려면:

1. **연결 설정** 도구를 더블 클릭합니다.
2. **시스템 계정** 탭을 선택합니다.
3. **시스템 연결의 활성화 유지**를 선택합니다.
4. **확인**을 클릭합니다.
5. 시스템 트레이 아이콘을 더블 클릭하여 Odyssey 액세스 클라이언트 관리자를 열고, 연결 상태를 확인합니다.
6. 시스템 계정 탭으로 돌아가 필요에 따라 연결 문제를 해결하고 재검사합니다.
7. 연결 설정을 수정한 경우, 연결 설정 대화 상자의 **시스템 계정** 탭을 선택하고 이전 설정을 복원합니다.

네트워크 어댑터 및 기타 Wi-Fi 지원 프로그램 제어

사용자가 네트워크 어댑터를 관리하거나, 기타 Wi-Fi 지원 프로그램을 사용해야 하는 정도를 융통성 있게 제어할 수 있습니다. (OAC는 Juniper Network Wi-Fi 지원 프로그램임.) 기본적으로, 사용자는 OAC 구성에서 네트워크 어댑터를 추가 또는 제거하고, OAC를 종료할 수 있습니다.

대부분의 경우, 사용자에게 이러한 유형의 융통성을 제공하는 것이 좋습니다. 예를 들어, 사용자는 제 3자 무선 지원 프로그램이 있는 어댑터를 사용하여 테스트 네트워크에 액세스할 수 있습니다.

그러나, 이러한 융통성이 있으면 회사 네트워크 정책을 무효화할 수도 있습니다. OAC 이외의 무선 액세스 클라이언트를 사용하면, 사용자가 Odyssey 액세스 클라이언트에 설정된 제한을 무시할 수 있습니다. 예를 들어, 잠긴 구성의 승인되지 않는 프로토콜을 사용하여 회사 이외의 네트워크에 액세스하는 데 다른 무선 지원 프로그램이 있는 Wi-Fi 어댑터를 사용할 수 있습니다. 또한, OAC에 비활성화되어 있는 승인되지 않은 프로토콜을 사용할 수도 있습니다.

OAC에서 관리하지 않는 비 802.1X 유선 네트워크 카드를 소지한 사용자가 암호화되지 않은 데이터를 전송할 수 있습니다.

이러한 위험들은 다음과 같은 방법으로 관리할 수 있습니다.

- 사용자의 종점 컴퓨터에 있는 유선 또는 무선 어댑터를 자동으로 관리하도록 OAC를 구성하여 그러한 위험 시나리오를 예방하고 OAC 배치 전에 병합 규칙의 해당 설정을 잠글 수 있습니다.

초기 설정 도구에서 **도구 > 옵션 > 인터페이스** 옵션을 선택하고, 시스템의 유선 또는 무선 네트워크 어댑터를 자동으로 구성하고 바인딩하도록 OAC를 구성합니다. OAC가 실행 중인 한, 사용자 시스템에 연결된 모든 네트워크 어댑터를 구성합니다.

- 권한 편집기에서 사용자가 OAC를 종료하지 못하도록 할 수 있습니다. **사용자가 Odyssey를 종료하는 것을 허용하지 않음**을 선택합니다.
- OAC에는 외부 프로그램에서 OAC 서비스를 비활성화할 수 있게 해주는 기능이 있습니다. 권한 편집기에서 외부 프로그램이 OAC를 비활성화하지 못하도록 할 수 있습니다. **사용자가 Odyssey를 비활성화하는 것을 허용하지 않음**을 선택합니다. 또한, 병합 규칙 도구를 사용하여 설정을 잠그고 사용자가 변경하지 못하도록 할 수도 있습니다.

3 장

시스템 계정 구성

이 항목에는 다음 정보가 포함됩니다.

- 시스템 계정 도구 개요 (페이지 22)
- 시스템 계정 설정을 위한 프로세스 흐름 (페이지 23)
- 시스템 계정 연결 활성화 (페이지 24)

시스템 계정 구성은 사용자가 아닌 네트워크로의 실제 시스템을 인증합니다. 이러한 유형의 구성은 정적으로 정의된 사용자 계정, 또는 시스템 ID가 Active Directory에서 설정될 때 생성된 시스템 자격 증명을 사용합니다. 정적으로 정의된 사용자 계정은 Active Directory에 설정되어 있는지 여부와 상관없이 유효한 로그인 자격 증명으로 구성됩니다.

사용자 로그인 전에 시스템을 네트워크에 연결하려면 시스템 계정을 사용합니다. 사전 구성된 사용자 이름 및 암호를 사용하거나, Windows 환경인 경우에는 시스템의 실제 Active Directory 자격 증명이나 인증서를 사용하면 됩니다.

시스템 계정 연결은 OAC가 네트워크에 연결을 시작할 수 있는 가장 빠른 시간이며, 야간 백업이나 업데이트 프로세스와 같이 사용자의 로그인과 상관 없이 수행되는 관리 작업에 유용합니다. 또한 시작 작업 동안 실행되는 Active Directory 도메인 정책 스크립트에도 유용합니다.

시스템(컴퓨터)에는 사용자가 로그인하기 전에 네트워크에 제출되는 이름과 암호가 있습니다. 시스템 연결을 활성화하면 시스템이 실행되는 한 사용자가 로그인하지 않은 경우에도 네트워크 IP 연결은 지속됩니다.

시스템 인증은 사용자 인증과는 다릅니다. 하지만 사용자가 네트워크에 로그인하고 로그아웃한 후 시스템 연결을 재개할 때 시스템 연결이 사용자 차원의 연결로 이동하도록 구성할 수 있습니다.



참고: 시스템 계정을 구성하고 설정을 파일로 저장한 후, 구성 설정이 클라이언트 시스템에 설치되면 재부팅을 해야 합니다.

시스템 계정 도구 개요

시스템 계정 도구는 초기 설정 도구와 유사합니다. 양쪽 보기 모두에서 사이드바가 동일하기 때문에, 프로필, 네트워크, 자동 스캔 목록, 신뢰할 수 있는 서버, 어댑터, 인프라넷 컨트롤러 등의 각 설정을 동일한 방식으로 구성할 수 있습니다. 하지만 두 옵션 간에 다른 점도 있습니다.

Odyssey 액세스 클라이언트 관리자의 **시스템 계정**을 더블 클릭하여 시스템 계정 도구를 엽니다.

시스템 계정 도구의 파일 메뉴에는 Odyssey 액세스 클라이언트 관리자에서 사용 가능한 암호 분실 및 임시 신뢰 분실 옵션이 들어 있지 않습니다. 이러한 옵션은 광범위 구성의 경우에는 적용되지 않는 로컬 사용자 옵션입니다.

시스템 계정 도구의 도구 메뉴 옵션의 수는 Odyssey 액세스 클라이언트 관리자 도구 메뉴의 옵션 수보다 적습니다.

시스템 계정 도구에서 **도구 > 옵션**을 클릭합니다. 다음과 같은 탭 카테고리가 표시 됩니다.

- 보안
- 인터페이스
- 선점 네트워크
- 통지

각 카테고리의 옵션은 Odyssey 액세스 클라이언트 관리자에서 **도구 > 옵션**을 선택 하면 나타나는 옵션과 같습니다.



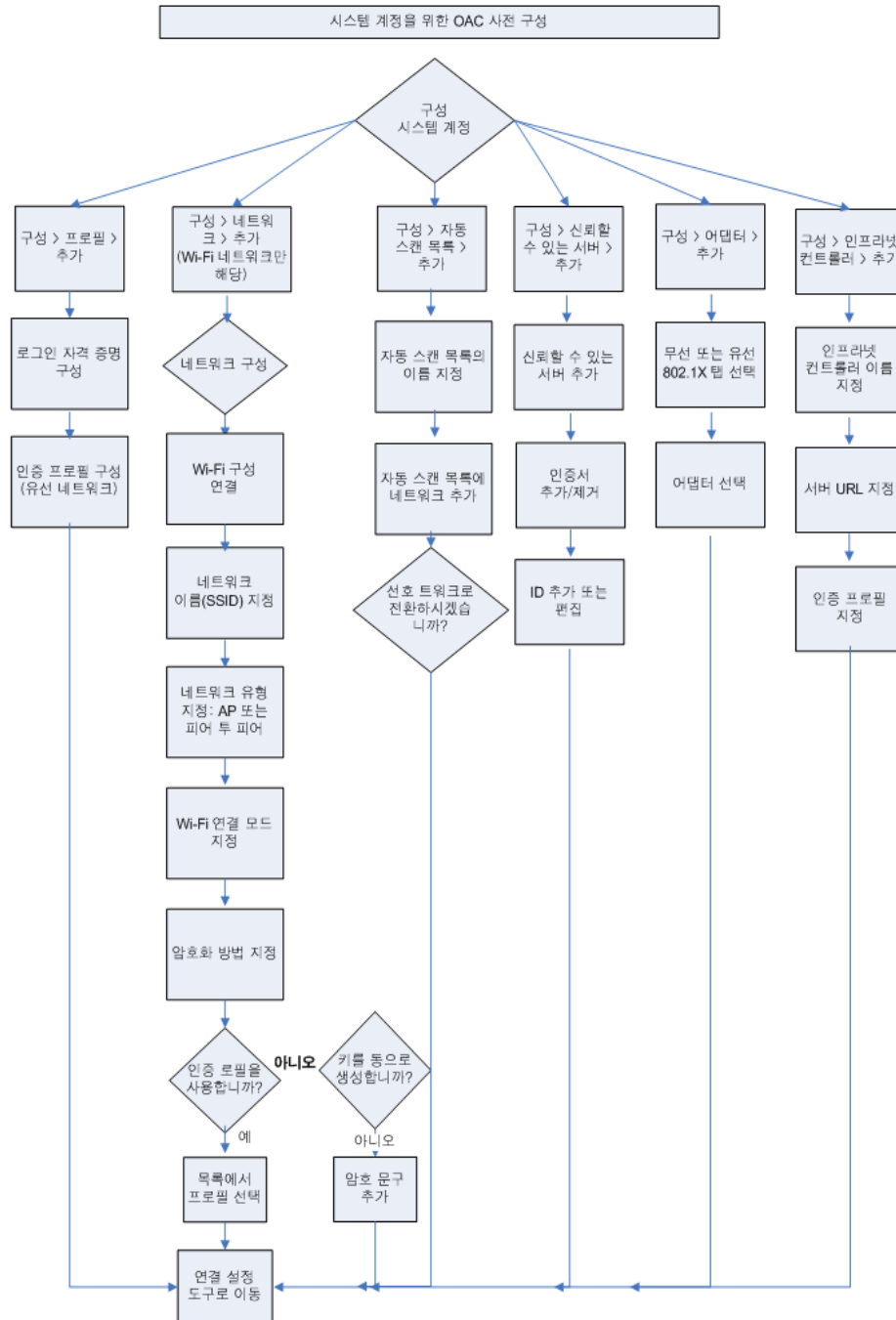
참고: 서버 임시 신뢰 활성화 및 스마트 카드 PIN 묻기의 두 가지 옵션은 사용할 수 없으므로 시스템 계정 도구에 희미하게 표시됩니다.

Odyssey 액세스 클라이언트 관리자에 있는 다음과 같은 옵션은 초기 설정 도구에는 표시되지 않습니다.

- Odyssey 액세스 클라이언트 관리자
- 주파수 조사
- 진단
- 스크립트 실행
- 새 스크립트 확인

시스템 계정 설정을 위한 프로세스 흐름

그림 4: 시스템 계정 설정을 위한 프로세스 흐름



시스템 계정 연결 활성화

연결 설정 도구에서 시스템 계정을 구성하려면:

1. **연결 설정을** 더블 클릭한 다음 **시스템 계정** 탭을 선택합니다.
2. **시스템 계정을 사용하여 네트워크 연결 활성화**를 선택합니다.
3. **시스템 연결의 활성화 유지; 사용자가 시스템 연결을 통해 연결됨**을 선택합니다. 이 경우, 사용자가 Windows에 로그인하지 않은 경우에도 시스템 계정은 활성화됩니다.

연결 설정 도구에서 시스템 차원 네트워크 연결을 구성한 후에는 시스템 계정 도구를 사용하여 프로필의 시스템 네트워크 연결 설정을 구성합니다. 이러한 유형의 구성은 Odyssey 액세스 클라이언트 관리자의 연결 설정을 구성하는 방법과 유사합니다.

시스템 계정은 사용자 계정을 위해 설정된 것과 다른 VLAN으로 할당될 수 있습니다. 사용자가 로그인 했을 때 시스템 계정이 사용자 계정으로 이동하도록 구성할 경우, 시스템에 대한 IP 주소는 다른 VLAN 할당 때문에 변경될 수 있습니다. 마찬가지로 사용자가 로그오프할 때 시스템 계정으로 돌아가도록 계정을 구성한 경우, IP 주소와 VLAN 할당도 원래대로 돌아갈 수 있습니다.

시스템 계정 설정 구성

Odyssey 액세스 클라이언트 관리자에서 구성한 것과 동일한 방식으로, 시스템 계정 설정 도구에서 다음과 같은 기능 집합을 구성합니다. 공통적인 구성 이미지를 배치할 개별 사용자 또는 사용자 그룹에 대해 이 작업을 수행합니다. 다른 사용자 그룹에 다른 설정이 필요하거나 한 그룹에 다른 그룹보다 많은 제한을 적용해야 하는 경우, 하나 이상의 구성 이미지를 만들 수 있습니다.

다음 카테고리의 설정이 초기 설정 도구 사이드바의 구성 아래 표시됩니다.

- **프로필—인증된 액세스를** 요구하는 특정 네트워크에 해당하는 인증 설정을 사전 구성합니다. 인증 프로필 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오. (유선 802.1X 연결에는 인증 프로필이 필요).



참고: 사용하는 인증 서버에서 OAC에서 사용 가능한 EAP 인증 방법을 모두 지원하지 않을 수도 있습니다. 표준 관행은 OAC에서 인증을 설정하기 전에 인증 서버가 허용하는 방법을 미리 파악해 두는 것을 권장합니다.

- **네트워크—여러 사용자에게** 배치할 구성 이미지 또는 사용자의 기본 네트워크를 구성합니다. 네트워크 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.
- **자동 스캔 목록—현재 사용자 또는 여러 사용자에게** 배치할 구성 이미지를 위한 자동 스캔 목록에 대한 네트워크를 사전 구성하고 정렬합니다. 무선 제거와 같은 자동 스캔 목록 및 기능 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

- 신뢰할 수 있는 서버—구성 업데이트를 위해 사용할 시스템의 로컬 시스템 인증서 저장소에 있는 신뢰할 수 있는 루트 CA 또는 중개 CA 인증서를 사전 구성합니다. 그 다음 초기 설정 도구에서 사용자를 위한 신뢰할 수 있는 서버를 구성합니다. 신뢰 설정은 개별적으로 구성할 수 있습니다. 신뢰할 수 있는 서버 구성 및 인증서 추가 또는 제거에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

신뢰 구성의 병합 규칙 설정을 관리하려면, "신뢰의 병합 규칙 설정" (페이지 51)을 참조하십시오. 이제 개별 인증서와 ID 항목에 대해 잠금과 같은 병합 규칙 설정을 관리할 수 있습니다.

- 어댑터—사용자가 가질 수 있는 유선 또는 무선 어댑터를 사전 구성합니다. 사용자가 시스템에 유사한 종류의 어댑터(유선 또는 무선)를 설치한 경우, 자신의 어댑터와 완전히 동일한 어댑터(이름과 모델은 다를 수 있음)를 가질 필요는 없습니다. 네트워크 어댑터 관리에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.
- 인프라넷 컨트롤러—사용자에 대해 하나 이상의 인프라넷 컨트롤러를 사전 구성합니다. 사용자 연결을 특정 인프라넷 컨트롤러에 잠그려면 **사용자는 이 IC에서 연결을 해제할 수 없습니다** 확인란을 클릭합니다. 이 기능을 사용하면 사용자가 네트워크에 연결되어 있는 한, 호스트 체커 정책과 종점 무결성 검사를 유지할 수 있습니다. 이 옵션은 초기 설정 도구에서만 사용할 수 있습니다. 네트워크 구성에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

시스템 계정 프로필 옵션

네트워크, 프로필, 자동 스캔 목록, 신뢰할 수 있는 서버, 어댑터, 인프라넷 컨트롤러 등을 시스템 계정에 대해 구성할 수 있습니다. 시스템 연결에는 시스템 계정 도구에서 구성한 네트워크, 프로필, 어댑터, 또는 인프라넷 컨트롤러만 사용됩니다.

시스템 계정 암호 자격 증명 설정

시스템 계정 프로필에 암호를 입력하고 사용자 정의 설치기를 생성하고자 하는 경우, 입력한 자격 증명은 이 설치기를 사용하는 모든 OAC 사본에 의해 사용됩니다. 사용자 자격 증명에 필요한 경우, 각 클라이언트 시스템에 수동으로 자격 증명을 입력하는 것이 좋습니다.

EAP-TLS를 위한 자동 인증서 선택 설정

인증을 위해 EAP-TLS가 필요하고 이 구성을 여러 사용자에게 배치하려는 경우, 시스템 연결을 위해 사용하는 프로필에서 **자동 인증서 선택 사용**을 선택합니다. *Odyssey 액세스 클라이언트 사용자 가이드*의 인증 프로필 구성에 대한 설명을 참조하십시오.

시스템 인증을 위한 신뢰 구성 요건

시스템 계정 도구의 신뢰할 수 있는 서버 대화 상자에서 시스템 연결에 대해 신뢰할 수 있는 루트 CA 또는 중개 CA 인증서를 구성합니다. 구성하기 전에 구성을 위해 사용할 시스템의 인증서 보관소에 인증서가 설치되었는지 확인하십시오. 인증서 추가 방법에 대한 정보는 *Odyssey 액세스 클라이언트 사용자 가이드*의 신뢰할 수 있는 서버 관리에 대한 설명을 참조하십시오.

시스템 계정 설정에 대한 제한사항

토큰과 연결된 것과 같이 사용자 상호작용을 필요로 하는 기본 로그인 이름, EAP-FAST 옵션 및 인증 방법은 시스템 계정 설정에 적용되지 않습니다. 따라서, 시스템 계정 도구의 프로필 속성 대화 상자는 Odyssey 액세스 클라이언트 관리자의 대화 상자와 약간 다릅니다.

시스템 암호 구성

Active Directory 목록과 비교하여 시스템 자격 증명을 확인하는 RADIUS 서버로 시스템을 인증할 때, 시스템 자격 증명(시스템 이름 및 시스템 도메인 암호)을 구성할 수 있습니다. 시스템 자격 증명은 시스템이 도메인에 합류할 때 자동으로 생성됩니다.

인증을 위해 시스템 자격 증명을 사용하려면:

1. 시스템 계정 도구에서 **구성 > 프로필 > 추가**를 선택하고, 프로필 추가 대화 상자의 **사용자 정보** 탭에서 **시스템 자격 증명 사용**을 선택합니다.

시스템 자격 증명 사용을 선택하면, OAC는 컴퓨터가 인증을 위해 도메인에 합류할 때 생성한 시스템 자격 증명을 사용합니다. 이 옵션을 선택하지 않으면, OAC는 로그인 이름으로 제공된 사용자 이름을 사용합니다.

2. (선택적) 영역(선택적): 상자(시스템 자격 증명 사용 확인란 아래 위치)에서 시스템 자격 증명을 꾸밀 영역 이름을 선택합니다. 그렇지 않을 경우, 이 필드를 공백으로 둡니다.

RADIUS 인증 서버가 RADIUS 프록시를 지원하도록 설정된 경우, 영역 이름 꾸미기가 필요할 수 있습니다.

3. TLS로 인증하지 않는 한, **암호를 사용한 로그인 허용 확인란**을 선택합니다.

시스템 자격 증명을 구성한 경우, 연결 설정 도구를 엽니다. **시스템 계정** 탭을 선택하고 **시스템 계정을 사용하여 네트워크 연결 활성화**를 선택합니다.

시스템 자격 증명을 지원하는 EAP 방법

시스템 자격 증명은 EAP-TTLS 또는 EAP-PEAP를 사용한 경우에만 유효합니다. 프로필에 대해 이 인증 방법 중 하나 이상을 선택하십시오. 그 다음 프로필 속성 대화 상자에서 TTLS 설정 탭 또는 PEAP 설정 탭에 대한 인증 옵션을 필요에 따라 구성합니다. 시스템 계정 프로필의 인증 프로토콜을 선택하는 방법에 대한 지침은 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

시스템 인증 활성화

UAC 네트워크 내 OAC는 Active Directory 시스템 인증 및 중점 평가를 지원합니다. 즉, 무결성 확인을 위하여 시스템 계정을 구성할 수 있습니다.



참고: 사용자 시스템에 OAC 시스템 계정을 설치하면, 설치 프로세스가 완료된 후 시스템을 수동으로 재부팅해야 합니다.

이 기능을 활성화하려면:

1. **시스템 계정** 도구를 더블 클릭하고, 사이드바에서 **프로필** 아이콘을 클릭합니다.
2. 사용자 정보 탭에서 로그인 이름을 지정하거나 **시스템 자격 증명 사용**을 선택합니다. 선택적으로, 기본값 이외에 영역 이름을 지정할 수 있습니다.
3. **TTLS** 탭을 클릭하고, 내부 프로토콜로서 **EAP**를 선택한 다음, **JUAC**를 내부 EAP 프로토콜로 선택합니다. (이 설정이 기본값입니다.)



참고: 시스템 차원 연결에 대한 중점 무결성 확인에 실패한 경우, 사용자 인터페이스가 없으므로 해결책 지침이나 기타 통지가 표시되지 않습니다. (Windows 로그온이 완료되기 전에 연결됨.) 이 경우, 시스템 인증에 대해 정의된 정책에 따라 자동 치료를 시작할 수 있는 보호된 VLAN으로 시스템이 리다이렉트될 수 있습니다.

4 장

네트워크 연결 실시 시기 및 방법 구성

이 항목에는 다음 정보가 포함됩니다.

- 연결 설정 도구 개요 (페이지 29)
- 연결 설정 구성을 위한 프로세스 흐름 (페이지 31)
- 사용자 계정 연결 구성 (페이지 33)
- 시스템 계정 연결 구성 (페이지 35)
- GINA를 사용하여 Windows 로그인 전에 연결을 구성 (페이지 37)

연결 설정 도구 개요

연결 설정 도구를 사용하면 OAC의 네트워크 연결 유형과 타이밍을 제어하는 옵션을 구성할 수 있습니다.

기본적으로 OAC는 Windows 데스크톱이 나타난 후 네트워크에 연결됩니다. Windows 시작 순서에서 먼저 실시할 특별한 프로세스가 없는 가장 일반적인 경우입니다. 그러나, 경우에 따라 인증된 연결을 먼저 설정할 필요가 있을 수도 있습니다. 예를 들어, 사용자 로그인 전에 도메인 인증을 활성화하거나, 시작 프로세스 중 특정한 시간에 스크립트를 실행해야 할 수도 있습니다.

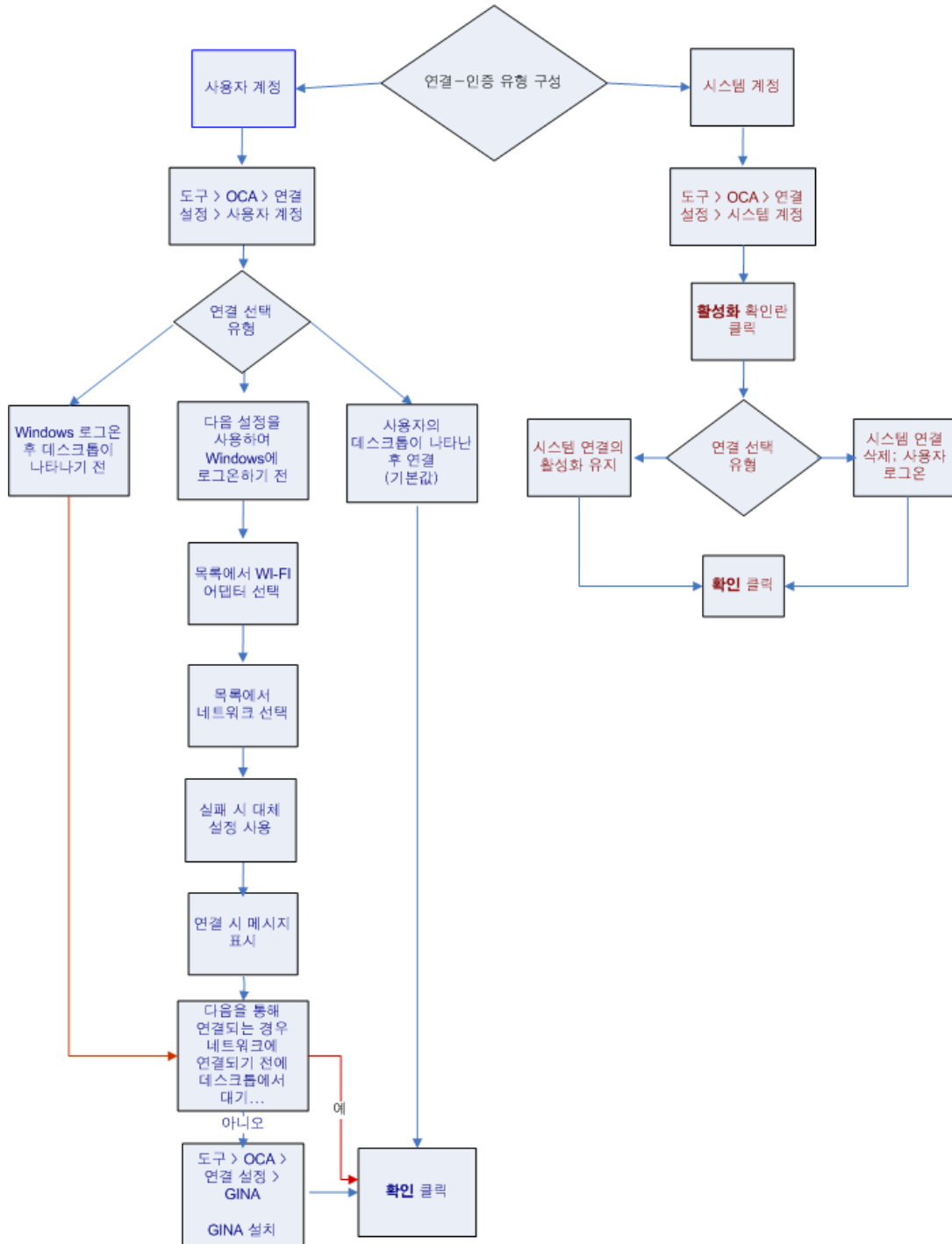
Odyssey 액세스 클라이언트 관리자에서 **연결 설정** 도구를 더블 클릭하십시오. 연결 설정 대화 상자에는 다음 3가지 탭이 포함되어 있습니다.

- 사용자 계정—사용자 네트워크 연결의 기본 타이밍을 구성할 때 이 설정을 사용합니다. 사용자 차원에서, 네트워크 연결에는 사용자 로그인 자격 증명도 필요하며, 사용자가 로그인해 있는 동안에는 네트워크 연결이 지속됩니다.
- 시스템 계정—시스템 자격 증명을 사용하여 Windows 시작 시 시스템 차원의 네트워크 연결을 구성할 때 이 설정을 사용합니다. 시스템 차원에서, 네트워크 연결은 사용자 또는 물리적 컴퓨터의 자격 증명을 사용합니다. 시스템 연결은 사용자 로그인 여부와 상관없이, 컴퓨터에서 Windows가 실행 중인 한 지속됩니다.

- GINA—Windows 시작 전에 인증을 제어할 때 Odyssey GINA (Graphical Identification and Authentication: 그래픽 식별 및 인증)를 사용합니다. GINA는 인증에 필요한 사용자 자격 증명을 수집할 수 있도록 Windows 로그인 프로세스 전에 실행되는 대체 가능한 DLL (dynamic link library: 동적 링크 라이브러리)입니다. GINA는 Windows 로그인 전에 발생하는 네트워크 연결을 허용하는 도구입니다. 다양한 판매업체에서 자체 버전의 GINA를 가지고 있습니다. Odyssey GINA 모듈은 OAC와 사용하도록 설계되었으며, 다른 업체의 GINA 모듈과도 호환됩니다. "GINA를 사용하여 Windows 로그인 전에 연결을 구성" (페이지 37)을 참조하십시오.

연결 설정 구성을 위한 프로세스 흐름

그림 5: 연결 설정을 위한 프로세스 흐름





참고: 사용자 계정 연결 설정을 구성하기 전에, 초기 설정 도구를 사용하여 사용자 계정을 구성하십시오. 같은 방법으로 시스템 계정 연결 설정을 구성하기 전에, 시스템 계정 설정 구성을 위해 시스템 계정 도구를 사용하십시오.

네트워크 연결 타이밍 정보

Windows 시작 및 인증과 같은 이벤트를 바탕으로 네트워크 연결을 실시할 시기를 제어할 수 있습니다. 연결 타이밍은 시스템 연결 차원 또는 사용자 로그인 차원에서 적용할 수 있으며, 상호 배타적입니다. 본 항목에 설명된 설정은 사용 가능한 옵션을 보여 줍니다.

사용자 차원 연결 옵션

사용자 차원 연결의 3가지 유형은 다음과 같습니다.

- 네트워크로의 사용자 차원 연결은 사용자가 Windows에 로그인하기 바로 전에 사용자 자격 증명을 바탕으로 발생합니다.
- 네트워크로의 사용자 차원 연결은 데스크톱이 나타나기 전, 사용자가 Windows에 로그인한 후에 사용자 자격 증명을 바탕으로 발생합니다.
- 네트워크로의 사용자 차원 연결은 Windows 데스크톱이 나타난 후 사용자 자격 증명을 바탕으로 발생합니다.

이러한 구성의 일부는 사용자가 선택한 다른 기능을 바탕으로 활성화 또는 비활성화됩니다.

다양한 네트워크 연결 옵션 구성에 대한 자세한 정보와 특정 시나리오를 선택해야 하는 경우 그 이유에 대한 정보에 대해서는 다음 항목을 참조하십시오.

- "시스템만 연결 구성" (페이지 36).
- "사용자 연결로 전환되는 시스템 연결 구성" (페이지 36).

시스템 차원 연결 옵션

시스템의 네트워크 연결에는 실제 컴퓨터의 로그인 자격 증명 또는 사용자의 자격 증명이 사용될 수 있습니다.

시스템 연결을 위해 다음 구성 옵션을 사용할 수 있습니다.

- 네트워크로의 시스템 차원 연결은 Windows를 시작할 때 발생합니다. 이 연결 유형으로 시스템이 실행하는 동안에는 사용자가 로그인하지 않은 경우에도 네트워크를 통해 시스템에 액세스할 수 있습니다. 이 옵션은 사용자의 로그인 여부에 관계없이 업데이트 스크립트와 백업을 배치할 때 유용합니다.
- 네트워크로의 시스템 차원 연결이 Windows 시작 시 발생하며 사용자가 Windows에 로그인하기 바로 전에 사용자 차원의 연결 및 인증으로 전환합니다.
- 네트워크로의 시스템 차원 연결이 Windows 시작 시 발생하며 사용자가 Windows에 로그인한 직후 데스크톱이 나타나기 전에 사용자 차원의 연결 및 인증으로 전환합니다.
- 네트워크로의 시스템 차원 연결이 Windows 시작 시 발생하며 데스크톱이 나타난 후에 사용자 차원의 연결 및 인증으로 전환합니다.

사용자 계정 연결 구성

네트워크 연결의 성공은 선택한 타이밍에 따라 다를 수 있습니다. 기본 옵션은 데스크톱이 나타난 후 네트워크 연결을 하는 것입니다. 하지만 네트워크에서 시작 스크립트를 실행하는 경우와 같이, 데스크톱이 나타나기 전에 사용자가 네트워크에 연결해야 할 경우, 그 보다 빠른 연결 시간을 선택할 수 있습니다.

연결 설정 도구에서 **사용자 계정** 탭을 선택하여 Windows 로그인 프롬프트가 표시되기 전에 또는 그 후에 연결이 실시되도록 구성하십시오. Odyssey 사용 아래 명시된 옵션을 사용하여 네트워크에 연결하십시오. 다음 옵션들은 로그인 프롬프트가 표시될 시기를 제어합니다.

- 사용자의 데스크톱이 나타난 후—사용자가 데스크톱이 나타나기 전에 네트워크 연결을 원하지 않을 경우, 이 옵션을 선택합니다. 이 옵션이 기본 설정입니다.
- Windows 로그인을 한 후와 데스크톱이 나타나기 전—데스크톱이 나타나기 전이지만 Windows 로그인을 한 후에 사용자가 네트워크 연결을 하도록 하려면 이 옵션을 선택하십시오. "Windows 로그인 후 데스크톱이 나타나기 전에 연결" (페이지 33)을 참조하십시오.
- 다음 설정을 사용하여 Windows에 로그인하기 전—사용자가 Windows에 로그인하기 전에 네트워크 연결을 하도록 하려면 이 옵션을 선택하십시오. "Windows 로그인 전에 연결" (페이지 34)을 참조하십시오.

사용자 정의 설치기에 대해 Windows 로그인 기능을 구성하거나 구성 설정을 업데이트하려면 "로그인 이름 형식 구성" (페이지 15)의 지침을 따르십시오.

Windows 로그인 후 데스크톱이 나타나기 전에 연결

데스크톱이 나타난 후 연결하는 경우, 다음 두 가지 옵션이 있습니다.

- 이 시스템의 사용자가 유선 어댑터를 통해 네트워크에 연결될 때마다 연결을 연기합니다. **유선 어댑터**를 선택하면 됩니다. 유선 어댑터가 802.1X 허브 또는 스위치에 연결되지 않은 경우에도 이 옵션이 적용됩니다.
- 사용자가 하나 이상의 지정된 어댑터에 연결될 때마다 연결을 연기합니다. **다음 어댑터 중 하나**를 선택하면 됩니다. 이 옵션은 열거된 모든 어댑터에 대해 유효합니다.

어댑터 목록을 편집하려면:

- a. **편집**을 선택합니다. 어댑터 선택 대화 상자가 나타납니다.
- b. 데스크톱이 나타난 후의 네트워크 연결을 위해 사용하려는 어댑터를 선택합니다.
- c. **확인**을 클릭하여 어댑터 대화 상자 선택을 닫습니다.

선택한 어댑터가 연결 설정 도구의 사용자 계정 탭, **편집** 단추 옆에 있는 목록에 표시됩니다.

Windows 로그인 전에 연결



참고: Windows 로그인 전에 연결 설정을 구성하려면, 연결 설정 도구의 **GINA** 탭을 우선 선택하고 Odyssey GINA 모듈을 먼저 설치합니다. "Odyssey GINA 모듈 설치" (페이지 38) 및 "Windows 로그인 시 실행되는 다른 모듈과의 GINA 호환성" (페이지 38)을 참조 하십시오.

네트워크 구성에 인증 시 암호가 필요한 프로필이 있는 경우, **구성 > 프로필 > 속성 > 사용자 정보**를 선택하고 암호 하위 탭의 **Windows 암호 사용** 상자를 클릭하십시오. *Odyssey 액세스 클라이언트 사용자 가이드*의 인증 프로필 구성에 대한 설명을 참조하십시오.

네트워크 구성에 EAP-TLS 또는 기타 인증서 기반 인증 방법을 지정하는 프로필이 필요한 경우, 프로필 속성 대화 상자의 사용자 정보 탭 아래 인증서 하위 탭에서 **내 스마트 카드 리더의 로그인 인증서 사용**을 선택하십시오. 이러한 연결을 구성하는 옵션은 다음과 같습니다.

- **실패 시 대체 설정 사용**—Windows 로그인 전에 실시할 연결에 대한 대체 우선 802.1X 어댑터와 프로필(또는 무선 어댑터 네트워크)을 제공합니다. 표시된 어댑터/네트워크 쌍을 사용한 연결 시도가 실패하고 실패 코드가 반환될 경우 대체 구성에 적용됩니다.

이 옵션을 사용하는 예를 들자면, Windows 로그인 이전의 연결을 위해 대체 802.1X 우선 어댑터(및 프로필)를 제공하는 경우를 들 수 있습니다. 또 다른 예로는 실패 시 대체 어댑터와 네트워크를 제공하는 것입니다. OAC가 대체 설정을 자동으로 사용하여 연결을 시도합니다.



참고: 대체 설정 옵션은 동일한 유형의 연결에 적용됩니다. 즉, 무선 연결이 실패한 경우, 대체 어댑터와 네트워크도 무선이어야 합니다. 연결 실패 시, 무선 연결에서 유선 연결로, 또는 유선에서 무선으로 연결을 전환하는 것은 유효하지 않습니다.

이 옵션에 대한 대체 설정을 구성하기 전에 초기 설정에서 대체 어댑터 및 프로필을 구성하십시오.

이 옵션을 선택한 후 **대체 설정 편집** 단추를 선택한 다음 대체 어댑터와 네트워크를 선택하십시오.

- **연결 시 확인 메시지 표시**—로그인 시 프롬프트 화면을 네트워크 연결 전에 표시할지 여부를 제어하는 3가지 옵션이 있습니다. 옵션:
 - **표시하지 않음**—연결 시 연결 시도가 실패하더라도 사용자에게 메시지가 표시되지 않도록 하려면 이 옵션을 선택합니다.
 - **연결 실패 시**—연결 시도가 실패한 경우에만 사용자에게 메시지를 표시하려면 이 옵션을 선택합니다.
 - **네트워크에 연결하기 전**—사용자가 Windows에 로그인할 때마다 메시지를 표시하려면 이 옵션을 선택합니다.
- **Odyssey 액세스 클라이언트를 사용하여 네트워크에 연결하기 전에 사용자의 데스크톱이 나타날 때까지 대기**—사용자가 네트워크 어댑터에 연결할 때 Windows에 로그인 하기 전 연결 설정을 덮어씁니다.

유선 어댑터를 선택하십시오. 그러면, OAC가 데스크톱이 나타난 후에 연결됩니다.

시스템 계정 연결 구성

시스템 계정의 목적은 사용자가 아닌 실제 시스템(컴퓨터)을 네트워크에 연결하고 인증하는 것입니다. 이 프로세스에는 해당 시스템에 할당된 IP 주소 지정이 포함됩니다(레이어 2 네트워크 연결). 네트워크 연결 IP 주소 할당은 사용자 로그인 전에 실시됩니다. 이는 사용자가 연결하기 전에 도메인 차원의 리소스와 드라이브 매핑을 설정하는 데 유용합니다.

사용자 인증의 경우, 네트워크에 연결할 때 다른 자격 증명이 필요하므로 시스템 인증과 다릅니다. 실제 시스템에 네트워크 액세스가 있을 수 있지만 사용자가 로그인하고 인증받으려면 별도의 프로세스가 필요합니다.

시스템 계정 연결을 구성할 경우, 시스템 계정 연결을 위해 인증 프로필 옵션(사용할 자격 증명, 사용 네트워크 등)도 구성해야 합니다. "시스템 계정 프로필 옵션" (페이지 25)을 참조하십시오.

사용자 자격 증명이 아닌 시스템 자격 증명을 사용하여 시스템 시작 시 네트워크에 연결하려면 연결 설정 도구에서 **시스템 계정** 탭을 선택하고, **시스템 계정을 사용하여 네트워크 연결 활성화** 확인란을 선택합니다. 그런 상호 다음 상호 배타적인 옵션 중 하나를 선택합니다.

- **시스템 연결의 활성화 유지, 사용자가 시스템 연결을 통해 연결됨**—사용자가 로그인한 후에도 시스템 차원의 네트워크 연결을 유지합니다. 이 옵션을 사용하면 사용자가 네트워크 연결을 제어할 수 있는 범위가 줄어들기는 하지만 네트워크 리소스에는 여전히 액세스할 수 있습니다. 사용자가 상태 정보를 보고 네트워크로 재연결할 수는 있지만 기존 OAC 구성을 변경할 수는 없습니다.

이 옵션은 여행사에서와 같이 여러 사용자가 유사한 작업을 수행하며 업무 수행을 위해 사무실 내 사용 가능한 컴퓨터를 무작위로 사용하는 환경을 지원합니다. 시스템은 인증되어야 하지만 사용자는 인증되지 않아도 됩니다.

- **시스템 연결 삭제, 사용자가 자체 자격 증명을 사용하여 연결해야 함**—시스템 연결을 해제하고 사용자가 로그인할 때 사용자의 Windows 자격 증명을 바탕으로 네트워크를 자동으로 연결합니다. 이 연결 유형을 사용하면 시스템 연결이 활성화된 상태보다 네트워크 액세스의 제한이 감소됩니다. 인증된 후에 사용자는 Odyssey 액세스 클라이언트 관리자를 사용하여 연결 설정을 수정하거나 볼 수 있습니다.

로그인한 사용자가 없을 때에도 종점 시스템이 연결되어야 하는 경우 이 옵션을 사용하십시오. 이 시스템 연결은 원격 관리 작업이나 근무 외 시간에 실행되는 시스템 서비스 스크립트를 지원할 때 사용됩니다. 해당 시스템에서 네트워크 액세스가 필요한 사용자의 경우, 사용자 자격 증명을 제공해야 합니다.

사용자가 로그오프하면, 연결이 시스템 계정으로 복귀됩니다.

이 옵션을 선택하면 **사용자 계정** 탭을 클릭하여 사용자 연결을 위한 타이밍을 설정하십시오.

다음 타이밍 옵션 중 하나를 선택합니다.

- 사용자 데스크톱이 나타난 후
- Windows 로그인 후 데스크톱이 나타나기 전
- 다음 설정을 사용하여 Windows에 로그인 하기 전

시스템 계정 연결 설정 구성

선택 사항을 바탕으로 연결 설정을 구성하려면:

1. Odyssey 액세스 클라이언트 관리자 에서 **연결 설정** 도구를 더블 클릭하여 엽니다.
2. 시스템 계정 탭에서 시스템 네트워크 연결 옵션을 선택합니다.
3. 네트워크 연결 설정을 구성합니다.
4. **초기 설정** 도구를 더블 클릭하여 새로운 사용자 계정 설정을 구성하여 시스템 연결이 설정된 다음 사용자가 자신의 자격 증명을 사용하여 연결하도록 합니다.

시스템만 연결 구성

사용자 자격 증명에 의존하지 않고 네트워크에서 클라이언트 시스템을 식별하기 위해, 시스템 인증을 사용하여 네트워크에 모든 클라이언트 시스템을 연결할 수 있습니다. 이러한 기능은 시스템 관련 시작 프로세스가 있는 경우 유용합니다. 이러한 기능을 이용하면 사용자가 로그오프 상태인 경우에도 클라이언트 시스템의 네트워크 연결을 유지할 수 있습니다. 그러면, 사용자가 로그인하지 않아도 Windows가 실행 중인 한 시스템이 항상 네트워크에 연결되어 있게 됩니다. 이 기능은 근무 외 시간에 스크립트를 실행하는 경우와 원격 관리 작업의 경우 유용합니다.

시스템만 연결을 구성하려면, 다음 단계를 따르십시오.

1. **연결 설정** 도구를 더블 클릭합니다.
2. 시스템 계정 탭을 클릭하고 시스템 계정을 사용하여 네트워크 연결 활성화를 선택합니다.
3. 시스템 연결의 활성화 유지를 선택합니다.
4. **확인**을 클릭합니다.
5. 시스템 계정 도구를 더블 클릭합니다. 네트워크, 어댑터, 프로파일 등을 비롯하여 시스템 네트워크 연결을 설정한 다음, 시스템 계정 도구를 닫습니다. 시스템 계정 프로필 지정에 대한 상세 정보는 "시스템 암호 구성" (페이지 26)을 참조하십시오.

사용자 연결로 전환되는 시스템 연결 구성

시스템 자격 증명을 사용하여 모든 클라이언트 시스템을 네트워크에 연결한 다음, 사용자가 로그인할 때 사용자 인증을 요구할 수 있습니다. 이 옵션을 사용하면 사용자가 로그인하기 전에 Windows 시작 시 네트워크 작업을 수행한 다음 사용자가 로그인할 때 인증된 사용자 차원 네트워크 연결로 전환할 수 있습니다. 즉, 야간이나 일반적으로 사용자가 사무실에서 근무하지 않는 시간 동안 유지관리 스크립트와 백업을 실행할 수 있음을 의미합니다.

사용자 연결로 전환하는 시스템 연결을 구성하려면:

1. Odyssey 액세스 클라이언트 관리자에서 **연결 설정** 도구를 더블 클릭합니다.
2. 시스템 계정 탭을 클릭하고 시스템 계정을 사용하여 네트워크 연결 활성화를 선택합니다.

3. 시스템 연결 삭제를 선택합니다.
4. 사용자 계정 탭을 선택하고, 사용 가능한 사용자 인증 타이밍 옵션 중 하나를 선택한 다음, 확인을 선택합니다.
5. 시스템 계정 도구를 더블 클릭합니다. 시스템 계정 대화 상자가 나타납니다. 네트워크 대화 상자, 신뢰 서버 대화 상자, 어댑터 대화 상자, 프로필 대화 상자를 사용하여 시스템 네트워크 연결을 구성합니다. 시스템 계정 프로필 지정에 대한 상세 정보는 "시스템 암호 구성" (페이지 26)을 참조하십시오.
6. 시스템 계정 도구를 닫습니다.
7. 초기 설정 도구를 더블 클릭합니다. 초기 설정 도구 대화 상자가 나타납니다. 프로필 대화 상자, 네트워크 대화 상자, 신뢰 서버 대화 상자, 어댑터 대화 상자 등을 이용하여 사용자 네트워크 연결을 구성합니다.
8. 병합 규칙 도구를 더블 클릭하여 잠가야 하는 구성 기능을 잠급니다.
9. 작업을 마치면 초기 설정 도구를 닫습니다.

GINA를 사용하여 Windows 로그인 전에 연결을 구성

GINA는 OAC 그래픽 식별 및 인증 모듈입니다. GINA는 Windows 로그인 프로세스가 완료되기 전에 실행되는 대체 가능한 DLL (dynamic link library: 동적 링크 라이브러리)입니다. GINA는 Windows 로그인 전에 네트워크 연결이 실시되도록 해주는 도구입니다. GINA는 Windows 로그인 대화 상자에서 사용자 로그인 자격 증명을 캡처하고, 실제 Windows 로그인을 지연시켜 다른 설정 프로세스와 스크립트가 먼저 실행될 수 있게 합니다. 사용자가 Windows 로그인 자격 증명을 입력하면, 로그인 프로세스와 네트워크 연결이 완료되기 전에 GINA가 이를 바로 캡처하여 사용자를 인증하는 데 사용합니다. 이렇게 함으로써 사용자가 연결되기 전에 네트워크에서 인증됩니다.

Windows 로그인 전에 연결하면 네트워크 연결이 필요한 시작 프로세스가 있을 때 유용합니다. 회사에서 Active Directory를 사용자 데이터베이스로서 사용하는 경우에도 유용한 도구입니다.




참고: 이러한 유형의 네트워크 연결을 사용할 수 있도록 하려면 Odyssey GINA 모듈을 설치해야 합니다.

Odyssey GINA는 Windows GINA 모듈에 익숙하고 사용법을 이해하는 관리자를 위한 고급 구성 도구입니다. Odyssey GINA 모듈은 Windows GINA를 선점하며 OAC 연결과 인증만을 위한 것입니다.



참고: Windows Vista 시스템에서 여기 설명된 GINA 관련 기능은 자격 증명 제공자가 제공합니다. Odyssey GINA 화면은 두 플랫폼 모두에서 동일하므로, 대화 상자는 자격 증명 제공자 도구를 GINA로 칭합니다.

Vista 시스템에서는 GINA 계정에 대한 별도의 로그인 타일(또는 아이콘)이 사용되며, 타일은 OAC 아이콘을 보여 줍니다 .

Odyssey GINA 모듈 설치

GINA 모듈을 설치하려면:

1. 연결 설정 도구의 GINA 탭에서 **Odyssey GINA 모듈 설치** 단추를 클릭합니다.
2. 연결 설정 도구의 사용자 계정 탭 아래에서 Windows 로그인 전에 연결 설정을 구성합니다.

Odyssey GINA 모듈 제거

Odyssey 액세스 클라이언트 GINA 모듈을 제거하려면:

1. 연결 설정 도구의 GINA 탭에서 **Odyssey GINA 모듈 제거** 단추를 선택합니다.
2. 시스템을 재부팅하여 GINA 모듈 제거 작업을 완료합니다.

제 3자 GINA 모듈과 Odyssey GINA의 사용

제 3자 GINA 모듈을 Odyssey GINA 모듈과 함께 사용하려면, 제 3자 GINA 모듈을 설치한 후 Odyssey GINA 모듈을 설치하십시오.

제 3자 GINA 모듈을 설치하기 전에 Odyssey GINA 모듈을 설치하려면:

1. "Odyssey GINA 모듈 제거" (페이지 38)의 지침에 따라 Odyssey GINA 모듈을 제거합니다.
2. 제 3자 GINA 모듈을 설치합니다.
3. "Odyssey GINA 모듈 설치" (페이지 38)의 지침에 따라 Odyssey GINA 모듈을 설치합니다.
4. 컴퓨터를 재부팅합니다. GINA 모듈 설치하는 시스템을 재부팅해야만 완료됩니다.

Windows 로그인 시 실행되는 다른 모듈과의 GINA 호환성

Odyssey GINA 모듈은 Windows 로그인 대화 상자를 나타내는 Windows GINA 모듈 전에 실행하며 작동합니다.

OAC와 다른 로그인 모듈 사이의 상호작용과 관련하여 다음 사항에 유의하십시오.

- Microsoft Windows 로그인 화면을 대체하는 일부 응용 프로그램에 대해 OAC가 자격 증명을 묻는 메시지를 표시할 수 있습니다.
- OAC는 단일 로그인 기능을 보존하면서, 여러 로그인 모듈과 호환될 수 있습니다.
- Windows용 Novell Client의 경우, OAC는 자격 증명 정보를 묻지 않고 로그인 시 Novell 자격 증명을 사용합니다.

스마트 카드와 GINA 사용

GINA 인증과 함께 스마트 카드를 사용하려는 경우, 다음을 수행해야 합니다.

1. 구성 > 프로필 > 프로필 속성을 선택하여, EAP-PEAP, EAP-TTLS 또는 EAP-TLS (TLS는 내부 인증 프로토콜)와 같은 인증서 기반 인증 프로토콜을 사용하는 인증 프로필을 생성합니다.
2. 사용자 정보 탭을 선택하고, 로그인 이름 상자에 텍스트 문자열을 입력합니다. (로그인 이름 상자를 공백으로 두면 인증이 실패합니다.)

인증을 위해 Juniper Networks Steel-Belted Radius를 사용할 경우, 모든 텍스트 문자열이 허용됩니다. 다른 AAA 인증 서버가 있는 경우, 이 문자열에 대한 요건이 달라집니다.

3. 사용자 정보 > 인증서 탭을 선택한 다음 인증서를 사용한 로그인 허용 및 내 스마트 카드 리더의 로그인 인증서 사용을 선택합니다.



참고: GINA를 설치하는 경우 Windows 로그인 전후의 인증을 위해 스마트 카드와 암호 기반 프로토콜을 사용하는 프로필을 구성할 수 있습니다. EAP-TLS는 GINA 로그인 시 스마트 카드를 사용해서만 작동합니다.

4. 확인을 선택하여 프로필을 저장합니다.
5. *Odyssey 액세스 클라이언트 사용자 가이드*의 지침에 따라 네트워크와 서버 신뢰를 구성합니다. 1단계의 프로필이 이 네트워크와 연결되어 있는지 확인하십시오.
6. 초기 설정 도구에서 도구 > 옵션을 선택하여 필요한 옵션을 구성합니다.
7. 초기 설정 도구를 닫습니다.
8. 연결 설정 도구를 더블 클릭하고 다음을 수행합니다.
 - a. "Odyssey GINA 모듈 설치" (페이지 38)의 설명에 따라 GINA가 이미 설치되어 있지 않은 경우 설치합니다.
 - b. 사용자 계정 탭에서 적절한 Windows에 로그인 하기 전 연결 옵션을 설정하고, 2단계에서 구성한 네트워크를 선택합니다.
9. 병합 규칙 도구를 더블 클릭하고, 1단계에서 만든 프로필을 잠급니다. 또한, 잠가야 하는 기타 기능을 모두 잠급니다.



참고: FIPS 모드를 켜면 OAC 스마트 카드 PIN 관리가 비활성화됩니다.

GINA 연결 설정에 대한 다음 설명을 참조하십시오:

- 초기 설정 도구에서 모든 기본 사용자 계정 네트워크 설정을 구성할 수 있습니다. 하지만 제한된 옵션은 기본적으로 초기 설정 도구에서 비활성화되지 않으므로, 네트워크 연결을 올바르게 구성하도록 하십시오.
- 사용자가 Odyssey 액세스 클라이언트 관리자 메뉴 모음에서 **도구 > Windows 로그인 설정** 을 선택하여 기본 Windows 로그인 설정을 덮어쓰는 경우에는, 초기 설정 도구에서 기본 Windows 로그인 설정을 구성할 때에만 적용되는 기능은 사용할 수 없습니다.
- 시스템 계정 도구에서 모든 시스템 계정 네트워크 설정을 구성할 수 있습니다. 시스템 계정 도구에서 제한된 옵션은 비활성화되어 있습니다.
- 암호, 토큰 및 PIN 프롬프트 제한사항은 사용할 때마다 열거된 프로토콜에 적용됩니다(내부 또는 외부 인증 프로토콜로서).
- 스마트 카드인증서를 사용한 EAP-TLS 및 EAP-TTLS 와 같은 암호 기반 프로토콜을 포함하는 Windows에 로그인하기 전 시스템 인증을 구성할 수 있습니다. 이 경우, 사용자가 로그인하기 위해 스마트 카드 또는 Windows 암호를 사용하도록 선택하는지의 여부에 따라 인증 방법이 달라집니다. 두 가지 옵션이 모두 로그인 프롬프트와 함께 나타나며 사용자는 하나를 선택해야 합니다.

5 장

개별 OAC 기능의 권한 설정

권한 설정 개요

권한 편집기 도구를 사용하면, 개별 OAC 구성 설정을 활성화, 비활성화 또는 숨길 수 있으며, 사용자가 보거나 액세스할 수 있는 기능을 제어할 수 있습니다. 권한 편집기를 사용하면 네트워크에서 지원되는 인증 프로토콜을 정하고, 네트워크에서 지원할 무선 네트워크 속성을 제어하며, Odyssey 액세스 클라이언트 관리자 인터페이스의 일부를 비활성화하여 네트워크나 인프라넷 컨트롤러에서 연결 및 연결 해제만 하면 되는 사용자에게 간단한 인터페이스를 제공할 수 있습니다.

고급 사용자에게는 네트워크를 생성 및 구성하거나 신뢰 설정을 변경하는 기능 등과 같이 보다 많은 기능에 대한 액세스를 제공할 수 있습니다. 이 경우, 고급 사용자에게 맞춰진 별도의 사전 구성된 구성을 생성하고 배치하며, 권한 편집기를 사용하여 해당 사용자 그룹에 적합한 옵션을 활성화합니다. 선택할 수 있는 옵션은 매우 다양하므로, 필요에 따라 융통성 있게 구성을 제어할 수 있습니다.

구성에서 OAC 특정 기능을 사용자가 사용 또는 수정할 능력에 대해 사용자 정의된 기능별 제한사항을 적용할 때 이 도구를 사용합니다. 이 도구로 사용자가 변경하기를 원하지 않는 설정을 비활성화하고, 어떤 경우에는 보기 메뉴에서 커도록 선택할 수 있는 일부 기능을 비활성화하는 대신 숨길 수도 있습니다.

권한 편집기 도구에 구성하는 설정은 OAC를 사전 구성하여 배치하기 위해 사용하는 시스템에 자동으로 적용됩니다. 한 명 이상의 사용자에게 권한 구성을 내보내는 파일을 생성할 수도 있습니다. "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)을 참조하십시오.

권한 편집기에서 비활성화하는 옵션 중 Odyssey 액세스 클라이언트 관리자의 모양 제어에 관여하지 않는 옵션도 메뉴나 대화 상자에 표시됩니다. 사용자가 비활성화된 옵션에 액세스를 시도하면, 관리자가 해당 옵션을 비활성화했다는 메시지가 대화 상자에 표시됩니다.

인증 프로토콜

이 카테고리의 옵션은 EAP-SIM과 같은 개별 외부 EAP 프로토콜을 활성화 또는 비활성화합니다. 개별 프로토콜을 비활성화할 때에도 프로토콜 선택 목록에 표시됩니다. 하지만 사용자가 **확인**을 클릭하여 프로필 설정을 저장하려 할 때 오류 메시지가 유효하지 않은 프로토콜을 식별하고 모든 설정이 유효하게 될 때까지 저장 작업이 진행되지 않도록 할 것입니다.

TTLS 내부 인증 프로토콜

이 카테고리의 옵션은 MS-CHAP와 같은 개별 프로토콜을 활성화 또는 비활성화합니다. 개별 프로토콜을 비활성화할 때에도 프로토콜 선택 목록에 표시됩니다. 하지만 사용자가 **확인**을 클릭하여 프로파일 설정을 저장하려 할 때 오류 메시지가 유효하지 않은 프로토콜을 식별하고 모든 설정이 유효하게 될 때까지 저장 작업이 진행되지 않도록 할 것입니다.

TTLS 내부 EAP 프로토콜

이 카테고리의 옵션은 EAP-일반 토큰 카드와 같은 개별 내부 EAP 프로토콜을 활성화 또는 비활성화합니다. 개별 프로토콜을 비활성화할 때에도 프로토콜 선택 목록에 표시됩니다. 하지만 사용자가 **확인**을 클릭하여 프로파일 설정을 저장하려 할 때 오류 메시지가 유효하지 않은 프로토콜을 식별하고 모든 설정이 유효하게 될 때까지 저장 작업이 진행되지 않도록 할 것입니다.

PEAP 내부 인증 프로토콜

이 카테고리의 옵션은 EAP-POTP와 같은 개별 내부 PEAP 프로토콜을 활성화 또는 비활성화합니다. 개별 프로토콜을 비활성화할 때에도 프로토콜 선택 목록에 표시됩니다. 하지만 사용자가 **확인**을 클릭하여 프로파일 설정을 저장하려 할 때 오류 메시지가 유효하지 않은 프로토콜을 식별하고 모든 설정이 유효하게 될 때까지 저장 작업이 진행되지 않도록 할 것입니다.

프로필 속성

이 카테고리의 옵션은 로그인 인증의 일부로서 유효한 인증서에 대한 요건을 활성화 또는 비활성화합니다.

옵션

이 카테고리의 옵션은 사용자의 임시 신뢰를 활성화 또는 비활성화합니다. 이 옵션은 비활성화된 후에도 초기 **설정 > 도구 > 옵션** 메뉴의 보안 탭에 계속 표시됩니다. 사용자는 비활성화된 경우 이 옵션을 변경할 수 없습니다.

네트워크 속성

이 카테고리의 옵션은 피어 투 피어 네트워크 또는 특정 암호화 프로토콜과 같은 특정 네트워크 옵션을 활성화 또는 비활성화합니다. 이 카테고리의 옵션 중 하나로 SSID를 브로드캐스트하지 않는 네트워크로의 액세스를 비활성화할 수 있습니다. 이 설정은 해당 네트워크가 SSID를 사용하여 OAC에서 구성된 경우라고 해도 SSID를 브로드캐스트하지 않는 무선 네트워크로의 액세스를 끕니다. 권한 편집기 설정은 OAC의 현재 설정을 덮어씁니다.

Odyssey 제어

사용자나 외부 프로그램이 OAC를 비활성화하기 위해 Windows 레지스트리 편집을 하는 것을 방지하는 보안 옵션입니다. 모든 어댑터 관리를 위한 초기 설정 도구의 옵션과 함께 이 옵션은 사용자가 보호된 네트워크 리소스에 액세스하기 위해 인증되지 않은 다른 무선 클라이언트를 사용하지 못하게 합니다. "네트워크 어댑터 및 기타 Wi-Fi 지원 프로그램 제어" (페이지 18)을 참조하십시오.

사용자 인터페이스 설정

이 카테고리의 설정을 사용하여 도움말 메뉴의 Odyssey 액세스 클라이언트 관리자 또는 라이선스 키를 제거합니다. Odyssey 액세스 클라이언트 관리자 사이드바의 개별 설정 디스플레이를 끄고 사용자가 네트워크 보안 정책을 피할 목적으로 다른 무선 액세스 클라이언트를 사용하기 위해 OAC를 비활성화하는 Windows 레지스트리를 편집하지 못하게 합니다.



참고: Odyssey 액세스 클라이언트 관리자에 대한 액세스를 비활성화할 때, 이 도구에 대한 사용자의 자체 액세스를 비활성화할 수 있습니다. *드라이브:\Program Files\Juniper Networks\Odyssey Access Client\odClientAdministrator.exe*에서 다시 시작할 수 있습니다.

사용자 인터페이스—섹션 숨기기

이 카테고리의 옵션은 사이드바의 개별 구성 폴더(프로필, 네트워크, 자동 스캔 목록, 신뢰할 수 있는 서버, 어댑터 및 인프라넷 컨트롤러)를 숨기거나 사이드바의 전체 구성 섹션을 숨깁니다.

비활성화되지는 않았으나 숨기도록 구성된 설정은 Odyssey 액세스 클라이언트 관리자 메뉴 모음의 보기 메뉴에 표시됩니다. 사용자가 보기 메뉴에 어떠한 설정이 숨겨져 있는지 확인하고, 해당 설정을 하나씩 다시 표시할 수 있습니다. 권한 편집기에서 설정을 숨기도록 구성하는 경우, 해당 설정은 사용자가 Odyssey 액세스 클라이언트 관리자를 시작할 때마다 숨기도록 재설정됩니다.

구성 옵션을 숨기지 않으면, 보기 메뉴가 Odyssey 액세스 클라이언트 관리자 메뉴 모음에 표시되지 않습니다.

사용자 인터페이스—섹션 비활성화 및 숨기기

이 카테고리의 옵션은 사이드바의 개별 구성 폴더(프로필, 네트워크, 자동 스캔 목록, 신뢰할 수 있는 서버, 어댑터 및 인프라넷 컨트롤러)를 비활성화하여 숨기거나 사이드바의 전체 구성 섹션을 숨깁니다. 숨겨지고 비활성화된 기능은 관리자의 제어 권한을 받으며 보기 메뉴에 표시되지 않습니다. 관리자만이 이 기능을 재활성화할 수 있습니다.

권한 또는 제약 설정

개별 구성 설정에 대해 권한이나 제약을 설정하려면, 권한 편집기 도구를 엽니다. 권한 편집기 내 설정은 다음 상태를 가질 수 있습니다.

- 활성화
- 비활성화
- 숨기기

숨겨진 설정은 사용자 인터페이스 제어 전용입니다.

Odyssey 액세스 클라이언트 관리자 기능에 대한 권한을 제한하려면:

1. 확인란을 선택하여 **EAP-SIM 비활성화**와 같은 표시된 제약을 설정합니다.
(Odyssey 액세스 클라이언트 관리자과 같은 일부 기능은 비활성화된 경우 사용자에게 표시되지 않습니다.)
2. 제한할 기능을 선택한 후에 **확인**을 선택합니다.

제약을 제거하려면 확인란을 다시 지웁니다.

권한 편집기 사용 지침

다음은 권한이나 제약을 설정 또는 변경할 때 적용되는 지침입니다.

- 병합 규칙 도구에서 제한한(잠금)기능은 권한 편집기 도구에서 구성된 제한사항에서 제외됩니다.
- 제한한 기능이나 옵션은 사용자가 구성하거나 사용할 수 없지만 표시될 수 있습니다.
- **[임의의] 네트워크 비활성화**를 선택할 경우, 사용자가 [임의의] 네트워크 기능을 사용하여 지정되지 않은 네트워크에 연결할 수 없습니다. *Odyssey 액세스 클라이언트 사용자 가이드*의 네트워크 액세스 관리에 대한 설명을 참조하십시오.
- **ad-hoc 네트워크 비활성화**를 선택할 경우, 사용자는 피어 투 피어 연결을 할 수 없습니다.
- **도구 메뉴에서 Odyssey 액세스 클라이언트 관리자 제거**를 선택하면, 사용자는 Odyssey 액세스 클라이언트 관리자에서 Odyssey 액세스 클라이언트 관리자에 액세스할 수 없습니다. 따라서 EE 및 FE 라이선스로 사용할 수 있는 Odyssey 액세스 클라이언트 관리자에 대한 액세스를 제한할 수 있습니다.
- **도움말 메뉴에서 라이선스 키 제거**를 선택할 경우, 사용자는 라이선스 키를 수정하거나 볼 수 없습니다.
- 인증되지 않은 옵션 비활성화 중 하나를 선택할 경우, 사용자가 네트워크 연결에 프로필을 할당하지 않으면 지정된 암호화 프로토콜을 사용하여 네트워크 구성을 생성할 수 없습니다.
- 인증되지 않은 삭제 연결 비활성화 옵션은 암호화 금지에 대해 구성된 네트워크 설명에 적용됩니다(네트워크 속성 대화 상자에서 암호화 방법으로 없음 선택).
- 인증된 옵션 비활성화 중 하나를 선택할 경우, 사용자가 네트워크 연결에 프로필을 할당하면 지정된 암호화 프로토콜을 사용하여 네트워크 구성을 생성할 수 없습니다.
- 설정을 숨기는(비활성화하지 않고) 경우, Odyssey 액세스 클라이언트 관리자 메뉴 모음에는 숨겨진 설정을 보여주는 보기 메뉴가 표시됩니다. 사용자는 옵션을 선택하여 토글할 수 있습니다. 숨겨진 설정이 구성되지 않는 경우, 보기 메뉴는 표시되지 않습니다.

- 사용자가 Odyssey를 종료하는 것을 허용하지 않음을 선택하여, 사용자가 OAC에서 종료되지 않도록 할 수 있습니다. 이 설정을 활성화하면 시스템 트레이의 OAC 아이콘에서 종료 옵션이 제거됩니다. 이 설정을 모든 무선(Wi-Fi) 어댑터를 관리하고 모든 유선(이더넷) 어댑터를 관리하기 위한 옵션과 함께 사용하면, 사용자가 다른 무선 지원 프로그램을 사용하여 네트워크 액세스 보안 정책을 잠정적으로 우회하지 않도록 방지할 수 있습니다.



참고: 사용자가 병합 규칙 도구를 사용하여 변경하지 못하도록 구성 설정의 개별 카테고리를 잠글 수 있습니다.

6 장

병합 규칙을 사용하여 업데이트 관리

병합 규칙 개요

병합 규칙을 사용하면 초기 설정 도구에 정의된 구성 설정을 추가, 대체 또는 잠글 수 있습니다. 병합 규칙은 OAC 구성 업데이트 관리를 지원하기 위한 기능입니다. 병합 규칙은 다음과 같은 구성 설정 카테고리에 적용될 수 있으며, 다음 각 카테고리는 병합 규칙 대화 상자의 탭에 해당됩니다.

- 프로필
- 네트워크
- 자동 스캔 목록
- 인프라넷 컨트롤러
- 신뢰
- 기타

병합 규칙 사용 사례

현재 사용자 구성에 대한 업데이트에 영향을 미치는 규칙을 구성하는 병합 규칙 사용의 사례는 다음과 같습니다.

- 사용자 또는 시스템 그룹에 대해 OAC를 정기적으로 업데이트.
- 기존 구성에 네트워크, 프로필, 자동 스캔 목록, 또는 인프라넷 컨트롤러를 추가.
- 사용자의 OAC를 새 버전으로 업그레이드.
- 잠긴 구성이 새로운 시스템에 설치되도록 설정. (기본 설정은 모든 구성 설정 활성화.)
- FIPS 모드나 신뢰 설정과 같이 사용자가 변경할 수 없도록 하려는 특정 설정을 잠금. 인프라넷 컨트롤러나 해당 프로필 구성을 잠그고, 사용자에게 특정 인프라넷 컨트롤러에 연결하도록 요구할 수도 있습니다.

병합 규칙 설정

개별 병합 규칙은 다음과 같습니다. 다음 규칙은 규칙이 적용되는 설정의 카테고리에 따라 사용 가능성 여부가 달라짐에 유의하십시오.

- 없음—기존 사용자 구성에 설정을 병합하지는 않지만 새로운 사용자 계정에 대해 설정합니다.
- 없을 경우 추가—기존 사용자 구성에 설정을 추가하나, 네트워크나 프로필 이름과 같이 동일한 이름을 가진 설정이 있는 경우 덮어쓰지는 않습니다. 이 옵션은 기타 탭의 이 옵션을 사용할 수 없는 일부 항목을 제외하고 병합 규칙 도구의 모든 탭에 대해 기본 옵션입니다. 이 모드는 OAC 설치의 새로운 사용자 및 현재 사용자를 위한 구성에 영향을 줍니다. 이러한 설정은 사용자가 수정할 수 있습니다.
- 설정, 있는 경우 대체—기존 사용자 구성에 설정을 추가하고, 같은 이름의 설정이 이미 있는 경우 덮어씁니다. 이 모드는 OAC 설치의 새로운 사용자 및 현재 사용자를 위한 구성에 영향을 줍니다. 이러한 설정은 사용자가 수정할 수 있습니다.
- 사용자 정보를 제외하고 잠금—프로필과 관련된 사용자 자격 증명 정보(사용자 이름, 암호 또는 사용자 인증서)를 제외하고, 모든 기존 사용자 구성 설정을 덮어씁니다.

이 옵션은 프로필에 대해서만 사용할 수 있습니다. 이로써 사용자는 자신의 자격 증명을 제외하고 잠긴 프로필의 어떤 부분도 편집할 수 없습니다. 이러한 유형의 잠금을 적용하려면, 초기 설정 도구에서 생성한 프로필에 대한 사용자 이름 및 암호 또는 사용자 인증서를 지정하지 마십시오.

- 잠금—모든 기존 사용자 구성 설정을 설정 또는 대체하고, 사용자가 편집하지 못하도록 합니다. 기능을 잠글 때 OAC는 동일한 이름을 가진 현재 사용자 설정을 삭제하며, 새로운 또는 현재 사용자가 이 기능을 편집하지 못하게 합니다. 잠긴 기능에 대한 다음 표시자 중 하나가 표시됩니다.
 - 대화 상자의 제목 표시줄은 대화 상자에 표시된 모든 기능이 잠긴 경우 읽기 전용으로 표시됩니다.
 - 대화 상자의 탭에 표시된 텍스트는 선택된 탭의 기능이 잠긴 것을 나타냅니다.

병합 규칙에서 정한 설정은 구성하려는 시스템의 모든 사용자 설정에 적용됩니다. 변경사항은 병합 규칙을 종료하는 순간 유효해집니다. 사용자에게 구성 업데이트를 제공하거나 새로운 설치기 파일을 생성할 때 이러한 병합 규칙을 사용할 수 있습니다.

병합 규칙 설정

초기 설정 및 Windows 로그인 구성을 현재 시스템에 또는 사용자 정의 설치기에서 생성한 구성 파일에 적용하기 위한 규칙을 할당하는 데 병합 규칙 도구를 사용합니다.

병합 규칙 설정을 시작하려면:

1. **병합 규칙** 도구를 더블 클릭합니다. 병합 규칙 대화 상자가 나타납니다.
2. 하나 이상의 프로필 업데이트를 관리하려면 **프로필** 탭을 선택합니다. (마찬가지로, 네트워크, 자동 스캔 목록, 또는 인프라넷 컨트롤러에 대한 업데이트를 관리하려면, 대화 상자에서 적절한 탭을 선택합니다.)
3. 목록에 표시된 프로필에 대한 업데이트를 관리하려면 **다음 프로필만 허용**을 선택합니다. 이 옵션은 다음과 같이 구성에 영향을 줍니다.
 - 사용자는 초기 설정 도구에서 구성된 프로필만 사용할 수 있습니다.
 - 모든 사용자 프로필에 대한 모든 옵션(사용자 자격 증명 제외)이 잠겨있습니다.
 - 사용자는 자신의 구성에 새로운 프로필을 추가할 수 없습니다.
 - 사용자는 구성하는 잠긴 프로필 각각에 대해 자신의 자격 증명을 편집할 수 있습니다.
 - 이전에 구성된 프로필은 사용자가 볼 수 없으며 비활성화되어 있습니다. 이러한 프로필을 표시하려면 **다음 프로필만 허용**을 선택 해제합니다.
 - 모든 프로필을 잠그고 하나 이상의 잠긴 프로필에 대해 사용자 자격 증명을 잠그려는 경우, 사용자 자격 증명을 잠그려는 프로필을 선택하고 마우스 버튼을 사용하여 **잠금**을 선택합니다.
4. **확인**을 선택합니다.

프로필을 위한 병합 규칙 설정

하나 이상의 프로필에 대한 병합 규칙을 설정하려면:

1. 목록에서 하나 이상의 프로필 구성을 마우스 오른쪽 버튼으로 클릭하고 프로필을 선택한 다음, **병합 규칙 설정**을 선택합니다. 모든 사용 가능한 병합 모드를 열거한 상황에 맞는 메뉴가 표시됩니다.
2. 메뉴에서 5가지 구성 모드(**없음**; **없을 경우 추가**; **설정**, **있을 경우 대체**; **사용자 정보만 제외하고 잠금**; **잠금**) 중 하나를 선택합니다.

인증 프로필 업데이트를 위해 필요한 기타 병합 규칙 모드에 대해서도 동일한 단계를 반복합니다.

네트워크를 위한 병합 규칙 설정

네트워크 구성에 대한 병합 규칙을 설정하려면:

1. 병합 규칙 도구에서 **네트워크** 탭을 선택합니다. 모든 네트워크를 잠그거나 개별 네트워크에 대해 병합 규칙을 설정할 수 있습니다.
2. 목록에 표시된 모든 네트워크를 잠그려면 **다음 네트워크만 허용**을 선택합니다. 선택할 경우 다음 변경사항이 적용됩니다.
 - 사용자는 초기 설정 도구에서 구성된 네트워크만 사용할 수 있습니다.
 - 모든 사용자 네트워크의 모든 구성요소가 잠깁니다.
 - 사용자는 자신의 구성에 새로운 네트워크를 추가할 수 없습니다.
 - OAC에서 이전에 구성된 모든 네트워크는 사용자가 볼 수 없으며 비활성화됩니다. 사용자에게 보이게 하는 유일한 방법은 **다음 네트워크만 허용**을 선택 해제하는 것입니다.

개별 네트워크를 위한 병합 규칙 설정

하나 이상의 네트워크에 대한 병합 규칙을 설정하려면:

1. 목록에서 하나 이상의 네트워크 구성을 선택합니다.
2. 메뉴에서 5가지 구성 모드(**없음; 없을 경우 추가; 설정, 있을 경우 대체; 사용자 정보만 제외하고 잠금; 잠금**) 중 하나를 선택합니다.



참고: FIPS 모드가 필요한 모든 네트워크를 잠급니다. (FE만 해당)

3. **확인**을 선택합니다.

초기 설정 도구에서 구성하려는 프로필에 적용시키려는 다른 병합 규칙 모드에 대해 이 단계를 반복합니다.

자동 스캔 목록의 병합 규칙 설정

자동 스캔 목록의 병합 규칙을 설정하려면:

1. 병합 규칙 도구에서 **자동 스캔 목록** 탭을 선택합니다. 모든 자동 스캔 목록을 잠그거나 개별 자동 스캔 목록에 대해 병합 규칙을 설정할 수 있습니다.
2. 모든 자동 스캔 목록을 잠그려면 **다음 자동 스캔 목록만 허용**을 선택합니다. 자동 스캔 목록을 잠그면 다음과 같은 결과가 나타납니다.
 - 사용자는 초기 설정에서 구성된 자동 스캔 목록에만 액세스할 수 있습니다.
 - 모든 사용자 자동 스캔 목록의 모든 구성요소가 잠깁니다.

- 사용자는 구성에 새로운 자동 스캔 목록을 추가할 수 없습니다.
- OAC에서 이전에 구성된 모든 자동 스캔 목록은 사용자가 볼 수 없으며 비활성화됩니다. 이 목록을 표시하려면, **다음 자동 스캔 목록만 허용**의 설정을 선택 해제합니다.

하나 이상의 개별 자동 스캔 목록의 병합 규칙을 설정하려면:

1. 목록에서 하나 이상의 자동 스캔 목록을 선택합니다.
2. 마우스 오른쪽 버튼을 사용하여 표시된 메뉴에서 구성 모드(**없음; 없을 경우 추가; 설정, 있을 경우 대체; 잠금**) 중 하나를 선택합니다.
3. 자동 스캔 목록의 업데이트를 위해 필요한 기타 병합 규칙 모드에 대해서도 동일한 단계를 반복합니다.

인프라넷 컨트롤러의 병합 규칙 설정

인프라넷 컨트롤러의 병합 규칙을 설정하려면:

1. 병합 규칙 도구에서 **인프라넷 컨트롤러** 탭을 선택합니다. 모든 인프라넷 컨트롤러를 잠그거나 개별 인프라넷 컨트롤러에 대해 병합 규칙을 설정할 수 있습니다.
2. 모든 인프라넷 컨트롤러를 잠그려면 **다음 인프라넷 컨트롤러만 허용**을 선택합니다. 인프라넷 컨트롤러를 잠그면 다음과 같은 결과가 나타납니다.
 - 사용자는 초기 설정 도구에서 구성된 인프라넷 컨트롤러만 사용할 수 있습니다.
 - 모든 인프라넷 컨트롤러의 모든 구성요소가 잠깁니다.
 - 사용자는 새로운 인프라넷 컨트롤러를 사용자 구성에 추가할 수 없습니다.
 - OAC에서 이전에 구성된 모든 인프라넷 컨트롤러는 사용자가 볼 수 없으며 비활성화됩니다. 이 목록을 표시하려면, **다음 자동 스캔 목록만 허용**의 설정을 선택 해제합니다.
3. **확인**을 선택합니다.

신뢰의 병합 규칙 설정

이전 OAC 릴리스에서는 신뢰의 병합 규칙 설정이 기타 탭에 있었으며, 병합 규칙 설정이 전체 신뢰 테이블에 확일적으로 적용되었습니다. 이제 신뢰 구성은 병합 규칙에 대한 세부적인 구성을 제공하며, 별도의 병합 규칙 신뢰 탭에 위치합니다.

예를 들어, Acme Corporation에는 Verisign과 같이 널리 신뢰를 받고 있는 유명 루트 CA에서 발행한 자체 인증서 기관(CA)이 있습니다.

Verisign CA (설정, 대체)

Acme CA (잠금)

<임의> (잠금)

Acme CA에서는 인프라넷 컨트롤러용 등 자체 용도로 인증서를 발행할 수 있습니다. 사용자 인증이 성공하려면 Acme 직원은 해당 인증서를 신뢰해야 합니다. 일반적으로 보안 담당자는 개별 사용자가 자체 신뢰 설정을 구성할 것으로 생각하지 않습니다. 따라서, 보안 담당자는 초기 설정 도구를 사용하여 신뢰 구성을 설정하고, 병합 규칙을 사용하여 잠긴 상태의 신뢰 구성을 사용자에게 배치합니다.

보안 담당자는 신뢰 설정을 업데이트하여 기타 종속 설정을 루트(Verisign)에 추가하거나 필요한 경우 제거할 수 있습니다. 이러한 사용 사례에서, Acme CA와 그 종속 사항은 모두 Verisign CA가 신뢰를 받는 한 신뢰됩니다.

신뢰의 병합 규칙 설정 관련 주의 사항

- 기존의 신뢰할 수 있는 서버 목록에 신뢰할 수 있는 서버 항목을 추가할 수 있습니다. 또한, 종속 인증서 ID를 추가하고 그에 대한 병합 규칙을 설정할 수도 있습니다.
- 신뢰 트리의 개별 노드를 잠그도록 병합 규칙 설정을 구성할 수 있습니다. 신뢰 트리에서 항목을 잠그면, 사용자는 해당 항목의 신뢰 설정을 수정할 수 없습니다. 잠금 설정은 노드에서 자녀 노드로 전파됩니다.
- 개별 신뢰 노드에 대해 설정한 **없음** 경우 추가 또는 **설정, 있을 경우 대체**에 대한 병합 규칙은 부모 노드에도 적용됩니다. 이러한 규칙은 별도로 설정하지 않는 한, 자녀 노드에는 적용되지 않습니다.
- **없음**을 선택하면 병합 규칙의 실행을 취소할 수 있습니다.

기타 탭의 병합 규칙 설정

병합 규칙 도구에서 기타 탭을 선택합니다. 다음 설정 카테고리에 대한 구성 업데이트 규칙을 할당할 때 이 탭을 사용합니다.

- Windows 로그인 설정
- 보안 및 EAP-FAST
- FIPS 모드
- 옵션: 인터페이스(무선 제거 및 네트워크 어댑터)
- 옵션: 선점 네트워크
- 옵션: 통지(경고 및 오류 메시지의 외양 및 표시 타이밍을 제어하는 설정)

FIPS 모드 설정

(FE만 해당) 초기 설정 도구에서 FIPS 모드 설정 이러한 설정에 대한 자세한 정보는 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오. 네트워크에 FIPS 모드 연결이 필요한 경우, 초기 설정 도구에서 **FIPS 모드 켜기**를 선택하고, **FIPS 모드** 설정을 병합 규칙으로 잠글 수 있습니다.

사용자 집합에 병합 규칙을 적용하는 작업에 대한 자세한 정보는 "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)을 참조하십시오.



참고: 확인을 선택하여 병합 규칙 도구를 닫는 경우, 경고 또는 오류 메시지가 나타날 수 있습니다. 예를 들어, 유효하지 않은 병합 규칙을 할당하려 할 때 오류 메시지가 나타납니다. 이러한 오류 메시지에는 병합 규칙 오류 또는 불일치를 처리할 수 있는 유용한 정보가 포함되어 있습니다.

7 장

배치 Odyssey 액세스 클라이언트

이 장에서는 새로운 그리고 업데이트된 OAC 구성을 하나 이상의 사용자에게 배치하는 데 사용할 수 있는 방법에 대해 설명합니다. 여기에는 차후 인프라넷 컨트롤러로 가져올 수 있는 XML 형식(ZIP 파일에 포함)의 구성으로 내보내는 기능이 포함됩니다. 배치 방법:

- MSI 파일을 사용하여 사전 구성된 설정 배치.
- MSI 파일을 사용하여 업데이트된 구성 설정 배치.
- 인프라넷 컨트롤러에서 사용할 수 있도록 구성 설정 내보내기.
- 스크립트를 사용하여 업데이트된 구성 설정 배치.

사용자 정의 설치기 도구 개요

Odyssey 액세스 클라이언트 관리자 도구로 구성했던 초기 사용자 또는 시스템 설정에서 사전 구성된 설치기(MSI) 파일 또는 설정 업데이트 파일을 만들 때 이 도구를 사용합니다. 또한, 이 도구를 사용하여 구성을 사용한 OAC 라이선스 키도 배치할 수 있습니다. 일단 MSI 파일에 구성 설정을 저장하면, SMS와 같이 대량 배포, 푸시 기술 소프트웨어를 사용하여 배치할 수 있습니다. 또는, 인프라넷 컨트롤러에서 배치하는 데 사용할 수 있도록 ZIP 파일로 설정을 내보낼 수도 있습니다.

사용자에게 배치하는 구성 설정은 초기 설정, 시스템 계정, 권한 편집기, 병합 규칙 도구 등에서 다음으로 구성된 설정들입니다.

- 하나 이상의 사용자와 시스템에 배치할 사전 구성된 OAC 사본.
- 기존의 사용자와 시스템에 대해 업데이트된 OAC 구성.
- 새로운 또는 업데이트된 라이선스.

사용자 정의 설치기 도구를 엽니다

사용자 정의 도구를 열려면, Odyssey 액세스 클라이언트 관리자에서 **사용자 정의 설치기**를 더블 클릭합니다.

사용자 정의 설치기 파일과 업데이트된 사용자 구성 파일은 Odyssey 액세스 클라이언트 관리자가 아닌 Odyssey 액세스 클라이언트 관리자 도구에서 설정한 기능에서 구성을 얻습니다.

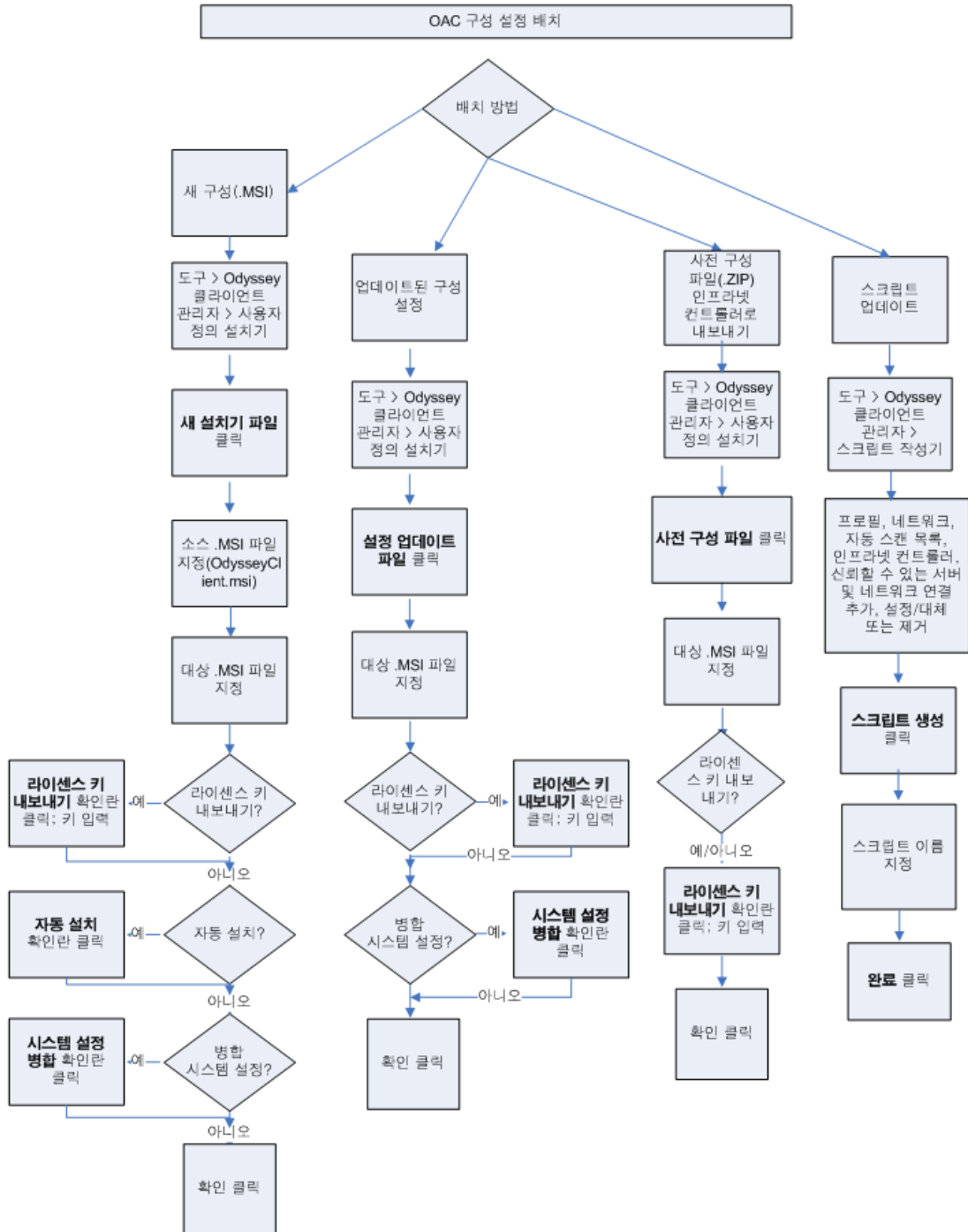
Odyssey 액세스 클라이언트 관리자에서 구성 설정을 구성 및 테스트한 다음, Odyssey 액세스 클라이언트 관리자의 사용자 정의 설치기 도구를 사용하여 템플릿에서 구성된 기본값을 사용하여 새로운 OAC 설치기 파일을 만듭니다. 구성 설정 테스트에 대한 자세한 정보는 "사용자 계정의 연결 타이밍 구성" (페이지 17)을 참조하십시오. 또한 "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)도 참조하십시오.



참고: 시스템 계정을 구성하고 설정을 MSI 파일로 저장한 후, 구성 설정이 클라이언트 시스템에 설치되면 재부팅을 해야 합니다.

배치를 위한 프로세스 흐름

그림 6: 배치를 위한 프로세스 흐름



새로운 설치기 파일 만들기

설치기 파일을 생성하려면:

1. **새로운 설치기 파일** 옵션 버튼을 선택합니다.
2. 소스 설치기(MSI) 파일을 지정합니다. 이 파일은 OAC의 완전한 제품 설치기 파일이어야 합니다. 파일 이름(및 경로)을 입력하거나 상단의 **찾아보기** 버튼을 선택합니다. 소스 파일 선택 대화 상자가 나타납니다.
3. 소스 파일 선택 대화 상자 하단의 **파일 유형** 목록을 사용하여 올바른 파일 유형을 검색합니다. 모든 현재 또는 이전 릴리스의 원본 OAC 설치기 파일 (OdysseyClient.MSI)을 소스 파일로 사용할 수 있습니다. 창에서 소스 파일을 더블 클릭하거나 **열기**를 선택합니다.
4. 필요한 경우 원하는 대상 디렉터리를 찾으려면 **찾아보기**를 선택합니다. 대상 파일 선택 대화 상자가 나타납니다. 새로운(대상) MSI 파일의 이름을 선택합니다. 파일의 이름을 입력하거나 현재 디렉터리의 기존의 파일에서 선택한 다음 **저장**을 선택합니다.

또는, **라이선스 키 내보내기**를 선택하고 배포하려는 사본 수에 대해 유효한 라이선스 키를 입력할 수도 있습니다.

5. 선택적으로, 설치 프로세스 동안 대화 상자를 표시하지 않고 설치를 실행하려면 **자동 설치**를 선택합니다. 이 옵션을 선택하고 라이선스 키를 내보내지 않은 경우, 설치한 제품에 대한 라이선스는 30일 이내에 만료됩니다.
6. 사용자 정의 설치기 파일을 생성하려면 **확인**을 선택합니다.

새로운 사용자 정의 설치기 파일 작성을 위한 지침

배치를 위해 새로운 사용자 정의 설치기 파일을 준비할 때 다음 지침에 유의하십시오.

- 사용자 정의 설치기 파일을 새로 작성하고, 라이선스 키를 내보내지 않은 경우, 설치한 제품에 대한 라이선스는 30일 이내에 만료됩니다.
- UAC 네트워크의 기본 OAC 라이선스가 제품에 기본 제공되므로, 라이선스 키를 확인하는 프롬프트는 표시되지 않습니다. 따라서, 라이선스 키를 확인할 필요가 없기 때문에 기본 라이선스 키를 바탕으로 한 사용자 정의 설치기는 항상 자동 설치됩니다.
- 병합 규칙에서 지정한 모든 잠금 규칙은 새로운 사용자 정의 설치기 파일에 적용됩니다. 사용자 정의 설치기 도구에서 **설정 업데이트 파일** 옵션을 선택하면, 병합 규칙의 관리 업데이트를 포함한 구성 파일을 생성하고 병합 규칙과 권한 편집기 도구에서 구성된 권한 제한사항을 생성할 수 있습니다. 새로운 설치기에는 설정 업데이트를 사용할 수 없습니다. "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)을 참조하십시오.

사용자 정의 업데이트 파일 작성

사용자 정의 업데이트 파일에는 사용자가 실시한 업데이트 구성 설정이 모두 들어 있습니다. 설정 업데이트 파일과 새로운 설치기 파일의 차이는 새로운 설치기 파일에는 OAC 설치를 위한 소프트웨어도 포함되어 있다는 것입니다.

사용자 정의 업데이트 파일을 작성하려면:

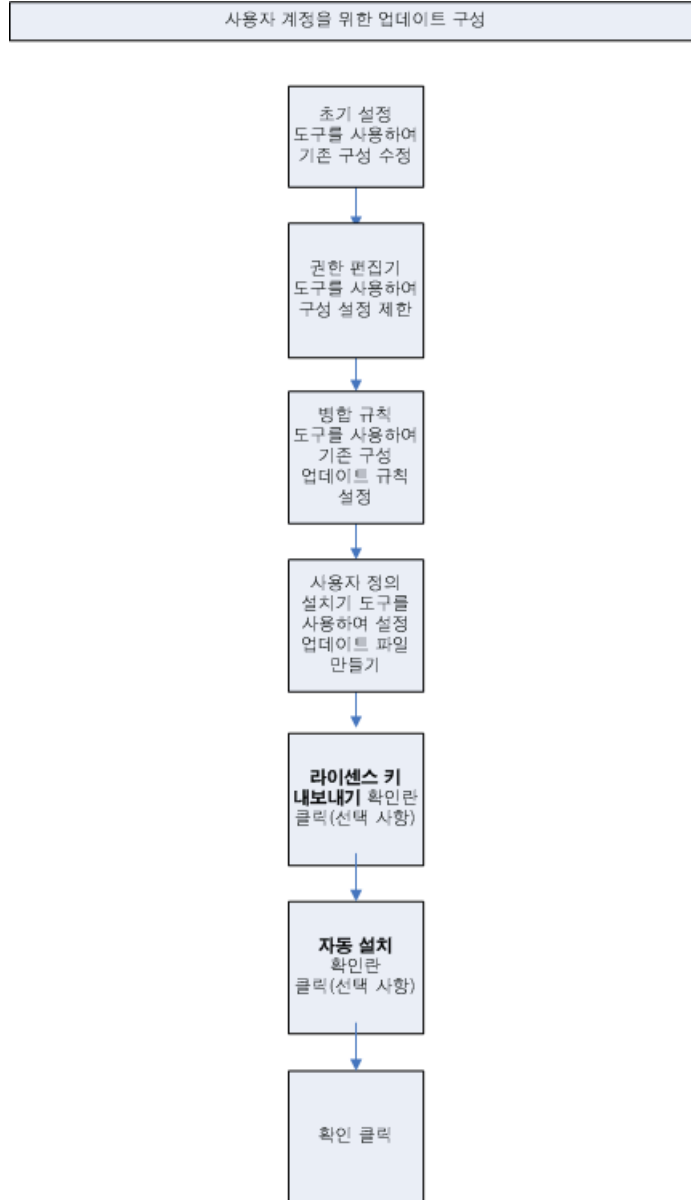
1. **설정 업데이트 파일**을 선택합니다.
2. 소스 설치기(MSI) 파일을 지정합니다. 파일 이름(및 경로)을 입력하거나 상단의 **찾아보기** 버튼을 선택합니다. **소스 파일 선택** 대화 상자가 나타납니다.
3. 소스 파일 선택 대화 상자 하단의 **파일 유형** 목록을 선택하여 올바른 파일 유형을 검색합니다. 모든 현재 또는 이전 릴리스의 원본 OAC 설치기 파일 (OdysseyClient.MSI)을 소스 파일로 사용할 수 있습니다. 이 파일을 찾지 못한 경우, 제품 CD의 클라이언트 디렉터리에서 이 파일을 찾으십시오. 창에서 소스 파일을 더블 클릭하거나 **열기**를 선택합니다.
4. 필요한 경우 원하는 대상 디렉터리를 찾으려면 **찾아보기**를 선택합니다. 대상 파일 선택 대화 상자가 나타납니다. 새로운(대상) MSI 파일의 이름을 선택합니다. 파일의 이름을 입력하거나 현재 디렉터리의 기존의 파일에서 선택한 다음, **저장**을 선택합니다.
5. 선택적으로, **라이선스 키 내보내기**를 선택하고, 배포하려는 사본 수에 대해 유효한 라이선스 키를 입력합니다.
6. 설치 프로세스 동안 대화 상자를 표시하지 않고 설치를 실행하려면 **자동 설치**를 선택합니다.
7. 사용자 정의 설치기 파일을 생성하려면 **확인**을 선택합니다.

"사용자 계정 설정 업데이트를 위한 프로세스 흐름" (58 페이지의 그림 7)을 참조하십시오.

시스템 계정 설정 업데이트에 이 도구를 사용하려면, "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)을 참조하십시오.

사용자 계정 설정 업데이트를 위한 프로세스 흐름

그림 7: 사용자 계정 설정 업데이트를 위한 프로세스 흐름



사전 구성된 파일 내보내기

인프라넷 컨트롤러로 가져와 사용자에게 배치할 때 특정 사용자 역할에 매핑할 수 있는 상세한 OAC 구성 파일을 내보내려면 이 옵션을 사용합니다. 이렇게 하면, 특정 사용자 역할에 맞게 OAC 구성 파일을 조정할 수 있습니다.



참고: 이 옵션은 특히 구성이 특정 사용자 역할과 관련된 UAC 네트워크에서 인프라넷 컨트롤러로 OAC 구성을 배치하는 작업과 관련이 있습니다. 이 기능 사용에 대한 자세한 정보는 *Unified Access Control Administration Guide*의 사전 구성 설치기 사용에 대한 설명을 참조하십시오.

다음은 사전 구성 파일 작성에 유효한 Odyssey 액세스 클라이언트 관리자 도구입니다.

- 연결 설정
- 초기 설정
- 시스템 계정
- 권한 편집기
- 병합 규칙

다음 정보가 사전 구성 파일에 포함될 수 있습니다.

- 상기 표시된 Odyssey 액세스 클라이언트 관리자 도구를 사용하는 모든 사전 구성 설정.
- 라이선스 키(선택적).
- GINA 설치 여부를 나타내는 플래그. 따라서, 사전 구성 파일은 GINA가 설치 또는 업그레이드 일환으로 설치되는지 여부를 제어할 수 있습니다.

사전 구성 파일 옵션을 사용하면, OAC 설정을 ZIP 파일로 저장하여 인프라넷 컨트롤러 관리자가 해당 설정을 가져와 사용자에게 배치할 수 있습니다. ZIP 파일 내용:

- XML 파일(preconfig.xml 및 properties.xml)
- 인증서(.pfx 파일)

인프라넷 컨트롤러로 가져올 사전 구성 설정 파일을 작성하려면:

1. **사전 구성 파일**을 선택합니다.
2. **찾아보기** 버튼을 선택하고, 설정을 ZIP 파일로 저장할 위치로 이동합니다. 대상 파일 저장 대화 상자가 나타납니다. 새로운(대상) MSI 파일의 이름을 선택합니다. 파일의 이름을 입력하거나 현재 디렉터리의 기존 파일에서 선택한 다음, **저장**을 클릭합니다.
3. 선택적으로, **라이선스 키 내보내기**를 선택하고, 지정된 역할에 대해 배포할 OAC 사본에 대해 유효한 라이선스 키(엔터프라이즈 또는 FIPS 버전)를 입력합니다.
4. **확인**을 클릭합니다.

사전 구성된 ZIP 파일을 가져와 인프라넷 컨트롤러에서 사용자 역할에 해당 파일을 매핑하는 것에 대한 자세한 정보는 *Unified Access Control Administration Guide*의 *인프라넷 컨트롤러 초기 구성에 대한 설명을 참조하십시오.*

자동 설치 옵션 사용

사용자 정의 설치기 대화 상자의 **자동 설치** 옵션을 선택하면, 사용자 정의 설치기 과일을 배치하여 "자동으로"(클라이언트 사용자의 동작 없이) 업데이트를 설치할 수 있습니다.

사용자 그룹에 대해 OAC 사전 구성

사용자 정의 설치기를 작성함으로써 사용자 그룹에 배치할 프로필과 네트워크를 사전 구성할 수 있습니다. 이 사용자 정의 설치기를 사용하여 설치한 모든 OAC 사본은 기본 네트워크 구성을 가집니다. 모든 사용자에게 동일한 네트워크 구성이 필요한 경우, 사용자 정의 설치기를 작성하면 최종 사용자가 구성 정보를 입력해야 할 필요성이 줄거나 없어집니다. 새로 OAC를 설치할 필요가 없는 사용자의 경우, 동일한 설정을 사용하여 그 구성을 업데이트할 수 있습니다.

OAC 구성 설정

Odyssey 액세스 클라이언트 관리자에서 사용할 수 있는 도구를 사용하여 정의한 구성은 설정을 잠그지 않는 한 사용자가 추후 수정할 수 있는 초기 구성을 배치하는 데 사용할 수 있습니다. 홈 오피스에서 사용되는 Wi-Fi 어댑터 및 프로필과 같이 사용자가 변경할 수는 없지만 기타 설정을 추가 또는 수정할 수 있는 연결 타이밍, 인증 프로토콜, 네트워크 등의 정확한 설정을 지정하는 구성을 설정할 수 있습니다. 일단 구성을 설정하면 이를 임의의 또는 모든 OAC 사용자에게 배치할 수 있습니다.

1. 구성을 지정하고자 하는 Windows 컴퓨터에 OAC를 설치하지 않은 경우, 사용자 정의 설치기의 구성을 정의하기 전에 다음 단계를 따르십시오.
2. 네트워크 구성과 연결 옵션을 구성합니다. 몇 가지 구성 옵션을 사용할 수 있습니다. 다음 항목에 설명된 절차 중 하나를 따르십시오.
 - 사용자 계정의 연결 타이밍 구성 (페이지 17)
 - 시스템 계정 연결 활성화 (페이지 24)
 - 사용자 연결로 전환되는 시스템 연결 구성 (페이지 36)
3. 권한 편집기에서 사전 구성된 설치기에 포함될 기능 액세스 또는 제어 제한을 구성합니다. "개별 OAC 기능의 권한 설정" (페이지 41)을 참조하십시오.
4. 병합 규칙 도구에서 사전 구성된 설치기에 포함될 잠금 옵션을 구성합니다. "병합 규칙을 사용하여 업데이트 관리" (페이지 47)를 참조하십시오.
5. 네트워크 연결을 테스트합니다. 기본 구성을 정의할 때, 각 네트워크 연결을 테스트할 수 있습니다. "사용자 계정의 연결 타이밍 구성" (페이지 17)을 참조하십시오.

이제 구성이 설정되었으므로, 사전 정의된 OAC 설치기를 작성할 수 있습니다.

여러 사용자에게 배포할 업데이트 구성 OAC

다수의 사용자를 위해 OAC 구성을 업데이트할 수 있습니다. 예를 들어, 새로운 OAC 기능으로 사용자 구성을 업데이트하려는 경우, 사용자 정의 설치기의 **설정 업데이트 파일**을 선택하여 업데이트된 사용자 정의 구성 파일을 생성할 수 있습니다.

이 옵션을 사용하여 사용자 정의된 OAC 구성 설정 파일을 생성하는 경우, 구성을 업데이트하기 위해 사용자에게 이 파일을 배포할 수 있습니다. 하지만 OAC의 버전 업데이트에는 이 옵션을 사용할 수 없습니다. OAC 업데이트 구성 파일을 생성하기 전에 업데이트된 OAC 구성을 사용자 시스템에 적용하는 방법을 지정하기 위해 병합 규칙을 구성할 수 있습니다.

연결 설정 도구에서 연결 설정을 바탕으로 한 업데이트된 구성 파일, 시스템 계정 도구에서 시스템 계정 설정, 초기 설정 도구에서 사용자 설정, 병합 규칙 도구에서 잠금 옵션 등을 생성하고 권한 편집기 도구에서 특정 기능 제한사항을 설정할 수 있습니다.

업데이트 구성 파일을 생성하려면:

1. **사용자 정의 설치기** 도구를 더블 클릭합니다.
2. **설정 업데이트 파일**을 선택합니다.
3. **찾아보기**를 선택하여 대상 파일을 찾습니다. 대상 파일 선택 대화 상자가 나타납니다.
4. 대상 상자에 저장하려는 구성 파일의 이름을 입력합니다.
5. **저장**을 선택합니다.
6. **확인**을 선택하여 사용자 정의 설치기 도구를 닫습니다.
7. 사용자 시스템에 파일을 설치합니다. 시스템에 대해 관리 권한이 있는 사용자만 자신의 시스템에서 사용자 정의 업데이트 파일을 실행할 수 있습니다.

사전 구성된 네트워크 연결의 예외

다음은 구성에서 지정할 수 있는 네트워크 연결 옵션의 예외입니다.

- 클라이언트 인증서는 사전 구성할 수 없습니다. 프로필 추가 대화 상자(초기 설정 또는 시스템 계정 도구의 프로필 대화 상자 내)의 인증 탭 아래에서 **EAP-TLS**를 선택하면, 클라이언트 시스템에서 처음으로 OAC를 실행할 때 클라이언트 인증서를 선택하라는 메시지가 표시됩니다. 그러나, 초기 설정 또는 시스템 계정 도구의 신뢰할 수 있는 서버 대화 상자의 신뢰할 수 있는 루트 서버에 대한 인증서는 구성할 수 있습니다.

OAC는 자동 인증서 선택을 지원하므로 사용자에게 인증서가 하나만 있는 경우, OAC가 인증서를 묻지 않고 해당 인증서를 설치합니다. 설치된 인증서가 없거나 하나 이상의 인증서가 있는 경우, OAC는 사용자에게 인증서를 지정하라는 프롬프트를 표시합니다. 인증서가 하나뿐이지만 만료된 경우, OAC가 동일한 일반 이름을 가진 인증서를 검색합니다.

- 저장된 암호나 로그인 이름은 사전 구성할 수 없습니다.

작업 요약: 시스템 계정에 대한 업데이트 설정 병합

사용자 정의 설치기 대화 상자의 **시스템 설정 병합** 옵션을 선택하여 사용자의 OAC 구성 설정을 업데이트하면, 설정이 기존의 구성과 병합되므로 기존 OAC 구성의 특정 부분을 유지할 수 있습니다. 구성된 기존의 시스템 계정 설정으로 시스템에서 업그레이드 또는 설정 업데이트를 위한 사전 구성된 설치기를 생성할 때, **시스템 설정 병합** 확인란을 활성화하여 네트워크, 프로필, 인프라넷 컨트롤러, 자동 스캔 목록에 대한 기존의 시스템 설정을 사용자 정의 설치기의 새로운 설정으로 병합할 수 있습니다. 중복 이름의 경우, 새로운 설정이 이전 설정을 덮어씁니다. 자동 스캔 목록에는 약간 다른 기능이 있습니다. 자동 스캔 목록이 일치하는 경우, 새로운 자동 스캔 목록의 네트워크는 목록 하단에 추가됩니다.



참고: 이 기능은 시스템 계정에만 적용됩니다.

이 옵션은 사용자 정의 설치기 또는 설정 업데이트 파일을 생성할 때만 적용됩니다. 다음 작업을 수행하려면 **시스템 설정 병합** 옵션을 선택합니다.

- 대상 시스템에 새로운 자동 스캔 목록, 인프라넷 컨트롤러, 네트워크 또는 인증 프로필 추가.

네트워크를 업데이트할 때 SSID와 네트워크 이름이 현재 네트워크의 해당 설정과 일치할 경우, 업데이트된 네트워크가 현재 버전을 대체합니다.

업데이트된 구성은 현재 네트워크 구성의 개별 설정을 덮어씁니다. 현재 네트워크가 AES 암호화를 사용하고 업데이트가 TKIP을 지정할 경우, 업데이트된 암호화 설정이 기존의 설정을 대체합니다.

- 대상 시스템의 기존 인프라넷 컨트롤러, 네트워크 또는 프로필 대체.

인증 프로필과 인프라넷 컨트롤러의 경우, 업데이트의 프로필 또는 인프라넷 컨트롤러 이름이 현재 프로필 또는 인프라넷 컨트롤러 이름과 일치하면 업데이트가 현재 버전을 대체합니다.

업데이트된 구성은 현재 네트워크 구성의 개별 설정을 덮어씁니다. 현재 프로필이 TLS 인증을 사용하고 업데이트가 PEAP를 지정할 경우, 업데이트된 인증 설정이 기존의 설정을 대체합니다.

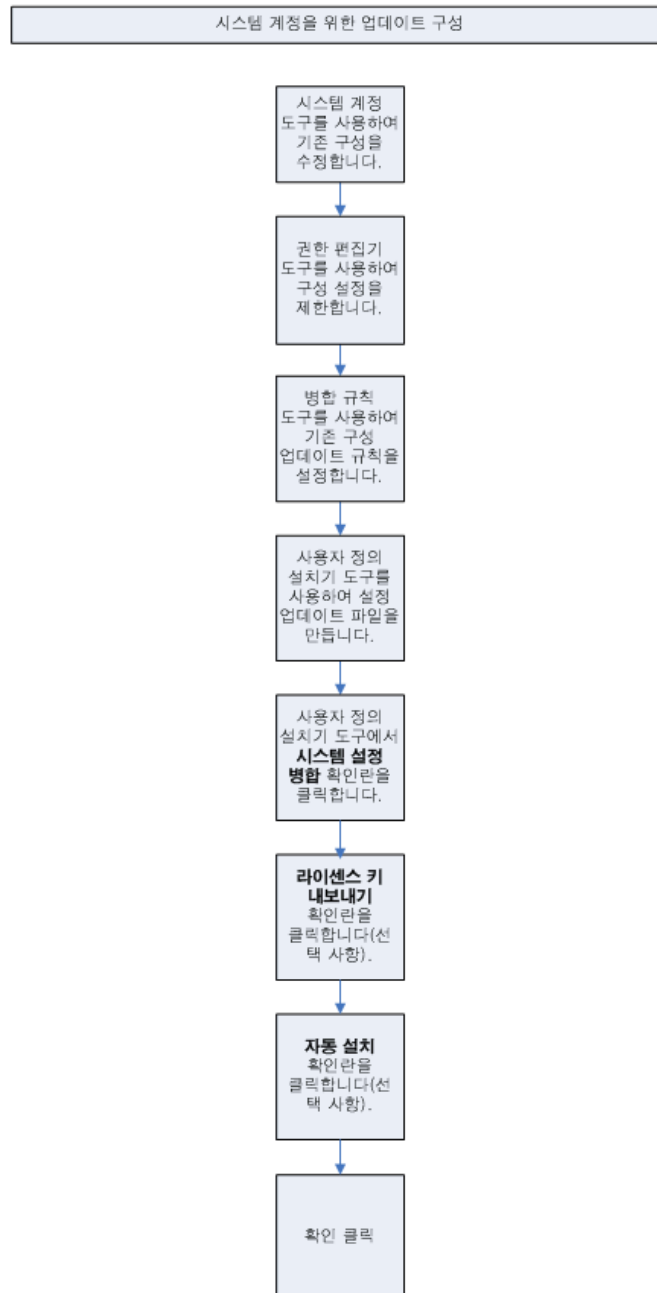
- 설치기의 자동 스캔 목록이 대상 시스템의 목록과 병합합니다. 자동 스캔 목록의 이름이 현재 자동 스캔 목록과 일치하는 경우, 업데이트의 내용은 현재 내용으로 병합되므로 업데이트에 포함되지 않은 현재 파일의 기존 네트워크가 유지됩니다.

이 옵션은 어댑터나 어댑터 설정에 적용되지 않으며 초기 설정 도구에서 정의된 구성 설정과 관련이 없습니다. "시스템 계정 설정 업데이트를 위한 프로세스 흐름" (63 페이지의 그림 8) 을 참조하십시오.

이 옵션을 활성화하려면 **시스템 설정 병합** 확인란을 선택하십시오.

시스템 계정 설정 업데이트를 위한 프로세스 흐름

그림 8: 시스템 계정 설정 업데이트를 위한 프로세스 흐름



스크립트를 사용한 OAC 배치

스크립트 작성기를 사용하여 업데이트된 구성 설정을 사용자에게 배포합니다. 이 업데이트는 네트워크, 프로필, 자동 스캔 목록에 적용됩니다. 사용자 정의 설치기 도구를 사용하여 초기 구성을 설정하고 배치한 후에는, 스크립트 작성기 도구로 기존의 구성 설정을 업데이트할 수 있습니다. 하나의 스크립트를 사용하여 프로필, 네트워크, 스캔 목록에 대한 업데이트를 배포할 수 있습니다. 스크립트의 데이터 형식은 XML입니다.



참고: 스크립트 작성기로 생성된 스크립트에는 인증서가 포함될 수 없습니다.

스크립트 작성기 개요

스크립트 작성기는 새로운 설정을 추가하고 기존 설정을 대체하거나 설정을 제거하는 OAC 구성을 업데이트하는 구성 스크립트를 만드는 데 사용됩니다. 스크립트를 사용하면 Odyssey 액세스 클라이언트 관리자가 들어 있지 않아서 Windows 데스크톱 시스템에 구성되고 MSI 파일이 아닌 스크립트로 배치되어야 하는, Windows 데스크톱 버전 이외의 플랫폼(Macintosh, Linux, Windows Mobile/CE 등)에 사전 구성된 OAC 설정을 배치할 수 있습니다.



참고: 스크립트 작성기는 설정이 구성된 시스템의 Odyssey 액세스 클라이언트 관리자 설정을 사용합니다. 스크립트는 시스템 데이터(초기 설정 도구에서 구성된 설정)가 아니라, 템플릿 시스템의 사용자 데이터에서 작성됩니다.

스크립트는 시스템 전반 데이터 또는 초기 구성 데이터와는 반대로 스크립트를 실행하는 사용자에게 영향을 주는 데이터를 향한다는 점에서 구성 파일과 다릅니다.

또한, 스크립트를 사용하면 신뢰할 수 있는 서버, 보안 및 EAP-FAST, 무선 제거, 선점 네트워크, Windows 로그인 타이밍 설정 등을 수정할 수 있습니다.

스크립트로 수행할 수 있는 작업은 다음과 같습니다.

- **추가**—사용자 구성에서 현재 정의되지 않은 설정을 추가합니다. 이 업데이트는 스크립트가 실행될 때 적용됩니다(사용자의 구성에 동일한 이름의 구성요소가 없을 경우만 해당). 추가할 수 있는 구성 설정은 로컬 시스템의 OAC 사본 내 설정이어야 합니다.
- **설정**—현재 설정을 설정 또는 대체합니다. 추가 또는 대체할 수 있는 구성 설정은 로컬 시스템의 OAC 사본 내 설정이어야 합니다.
- **제거**—구성 설정을 제거합니다. 이 설정은 로컬 시스템 구성의 일부가 아니어도 됩니다.
- **연결**—자동 연결을 활성화합니다. 무선 연결을 위해 유선 연결이나 네트워크 또는 자동 스캔 목록에 대한 프로필을 선택합니다. 사용된 어댑터는 해당 사용자에게 대해 OAC에서 구성된 첫 번째 해당 어댑터입니다.

또는, 명령행 인터페이스를 사용하여 전체 구성을 스크립트로 내보낼 수도 있습니다.



참고: 현재 클라이언트 구성의 병합 규칙으로 잠긴 설정과 이름과 유형이 동일한 스크립트에 네트워크와 같은 구성 설정이 있는 경우, 스크립트 내 업데이트 설정은 병합 규칙 도구에서 설정이 잠금 해제될 때까지 클라이언트에서 업데이트되지 않습니다. 설정이 잠금 해제된 경우, 스크립트에 가져온 업데이트된 값이 표시되며 유효하게 됩니다. 사용자가 Odyssey 액세스 클라이언트 관리자에 대한 액세스 권한을 가지고 일부 설정을 로컬에서 잠근 경우 이러한 상황이 발생할 수 있습니다.

스크립트 파일을 생성하여 배포한 후에, 사용자는 Odyssey 액세스 클라이언트 관리자에서 **도구 > 새 스크립트 확인** 메뉴 명령을 클릭하여, 이 스크립트에 액세스할 수 있습니다. "스크립트를 사용하여 증분 업데이트 배치" (페이지 70)를 참조하십시오.

스크립트 생성

스크립트 작성기로 스크립트를 생성하려면:

1. 추가 또는 수정하려는 설정을 포함하도록 구성을 설정합니다. 스크립트 작성기는 설정이 구성된 시스템의 Odyssey 클라이언트 관리자 설정을 사용합니다. 스크립트는 시스템 데이터(초기 설정 도구에서 구성된 설정)가 아니라 템플릿 시스템의 사용자 데이터에서 작성됩니다.

개별 구성 설정에 대한 자세한 정보는 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

2. **스크립트 작성기** 도구를 더블 클릭합니다. 스크립트 작성기 대화 상자가 나타납니다.
3. 생성하려는 각 스크립트에 대해 추가, 제거 또는 수정하려는 모든 항목에 대한 스크립트 작성기 설정을 구성합니다.
4. **스크립트 생성**을 선택합니다. 대상 파일 선택 대화 상자가 나타납니다.
5. 스크립트에 대한 파일 형식을 지정합니다.
 - 자동 스크립트로 스크립트를 저장하여 OAC가 사용자 개입 없이 스크립트를 실행하도록 하려면, `.odyClientScriptAuto` 파일 유형을 선택합니다.
 - 사용자가 스크립트를 실행할 선택권을 가지도록 스크립트를 저장하려면, `.odyClientScript` 파일 유형을 선택합니다.
6. 파일 유형을 선택한 다음 파일 이름을 입력합니다.
7. **저장**을 선택합니다.
8. **완료**를 선택합니다.
9. 사용자 시스템 내 올바른 디렉터리로 스크립트를 이동합니다.

스크립트를 사용한 프로필 추가 또는 설정

동일한 스크립트에서 Odyssey 액세스 클라이언트 관리자에서 구성한 임의의 수의 프로필을 추가 또는 설정할 수 있습니다.

스크립트 작성기에서 프로필을 추가 또는 설정하려면:

1. 스크롤링 목록의 추가 또는 설정 카테고리 아래에서 **프로필**을 선택합니다. Odyssey 액세스 클라이언트 관리자에서 구성한 모든 프로필이 오른쪽 목록에 표시됩니다.
2. 이 작업 카테고리에 포함하려는 모든 프로필을 선택합니다.
3. 변경 후 **완료**를 선택합니다.

주의 사항:

- 선택한 프로필에 이름 또는 암호와 같은 사용자 ID 정보를 포함시키는 경우, 결과 스크립트를 실행하는 사용자에게 전달됩니다. 암호는 암호화됩니다.
- 선택한 프로필의 사용자 ID 정보를 공백으로 두면, 해당 스크립트를 실행할 때 OAC가 이름 및/또는 암호를 사용자의 Windows ID로 대체하도록 시도합니다. 이 작업이 불가능한 경우, 사용자가 네트워크 OAC에 처음 연결할 때 사용자에게 ID 자격 증명을 묻는 메시지가 표시됩니다.
- 인증서 정보는 스크립트를 통해 전달되지 않습니다.

스크립트를 사용하여 프로필 제거

제거하려는 프로필의 이름을 가지고 있는 경우 사용자가 구성한 프로필을 제거할 수 있습니다.

프로필을 제거하려면, 다음의 단계를 따르십시오.

1. 스크롤링 목록의 제거 카테고리 아래에서 **프로필**을 선택합니다.
2. 제공된 텍스트 영역에 제거하려는 프로필 이름을 입력합니다.

스크립트를 사용하여 유선 연결을 위한 프로필 활성화

OAC 유선 연결을 위한 프로필을 활성화하려면:

1. 스크롤링 목록의 제거 카테고리 아래에서 **프로필**을 선택합니다.
2. **완료**를 선택합니다.

스크립트를 사용한 네트워크 추가 또는 설정

동일한 스크립트에서 Odyssey 액세스 클라이언트 관리자에서 구성한 하나 이상의 네트워크를 추가 또는 설정(가능할 경우 대체)할 수 있습니다.

네트워크를 추가 또는 설정하려면, 다음의 단계를 따르십시오.

1. 추가 또는 설정 카테고리에서 **네트워크**를 선택합니다. Odyssey 액세스 클라이언트 관리자에서 구성한 모든 네트워크가 오른쪽 목록에 표시됩니다.
2. 이 카테고리에 포함하려는 모든 네트워크를 선택합니다.
3. 변경 후 **완료**를 선택합니다.

스크립트를 사용하여 구성된 네트워크 제거

사용자가 구성된 네트워크의 올바른 이름(SSID)과 해당 설명을 알고 있는 경우, 해당 네트워크를 제거할 수 있습니다. 또는, 동일한 SSID를 가진 네트워크를 모두 제거하고 각 설명을 별도로 지정하지 않아도 됩니다.

모든 구성 구성요소를 제거할 수 있습니다. Odyssey 액세스 클라이언트 관리자에서 구성요소를 제거하도록 구성하지 않아도 됩니다. 스크립트가 제거하도록 이름을 입력한 구성요소는 결과 스크립트를 실행할 때 사용자 구성에서 제거됩니다.

하나 이상의 네트워크를 제거하려면, 다음의 단계를 따르십시오.

1. 스크롤링 목록의 제거 카테고리 아래에서 **네트워크**를 선택합니다.
2. 제공된 텍스트 영역에 제거하려는 이름(SSID)과 해당 네트워크의 설명(있는 경우)을 입력합니다. Odyssey 액세스 클라이언트 관리자에 나타나는 특별 네트워크 설명 구문을 사용해야 합니다. 다음 형식으로 이름/설명 쌍을 제공해야 합니다.

설명 SSID

3. 이 스크립트로 제거하려는 추가 네트워크를 입력하고, 제거하려는 각 네트워크의 이름과 설명을 입력한 후 입력을 누릅니다.
4. 변경 후 **완료**를 선택합니다.

스크립트를 사용하여 유선 연결을 위한 네트워크 활성화

OAC 무선 연결을 위한 네트워크를 활성화하려면:

1. 스크립트 작성기에서 연결 아래 **네트워크**를 선택합니다.
2. **완료**를 선택합니다.

스크립트를 사용하여 자동 스캔 목록 추가 또는 설정

Odyssey 액세스 클라이언트 관리자에서 구성한 자동 스캔 목록을 추가 또는 설정하려면:

1. 스크립트 작성기에서 추가 또는 설정 카테고리 아래 **자동 스캔 목록**을 선택합니다. Odyssey 액세스 클라이언트 관리자에서 구성한 모든 자동 스캔 목록이 오른쪽 목록에 표시됩니다.
2. 이 카테고리에 포함시킬 자동 스캔 목록을 모두 선택합니다.
3. **완료**를 선택합니다.

스크립트를 사용하여 자동 스캔 목록 제거

하나 이상의 자동 스캔 목록을 제거하려면:

1. 제거 카테고리 아래에서 **자동 스캔 목록**을 선택합니다.
2. 제공된 텍스트 영역에 제거하려는 자동 스캔 목록 이름을 입력합니다.
3. 이 스크립트를 사용하여 제거할 자동 스캔 목록의 추가 이름을 입력하고 제거할 각 자동 스캔 목록의 이름을 입력한 후 입력을 누릅니다.
4. **완료**를 선택합니다.

OAC 무선 연결에 사용할 자동 스캔 목록을 활성화하려면, 스크립트 작성기에서 연결 카테고리 아래 자동 스캔 목록을 선택합니다.

스크립트를 사용한 기타 탭의 설정 관리

추가 또는 설정 중에서 선택한 스크립트 작성기 작업 카테고리에 따라, 각 카테고리에 대한 설정 수정의 옵션이 하나 이상 제공됩니다.

- 신뢰할 수 있는 서버
- 보안 및 EAP-FAST
- 인터페이스(무선 제거 및 네트워크 어댑터)
- 선점 네트워크
- 통지(경고 및 오류 메시지의 외양 및 표시 타이밍을 제어하는 설정)
- Windows 로그인 설정

설정 구성에 대한 자세한 정보는 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

스크립트를 사용하여 신뢰 트리 추가 또는 설정

Odyssey 액세스 클라이언트 관리자의 신뢰할 수 있는 서버 대화 상자에서 구성된 전체 신뢰 트리를 추가 또는 설정하려면:

1. 스크립트 작성기에 서 추가 또는 설정 카테고리 아래 **기타**를 선택합니다.
2. **신뢰할 수 있는 서버** 확인란을 선택합니다. 사용자가 추가한 신뢰 트리에 대해 결과 스크립트를 실행할 경우, 새로운 신뢰 항목이 기존의 신뢰 트리에 삽입됩니다. 사용자가 설정한 신뢰 트리에 대한 결과 스크립트를 실행할 경우, 전체 신뢰 트리가 대체됩니다.
3. **완료**를 선택합니다.

스크립트를 사용하여 옵션 설정 대체

Odyssey 액세스 클라이언트 관리자에서 **도구 > 옵션**을 선택하여 구성된 옵션 설정을 설정(대체)하려면:

1. 스크립트 작성기에서 추가 또는 설정 아래 **기타**를 선택합니다.
2. 선택적으로, **도구 > 옵션 > 보안 또는 도구 > 옵션 > EAP-FAST**를 선택하여, 보안 및 EAP-FAST 탭에서 구성된 설정을 포함시킵니다.
3. 선택적으로, **도구 > 옵션 > 인터페이스 > 무선 제거**를 선택하여 인터페이스 탭에서 구성된 설정을 포함시킵니다.

도구 > 옵션 > 인터페이스 탭에는 모든 유선(이더넷) 어댑터를 관리하고, 모든 무선(Wi-Fi) 어댑터를 관리할 수 있는 옵션도 포함됩니다.
4. 선택적으로, **도구 > 옵션 > 통지**를 선택하여, OAC 사용자에게 표시될 경고 및 오류 통지 메시지의 외양을 관리합니다.
5. 선택적으로, **도구 > 옵션 > 선점 네트워크**를 선택하여 Odyssey 액세스 클라이언트 관리자의 **도구 > 옵션 > 선점 네트워크** 대화 상자에서 구성된 설정을 포함시킵니다.
6. **완료**를 선택합니다.

스크립트와 SSID를 사용하여 네트워크 제거

네트워크 이름 또는 설명 문구를 사용하지 않고, SSID로 네트워크를 제거할 수 있습니다. 사용자가 하나 이상의 SSID를 제거하는 스크립트를 실행할 경우, 지정된 SSID를 가진 모든 네트워크는 사용자의 OAC 구성에서 제거됩니다.

SSID로 하나 이상의 네트워크를 제거하려면:

1. 스크롤링 목록의 제거 카테고리 아래에서 **SSID**를 선택합니다.
2. 제공된 텍스트 영역에서 제거하려는 네트워크의 SSID를 입력합니다. 특별 문구를 사용하지 않아도 됩니다.
3. 제거하려는 각 SSID의 이름과 설명을 지정한 다음 입력을 눌러 이 스크립트로 제거하려는 추가 SSID를 입력합니다.
4. **완료**를 선택합니다.



참고: 동일한 SSID를 지정하는 몇 가지 네트워크 설명을 제거하려면, 스크립트 작성기에서 네트워크 카테고리에 각 네트워크를 별도로 입력하는 것보다 이 SSID를 가진 모든 네트워크 제거를 위해 SSID 카테고리를 사용하는 것이 간편합니다.

스크립트를 사용하여 FIPS 옵션(FE만 해당) 설정 또는 대체

초기 설정 도구에서 사용자의 FIPS 모드 설정을 설정하거나 변경할 수 있습니다.

사용자의 FIPS 모드를 선택 또는 선택 취소하려면:

1. 초기 설정 도구를 더블 클릭합니다.
2. 파일 메뉴 옵션에서 **FIPS 모드 켜기** 또는 **FIPS 모드 끄기**를 선택합니다. 이러한 옵션은 FIPS 라이선스를 사용하는 경우에만 표시됩니다.

스크립트를 사용하여 증분 업데이트 배치

하나 이상의 사용자에게 대해 OAC 구성을 업데이트할 수 있습니다. 예를 들어, 네트워크에 새 SSID를 추가하면 일단 네트워크를 Odyssey 액세스 클라이언트 관리자 구성한 다음 업데이트된 구성을 하나 이상의 사용자에게 배치하는 스크립트를 생성할 수 있습니다.

사용자의 OAC 설정을 업데이트하기 위한 구성 스크립트는 다음과 같은 두 가지 유형으로 나뉩니다.

- OAC가 새로운 스크립트를 폴링할 때마다 자동으로 실행되는 스크립트를 전달할 수 있습니다.
- 사용자가 선택하여 실행할 수 있는 스크립트를 전달할 수 있습니다. 스크립트와 관련된 사용자 상호 작용에 대한 자세한 정보는 *Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

구성 스크립트를 제공하여 사용자 구성을 업데이트하려면:

1. 스크립트 작성기 또는 명령행 인터페이스를 사용하여 하나 이상의 스크립트를 생성합니다.
 - 스크립트 작성기를 사용하여 스크립트를 생성하는 작업에 대한 정보는 "스크립트를 사용한 OAC 배치" (페이지 64)를 참조하십시오. 자동 스크립트 또는 일반 스크립트에 대해, 정확한 확장자를 사용하여 스크립트를 저장해야 합니다.
 - "명령을 사용하여 OAC스크립트 생성 및 로드" (페이지 71)를 참조하십시오. 사용자는 명령행 인터페이스를 사용하여 생성된 암호화된 스크립트를 실행할 수 없습니다.
2. 사용자 컴퓨터의 다음 경로에 설명된 디렉터리로 스크립트를 전달합니다.

`Application Data\Funk Software\Odyssey Client\newScripts`

여기서 `Application Data`는 일반적으로 다음 위치에 있습니다.

`volume:\Documents and Settings\username\Application Data`

영어 이외의 OS 버전에서는 이 위치가 다를 수 있습니다.



참고: Application Data 디렉터리를 보려면, 숨겨진 파일과 폴더를 표시해야 합니다.

사용하는 운영 체제에 따라, Application Data 폴더의 실제 경로는 항상 Windows 셸 프로그래머들이 사용하는 CSIDL_APPDATA 경로입니다. 일단 Application Data 폴더의 위치를 확인하면, Odyssey 액세스 클라이언트\newScripts 아래 스크립트에 액세스할 수 있습니다.

OAC는 새로운 스크립트에 대해 이 디렉터리를 자주 폴링합니다. 새 스크립트는 다음과 같이 취급됩니다.

- OAC에서 감지하면 자동으로 자동 스크립트가 실행됩니다.
- 사용자가 Odyssey 액세스 클라이언트 관리자에서 **도구 > 새 스크립트 확인**을 선택하면 다른 스크립트를 실행 또는 삭제할 수 있습니다.

스크립트가 자동 스크립트가 아니어서 수동으로 실행해야 하는 경우, 파일 시스템 내 특정 위치에 스크립트를 보관해야 하는 것은 아닙니다.

병합 규칙 또는 권한 제한이 사용자 구성에 적용되도록 하려면, "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)의 지침을 준수하십시오.

명령을 사용하여 OAC 스크립트 생성 및 로드

명령행 인터페이스를 사용하여 전체 Odyssey 액세스 클라이언트 관리자 구성을 내보내는 스크립트를 생성할 수 있습니다. 구문은 다음과 같습니다.

`odClientAdministrator arguments`

Odyssey 액세스 클라이언트 관리자 구성을 저장(내보내기)하기 위해 또는 저장된 구성을 Odyssey 액세스 클라이언트 관리자로 복원(가져오기)하기 위해 사용할 수 있는 인수는 다음과 같습니다.

```
/E[xport] = filename
/I[mport] = filename
/K = encryptionKey
/N[oSavePrivateData]
/S[ilent]
```

다음 인수를 임의로 조합하여 사용할 수 있습니다.

- `/E = filename`
- `/E = filename /N`
- `/E = filename /S`
- `/E = filename /K = encryptionKey /N`
- `/E = filename /K = encryptionKey /N /S`
- `/E = filename /K = encryptionKey`
- `/E = filename /K = encryptionKey /S`

- $I = filename$
- $I = filename /S$
- $I = filename /K = encryptionKey$
- $I = filename /K = encryptionKey /S$

이러한 명령행 인터페이스의 동작에 대한 다음과 같은 지침에 유의하십시오.

- 관리 권한이 있는 사용자만 명령행에서 스크립트를 내보내거나 가져올 수 있습니다. 단, Odyssey 액세스 클라이언트 관리자에서 **도구 > 스크립트 실행**을 선택하면 사용자가 스크립트를 가져올 수 있습니다. 사용자가 OAC 관리자에서 **도구 > 스크립트 실행** 명령을 선택함으로써 저장된 구성을 가져오게 하려는 경우, 구성을 저장할 때 `.odyClientScript` 파일 확장자를 사용하십시오.
- 사용자가 수동으로 실행할 암호화되지 않은 구성 스크립트를 저장할 때 `.odyClientScript` 파일 확장자를 사용하십시오. 이 확장자를 사용할 때, 사용자에게 Odyssey 액세스 클라이언트 관리자에서 **도구 > 스크립트 실행**을 선택하고, 이 명령행 인터페이스를 사용하여 생성한 암호화되지 않은 스크립트를 찾아보라는 지침과 함께 스크립트를 제공할 수 있습니다.
- 자동 스크립트용으로 의도된 암호화되지 않은 구성을 저장할 때 `.odyClientScriptAuto` 파일 확장자를 사용합니다. OAC는 사용자가 "스크립트를 사용하여 증분 업데이트 배치" (페이지 70)에 설명된 절차의 지침에 따라 자동 스크립트를 전달할 때 자동 스크립트를 자동으로 실행합니다.
- 여러 스위치를 사용하는 경우, 각 스위치 명령 사이에 공백을 두십시오.
- `/S`(자동 모드) 스위치를 사용하지 않는 한, 내보내기 또는 가져가기 작업 후 Odyssey 액세스 클라이언트 관리자는 항상 메시지를 표시합니다.
- 오류 수준이 항상 반환되므로, 배치 파일의 `errorlevel` 명령을 사용하여 오류 수준을 반환할 수 있습니다. 0은 성공을 의미하며, 오류 시에는 0이 아닌 값이 반환됩니다.
- 이 명령행 인터페이스를 사용하여 생성한 스크립트는 새로운 항목을 Odyssey 액세스 클라이언트 관리자 구성에 추가하고, 같은 이름의 항목이 있는 경우 기존 항목을 대체합니다.
- 암호화 키를 지정하지 않으면, OAC가 설치된 임의의 사용자가 이 스크립트를 실행할 수 있도록, OAC가 암호, WEP 키, 암호 문구를 암호화합니다. 내보낸 스크립트를 사용하여 `/K` 암호화 키 스위치를 지정한 경우, 이 Odyssey 액세스 클라이언트 관리자 구성 스크립트를 사용자 또는 다른 사용자가 가져올 때에도 지정된 암호화 키를 사용해야 합니다.
- 스크립트를 내보낼 때 `/K` 스위치를 지정하면, 이 키에 대해 다음 기호는 사용할 수 없습니다. `|, &`
- 구성을 내보낼 때 `/N` 스위치를 지정한 경우, 개인 데이터(사용자 이름, 암호 및 지정한 WEP 키)는 전혀 내보내지 않습니다.
- 인증서를 내보낼 때는 이 명령행 인터페이스를 사용하지 않습니다.

- 어댑터 유형(유선 또는 무선)은 내보내지만, 어댑터 상세 정보는 내보내지 않습니다.
- 스크립트 작성기 도구를 사용하여 생성한 OAC 스크립트와 마찬가지로, Odyssey 액세스 클라이언트 관리자에서는 잠겨 있어도 내보낸 기능은 잠겨 있지 않습니다. 기능을 잠그려면, 병합 규칙 도구를 사용하고 사용자 정의 업데이트 파일을 생성하십시오. "작업 요약: 시스템 계정에 대한 업데이트 설정 병합" (페이지 62)을 참조하십시오.

8 장

PAC (Protected Access Credentials: 보호 액세스 자격 증명) 관리

PAC 관리자 도구는 EAP-FAST의 PAC (protected access credentials: 보호 액세스 자격 증명)를 관리(보기 또는 삭제)합니다.

PAC는 EAP-FAST 인증 동안 보안 ACS (access control server: 액세스 제어 서버)를 사용하여 상호 인증을 수행하는 데 사용됩니다. PAC에는 TLS 터널을 설정할 때 사용하는 임의로 생성한 암호화 키가 있으며 인증서 대신 사용됩니다.

PAC에 대한 설명 및 생성되고 서버에 제공되는 방법에 대해서는 ACS 문서를 참조하십시오.

현재 사용 중인 보호 액세스 자격 증명을 보거나 삭제하려면, **PAC 관리자** 도구를 더블 클릭하십시오.

PAC 관리자 디스플레이 새로그침

선택한 PAC 목록에 대한 디스플레이를 업데이트하려면, **새로그침**을 선택합니다.

PAC 삭제

목록에서 선택한 하나 이상의 PAC를 삭제하려면 **삭제**를 선택합니다.

PAC 관리자 종료

PAC 관리자 도구를 종료하려면 **닫기**를 선택합니다.

9 장

관리 워크플로우 예제

본 항목에서는 일반적인 관리 작업을 보여주고, 그러한 작업을 수행하기 위한 워크플로우 단계를 제공합니다. 이러한 작업을 수행하려면, OAC 관리자와 Odyssey 액세스 클라이언트 관리자를 능숙하게 사용할 수 있어야 합니다.

Windows 로그인 전에 연결하면 사용자에게 네트워크 연결을 필요로 하는 시작 프로세스가 있을 때 유용합니다. 예를 들어, OAC 및 OAC GINA 모듈을 사용하여 Windows 로그인 전에 EAP-TTLS 또는 EAP-PEAP을 인증할 수 있도록 OAC를 구성할 수 있습니다. Windows 사용자가 로그인 전에 Windows 로그인 자격 증명을 사용하여 네트워크에 연결할 수 있도록 하려면 OAC GINA 모듈을 사용합니다.



참고: OAC GINA 모듈을 설치하지 않고는 이 기능을 사용할 수 없습니다.

TTLS 또는 PEAP용 단일 사인온

서버 유효성 검사에 사용할 인증서 기관(CA) 인증서가 설치되어 있고 그 이름을 알고 있어야 합니다. 인증서는 로컬 시스템의 신뢰할 수 있는 루트 인증서 저장소에 설치되어야 합니다.

Windows 로그인 연결 전에 OAC를 구성하려면:

1. 초기 설정 도구를 사용하여 네트워크 구성을 생성합니다.
2. 연결 설정 도구를 사용하여 사용자 계정과 GINA 연결 설정을 설정합니다.
3. 연결 설정을 테스트하고 초기 설정 도구, 연결 설정 도구, 또는 두 도구 모두에서 필요에 따라 구성 설정을 업데이트합니다.

GINA를 사용하여 Windows 로그인 전에 구성을 구성

Windows 로그인 전에 연결 설정을 완료하려면 초기 설정 도구에서 네트워크 구성을 정의해야 합니다.

네트워크 구성을 구성하려면, OAC 관리자를 위한 단계와 동일한 단계를 따르십시오.

1. 어댑터를 설정합니다.
2. 프로필을 만듭니다. GINA와 함께 사용할 프로필을 생성할 때 로그인 이름은 비워둡니다.
3. 네트워크를 추가합니다.
4. 신뢰할 수 있는 서버 인증서를 설정합니다.
5. 네트워크에 연결합니다.

각 단계별 지침은 *Juniper Networks Odyssey 액세스 클라이언트 사용자 가이드*를 참조하십시오.

사용자 계정 연결 설정 및 OAC GINA 설치 지정

연결 설정을 구성하고 Odyssey GINA를 설치하려면:

1. Odyssey 액세스 클라이언트 관리자에서 **연결 설정** 도구를 더블 클릭합니다.
2. GINA 탭을 선택하고 **Odyssey GINA 모듈 설치**를 선택합니다. GINA 모듈이 설치되어 있는 경우에는 이 단계는 건너뜁니다.
3. **사용자 계정** 탭을 선택하고, **다음 설정을 사용하여 Windows에 로그인하기 전**을 선택합니다.
4. 구성 설정을 완료한 다음 **확인**을 선택합니다.

시스템 시작 시간에 인증이 필요한 경우, 사용자가 시스템 시작 시간에 시스템 계정을 사용하여 네트워크에 연결한 다음 그 연결을 해제하고 Windows 로그인 전에 사용자 자격 증명을 사용하여 네트워크에 연결하도록 시스템 계정 설정을 구성할 수 있습니다. 이 경우, 연결 설정의 시스템 계정 탭에서 시스템 계정 설정을 구성한 다음, **확인**을 선택하십시오.

Windows가 아닌 외부 데이터베이스로의 단일 사인온 인증을 위해 OAC를 사용하고자 하는 경우, **네트워크에 연결하기 전에** 묻기를 선택한 다음 **확인**을 선택하여 연결 설정 도구를 닫으십시오.

Windows 로그인 전에 설정 테스트

Windows 로그인 전에 설정을 테스트하려면:

1. 초기 설정 도구를 더블 클릭하고, 도구 > 초기 설정 다시 로드 및 테스트를 선택합니다.
2. OAC 관리자를 엽니다.
3. 사용 중인 네트워크 연결 유형(유선 또는 무선)에 따라, Wi-Fi 또는 이더넷 대화 상자에서 연결 상태를 확인합니다.
4. 초기 설정 또는 연결 설정 도구에서 설정을 수정하고, 필요한 경우 초기 설정 도구에서 다시 테스트합니다.

색인

A

| | |
|------------------|----|
| Active Directory | |
| 시스템 계정 | 26 |

E

| | |
|-----------------|----|
| EAP 방법 | |
| 시스템 자격 증명 | 26 |
| EAP-FAST 옵션 | |
| 시스템 계정 | 26 |
| EAP-TTLS | |
| 스마트 카드 | 39 |

G

| | |
|---------------------------|--------|
| GINA | |
| Novell Client 자격 증명 | 38 |
| 개요 | 37 |
| 기타 제품과의 호환성 | 38 |
| 설치 | 37, 38 |
| 스마트 카드 | 39 |
| 제거 | 38 |

O

| | |
|---------------------------------|----|
| odClientAdministrator.exe | 5 |
| odyClientScriptAuto | 65 |
| Odyssey 건너뛰기 | 34 |
| Odyssey 액세스 클라이언트 관리자 | |
| 비활성화 | 44 |
| Odyssey 통과 | 34 |
| OdysseyClient.msi | 57 |

P

| | |
|----------|---|
| PAC 관리자 | |
| 사용 | 7 |

S

| | |
|---------------------|----|
| SIM 카드 관리자 | 10 |
| SSID | |
| 스크립트를 사용하여 제거 | 69 |

V

| | |
|--------------|----|
| VLAN | |
| 시스템 계정 | 24 |

W

| | |
|-------------------------|----|
| Windows GINA | |
| Odyssey GINA와 호환성 | 38 |
| Windows 로그인 | |
| 건너뛰기 | 34 |
| 지연 | 37 |
| 타이밍 옵션 | 33 |
| Windows 로그인 | |
| 기본값 덮어쓰기 | 14 |
| Windows 로그인 설정 | 14 |
| Windows에 로그인하기 전 | |
| 덮어쓰기 | 34 |
| Windows용 Novell Client | |
| GINA와 호환성 | 38 |

ㄱ

| | |
|-----------------------|--------|
| 관리 도구 | |
| 개요 | 5 |
| 구독자 ID 모듈 | 10 |
| 구성 | |
| 계획 | 3 |
| 대체 | 34 |
| 사용자 정의 | |
| 설치기, 만들기 | 54 |
| 설정 대체 | 48 |
| 설정 배치 | 48 |
| 설정 잠금 | 48 |
| 설정 제거 | 64 |
| 설정 테스트 | 17 |
| 시스템 연결 | 22 |
| 시스템 이름 | 26 |
| 인프라넷 컨트롤러로 내보내기 | 14 |
| 클라이언트 업데이트 | 61 |
| 푸시 | 61 |
| 구성 설정 | |
| 테스트 | 10 |
| 구성 설정 테스트 | 10 |
| 권한 | |
| 활성화 또는 비활성화 | 43 |
| 권한 편집기 | |
| 사용 | 7 |
| 그래픽 식별 및 인증 | |
| GINA를 참조하십시오 | |
| 기본 | |
| 초기 사용자에게 대해 설정 | 13 |
| 기본 네트워크 | |
| 구성 | 13, 24 |

L

- 내보내기
 - 라이센스 키 57, 59
 - 명령행 71
 - 스크립트 71
 - 제약 41
- 내부 인증
 - 스마트 카드 로그인을 위한 프로토콜 39
- 네트워크
 - ad-hoc 비활성화 44
 - 기본 구성 13, 24
 - 모두 비활성화 44
 - 선점 10
 - 선호 10
 - 스크립트 67
 - 스크립트를 사용하여 제거 67
 - 시스템 인증 35
 - 자동 연결 활성화 64
 - 잠금 또는 제한 50
- 네트워크 어댑터 13, 25
- 네트워크 연결
 - Windows 로그온 전 33
 - 가장 빨리 21
 - 시스템 및 사용자 36
 - 시스템 차원 32
 - 옵션 32
 - 시스템만 36
 - 타이밍 설정 14
 - 타이밍 옵션 33
 - 타이밍 제어 32
 - 프롬프트 화면 필요 34
- 네트워크 연결 타이밍
 - 기본 설정 덮어쓰기 10

E

- 단일 로그인 5
- 대체 설정
 - 편집 34
- 대체 어댑터
 - 유선 802.1X 34
- 덮어쓰기
 - Windows 로그온 34
 - 기본 연결 설정 14
- 도메인 암호
 - 시스템 26
- 도움말 메뉴 옵션 10

R

- 라이센스 키
 - OAC 버전 ix
 - 도움말 메뉴에서 제거 44
- 로그 뷰어 10
- 로그온
 - 자격 증명 캡처 37

로그인

- Windows
 - 기본값 덮어쓰기 14
 - 신뢰, 설정 14
 - 기본 이름 구성 15
 - 사용자 정의 이름 16
- 로그인 이름
 - 꾸미기 16
- 릴리스 노트 xii

M

- 명령행
 - 내보내기 스크립트 71
 - 스크립트 71

B

- 배치
 - 구성 업데이트 53
 - 라이센스 업데이트 53
- 병합 규칙
 - 네트워크 50
 - 사용 7, 49
 - 사용 사례 47
 - 사용자 정의 설치기 60
 - 설정 48, 49
 - 자동 스캔 목록 50
 - 정기 업데이트 47
 - 프로필 49
- 비활성화
 - 구성 옵션 41
 - 기능 43

U

- 사용자 계정
 - 제한된 옵션 40
- 사용자 정의 설치기
 - 관리 도구 54
 - 사용 7, 53
 - 설정 업데이트 파일 61
- 사용자 차원 연결
 - 설정 33
 - 옵션 32
 - 타이밍 관리 32
- 사전 구성 13, 25
 - 루트 CA 13, 25
 - 인프라넷 컨트롤러 14, 25
- 사전 구성된 설정 13, 24
- 설정
 - 병합 규칙 49
 - 사전 정의 9
 - 업데이트 파일 61
 - 초기 사용자 기본값 13
- 설치
 - GINA 37
 - 자동 57
- 설치기
 - 만들기 및 사용자 정의 54
 - 새 파일 57
 - 업데이트 파일 57

| | | | |
|-----------------------------|--------|--------------------------|--------|
| 세션 재개 | 10 | 신뢰 | |
| 스마트 카드 | | 시스템 계정 요건 | 25 |
| EAP-TTLS | 39 | 신뢰할 수 있는 루트 CA | |
| GINA 사용 | 39 | 사전 구성 | 13, 25 |
| Windows 로그인용 GINA와 사용 | 39 | 신뢰할 수 있는 서버 | |
| 스크립트 | | 덮어쓰기 | 14 |
| EAP-FAST 설정 관리 | 68 | 사전 구성 | 13, 25 |
| SSID, 제거 | 69 | 잠금 | 52 |
| Windows 로그인 설정 관리 | 68 | | |
| 네트워크 | 67 | ○ | |
| 네트워크 어댑터 관리 | 68 | 암호 | |
| 네트워크 제거 | 67 | 시스템 | 26 |
| 네트워크 추가 또는 대체 | 67 | 시스템 계정 | 25 |
| 대상 파일 | 65 | 업그레이드 | |
| 데이터 형식 | 64 | 사용자 정의 설치기 | 54 |
| 명령행 | 71 | 업데이트 | |
| 무선 제거 관리 | 68 | EAP-FAST 설정 | 64 |
| 방향 | 70 | Windows 로그온 타이밍 설정 | 64 |
| 보안 설정 관리 | 68 | 무선 제거 설정 | 64 |
| 사용자에게 파일 전달 | 70 | 보안 설정 | 64 |
| 선점 네트워크 관리 | 68 | 사용자 구성 | 53, 61 |
| 신뢰 설정 관리 | 68 | 선점 네트워크 설정 | 64 |
| 인증서 | 66 | 스캔 목록 | 64 |
| 자동 스캔 목록 제거 | 68 | 신뢰할 수 있는 서버 설정 | 64 |
| 자동 스캔 목록 추가 | 68 | 연결 설정 | 64 |
| 통지 관리 | 68 | 프로필 | 64 |
| 프로필 | 66 | 연결 | |
| 프로필 제거 | 66 | Windows 로그온 타이밍 제어 | 33 |
| 프로필 추가 또는 설정 | 66 | 설정 | |
| 프로필 활성화 | 66 | GINA 요건 | 34 |
| 스크립트 가져오기 | | 유선 네트워크 | |
| 명령행 | 71 | Odyssey GINA 덮어쓰기 | 34 |
| 스크립트 생성 | 65 | 연결 설정 | |
| 스크립트 작성기 | | 개요 | 29 |
| 사용 | 7 | 사용 | 6 |
| 정의 | 64 | 연결 시 확인 메시지 표시 | |
| 시스템 계정 | | 옵션 | 34 |
| 개요 | 21 | 영역 | |
| 관리 도구 | 22 | 시스템 자격 증명 | 26 |
| 도메인 암호 | 26 | 온라인 도움말 | xii |
| 사용 | 6, 21 | 인증 | |
| 암호 자격 증명 | 25 | 레이어 2 | 2 |
| 연결 | | 레이어 3 | 2 |
| 구성 | 22 | 사용자 | 17 |
| 사용자 로그온 없이 | 36 | 설정 사전 구성 | 13, 24 |
| 사용자 로그온 전 | 36 | 스마트 카드 로그인을 위한 프로필 | 39 |
| 연결 설정 | 24, 35 | 암호 기반 | 34 |
| 연결 테스트 | 18 | 이벤트의 흐름 | 2 |
| 인증서 | 26 | 인증서 기반 | 34 |
| 자격 증명 | 26 | 인증서 | |
| 계약 | 26 | 스마트 카드 | |
| 활성화 | 24 | GINA 사용 | 40 |
| 시스템 이름 | | 스크립트 | 66 |
| 구성 | 26 | 시스템 계정 | 26 |
| 시스템 차원 연결 | | 시스템 계정에 대해 자동 선택 | 25 |
| 목적 | 32 | 시스템 계정용 CA | 25 |
| 설정 | 35 | 암호 기반 프로토콜로 구성 | 39 |
| 타이밍 | 32 | | |

인프라넷 컨트롤러
 사전 구성 14, 25
 잠금 47, 51
 인프라넷 컨트롤러의
 병합 규칙 51

ㄷ

자격 증명
 시스템 26
 자동
 설치 56
 스크립트 내보내기 71
 자동 스캔 목록
 내용 사전 구성 13, 24
 숨기기 51
 스크립트를 사용하여 추가 68
 잠금 50
 자동 스캔 목록 제거
 스크립트를 사용 68
 자동 스크립트
 전달 70
 자동 재인증 10
 잠금
 FIPS 모드 설정 52
 OAC 기능 41
 기능
 병합 규칙 49
 네트워크 50
 신뢰할 수 있는 서버 52
 인프라넷 컨트롤러 51
 자동 스캔 목록 50
 프로필 49
 재인증
 빈도수 설정 10
 자동 10
 저장
 사용자 정의 설치기 54
 설정 업데이트 파일 61
 제약
 OAC 기능 41
 PIN 프롬프트 40
 로그인 설정 40
 사용자 계정 설정 40
 암호 40
 제거 44
 토큰 40
 제품 설명서 xii

ㄹ

초기 설정
 개요 9
 관리 도구 13
 및 사용자 정의 설치기 14
 병합 규칙 9
 사용 6

ㄴ

클라이언트 업데이트 61

ㄷ

테스트
 관리 설정 17
 템플릿
 사용자 정의 설치기 54

표

푸시
 구성 61
 프로필
 스크립트를 사용하여 구성 66
 스크립트를 사용하여 활성화 66
 제한 또는 잠금 49

ㅎ

호환성
 GINA 38