



Mi-Token Enterprise Edition Installation and Administration Guide

Mi-Token version 4.3.7. Document version 1, October 2014.

© 2014 Mi-Token Inc. All rights reserved.

Mi-Token Enterprise Edition Installation and Administration Guide

© 2014 Mi-Token Inc.

All rights reserved. No parts of this work may be reproduced in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Mi-Token version 4.3.7. Document version 1, October 2014.

Published: October 2014 in Austin, Texas, United States of America

Table of contents

TABLE OF FIGURES.....	6
TABLE OF PROCEDURES	9
1 INTRODUCTION	11
1.1 ABOUT THIS DOCUMENT	11
1.2 RELATED PRODUCTS	11
1.3 AUDIENCE	11
1.4 DOCUMENT CONVENTIONS	11
1.5 OTHER DOCUMENTATION	12
1.6 TERMINOLOGY	12
1.7 OVERVIEW	14
1.8 TYPICAL USAGE SCENARIO	15
1.9 REMOTE ACCESS SYSTEMS	16
1.10 MI-TOKEN DESKTOP LOGIN INSTALLATION	16
2 PLANNING YOUR INSTALLATION	18
2.1 INSTALLATION TIMELINE	18
2.2 PERFORMANCE AND LOADING	18
2.3 MI-TOKEN COMPONENTS AND INSTALLATION OPTIONS	19
3 PREPARING FOR YOUR INSTALLATION.....	22
3.1 PREREQUISITES	22
Prerequisite knowledge	22
Connectivity	22
Server hardware	22
End-user hardware	22
Database	23
Mi-Token Windows Server	23
Windows Server 2012 components	24
Prerequisites for optional components	24
Administrative and infrastructure requirements	25
3.2 ACTIVE DIRECTORY MODIFICATIONS	26
3.3 SERVER HARDENING	26
3.4 PORTS AND PROTOCOLS TABLE	28
3.5 DEPLOYMENT TO END-USERS	29
3.6 DOWNLOAD THE MI-TOKEN SOFTWARE	29
4 MINIMAL MI-TOKEN INSTALLATION	30
4.1 QUICK-START GUIDE TO A MINIMAL MI-TOKEN INSTALLATION	30
4.2 AUTHENTICATION SERVER	30
Installing the primary authentication server	31
Windows audit logging	35
Configuring the primary server	36
4.3 INSTALLING ACTIVE DIRECTORY USER INTERFACE TOOLS	42
4.4 TESTING RADIUS SERVER INSTALLATION AND CONFIGURATION	43
4.5 SUMMARY	45
5 MINI-MANUAL FOR END-USERS	46
5.1 USING MI-TOKEN WITH THE DESKTOP TOKEN	46
Desktop Token without the Mi-Token Intranet Provisioning Website	46
Desktop Token using the Mi-Token Intranet Provisioning Website	49
Using the Desktop Token	53
Other actions with the Desktop Token	53
5.2 USING MI-TOKEN WITH SMART PHONES	55
Smart phone app without the Mi-Token Intranet Provisioning Website	56

	Smart phone app with the Mi-Token Intranet Provisioning Website	57
	Using the smart phone app	61
	Other actions with the smart phone app	61
6	ALL-ON-ONE-MACHINE INSTALLATION	63
6.1	MI-TOKEN REPORTING	63
	Installing the ODBC driver and Mi-Token Reporting	63
	Configuring Mi-Token Reporting	67
	Installing the Event Collector Service	68
	Installing the Reporting website	71
6.2	MI-TOKEN INTRANET PROVISIONING WEBSITE	73
	Installing the Mi-Token Intranet Provisioning Website	73
6.3	SUMMARY	76
7	INTRANET PROVISIONING WEBSITE ADVANCED TOPICS	78
7.1	CONFIGURING THE INTRANET PROVISIONING WEBSITE	78
7.2	INTRANET PROVISIONING WEBSITE CONFIGURATION FILES	79
	The configuration file customer.settings.config	79
	The configuration file sensitive.settings.config	84
7.3	CONFIGURING AN EMAIL ADDRESS FOR THE ADMINISTRATOR	84
7.4	TOKENS BY SMS	84
8	FULL INSTALLATION	85
8.1	INSTALLING A REPLICA AUTHENTICATION SERVER	85
8.2	INSTALLING THE API SERVICE	87
8.3	ACTIVE DIRECTORY FEDERATION SERVICES	93
8.4	SUMMARY	95
9	LICENSING	96
9.1	MI-TOKEN LICENSING SYSTEM	96
9.2	ACCESSING YOUR INSTALLATION CERTIFICATE AND ACTIVATING MI-TOKEN	97
9.3	IMPORTING LICENSE DATA	98
10	MANAGEMENT TOOLS OVERVIEW	99
11	ACTIVE DIRECTORY USERS AND COMPUTERS	100
11.1	ORGANIZING TOKENS	100
11.2	SEARCHING FOR TOKENS	101
11.3	ASSIGNING USERS TO TOKENS	102
11.4	UNASSIGNING USERS FROM TOKENS	103
11.5	TOKEN PROPERTIES	104
	Modifying token properties	104
	Adding or resetting a token PIN	105
	Resetting tokens	105
	Multiple assignation	105
	Auto-assignment	106
11.6	MANUAL PROVISIONING OF SOFT-TOKENS	106
11.7	DISABLING AND RE-ENABLING TOKENS	107
11.8	DELETING TOKENS	108
11.9	CREATING TEMPORARY TOKENS	108
11.10	BACKUP MI-TOKEN	108
11.11	PROPERTIES DIALOG BOX	109
12	ACTIVE DIRECTORY TOKENS PROPERTIES DIALOG BOX.....	110
12.1	GENERAL TAB	110
12.2	INSTALLATION INFO TAB	110
12.3	SECURITY ROLES TAB	110
12.4	SECURITY PERMISSIONS TAB	112
12.5	DOMAIN SETTINGS TAB	113
12.6	API CLIENTS TAB	114
12.7	MISCELLANEOUS TAB	116

12.8	RATE LIMITING TAB	119
12.9	INSTANCE SET TAB	119
12.10	PROXY SETTINGS TAB	119
12.11	RADIUS ATTRIBUTES TAB	120
13	MI-TOKEN UI HELPER.....	122
13.1	REQUIRED WINDOWS GROUP	122
13.2	NO-TOKEN BYPASS	123
13.3	RATE LIMITING ENABLE AND DISABLE	123
14	TROUBLESHOOTING	124
14.1	GENERAL TROUBLESHOOTING HINTS	124
14.2	TROUBLESHOOTING USER AUTHENTICATION	124
14.3	TROUBLESHOOTING RADIUS PLUGIN FAILURE	125
14.4	TROUBLESHOOTING REPLICATION	125
14.5	TROUBLESHOOTING MISSING AUDIT LOGS	126
14.6	TROUBLESHOOTING THE MI-TOKEN INTRANET PROVISIONING WEBSITE	126
	Installing the Mi-Token Intranet Provisioning Website	126
	Running the Mi-Token Intranet Provisioning Website	127
14.7	FAQs	127
14.8	ADDITIONAL SUPPORT	128
15	INSTALLATION CHECKLISTS.....	129
15.1	INFORMATION TO BE COLLECTED	129
15.2	REQUIRED FACILITIES	130
15.3	ACTIVITIES	130
16	UPGRADING	131
16.1	UPDATING THE MI-TOKEN RADIUS PLUGIN AND AD LDS DATABASE	131
17	ABOUT MI-TOKEN	133
	Contact information	133

Table of figures

Figure 1. High-level overview of a typical system using Mi-Token	15
Figure 2. Windows logon screen, showing the OTP field	17
Figure 3. Overall structure of a full Mi-Token installation	19
Figure 4. Three types of installation and possible upgrade paths	21
Figure 5. Table of ports and protocols	28
Figure 6. An authentication server, showing AD LDS, NPS and Mi-Token's NPS plugin	30
Figure 7. RADIUS plugin welcome dialog box	31
Figure 8. RADIUS plugin setup progress	31
Figure 9. RADIUS plugin end-user license agreement	32
Figure 10. RADIUS plugin installation progress	32
Figure 11. Create AD LDS Instance	32
Figure 12. AD LDS parameters	33
Figure 13. Specify the administrator account	33
Figure 14. RADIUS Plugin wizard completed	34
Figure 15. RADIUS setup successful	35
Figure 16. Group policy management	35
Figure 17. Group Policy Management Editor, showing audit policies	36
Figure 18. Mi-Token Administration UI Quick-Start icon	36
Figure 19. Mi-Token Administration UI Quick-Start, showing the <i>RADIUS plug-in management</i> tab	37
Figure 20. Mi-Token UI Helper root	37
Figure 21. Configure RADIUS client	38
Figure 22. Setting up a connection request policy	38
Figure 23. Select OTP only or OTP and Windows credentials	39
Figure 24. Connections to Microsoft routing and remote access server	40
Figure 25. Select Grant access	40
Figure 26. Allow unencrypted authentication	41
Figure 27. UI Helper: Enable Mi-Token authentication	41
Figure 28. RADIUS plugin welcome dialog box	42
Figure 29. AD UI end-user license agreement	42
Figure 30. AD UI Setup Successful	43
Figure 31. Active Directory Users and Computers	43
Figure 32. The RADIUS Tester on launch	44
Figure 33. Example ACCESS_ACCEPT	44
Figure 34. Token activation website	46
Figure 35. Download Desktop Token installer	47
Figure 36. Desktop Token end-user license agreement	47
Figure 37. Desktop Token installation	47
Figure 38. Desktop Token	48
Figure 39. Desktop Token, displaying loading code	48
Figure 40. Desktop Token, dialog box requesting a passcode	48
Figure 41. Desktop Token, displaying a 6-digit token	49
Figure 42. Mi-Token Intranet Provisioning Website activation	50
Figure 43. Download the Desktop Token installer	50
Figure 44. The Desktop Token end-user license agreement	50
Figure 45. Installing the Desktop Token	51
Figure 46. Desktop Token	51
Figure 47. Desktop Token, displaying loading code	51
Figure 48. Desktop Token, dialog box requesting a passcode	52
Figure 49. Desktop Token, displaying a 6-digit token	52
Figure 50. Desktop Token, showing the menu	53
Figure 51. Smart phone compatibility list	55
Figure 52. Mi-Token app initialization (Android)	56
Figure 53. Mi-Token app downloading, and ready (Android)	56
Figure 54. Mi-Token app activation code (Android)	57
Figure 55. Mi-Token Intranet Provisioning Website	58

Figure 56. Mi-Token Intranet Provisioning Website requesting a PIN	58
Figure 57. Mi-Token Intranet Provisioning Website about to send initialization link	58
Figure 58. Mi-Token app initialization (Android)	59
Figure 59. Mi-Token app downloading, and ready (Android)	59
Figure 60. Mi-Token app activation code (Android)	60
Figure 61. Smart phone app, showing the menu	61
Figure 62. Reporting Setup welcome	64
Figure 63. ODBC driver welcome dialog box	64
Figure 64. ODBC driver end-user license agreement	64
Figure 65. ODBC driver installation	64
Figure 66. Reporting Setup end-user license agreement	65
Figure 67. Reporting Setup wizard completed, Reporting setup successful	65
Figure 68. Reporting Setup tool	65
Figure 69. New ODBC Data Source	66
Figure 70. SQL Server cannot be found in the current domain	67
Figure 71. Select the database	67
Figure 72. ODBC data source successfully installed	67
Figure 73. Reporting Setup dialog box with 4 tabs	68
Figure 74. RADIUS Server tab: added a RADIUS server	68
Figure 75. Reporting Setup – Event Collector tab	69
Figure 76. Event Collector Service installer	69
Figure 77. Event Collector setup wizard	69
Figure 78. Event Collector end-user license agreement	70
Figure 79. Event Collector installer, showing the installation options	70
Figure 80. Event Collector installation wizard completed	70
Figure 81. Install Reporting website	71
Figure 82. Reporting end-user license agreement	71
Figure 83. Reporting IIS Settings	72
Figure 84. Reporting installation successful	72
Figure 85. Sample Mi-Token Reporting website	72
Figure 86. Mi-Token Intranet Provisioning Website welcome	74
Figure 87. Mi-Token Intranet Provisioning Website end-user license agreement	74
Figure 88. Mi-Token Intranet Provisioning Website IIS settings	74
Figure 89. Mi-Token Intranet Provisioning Website wizard complete	75
Figure 90. Mi-Token Intranet Provisioning Website setup successful	75
Figure 91. Mi-Token Intranet Provisioning Website	76
Figure 92. IIS, showing application pools	79
Figure 93. Primary and replica Mi-Token servers	85
Figure 94. Create a replica	86
Figure 95. Replica AD LDS parameters	86
Figure 96. Replica: identify the existing instance	86
Figure 97. API Service welcome dialog box	87
Figure 98. API Service setup progress	88
Figure 99. API Service end-user license agreement	88
Figure 100. API Service Custom Setup	88
Figure 101. API Service Custom Setup, showing the installation options	89
Figure 102. API Service Custom Setup, ready to install	89
Figure 103. API Service Custom Setup installation progress	90
Figure 104. API Service Custom Setup certificate generated	90
Figure 105. API Service setup completes	91
Figure 106. IIS Manager – edit bindings	91
Figure 107. API install add binding	92
Figure 108. API add site binding	92
Figure 109. AD FS welcome	93
Figure 110. AD FS end-user license agreement	94
Figure 111. AD FS adds client certificate to the Mi-Token installation	94
Figure 112. AD FS setup wizard completed	94
Figure 113. AD FS setup successful	95
Figure 114. Installation Info tab, showing your installation certificate	97

Figure 115. Importing license files	98
Figure 116. Search by Serial Number	101
Figure 117. Search by User ID	101
Figure 118. Search by YubiKey OTP	102
Figure 119. Assigning tokens	102
Figure 120. Assign token to user	103
Figure 121. Unassign Tokens	103
Figure 122. Tokens Unassigned	103
Figure 123. Token Properties	104
Figure 124. Token properties – PIN required	105
Figure 125. Auto-assignment tab	106
Figure 126. Provision soft token	107
Figure 127. Disable a token	107
Figure 128. Confirmation of temporary token	108
Figure 129. Properties dialog box	109
Figure 130. Adding a token operator	111
Figure 131. Modifying Role Permissions	112
Figure 132. Domain Settings tab	113
Figure 133. API Clients tab	114
Figure 134. New API client dialog box	115
Figure 135. View certificate	116
Figure 136. User interface dialog box, Miscellaneous tab	116
Figure 137. The Group Settings dialog box, as installed and example in use	117
Figure 138. Rate Limiting tab	119
Figure 139. Configure proxy RADIUS server	120
Figure 140. RADIUS attributes tab	120
Figure 141. UI Helper showing a connection request policy	122
Figure 142. Upgrade RADIUS plugin	131

Table of procedures

• This is the heading for a procedure	11
• To download and extract the Mi-Token software	29
• To install Mi-Token's NPS plugin	31
• To enable audit logging	35
• To add RADIUS clients	36
• To create or edit a connection request policy	38
• To test your primary RADIUS server configuration	43
• To download the Desktop Token without using the Mi-Token Intranet Provisioning Website	46
• To set up the Desktop Token without using the Mi-Token Intranet Provisioning Website	47
• To download the Desktop Token from the Mi-Token Intranet Provisioning Website	49
• To set up the Desktop Token using the Mi-Token Intranet Provisioning Website	51
• To set up the smart phone app without using the Mi-Token Intranet Provisioning Website	56
• To set up the smart phone app using the Mi-Token Intranet Provisioning Website	57
• To install the ODBC driver and Mi-Token Reporting	63
• To configure Mi-Token Reporting	67
• To add, edit or remove RADIUS servers	68
• To install the Event Collector Service	68
• To install the Reporting website	71
• To install a Key Encryption Key	73
• To install the Mi-Token Intranet Provisioning Website	73
• To configure the Intranet Provisioning Website	78
• To configure an email address for the administrator	84
• To install a replica authentication server	85
• To install the API Service	87
• To configure the HTTPS port for the API Service	91
• To disable Windows Authentication	92
• To determine the base URL of the API	92
• To install Active Directory Federation Services	93
• To access the installation certificate	97
• To import license data	98
• To access the Mi-Token Enterprise Edition UI:	100
• To set up a container	100
• To search for LCD and other hard tokens by serial number	101
• To search for tokens by assigned username	101
• To search for a Yubikey via OTP output	102
• To assign a token to a user manually	102
• To unassign a token from a user manually	103
• To view and modify a token's properties	104
• To modify a token's description and notes	104
• To manage PINs	105
• To reset event-based tokens	105
• To reset time-based tokens	105
• To access auto-assignment	106
• To manually provision a soft token to a user	106
• To disable a token from use	107
• To re-enable a token so that it can be used by a user	107
• To delete a token	108
• To create a temporary token	108
• To view user properties	109
• To find the version number you are currently running	110
• To modify assignments for the Mi-Token roles	111
• To add and remove roles	112

• To modify permissions for the Mi-Token roles	112
• To enable Mi-Token support for a selected domain	113
• To add a new partition	113
• To redesignate the primary and replica servers	113
• To manage clients	114
• To create a new client or partition	114
• To access SSL certificate details	115
• To import SSL certificates (not keys)	116
• To export SSL certificates (not keys)	116
• To enable/disable temporary tokens	117
• To add a group	119
• To remove a group	119
• To change an authentication mode in Group Settings	119
• To add or remove a row on the Rate Limiting tab	119
• To configure proxy RADIUS server support:	120
• To access the UI Helper	122
• To set a Windows group	122
• To set No-Token Bypass	123
• To set Rate Limiting	123
• To upgrade the Mi-Token RADIUS plugin	131
• To upgrade Mi-Token (Active Directory UI)	132

1 Introduction

1.1 About this document

This document is the installation and administration guide for Mi-Token Enterprise Edition, one of three primary versions of the Mi-Token two-factor authentication solution developed by Mi-Token, Inc. This guide is for installation and administration of Mi-Token on Windows Server 2012 and Server 2008.

This guide contains an overview of Mi-Token and describes, in depth, how it should be installed, configured, and managed.

If you require information about Mi-Token Enterprise Edition that you cannot locate in this manual please contact support@mi-token.com.

1.2 Related products

This document is relevant to Mi-Token Enterprise Edition (out-of-the-box). Other related products are

- API
- Cloud Services edition
- customized Banking edition

1.3 Audience

Most of this manual is directed toward systems administration personnel who are responsible for the installation, configuration and day-to-day administration of Mi-Token Enterprise Edition. Under most circumstances, Mi-Token administration responsibilities are managed by Windows system administrators. The management interface for Mi-Token Enterprise Edition is based on Microsoft's MMC management tools.

One chapter of this manual, *Mini-manual for end-users*, is directed at end-users.

Additional documentation is available from www.mi-token.com.

1.4 Document conventions

The following conventions are used throughout this manual:

Text written ***in this style*** represents commands, keywords or UI elements.

In addition:



This is the heading for a procedure



Highlights important features or instructions



Indicates care should be taken at this point in the procedure. Possible data loss could occur.

1.5 Other documentation

Related information can be found in

Mi-Token Desktop Login Experience Installation Guide

Mi-Token API GET/POST Documentation

Mi-Token Enterprise Edition Add-ins

1.6 Terminology

Mi-Token Enterprise Edition leverages a number of open source and proprietary standards together with extended features that ship with Microsoft Windows Server operating systems. To assist comprehension of the various terms and acronyms the following provides a brief description of the technology employed as part of Mi-Token Enterprise Edition.

Terminology	Description
Two-factor authentication	A mechanism whereby users must present two separate types of credentials to gain access to a system. Typically, one of these credentials is a password/PIN that the user knows. The second type of credential is usually generated by a hardware device that the user has in his/her possession, and can also be generated by software, e.g. smart phone applications. With Mi-Token, the second type of credential is a One-Time Password (OTP). Mi-Token allows enterprises to secure remote access by securing VPNs, SSL VPNs, and so forth, with RADIUS and also offer API functionality to secure corporate websites.
Active Directory	A database containing information about users, computers and other objects in a Windows domain. The Mi-Token solution for Windows uses Active Directory to look up users, their passwords, their email addresses, and cell phone numbers as required.
Active Directory Lightweight Directory Service – AD LDS	<p>This is a standalone version of the same database engine that powers the Active Directory. It has essentially the same feature set, but is separate from the core Active Directory database, thus ensuring that changes to the LDS schema as required by Mi-Token are not propagated to the underlying Active Directory database.</p> <p>Mi-Token uses AD LDS as a database to store details about tokens and to link them to users. AD LDS enables straightforward and efficient integration with a Windows domain without having to extend the domain's Active Directory schema.</p> <p>For further explanation, see <i>Active Directory modifications</i>.</p>
Active Directory UI or AD UI	Active Directory User Interface. This is a user-facing part of Active Directory, built within the MMC framework.
De-Militarized Zone – DMZ	This is a physical or logical sub-network that allows the organization to separate its corporate network from an external network (i.e. Internet), thus adding an extra layer of network security. It only exposes the organization's required external services, thus isolating the internal network from the external networks.
Hardware or hard token	A physical device (for example, a USB device or a device with an LCD display) that the user must have in their physical possession to gain access to a system.

Terminology	Description
Mi-Token server	This term denotes a Network Policy Server (NPS) with the Mi-Token plugin, connected to an AD LDS server, and communicating via LDAP.
Microsoft Management Console – MMC	MMC is a framework for a set of tools provided by Microsoft and other manufacturers. Mi-Token integrates directly with it. Mi-Token almost exclusively uses standard Windows interface paradigms, resulting in an intuitive administrative user interface.
Network Policy Server – NPS	NPS is Microsoft's RADIUS server implementation. It is included with Windows 2008 and 2012. Mi-Token provides a plugin for NPS 2008 and 2012 which checks two-factor authentication credentials.
Initiative for Open Authentication – OATH	A consortium that has defined standards for hardware-based One-Time Password tokens (amongst other standards). These are: <ul style="list-style-type: none"> • Event-based tokens. OTPs are seeded from a secret key and an incrementing counter. • Time-based tokens. OTPs are seeded from a secret key and the current time. Time-based OTPs have a potential security advantage over event-based designs as stolen codes (e.g. generated by touching a token on someone's desk) will expire within minutes. Note, however, that there is also a disadvantage – compensating for time drift can be more difficult than compensating for unused tokens from an event-based token. Mi-Token supports both of these types of tokens from any OATH-compliant vendor.
One-Time Password – OTP	These are generated by hardware and software tokens of all kinds. These codes have several characteristics: <ul style="list-style-type: none"> • Unpredictability. Only the generator/verifier can calculate the next OTP, so it cannot be guessed by anyone else. • Single-use. The verifier keeps track of the last-used OTP, implicitly or directly. This OTP cannot be used again. This prevents attackers from replaying OTPs.
Remote Authentication Dial In User Service – RADIUS	A protocol that enables users to be authenticated by having their credentials forwarded and checked by a centralized authentication server. RADIUS is a very widely implemented protocol, and enables the Mi-Token server (running Microsoft's NPS) to provide two-factor authentication for many uses. The Pluggable Authentication Module (PAM) system popular in Linux/Unix also has RADIUS support, and RADIUS is widely used on multiple platforms and platform combinations. RADIUS is used by many security hardware vendors, such as suppliers of SSL VPN appliances and the like.
Software Token	Also known as a soft-token. This is another type of token which is generated by software. This software is not exclusively specific to a single hardware. This includes a number of platforms such as smart phones, as well as standard desktop PC applications to generate OTPs. Mi-Token supports soft-tokens for a wide range of smart phones as well as older phones.
Short Message Service – SMS	A widely-used method for delivering messages to mobile phones. Mi-Token provides a service whereby users can dial a specific phone number to request an OTP. This OTP is delivered via an SMS message to the user's handset.

Terminology	Description
YubiKey	<p>A novel hardware authentication system developed by Yubico. It generates 40+ character OTPs from a very small battery-less USB device. By pretending to be a USB keyboard, the YubiKey types in the OTP so the user doesn't have to.</p> <p>Mi-Token supports an easy-to-use user self-assignment for YubiKeys. This reduces deployment costs by letting administrators simply hand out tokens to users without having to manually assign them. The Mi-Token server then assigns the YubiKey to the first user who successfully logs in with it.</p>
Crystal Tokens	An LCD hard token that displays OTP on a crystal screen. It runs on a long-lasting battery and turns off automatically when it is not in use for generating an OTP.
Secure Sockets Layer Virtual Private Network – SSL VPN	In contrast to regular VPN, SSL VPN does not require any special software installation on a client computer and can use a standard Web browser. When SSL VPN is used communication between the web browser and VPN device is encrypted using Secure Socket Layer protocol.
Active Directory Federation Services – AD FS	Software component that enables Single Sign-On (SSO) access to external services and web apps like Google Apps, Salesforce.com, Outlook Web App and others using your Active Directory credentials. Mi-Token can be integrated with AD FS to enable two-factor authentication on AD FS supported services and web apps.
Security Assertion Markup Language – SAML	An XML-based open standard data format for exchanging authentication data between parties like identity and service providers.

1.7 Overview

Mi-Token Enterprise Edition is a token-agnostic One-Time Password (OTP) two-factor authentication solution. It combines the reliability of a hardware based token with the mobility and flexibility of Soft-Tokens implemented on smart phones or desktops, together with the option of Short Message Service (SMS) as a backup authentication path. Thus, it gives an organization a reliable, flexible and highly secure solution to their two-factor authentication requirements.

Overall operation of Mi-Token is depicted in Figure 1 and a *Typical usage scenario* is presented.

Mi-Token utilizes open industry standards such as time-based OTPs and Open Authentication (OATH) Standards, with best-practice security approaches to deliver a secure two-factor authentication solution. It is a flexible delivery solution that is, at once, easy to use and highly robust in its level of security.

Mi-Token caters for a range of platforms including Enterprise Edition (out-of-the-box), API and Cloud Services editions, and our customized Banking edition.

Mi-Token Enterprise Edition leverages several key Microsoft Windows components. These include the Network Policy Server (NPS) as the RADIUS server, Internet Information Services (IIS) to host the Mi-Token Reporting website, the Mi-Token Intranet Provisioning Website, and Active Directory Lightweight Directory Services (AD LDS) as a distributed replicating fault-tolerant database for tokens issued to users.

Mi-Token Enterprise Edition does not modify the Active Directory schema, neither the forest schema nor the schema of the domain(s) it is installed in. Nor does it require a 'dedicated' server, unlike products from many other vendors.

For more information regarding the Mi-Token API and Cloud Services Edition, and the enhanced security Mi-Token Banking Edition, please contact us at sales@mi-token.com.

For all technical questions, please contact support@mi-token.com.

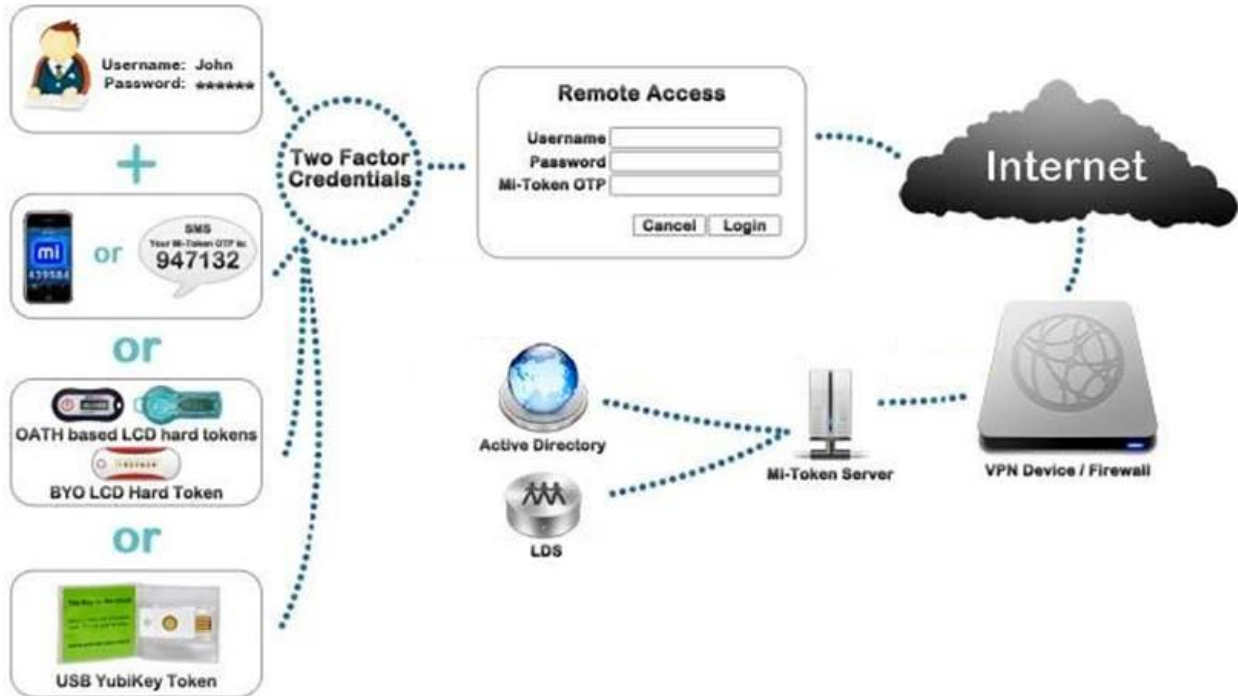


Figure 1. High-level overview of a typical system using Mi-Token

1.8 Typical usage scenario

The following scenario is a typical end-to-end situation which might occur with Mi-Token authentication, involving an employee, Bob.

1. An IT systems administrator installs Mi-Token Enterprise Edition on to an NPS server.
2. The systems administrator then uses the Active Directory Users and Computers snap-in to import some tokens and assigns one of them to a user, Bob.
3. That evening, an innovative solution to a problem occurs to Bob and, rather than wait until morning, Bob decides to work from home using the newly-installed remote-access infrastructure.
4. Bob connects to an SSL VPN appliance which has a login interface containing fields in which he is to enter
 - His username
 - His Windows password
 - The code displayed on his token's LCD screen, that is, the OTP
5. Bob's details, encrypted by SSL, are transmitted to the appliance running in the corporate DMZ.
6. The appliance uses its Active Directory integration feature to verify Bob's username and password.

7. The appliance, which supports multiple authentication servers, generates a RADIUS Access-Request packet and sends it to the Mi-Token authentication server, located in the internal network. The Access-Request packet contains the original username and Bob's OTP. The Windows password has already been verified by the appliance.
8. On the Mi-Token authentication server, NPS receives the RADIUS request and decrypts the access packet. Its contents are then passed to the Mi-Token plugin.
9. The Mi-Token plugin:
 - Searches for the user in AD, retrieving Bob's unique identifier and possibly his mobile phone number
 - Searches its database for all tokens that have been assigned to Bob and tries to verify the provided OTP against each token found
 - Upon successful verification, updates the database to prevent OTP re-use
 - If the OTP fails to verify, tells NPS to send back an Access-Reject message
10. NPS usually tries to verify the password using Windows authentication. Since it has already been verified by the SSL-VPN appliance, the administrator has configured NPS to skip this check. Therefore, NPS responds with an Access-Accept message.
11. Upon receiving the Access-Accept, the SSL-VPN gives Bob access to the network.
12. Bob is able to work productively from home and work on his solution, resulting in satisfaction both for him and his employer.

1.9 Remote access systems

There are several ways in which the Mi-Token Enterprise Edition solution can be leveraged to protect your business, clients, and intellectual property. Organizations typically use Mi-Token Enterprise Edition authentication to integrate with the following devices and software solutions:

- **SSL VPN and firewall devices**, for example, devices from Juniper, Cisco, and others.
- **Outlook Web Access**, via Microsoft Forefront Unified Access Gateway.
- **Windows Desktop Login, via Microsoft's GINA/CP API**. This implementation integrates Mi-Token Enterprise Edition with the standard Windows logon UI, thus providing two-factor authenticated logon for local and remote Windows logins. It can also be used to log on virtual machines through remote desktop sessions. See additional information under *Mi-Token Desktop Login installation*.
- **SSO SAML supported apps, via Active Directory Federation Services (AD FS)**. AD FS enables you to provide two-factor authentication using AD credentials for websites external to the organization, for example, Gmail, Salesforce, Google Apps or Hightail, and many other publicly accessible websites.

1.10 Mi-Token Desktop Login installation

Mi-Token Desktop Login allows two-factor authentication for the standard Windows desktop logon process. This component can be installed on any domain member PC or server and once installed forces two-factor authentication for standard Active Directory logon requests. It achieves this by adding an extra field to the familiar Windows logon screen.



Figure 2. Windows logon screen, showing the OTP field

The component that is installed depends on your operating system:

- Mi-Token GINA (Windows XP and Windows Server 2003)
- Mi-Token Credential Provider (Windows Vista, Windows Server 2008 and newer)

Mi-Token, Inc provides a copy of GINA/CP (Credential Provider). The GINA and Credential Provider components both provide the same functionality but are implemented slightly differently to support the OS changes between Windows XP / Server 2003 and Windows Vista / Windows 7 / Server 2008 / Windows 8.x / Server 2012. The user interfaces are different but remain compatible with the selected OS themes.

For detailed information on how to install, configure and use Mi-Token Desktop Login on client computers, consult the *Mi-Token Desktop Login Experience Installation Guide*.

2 Planning your installation

Mi-Token Enterprise Edition has been designed to make the installation and management of two-factor authentication simple and secure. Further, once you have installed Mi-Token Enterprise Edition, you will find it easy to use, in particular in such help-desk operations as token assignment and PIN resets. Mi-Token Enterprise Edition tends to be somewhat quicker and more convenient with Mi-Token than most other legacy solutions.

Mi-Token administrators can:

- import and manage tokens
- manage Mi-Token roles
- customize permissions to Mi-Token roles
- create replicas of the AD LDS database with corresponding additional instances of the Mi-Token API Server and of the NPS with the Mi-Token RADIUS plugin
- perform all other Mi-Token administration tasks

2.1 Installation timeline

Mi-Token Enterprise Edition requires several pre-requisite steps be carried out before you install Mi-Token Enterprise Edition itself. This means that planning will help in ensuring a successful installation.

Assuming that all prerequisites are installed on the server before Mi-Token Enterprise Edition installation is started, installation of Mi-Token Enterprise Edition should take one to two hours when performed by a competent systems administrator.

This time will vary depending on the complexity of the environment and whether or not any Mi-Token Enterprise Edition optional components are being installed. Often the greatest delays are experienced in the configuration and interoperability between Mi-Token Enterprise Edition and remote access devices. Some SSL VPN and firewall devices require additional time to configure and possibly further time spent debugging authentication issues. The complexity of the network environment and the possible need to coordinate changes across multiple systems management teams will also have an effect on the overall installation time for Mi-Token Enterprise Edition.

To minimize installation effort, Mi-Token has provided a detailed set of *Installation checklists*.

- *Under normal circumstances, expect to spend more time installing prerequisite software and configuring security devices than you will spend actually installing Mi-Token Enterprise Edition.*

2.2 Performance and loading

Performance will depend greatly on your environment, for example: how many users are logging in concurrently, network/disk performance, domain controller performance and the existing workloads.

Normally, Mi-Token two-factor authentication places minimal loads on existing domain controllers and can be easily installed into most environments. However, peak loads or wide geographical distribution can indicate a need for replicated authentication servers. Mi-Token offers the ability to replicate authentication servers so that your installation is scalable to your needs.

The authentication server instances exchange data using Microsoft AD LDS replication technology, and they do this without extra cost. Further details are available here <http://technet.microsoft.com/en-au/library/cc770465.aspx> and in this manual under Installing a replica authentication server.

Having multiple AD LDS instances, along with a load-balancing solution utilizing several authentication servers (Microsoft NPS or Mi-Token API) makes for scalability and also contributes to reliable data storage with the Mi-Token database distributed between several automatically replicating locations.

In any case, Mi-Token Inc. recommends benchmarking and stress testing the entire system to gauge more precise requirements, and also recommends load balancing if there are multiple servers.

2.3 Mi-Token components and installation options

Mi-Token is based on Microsoft's Active Directory Lightweight Directory Services (AD LDS), and cannot function without AD LDS. AD LDS may be replicated.

Mi-Token proper has six core components.

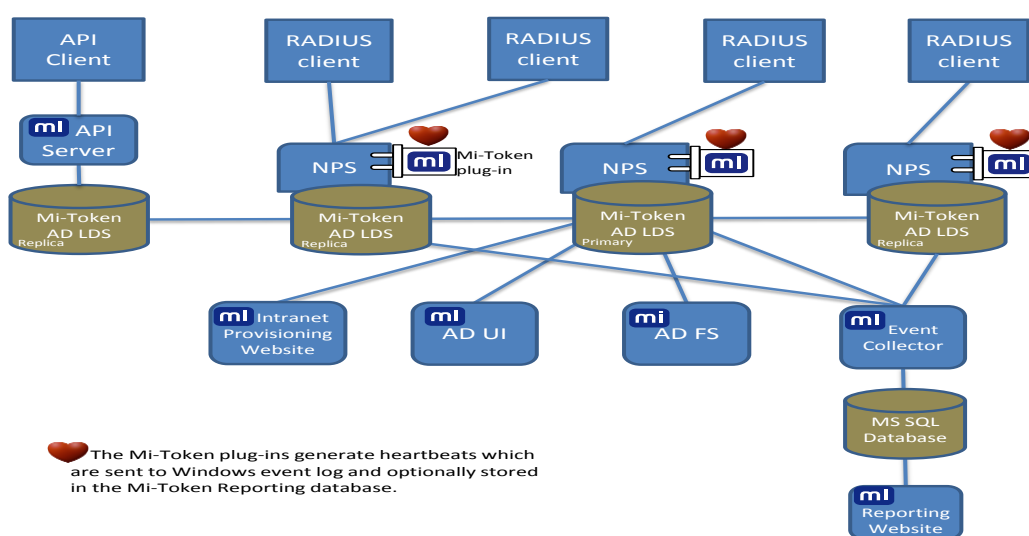


Figure 3. Overall structure of a full Mi-Token installation

It is **mandatory** for a Mi-Token installation to have a provider of authentication services. These are usually provided by Network Policy Server (NPS) with Mi-Token's NPS plugin. Alternatively, they can be provided via the API, but for most purposes, the NPS plugin is regarded as mandatory.

As Figure 3 shows, if there are multiple replications of AD LDS, each has its own authentication provider. This means that Mi-Token offers scalability in the face of geographic spread or the need for load balancing.

It is also **mandatory** for a Mi-Token installation to have the Mi-Token User Interface (UI), which is an interface to your AD LDS. It is available in a 32- and a 64-bit version.

That is, all Mi-Token installations have the UI and most have the NPS plugin.

In addition to the NPS plugin and the UI, there are another four **optional** components.

- **Mi-Token Reporting.** This provides extensive high-level graphic and detailed text-based reporting of token usage, audit events, error messages, statistics and Mi-Token metrics. Mi-Token Reporting consists of 3 sub-components: Reporting Website, Event Collector Service and SQL Server database.
- **Mi-Token Intranet Provisioning Website.** Installed on an internally-accessible web server, this enables your end-users to set up their own soft tokens with no intervention by an administrator.
- **API Service.** The Mi-Token API provides alternate administration and authentication channels for Mi-Token, on top of using the UI to manage user-token assignments and NPS for authentication. An AD LDS instance may have both NPS and API associated with it.

The Mi-Token API Service requires additional licensing over that of Mi-Token Enterprise Edition. Please contact sales@mi-token.com if your organization would like the Mi-Token API Service.

- **Active Directory Federation Services (AD FS).** Mi-Token Enterprise Edition integrates with AD FS to provide two-factor authentication for websites external to the organization, for example, Gmail, Salesforce, Google Apps or Hightail, and many other publicly accessible websites.

Another two add-ins are available for special purposes: Two-Phase Authentication and Credential Provider. See *Mi-Token Enterprise Edition Add-ins*.

As a result of this modularity, Mi-Token offers wide flexibility, but broadly speaking, there are three ways to install Mi-Token.

- **Minimal installation.** Install the NPS plugin and the User Interface only.

When you have completed a minimal installation, you will have a functioning Mi-Token environment. Your users will be able to use hard and soft tokens for authentication with some intervention by an administrator to register new users.

A minimal installation provides an opportunity for testing and evaluation, but is also a viable environment for a smaller organization.

- **All-on-one-machine installation.** Such an installation includes Mi-Token Reporting and the Mi-Token Intranet Provisioning Website feature, all installed on a single machine.

This installation offers two features in addition to those of a minimal installation. Firstly, you will have extensive reporting capability. Secondly, your users will have access to the Mi-Token Intranet Provisioning Website.

- **Full installation.** Here, all the features of Mi-Token are installed, including deployment on several servers.

This installation offers the features mentioned above, and more. You will be able to have NPS performing RADIUS authentication on multiple servers in multiple locations, address scalability and data reliability at a high standard, and you will have access to the Mi-Token API and to Active Directory Federation Services.

It is straightforward to progress from a minimal to an all-on-one-machine installation, and from a minimal to a full installation. An all-on-one-machine installation can be upgraded to a full one, but you may need to uninstall some components and reinstall them on different machines.

INSTALLATION PATHS

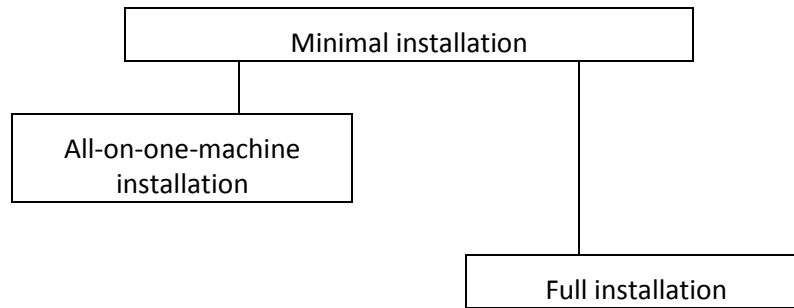


Figure 4. Three types of installation and possible upgrade paths

3 Preparing for your installation

To help you to keep track of prerequisites, Mi-Token has provided a detailed set of *Installation checklists*.

3.1 Prerequisites

Prerequisite knowledge

The person performing the install should be familiar with the principles of Windows and RADIUS authentication.

Connectivity

Generally, you will need an active Internet connection. Once you have downloaded the software from Mi-Token, you will still need to be connected if .NET Framework 4.0 is not preinstalled as installers of all Mi-Token components will attempt to download and install it if needed. In cases where .NET Framework 4.5 is pre-installed, no other version of the Framework is downloaded.

Users installing Desktop Tokens will need to be connected. They will almost certainly be on the organization's premises while they do such installs. After the installation is complete, the Desktop Tokens can function (and generate OTPs) independently, without having networking enabled.

Users with smart phones will need Wi-fi or other Internet connectivity if they wish to install and activate Mi-Token smart phone apps.

Server hardware

Mi-Token Enterprise Edition fully supports the use of virtualized hardware solutions such as VMware, Xen, or Hyper-V.

For the most part, Mi-Token Enterprise Edition is a 64-bit product and requires 64-bit hardware. The exception on the server side is

- The Mi-Token AD User Interface, which is available in 32- and 64-bit versions and therefore can run on platforms of both bitnesses.

 *Mi-Token, Inc does not recommend running Mi-Token Enterprise Edition on obsolete or obsolescent operating systems. Owing to the lack of support from the manufacturer, such operating systems are more vulnerable to security attacks. As of late 2014, Windows XP and Server 2003 are in this category.*

End-user hardware

Mi-Token Enterprise Edition is a Windows product. However, it can be used by almost any end-user hardware, such as an SSL VPN appliance. This includes situations where an SSL VPN appliance collects the credentials, perhaps by use of an internal web server which serves to the end-user, who could be running, for example, Linux.

The requirements are that, firstly, the end-user hardware must support authentication via the RADIUS protocol, either directly or via a proxy device of some sort.

Also, in order to support two-factor authentication, the device must somehow allow the user to provide a secondary password in the logon interface. Newer remote access devices support the use of a third field specifically for OTP or secondary passwords, and this is desirable for usability reasons. However, many remote-access devices only provide username and password fields. In this case, Mi-Token allows for concatenating the password and token (or OTP), and optionally a PIN, in a single user interface logon password field. The exact format will vary depending on the device. Mi-Token Enterprise Edition breaks a single password field down into the correct substrings to allow the inclusion of a password, the OTP, and optionally, a PIN.

These two methods of supplying OTPs to the Mi-Token Enterprise Edition will require different installation configurations when adding a remote access device as a RADIUS client on the Mi-Token Enterprise Edition server:

- **Concatenated password and OTP** – In this case, the remote access system is configured to relay the username and password fields via RADIUS to the Mi-Token server. For example, mypassword634789. Upon verification, the OTP (634789 in this example) is removed from the password string and NPS is left with mypassword.
- **Password and OTP in separate fields** – In this case, the remote access system will verify the password and the Mi-Token server only verifies the OTP field.

The configuration is described under *Authentication server*.

Finally, if you wish to use the Desktop Token, it is bitness-agnostic and can run on both 32-bit and 64-bit platforms.

Database

Mi-Token uses AD LDS as its database, with default name Mi-Token.

Mi-Token Enterprise Edition is usually installed on existing domain controllers.

If you install Mi-Token Reporting, you will need an SQL database.

It is possible, by using Mi-Token's User Interface, to create extra data partitions inside AD LDS. This feature is useful if you are working with different domains, when you would map each domain to its own partition. Note that in such a case the User Interface will at any time only show data in the partition mapped to the current domain on which Mi-Token is running. This arrangement, coupled with Mi-Token security settings, can ensure that administrators of one domain can only see and manage tokens belonging to the users of their respective domain.

For information, see *Domain Settings tab*.

It is also possible, by using Microsoft AD LDS replication technology, to achieve scalability and reliability by replicating AD LDS and install an authentication server on each instance, at no extra cost. Further details are available here <http://technet.microsoft.com/en-au/library/cc770465.aspx> and under *Installing a replica authentication server*.

If you need to access Active Directory features (during the installation of the RADIUS plugin and the API Service) you will require an account with Domain Administrator rights.

Mi-Token Windows Server

Any version of Windows 2012 or 2012 R2 (64-bit) that supports the Microsoft domain controller role can be used as the basis for a Mi-Token Enterprise Edition installation. It can be, and usually is, installed on an existing Microsoft domain controller or on a member server. If you prefer, it can also be installed on a standalone server.

Mi-Token Enterprise Edition supports multiple domain environments. The only core requirement is that a Mi-Token Enterprise Edition installation must be installed in the same forest (either in the same or on a separate domain) as the user accounts that require two-

factor authentication services. Multiple forest deployments are supported but only by installing multiple Mi-Token Enterprise Edition instances, one or more for each forest where two-factor authentications is required.

When installing Mi-Token Enterprise Edition on a domain controller, an account with domain administration rights is required. When installing Mi-Token Enterprise Edition on a standalone server, an account with local administration rights is required. If you need to access Active Directory features during the installation you will require an account with domain administration rights.

See the Microsoft software component requirements for each Windows Server 2012 and Windows Server 2012 R2 below.

Windows Server 2012 components

All Mi-Token Enterprise Edition deployments require these software components.

- Network Policy Server with Network Policy role enabled – to provide RADIUS services
- Active Directory Lightweight Directory Services (AD LDS) for database storage of metadata and token seed keys
- .NET Framework 4.0

The installation process itself downloads installs .NET Framework 4.0, it being freely redistributable.

The database server may be installed locally or remotely.

Depending on the components you choose to install, you may need one or both of these.

- Internet Information Services (IIS) to serve Mi-Token Reporting and the Mi-Token Intranet Provisioning Website
- Microsoft Redistributable Package for Visual C++ 2010 SP1

The installer has Microsoft Redistributable Package for Visual C++ 2010 SP1 embedded, and installs it.

As the installation proceeds, Mi-Token Enterprise Edition checks to ensure that prerequisites are installed. If a component is missing, the installer will alert you and roll back to a known good state before aborting the installation. If this occurs, install the missing components and resume the installation.

Prerequisites for optional components

As mentioned, Mi-Token Enterprise Edition includes four optional components. They are Mi-Token Reporting, Mi-Token Intranet Provisioning Website, API Service and Active Directory Federation Services. Three of these, Mi-Token Reporting, Mi-Token Intranet Provisioning Website and API, have their own prerequisites.

- Mi-Token Reporting requires a suitable database server and Microsoft Internet Information Server (IIS).
- Mi-Token Intranet Provisioning Website requires IIS.
- The API requires IIS.

IIS and the database server may be installed locally or remotely but (absent domain trust) they must be within the same domain as the one where Mi-Token is installed.

As well as these major components, the optional Two-Phase Authentication feature requires a means of delivering a token. This will be email, or an SMS provider operating via email, SMPP or HTTP.

Database servers

The following database servers are supported for the implementation of these Mi-Token Enterprise Edition optional components.

- SQL Server 2005, 2008, 2008 R2, 2012 and 2014
- SQL Standard, free Express and Enterprise Editions

Mi-Token Reporting requires ODBC. If it is not already present, the Mi-Token Reporting installer will install it.

Web servers

The following versions of Internet Information Server are supported for the implementation of these Mi-Token Enterprise Edition optional components.

- IIS 7.0 with IIS 6 Metabase compatibility
- IIS 7.5 with IIS 6 Metabase compatibility
- IIS 8.0

IIS features required for installation include ASP.NET (both Reporting and Provisioning websites) and Windows Authentication (Reporting website only).

Mail and SMS connections

The Mi-Token Intranet Provisioning Website requires access to a suitably configured SMTP server if soft token provisioning to the users will be done by emails and requires an SMS provider if provisioning will be done by SMS.

Two-Phase Authentication requires an SMTP server or SMS provider.

Administrative and infrastructure requirements

For your primary RADIUS installation, you will need to determine

- Instance name
- LDAP port
- SSL port

The installer suggests values for all of these. Mi-Token recommends that you accept the defaults, particularly the ports, and if you do not, you will need to make equivalent changes in other Mi-Token installation steps and you may also need to modify firewall configurations and plan accordingly.

- AD LDS database administrators

You will need the names of the AD LDS database administrators, and Mi-Token strongly recommends that you choose an AD group rather than a single account. This user or group will have full access to the AD LDS database. Unless you add more users and/or groups after installation, only the user or AD group members who have installed Mi-Token will be able to access Mi-Token.

Mi-Token recommends that the AD default group Domain Administrators be assigned to this role. Alternatively, you can create a new AD group specifically for Mi-Token administration and select that group at this time.

- Friendly name, address and shared secret for each remote access device which will be a RADIUS client.
- Ascertain which of these strategies you require (see step 3 under *To create or edit a connection request policy* and *End-user hardware*):

- The plugin only verifies the OTP and the remote access device verifies the normal user credentials.
- The plugin verifies both the OTP and the Windows password.

3.2 Active Directory modifications

When AD LDS is installed, the Microsoft installer creates a standard Service Connection Point (SCP) object on the computer on which AD LDS is being installed. This object allows for Mi-Token AD LDS instances to be remotely accessed and identified as required, for both direct-access and replication operations. These operations need the location of this SCP and Mi-Token supplies this location by appending the `otherWellKnownObjects` attribute to the list of such attributes which already exists in the Active Directory.

This is the **only** modification made to Active Directory and Mi-Token observes well-known Microsoft standards as used by Microsoft itself for products such as Exchange Server. It is very unlikely to cause any disturbance to the functionality of Microsoft or third-party applications.

It is worth noting that Mi-Token Enterprise Edition creates and maintains its own separate LDS schema and makes no changes to the Active Directory schema.

Mi-Token does not require a dedicated server.

3.3 Server hardening

Each Mi-Token server hosts a token database (Microsoft AD LDS) and, usually, a RADIUS server (Microsoft NPS). It is important to ensure that the information held on this server is kept secure at all times. From an IT security perspective, a server hosting Mi-Token Enterprise Edition should be secured at least as well as the level of security applied to your organization's Active Directory domain controllers.

Mi-Token Inc. recommends that you consult Microsoft's server hardening guidelines.

SECURE DOMAIN ADMINISTRATIVE ACCOUNTS

This includes domain/enterprise administrators, Mi-Token administrators, who are typically domain administrators anyway. Each of these accounts could potentially gain access to the Mi-Token server and compromise the secret key of every token. Some potentially useful strategies include:

- Ensuring administrative accounts have very strong passwords, for example, 20 characters in multiple-case alphanumeric, possibly with symbols.
- You may consider requiring administrative logons to use two-factor authentication.

MI-TOKEN SERVER ON A SEPARATE VLAN

Put the Mi-Token server on a separate VLAN and only give selected administrators access to it. This can be achieved via firewall policy, or more securely using IPSec tunnels or 802.1X.

BACKUPS

Make sure backups of the Mi-Token Enterprise Edition server are stored securely, preferably in an encrypted form. See *Backup Mi-Token*.

DELETE THE INITIAL TOKEN SECRET KEY

Delete the token secret key files used for the initial import once they have been successfully imported into Mi-Token Enterprise Edition. The files come from Mi-Token, Inc and contain seeds – starting points for the computation of OTPs. If you wish to retain copies, keep them separately in a secure location.

3.4 Ports and protocols table

This table can be used by network administrators configuring firewalls in a Mi-Token Enterprise Edition environment. If you make changes to the default port assignments, you must correspondingly change your firewall rules.

Except for port 5000, all of the entries in this table are standard Microsoft requirements for various types of Windows- and Active Directory-related traffic with only the port 5000 being proprietary to Mi-Token.

The different Mi-Token components (the plugin, UI, Reporting and so on) can be installed on the same machines as existing domain controllers or on one or more standalone servers. In either case, these servers are part of the internal corporate network and are not generally separated by firewalls.

Protocol and port	Notes	Communication path
TCP and UDP 53	Domain Name Server (DNS) traffic.	Various – DNS
TCP and UDP 88	Kerberos.	AD LDS – AD LDS
TCP 80	HTTP is used for some 2-phase deployments.	Users – IIS
UDP 123	Network Time Protocol (NTP).	Windows time server
TCP 135	Remote Procedure Call (RPC) endpoint mapper.	AD LDS – AD LDS
TCP, UDP 389	Lightweight Directory Access Protocol (LDAP).	NPS – AD
TCP 443	HTTPS traffic. Reporting, Mi-Token Intranet Provisioning Website, external providers (for example, SMS), API.	Various, as noted
TCP and UDP 445	Remote Procedure Call (RPC) communications, including Server Message Block (SMB).	AD LDS – AD LDS
TCP 1433	SQL Server traffic.	Event collector– SQL Reporting server – SQL
UDP 1434	SQL Server Browser service. Optional, used by Reporting setup.	Browser – SQL
TCP and UDP 1812	RADIUS authentication.	SSL VPN appliance – NPS
TCP 3268	LDAP Global Catalog (GC).	AD UI – AD
TCP 5000	AD LDS LDAP port.	AD UI – AD LDS AD LDS – AD LDS
RPC dynamic assignment TCP 1024–65535 on Win 2k/2003 TCP 49152–65535 on Win 2008+	Also known as TCP high ports. By default, any high port can be used by the dynamic RPC protocol, however, the port range can be reduced. For information on reducing the port range, see this page http://social.technet.microsoft.com/wiki/contents/articles/584.active-directory-replication-over-firewalls.aspx .	Various

Figure 5. Table of ports and protocols

3.5 Deployment to end-users

Mi-Token Windows Desktop Login in particular must be installed by a knowledgeable person. Mi-Token recommends that trained help-desk staff perform the installations, owing to the risk that a desktop could be locked with no way of entering credentials to unlock it.

You will need to carefully plan the rollout if your organization is large, with contingency plans for users who lose their tokens in the early stages. You will probably have to plan for a user community that initially includes some users with tokens and some without. Mi-Token offers a bypass feature that can help during this process – refer to *No-Token Bypass*.

3.6 Download the Mi-Token software

Mi-Token Enterprise Edition is delivered as a self-extracting zipped executable (of approximately 110 MB) which expands into six installers.

Upon registration, Mi-Token Inc. will email you a link to download the Mi-Token Enterprise Edition software online, along with login credentials allocated to your organization. While Mi-Token software can be freely downloaded for evaluation purposes, a fully functional Mi-Token Enterprise Edition instance requires a valid license.

Mi-Token Inc. strongly recommends that you keep this information private and that you avoid sharing it with others except approved system administrators within your organization. Failure to do so may result in the unintended compromise of your Mi-Token Enterprise Edition installation. While Mi-Token installations are protected by cryptographic encryption, divulging the contents of this email may reduce the security of your installation. Mi-Token Inc. maintains and retains audit logs of all access to publicly available Mi-Token Inc. websites. Should your Mi-Token Inc. login details be compromised, we will contact you and access to the Mi-Token Inc. website for your organization may be restricted until any issues can be resolved.



To download and extract the Mi-Token software

1. Following the instructions in the email, download the installation file to a convenient location. It is a self-extractor and will have a name similar to `Mi-Token_x64_7491_57185319d0f9_Full.exe`.
2. Double-click on the downloaded file. The extractor will launch and offer you a default destination folder, and the option to change it. Mi-Token, Inc. recommends that you retain the default presented.

The installation file extracts six .exe files.

3. If you need the 32-bit version of the AD UI, download it separately, again following instructions emailed by Mi-Token. This download is another self-extractor.

4 Minimal Mi-Token installation

This section takes you step by step through the process of installing and configuring a minimal Mi-Token Enterprise Edition instance on Windows 2012 servers.

You may choose to use the *Installation checklists* as an aid in working through the process.

- ④ *Note that in the future, version and build numbers may advance, resulting in minor differences between the dialog boxes shown here and those that you see.*

4.1 Quick-start guide to a minimal Mi-Token installation

You may use this abbreviated procedure to install a minimal Mi-Token system. The remainder of this Chapter sets out this procedure in more detail.

1. Install the Mi-Token NPS plugin.
2. Configure NPS.
That is, add each remote access device as a RADIUS client.
3. Enable Windows audit logging, so that Windows logs Mi-Token's heartbeats.
4. Install Active Directory User Interface (AD UI).
5. Use RADIUS Tester (installed by default) to test RADIUS authentication.

Note that you must use the true IP address; the localhost or loop-back address 127.0.0.1 will not work.

This installs a workable Mi-Token 2-factor authentication system. To assign soft tokens to your users, see *Manual provisioning of soft-tokens*.

4.2 Authentication server

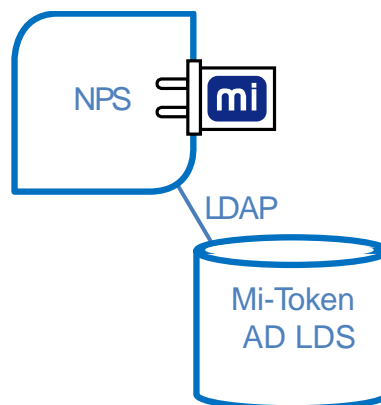


Figure 6. An authentication server, showing AD LDS, NPS and Mi-Token's NPS plugin

The following describes

- how to install the Mi-Token plugin to NPS
- how to configure the primary (or only) authentication server
- how to test the primary authentication server

Installing the primary authentication server



To install Mi-Token's NPS plugin

Since NPS is a RADIUS server, this plugin is sometimes known as the RADIUS plugin.

1. Ensure that you are logged in with an account that has domain administrator privileges.
2. Check that all prerequisites have been installed on the server. They are listed at *Prerequisites*.
3. Double-click the **Mi-Token RADIUS Plugin executable**, downloaded under *Download the Mi-Token software*. Its name is Mi-Token RADIUS plugin_64bit.exe or similar.

The installation process starts the Mi-Token AD LDS configuration wizard.



Figure 7. RADIUS plugin welcome dialog box

4. Click **Next**. The Mi-Token installer automates much of the installation process. You will be prompted for further information as required.

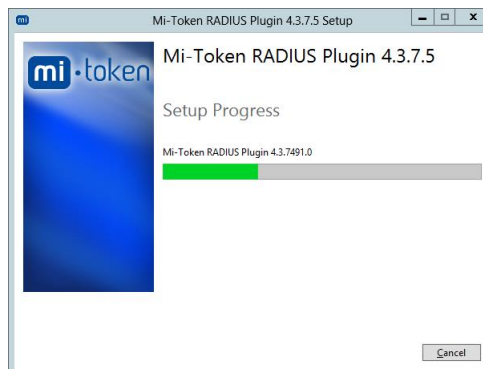


Figure 8. RADIUS plugin setup progress



Figure 9. RADIUS plugin end-user license agreement

5. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Install**.

The installation continues.

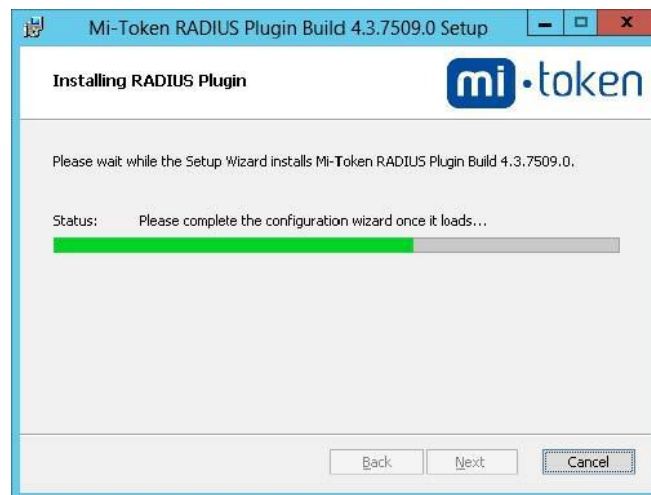


Figure 10. RADIUS plugin installation progress

The installation wizard displays the option to create a new AD LDS instance or to use an existing one (if available).

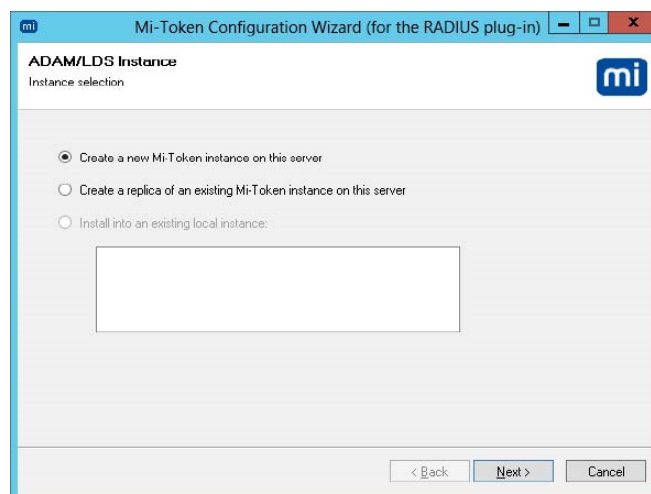


Figure 11. Create AD LDS Instance

6. Since this is the primary authentication instance, select **Create a new Mi-Token instance on this server**.

You are prompted to enter an instance name and to select TCP port numbers for LDAP and SSL respectively, and select a folder which will contain the AD LDS database.

- If the default port numbers are modified, you will need to make equivalent changes in other Mi-Token installation steps and you may also need to modify firewall configurations accordingly.

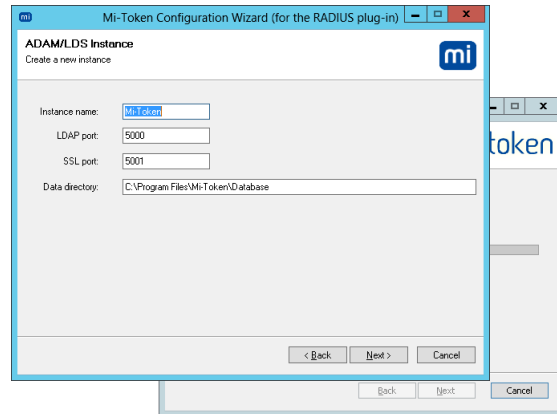


Figure 12. AD LDS parameters

Mi-Token Inc. recommends that you do not change the defaults presented.

7. Click **Next>**. An AD LDS instance will be created with the parameters specified.

You must now enter a suitable Administrator account or group.

This will have been part of your planning, as described under *Prerequisites, Administrative and infrastructure requirements*.

- Mi-Token strongly recommends that you choose an AD group rather than a single account.

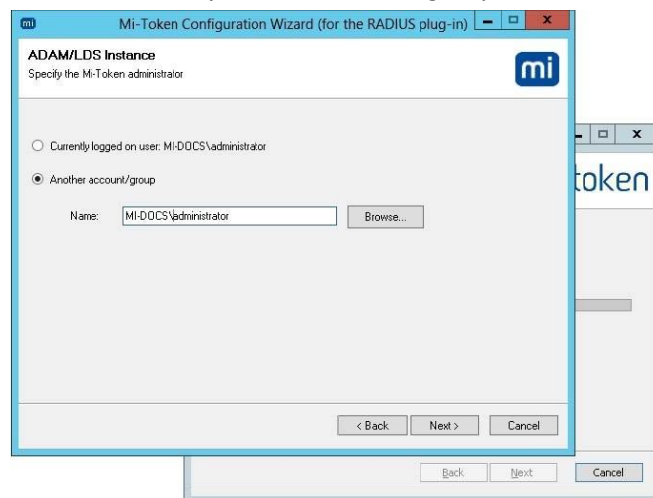
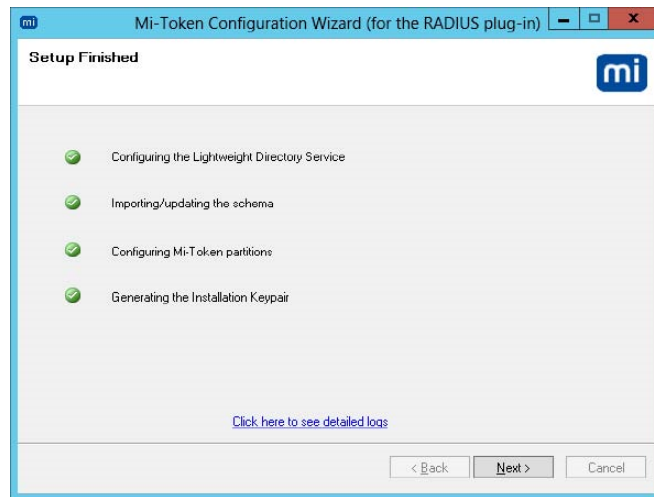
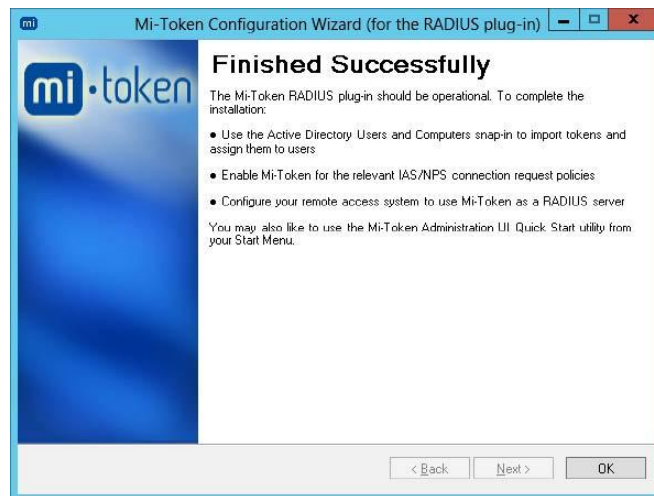


Figure 13. Specify the administrator account

8. Enter an appropriate account/group and click **Next>**.



9. Click **Next** again.



10. Click **OK** to complete the wizard.

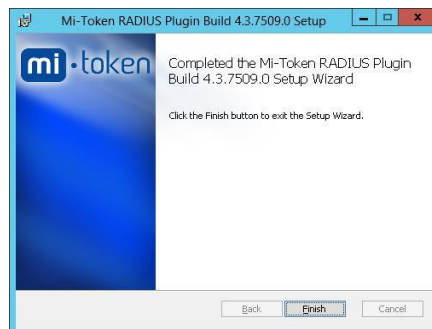


Figure 14. RADIUS Plugin wizard completed

11. Click **Finish** to close.

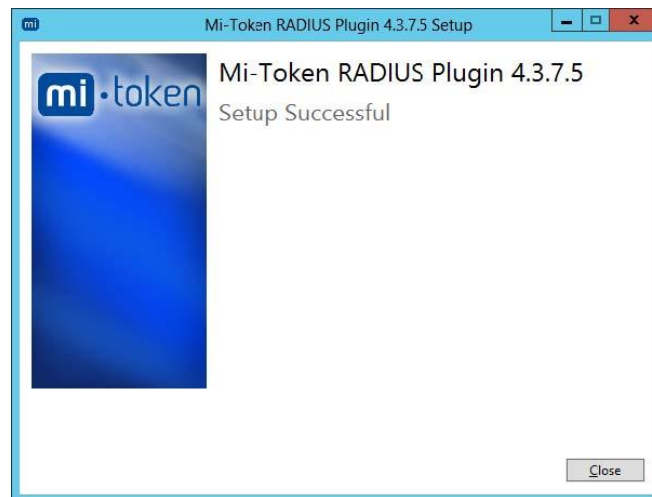


Figure 15. RADIUS setup successful

The server now has an AD LDS instance installed, with schema, and your NPS has the Mi-Token plugin enabling it to communicate with AD LDS.

Windows audit logging

The Mi-Token plugin generates heartbeats. You must enable audit logging so that Windows logs them.



To enable audit logging

1. From the Windows logo, open Group Policy Management and navigate to your server, and to **Default Domain Policy**.
2. Right-click on **Default Domain Policy**.

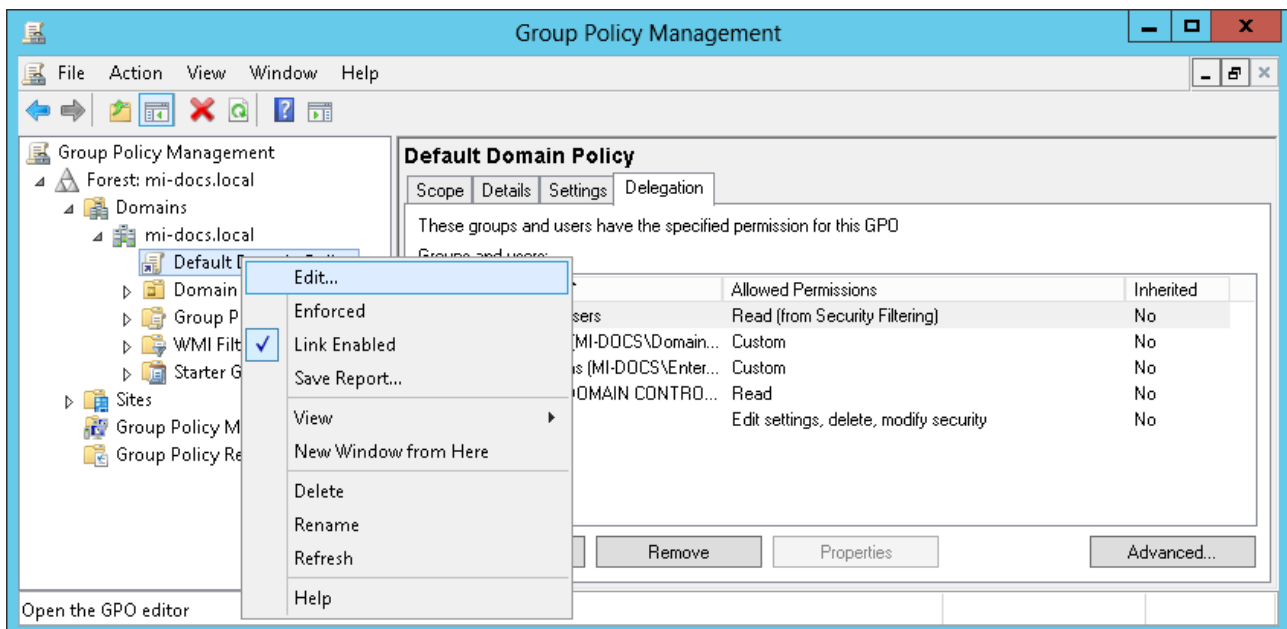
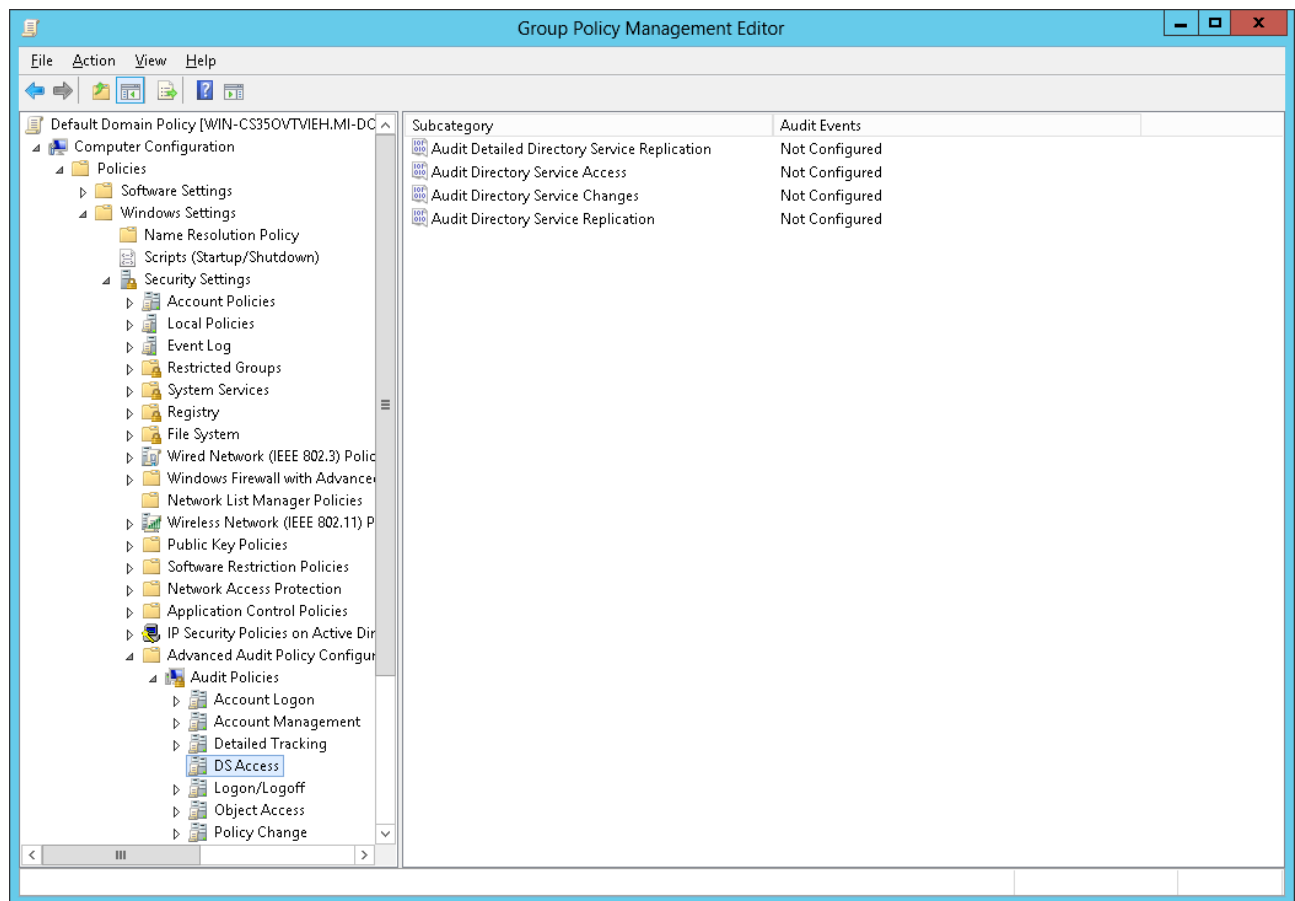


Figure 16. Group policy management

3. Click **Edit...** to open the Group Policy Management Editor.
4. Navigate to **Default Domain Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > DS Access**.



(Standard Windows dialog box)

Figure 17. Group Policy Management Editor, showing audit policies

5. Configure **Success** audit events for **Audit Directory Service Changes**.
6. Apply the policy update by running **gpupdate** in a command window.

Configuring the primary server



To add RADIUS clients

1. Go to the Windows Start desktop (that is, press the Windows logo key). You will find a new icon, **Mi-Token Administration UI Quick-Start**.

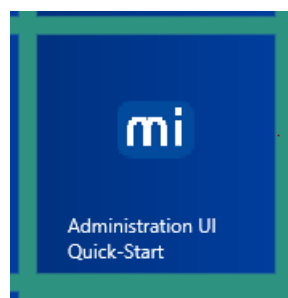


Figure 18. Mi-Token Administration UI Quick-Start icon

2. Click the icon (or perform a search for **Administration UI Quick-Start**). Select the **RADIUS plug-in management** tab.

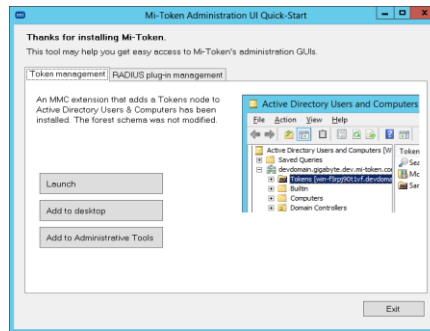


Figure 19. Mi-Token Administration UI Quick-Start, showing the *RADIUS plug-in management* tab

3. Click **Launch**. This launches the Mi-Token UI Helper.

ⓘ In the case of Windows 2008, the Server Manager is launched instead of Mi-Token UI Helper with the same custom Mi-Token functionality and graphical interface.

(Note for reference that detailed documentation on the UI Helper is provided under *Mi-Token UI Helper*. The instructions following refer solely to the task at hand, namely, configuring your primary server.)

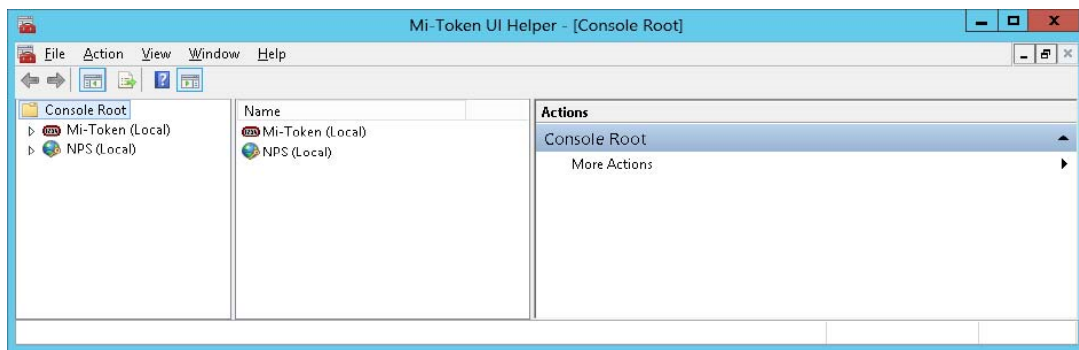


Figure 20. Mi-Token UI Helper root

4. Expand the tree in the left pane: **NPS (Local)** > **RADIUS Clients and Servers** > **RADIUS Clients**. (See Figure 21.)
5. Add each remote access device that will use Mi-Token authentication as a RADIUS client. To add a RADIUS client, click **New** in the right (Action) pane.

- Enter the **Friendly name** of the remote access device (RADIUS client).
- Enter the **Address** of the RADIUS client.
- Enter the shared secret (that is, shared with the RADIUS client). If you select **Manual**, you must enter a suitable shared secret. If you select **Generate**, a **Generate** button appears which you may click to generate a random shared secret.

The clients may have their own individual secrets.

ⓘ Ensure that you use very strong shared secrets. Mi-Token recommends a random string with multi-case letters, numbers and symbols of at least 20 characters. The shared secret is only entered four times for each remote access device so using a very strong one is not onerous.

- Click **OK**.

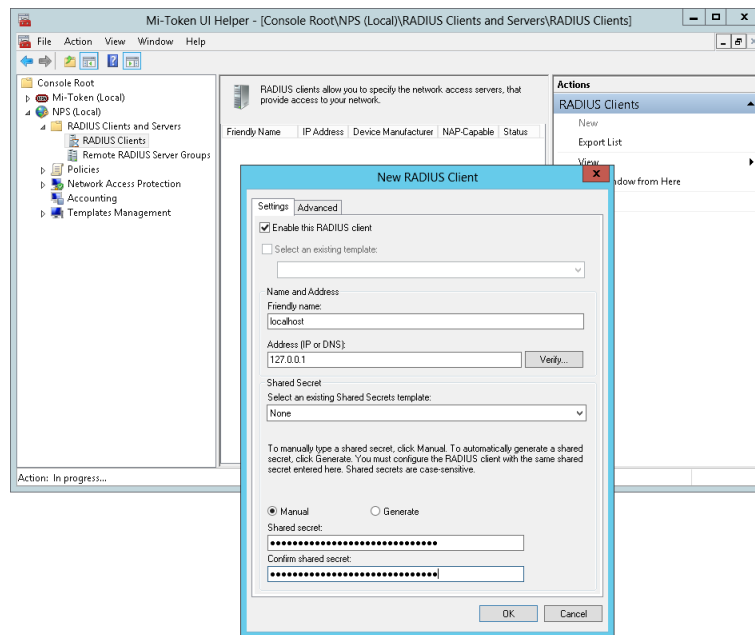


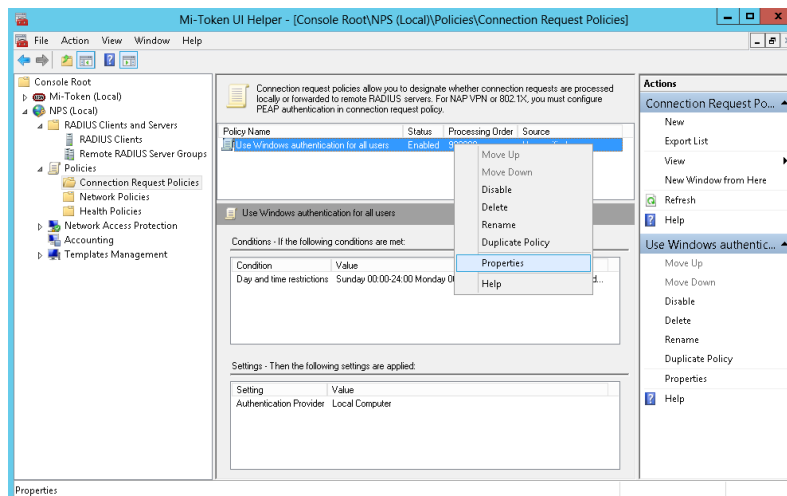
Figure 21. Configure RADIUS client

Your new RADIUS client appears in the center pane.



To create or edit a connection request policy

1. Expand the tree in the left pane and navigate to **NPS (Local) > Policies > Connection Request Policies**. You will find a policy called **Use Windows Authentication for all users**.

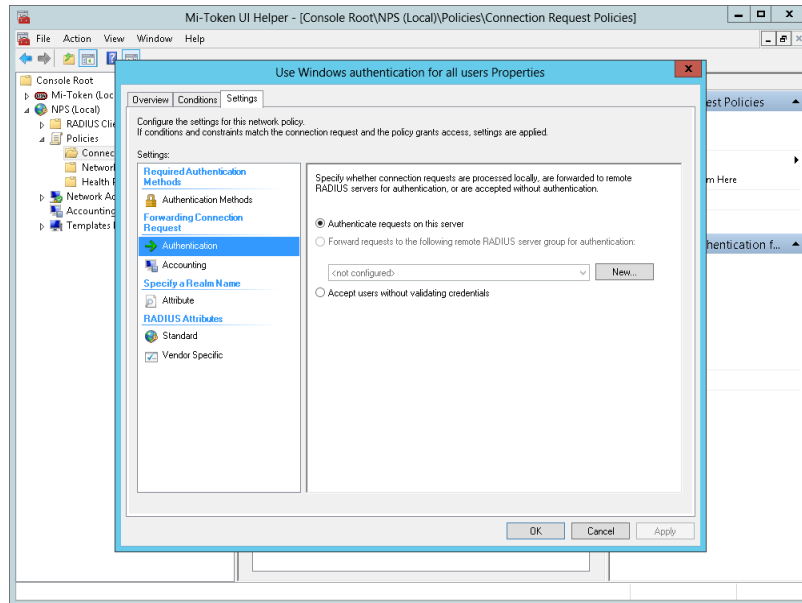


(Standard Windows dialog box)

Figure 22. Setting up a connection request policy

2. In the center pane, right-click **Use Windows Authentication for all users** and select **Properties**.

- Click on the **Settings** tab and click **Authentication**.



(Standard Windows dialog box)

Figure 23. Select OTP only or OTP and Windows credentials

- This step depends on whether the plugin verifies the OTP only or verify both the OTP and the Windows password. This in turn depends on the end-user hardware. See *End-user hardware*.

The end-user device allows for entry of two passwords. In this case, the remote access device verifies the normal user credentials and Mi-Token verifies the OTP only. Either set up a connection request policy or modify the existing one, **Use Windows authentication for all users**, and enable **Accept users without validating credentials**. Click **OK**. At this point, omit the next few steps and skip to step 12.

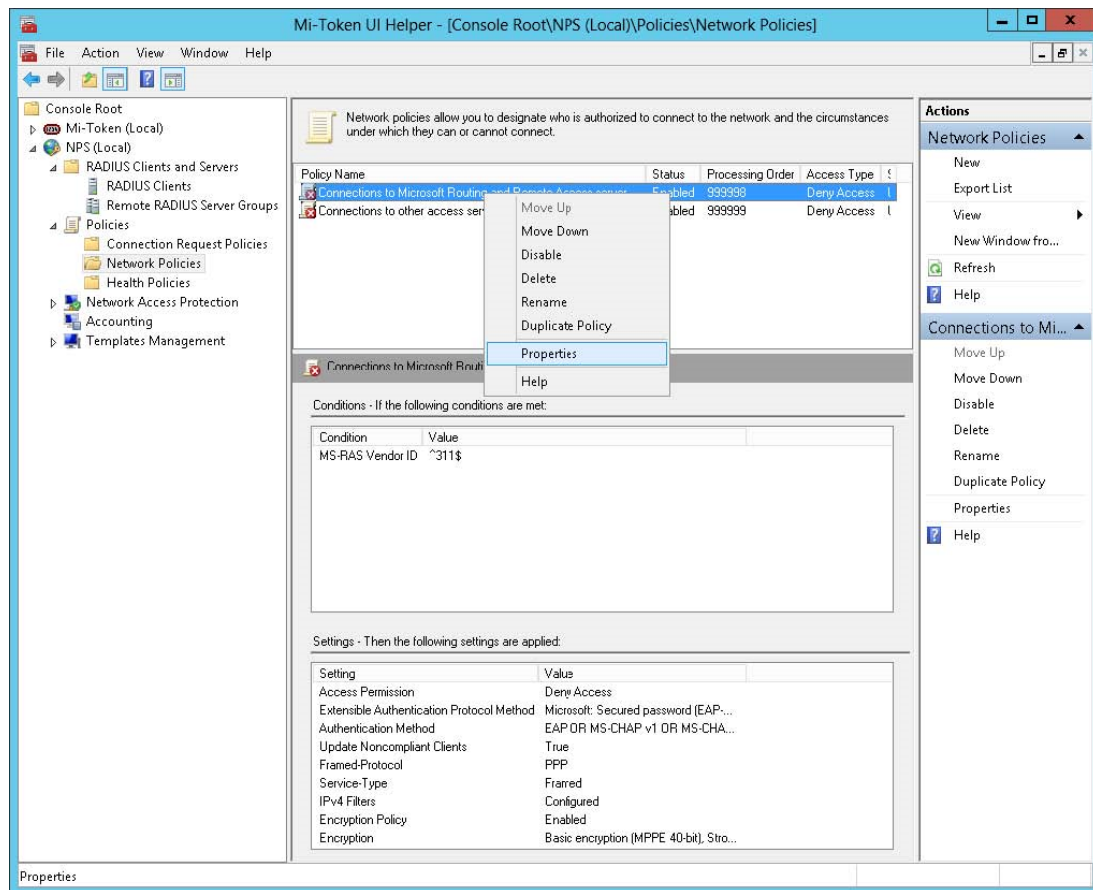
The end-user device allows for entry of only one password. Here, the user concatenates the two passwords and Mi-Token must

- separate them
- verify the OTP
- pass the Windows password to NPS for verification

Either use the existing **Use Windows authentication for all users** connection request policy or create a new policy and set its profile to match the existing policy. Select **Authenticate requests on this server**. (“This server” refers to the Mi-Token server.) Click **OK**.

In this latter case, you must set up a new Network Access policy or use the built-in policy **Connections to Microsoft Routing and Remote Access server**. This process is described in steps 5 through 11.

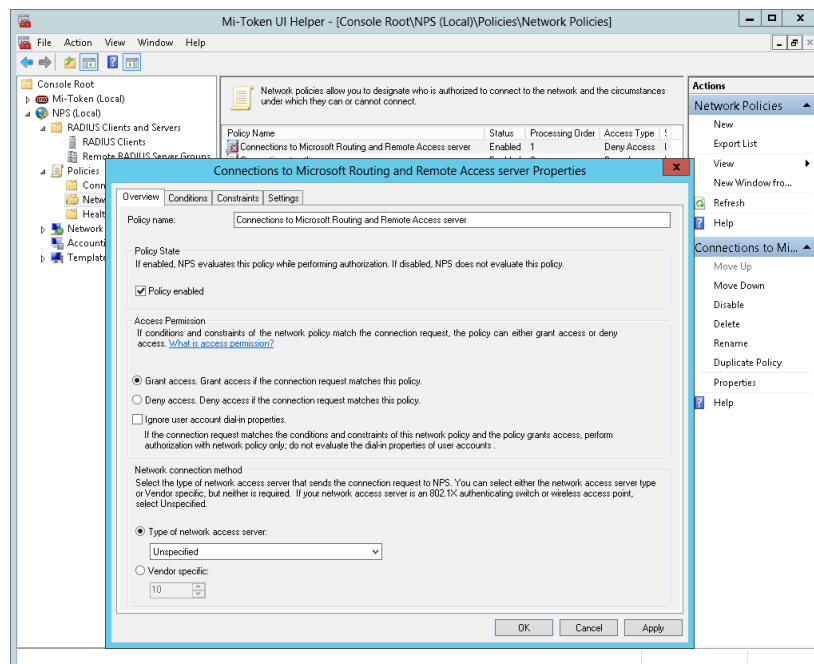
- Expand the tree in the left pane: **NPS (Local) > Policies > Network Policies**. Click **Network Policies**.



(Standard Windows dialog box)

Figure 24. Connections to Microsoft routing and remote access server

6. Right-click **Connections to Microsoft Routing and Remote Access server**. Click **Properties**.
7. Check **Grant access**. **Grant access if the connection request matches this policy**.

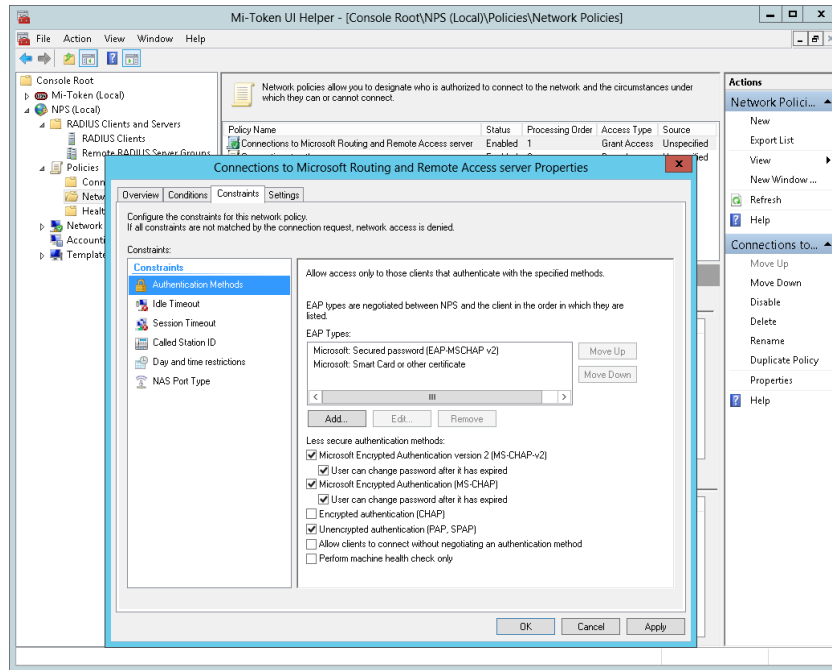


(Standard Windows dialog box)

Figure 25. Select Grant access

8. Click the **Constraints** tab and select **Authentication Methods**.

9. Check **Unencrypted authentication (PAP, SPAP)**. Click **OK**.

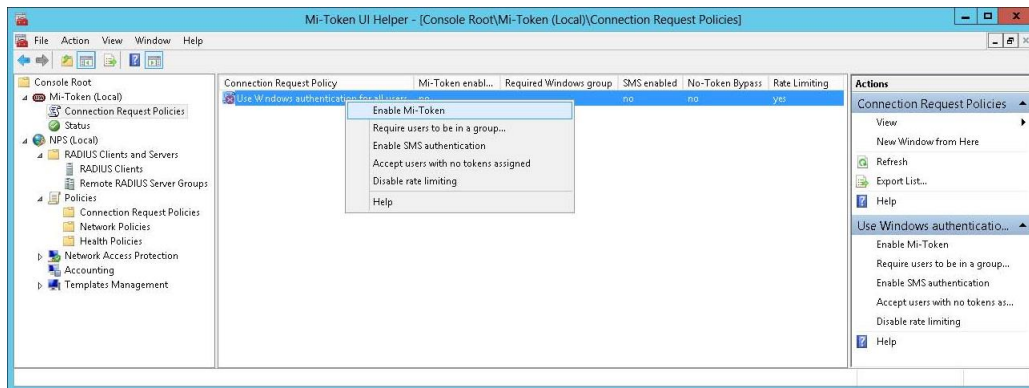


(Standard Windows dialog box)

Figure 26. Allow unencrypted authentication

You see a message indicating that you have selected an insecure authentication method. Despite this message, the authentication is actually encrypted using the RADIUS secret key and therefore still secured.

10. Click **No** on the message dialog box.
11. In the left pane, navigate to **Mi-Token (Local) > Connection Request Policies**. Right-click the policy you want to enable Mi-Token with and select **Enable Mi-Token**. Mi-Token authentication is now enabled.



(Standard Windows dialog box)

Figure 27. UI Helper: Enable Mi-Token authentication

Again, note for reference that detailed documentation on the UI Helper is provided under *Mi-Token UI Helper*.

12. Check the Windows event log and the NPS administrative consoles for any errors or warnings.

This concludes the installation of your primary RADIUS server. If you need to scale up and install replica servers, refer to *Installing a replica authentication server*.

4.3 Installing Active Directory User Interface tools

Mi-Token Enterprise Edition User Interface tools can be deployed on any number of domain member servers or workstations.

- The installer requires local Administrator rights.
- The User Interface requires access to the AD LDS instance. The instance should have been already created by running the Mi-Token installer (with Domain Administrator rights) for either the RADIUS plug-in or API Server on any domain member server.

Active Directory User Interface is often abbreviated to Active Directory UI or AD UI.

1. Check that all prerequisites have been installed on the server. They are listed at *Prerequisites*.
2. Ports must be opened as required on any intervening firewalls. See *Ports and protocols table* for further information.
3. Double-click the **Mi-Token Active Directory UI** installer, downloaded under *Download the Mi-Token software*. Its name is Mi-Token Active Directory UI_64bit.exe or similar. If you are installing the 32-bit version, you will have downloaded and extracted it separately.



Figure 28. RADIUS plugin welcome dialog box

4. Press **Install** and follow the installation steps.



Figure 29. AD UI end-user license agreement

5. The installation proceeds and concludes with the Setup Successful dialog box.



Figure 30. AD UI Setup Successful

- Go to the Windows Start desktop (that is, press the Windows logo key) and click the **Active Directory Users and Computers** icon. There will be a **Tokens** node visible in the tree in the left pane.

(As an alternative, you can also launch this by clicking **Launch** on the **Token management** tab of **Administration UI Quick-Start**.)

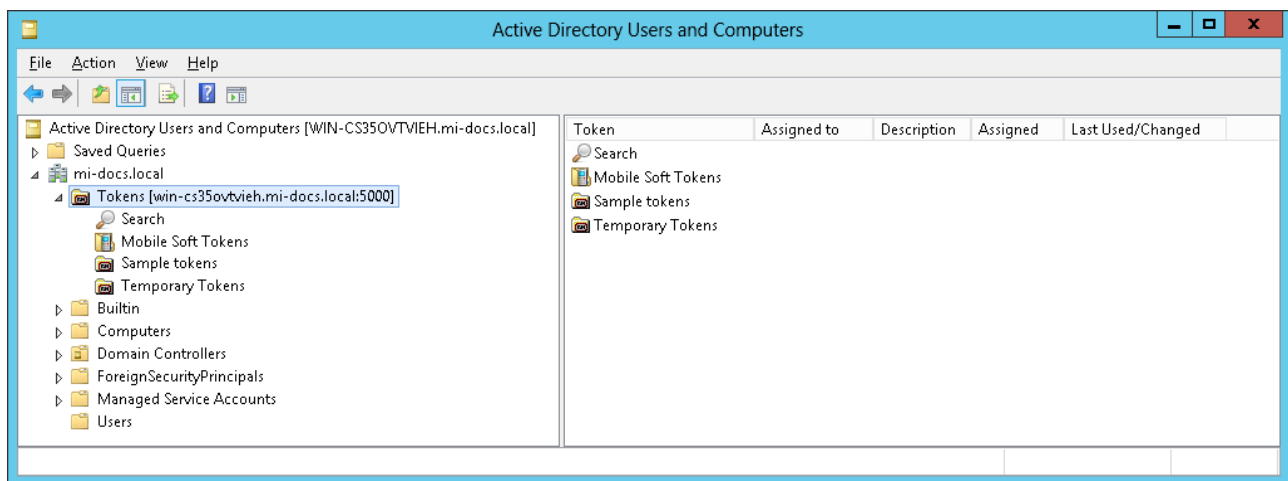


Figure 31. Active Directory Users and Computers

This indicates that you have successfully installed Active Directory User Interface tools.

(Note for reference that detailed documentation on the UI tools is provided under *Active Directory Users and Computers*.)

4.4 Testing RADIUS server installation and configuration

The Mi-Token RADIUS Tester is installed by default on all Mi-Token RADIUS plugin installations. This tool is used to test whether the Mi-Token RADIUS plugin was installed and configured correctly.



To test your primary RADIUS server configuration

- Launch **RADIUS Tester**, either by pressing the Windows logo key or from its exe in the default location: C:\Program Files\Mi-Token\RADIUS Tester.

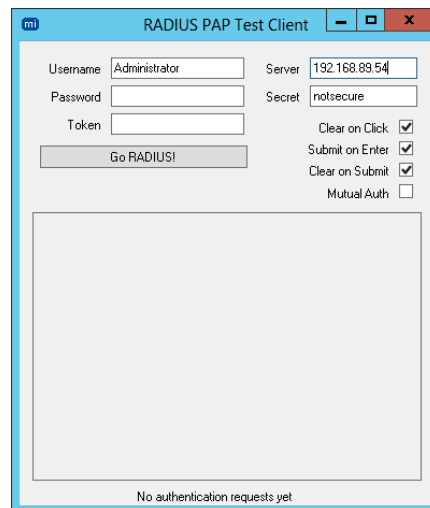


Figure 32. The RADIUS Tester on launch

2. Enter the RADIUS Server IP address and shared secret, and a user's username, password (if required) and token.

Note that you must use the true IP address even though you are most likely still on the same machine; the localhost or loop-back address 127.0.0.1 will not work.

The RADIUS Server IP address and shared secret were set up during the installation process at step 5, see Figure 21).

Experienced users may at this point care to create a temporary token if an assigned token OTP isn't conveniently available. See *Creating temporary tokens*.

3. Conversely, ensure that the RADIUS server has the true IP address of the RADIUS Tester, and not the localhost or loop-back address.
4. Click **Go RADIUS!**. One of these results will appear:
 - **ACCESS_ACCEPT**: You have successfully authenticated and have configured Mi-Token and NPS correctly.
 - **ACCESS_REJECT**: You haven't successfully authenticated, but have configured Mi-Token and NPS correctly. This likely due to the wrong username, password, shared secret or OTP being incorrectly inserted.
 - **Timed out waiting for a RADIUS reply**: Mi-Token and NPS wasn't configured correctly or the wrong server IP was inserted into the RADIUS tester.

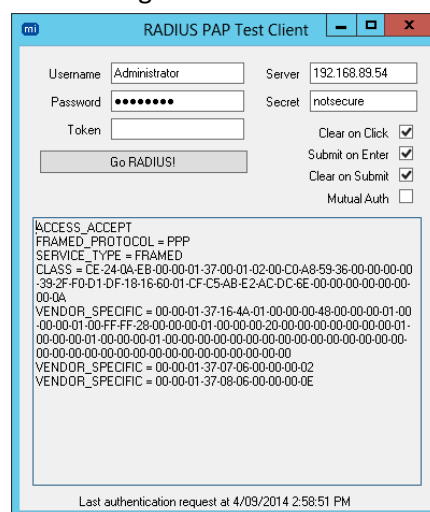


Figure 33. Example ACCESS_ACCEPT

5. Repeat the test until you are satisfied.

4.5 Summary

You have now installed a workable Mi-Token 2-factor authentication system. You can now require your users to enter a token as part of the authentication process. To assign soft tokens to your users, see *Manual provisioning of soft-tokens*.

To assist your users, you may provide *Mini-manual for end-users* to them.

5 Mini-manual for end-users

The procedures here are the ones you will follow to set up and use soft tokens on your desktop or smart phone.

Note here the term **token**. This term has two meanings. It can mean a 6-digit number, used as a password. Elsewhere in this documentation, this is often referred to as a “one-time password” or OTP. It is a password that is used once only and then discarded.

It can also mean the device from which you obtain the 6-digit number. That can be a piece of software on your desktop (the Desktop Token, described below), or a smart phone app (described under *Using Mi-Token with smart phones*), or a small custom device.

A 6-digit number obtained from a smart phone or desktop is known as a **soft token**. A 6-digit number obtained from a small custom device you carry with you is known as a **hard token**.

5.1 Using Mi-Token with the Desktop Token

The Desktop Token is a small piece of software that runs on your computer. This is a download of some 40 MB, because it contains various pieces of .NET infrastructure which may or may not be present on your machine.

Some organizations choose to install the Mi-Token Intranet Provisioning Website and some do not. There are alternative procedures below for organizations with and without this website.

Desktop Token without the Mi-Token Intranet Provisioning Website



To download the Desktop Token without using the Mi-Token Intranet Provisioning Website

1. Get in touch with your system administrators and ask for a Desktop Token. They will send you a URL.
2. Browse to this URL. Usually this will be

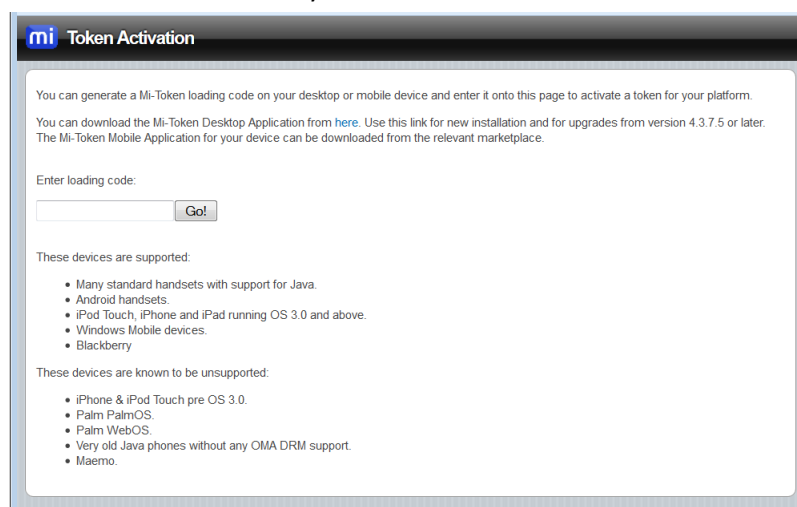


Figure 34. Token activation website

3. Notice the link inviting you to download the Desktop Token software. Click this link. You see the usual browser download dialog boxes.

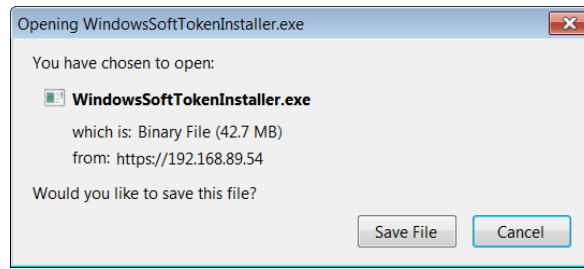


Figure 35. Download Desktop Token installer

4. Download the installer and save it in a convenient place on your hard drive.
5. Execute the installer. The installer starts and displays the end-user license agreement.

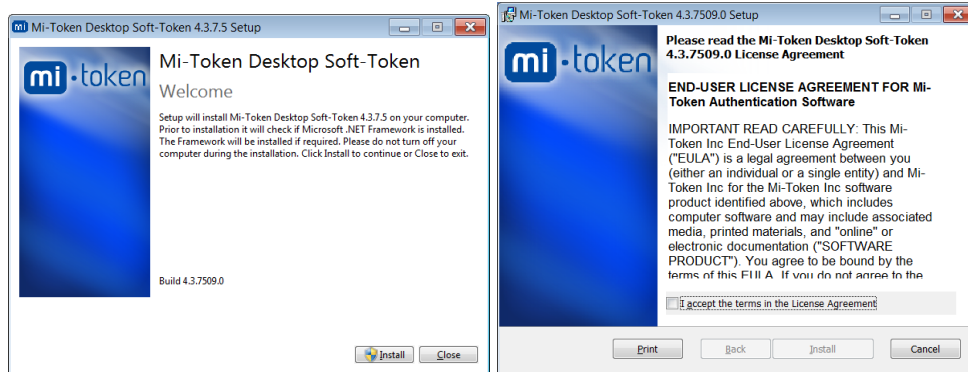


Figure 36. Desktop Token end-user license agreement

6. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Next**.

The installation continues.

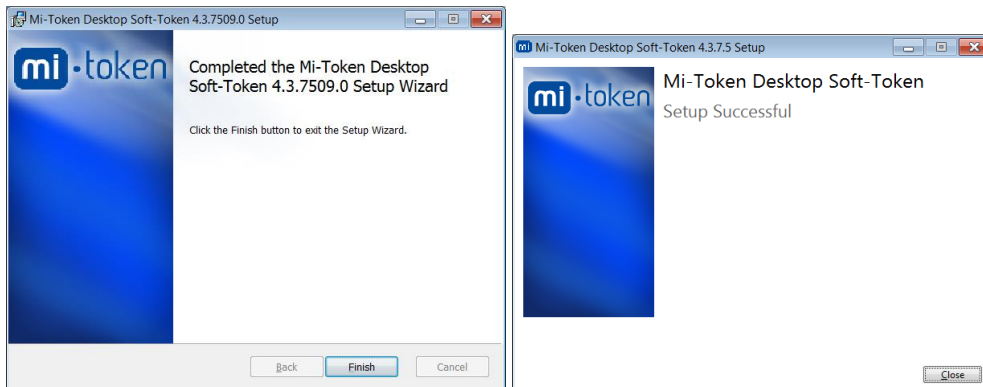


Figure 37. Desktop Token installation

7. Click **Close**. The Desktop Token is installed, including a desktop shortcut icon.



To set up the Desktop Token without using the Mi-Token Intranet Provisioning Website

1. Launch the Desktop Token, either from the Windows Start menu or via the desktop icon.



Figure 38. Desktop Token

2. Click **New Token**. The Desktop Token displays a loading code.

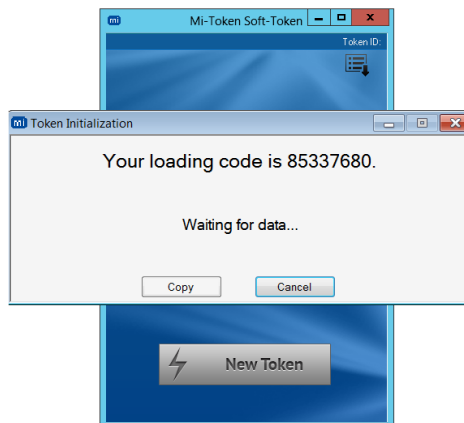


Figure 39. Desktop Token, displaying loading code

3. You must now send this 8-digit loading code to Mi-Token. Enter it into the activation website (that is, Figure 34). You can do this just by transcribing it but the dialog box offers the **Copy** button, which copies the loading code to the Windows clipboard.

Enter the loading code into the activation window of the website.

Enter a 4-digit PIN into the activation window of the website. Make sure that you remember it, because you will need it to authenticate.

4. Click **Go!**.

The website should report **Success!**, and the Desktop Token requests a passcode.

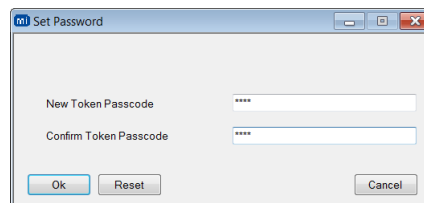


Figure 40. Desktop Token, dialog box requesting a passcode

This passcode is strictly local to the Desktop Token and the machine it is loaded on, and is to ensure that only you access your Desktop Token. (Much in the same way as cell phones require a passcode when you switch them on.)

You can change the passcode at any time from the menu at the top right of the Desktop Token.

The passcode may be blank.

Note that some screens refer to it as a passcode and some as a password.

5. Enter your chosen passcode twice, as required.

The Desktop Token and your organization's servers have interacted in a cryptographically secure manner so that they share certain secure information, known as a seed. In the future, when you try to log in, the server will, by an indirect process, verify this information and be 99.999% certain that it is indeed you that is logging on.

The Desktop Token is now ready for use.



Figure 41. Desktop Token, displaying a 6-digit token

The 6-digit number is the token which you must use, along with your password, to authenticate yourself when you log in remotely.

This 6-digit token is calculated by combining the fixed seed mentioned above with the current clock time. Because it depends on the current clock time, it changes periodically and has a limited life.

Desktop Token using the Mi-Token Intranet Provisioning Website



To download the Desktop Token from the Mi-Token Intranet Provisioning Website

Your system administrators will advise you of the URL for the Mi-Token Intranet Provisioning Website. Note that the Mi-Token Intranet Provisioning Website is only available on your organization's intranet.

1. Browse to the Mi-Token Intranet Provisioning Website URL and log in. Click on the **Assign Desktop Token** icon.

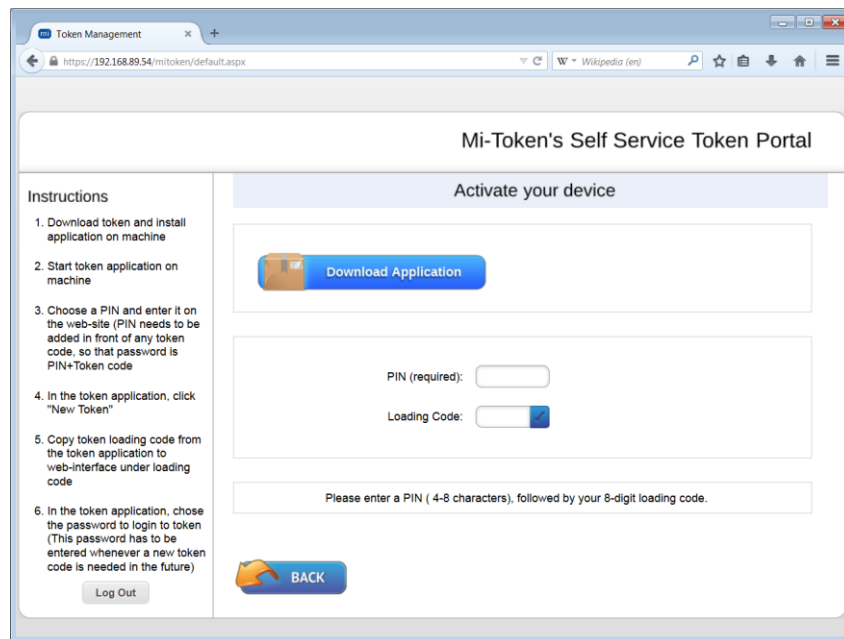


Figure 42. Mi-Token Intranet Provisioning Website activation

2. This window is inviting you to download the Desktop Token software.
Notice that this window also outlines the setup procedure, which is set out below in more detail.
3. Click **Download Application**. You see the usual browser download dialog boxes.

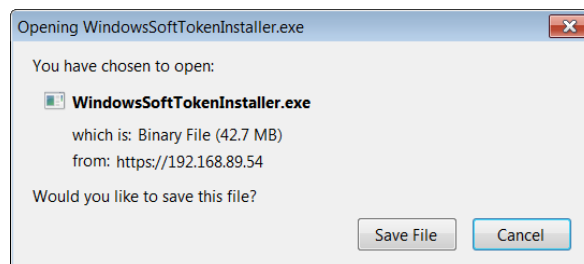


Figure 43. Download the Desktop Token installer

4. Download the installer and save it in a convenient place on your hard drive.
5. Execute the installer. The installer starts and displays the end-user license agreement.



Figure 44. The Desktop Token end-user license agreement

6. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Next**.
The installation continues.

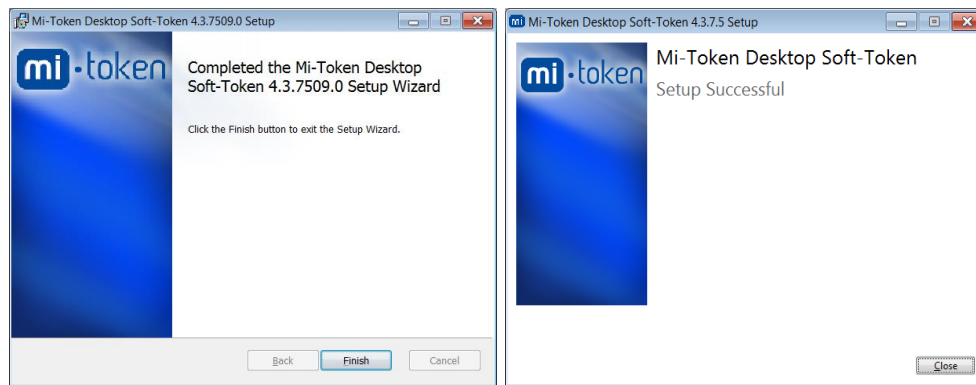


Figure 45. Installing the Desktop Token

7. Click **Close**. The Desktop Token is installed, including a desktop shortcut icon.



To set up the Desktop Token using the Mi-Token Intranet Provisioning Website

1. Launch the Desktop Token, either from the Windows Start menu or via the desktop icon.



Figure 46. Desktop Token

2. Click **New Token**. The Desktop Token displays a loading code.

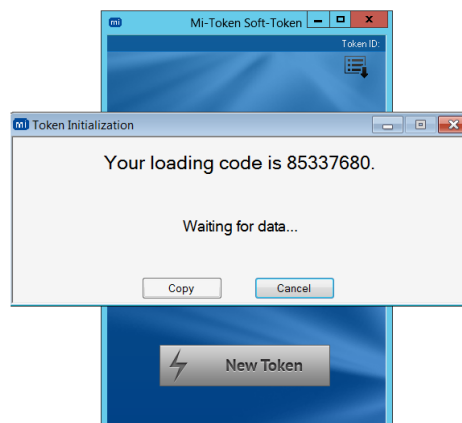


Figure 47. Desktop Token, displaying loading code

3. You must now send this 8-digit loading code to Mi-Token by entering it into the activation window of the website (that is, Figure 42). You can do this just by transcribing it but the dialog box offers the **Copy** button, which copies the loading code to the Windows clipboard.

Enter the loading code into the activation window of the website.

Enter a 4-digit PIN into the activation window of the website. Make sure that you remember it, because you will need it to authenticate.

4. Click the check mark next to the loading code on the activation window of the website.
The website should report **Success**, and the Desktop Token requests a passcode.

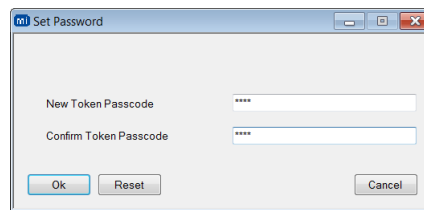


Figure 48. Desktop Token, dialog box requesting a passcode

This passcode is strictly local to the Desktop Token and the machine it is loaded on, and is to ensure that only you access your Desktop Token. (Much in the same way as cell phones require a passcode when you switch them on.)

You can change the passcode at any time from the menu at the top right of the Desktop Token.

The passcode may be blank.

Note that some screens refer to it as a passcode and some as a password.

5. Enter a passcode twice, as required.

The Desktop Token and the Mi-Token Intranet Provisioning Website have interacted in a cryptographically secure manner so that they share certain secure information, known as a seed. In the future, when you try to log in, the server will, by an indirect process, verify this information and be 99.999% certain that it is indeed you that is logging on.

The Desktop Token is now ready for use.



Figure 49. Desktop Token, displaying a 6-digit token

The 6-digit number is the token which you must use, along with your password, to authenticate yourself when you log in remotely.

This 6-digit token is calculated by combining the fixed seed mentioned above with the current clock time. Because it depends on the current clock time, it changes periodically and has a limited life.

Using the Desktop Token

This is the procedure to follow when you need to authenticate yourself during a remote log in.

1. In the course of attempting to log in, your organization's portal or gateway system will ask you for a token. Launch the Desktop Token, either from the Windows Start menu or via the desktop icon.
2. Type into the authentication screen
 - your user name
 - your password
 - if your administrators have determined that it is required, your PIN
 - the 6-digit number from the Desktop Token

You may need to concatenate the password, PIN and 6-digit number. Your administrators will advise.

3. Proceed with the login procedure.

Other actions with the Desktop Token

The Desktop Token has a menu button to its top right.



Figure 50. Desktop Token, showing the menu

New Token

This option initiates a repeat of the process listed under *To set up the Desktop Token using the Mi-Token Intranet Provisioning Website*. You can use this option if the server loses synchronization with you.

Token Management

This option launches a dialog box that enables you to remove your identity from the Desktop Token or to load a new one. You might use these functions if you are giving your computer to a colleague.

Change Token Access Password

This option enables you to change the passcode (sometimes referred to as a password). Recall that this passcode is local to the Desktop Token and the machine it is loaded on, and is to ensure that only you access your Desktop Token, much in the same way as cell phones require a passcode when you switch them on.

Copy to Clipboard

This option copies the current 6-digit token to the Windows clipboard, for convenience in pasting it into authentication dialog boxes.

Check time

Recall that the token is calculated from certain secure information and the current clock time. This means that if your computer clock deviates from the correct time, the token will not match with the server's. This option forces the Desktop Token to check its time with Internet time servers (known as NTP servers).

Generate Log

This option generates a log file containing information that may be useful to MI-Token technical support staff. They will ask you for it if necessary.

About

This option displays useful information about the Mi-Token product.

Settings

This option contains settings under three headings.

Proxy Server. If you are using a proxy server for Mi-Token, enter the configuration settings here.

Time Settings. You may switch off the facility to use an NTP time server.

Reset WindowsSoftToken. You may reset the Desktop Token so that you will need to generate a new token as described under *To set up the Desktop Token using the Mi-Token Intranet Provisioning Website*.

5.2 Using Mi-Token with smart phones

Some organizations choose to install the Mi-Token Intranet Provisioning Website and some do not. There are alternative procedures below for organizations with and without this website.

Mi-Token can be used with these smart phones, with the limitations noted.

OS	Requirements	Notes
iOS	iOS 2.0 or greater	Works on any iOS device, including iPhones, iPod touches, and iPads.
Android	Android 1.5 or greater	We recommend using the native browser.
Windows Phone	Windows Phone 7 or greater	Should be downloaded directly from the Windows Phone Store. A desktop is then required to activate the user's token.
Windows Mobile	Windows Mobile 5 or greater	We recommend using Internet Explorer to download the Mi-Token application. You can choose to either save or open the file. You should install the application on to the phone's internal storage. It will then be present under Start > Programs .
BlackBerry 10	BlackBerry 10.0 or greater	Should be downloaded directly using BlackBerry World. A desktop is then required to activate the user's token.
Blackberry	Requires Blackberry 4.0 to 7.1	The application should be downloaded to phone memory. The user may receive a warning that the application is untrusted – this should be ignored. The Mi-Token App is installed in the Applications menu and may be under the Downloads, Installations, My Stuff or My Own submenus.
Java ME / Symbian	Requires CLDC 1.0/MIDP 2.0. This should be present on newer Java phones.	The app should be downloaded to phone memory. The user may receive a warning that the application is untrusted – this should be ignored. The Mi-Token App is installed in the Applications menu and may be under the Downloads, Installations, My Stuff or My Own submenus.

Figure 51. Smart phone compatibility list

Smart phone app without the Mi-Token Intranet Provisioning Website

You will need web access and your smart phone.

There are two ways to set up the smart phone app; one requires your smart phone to be able to receive email (via webmail if necessary) and one does not.



To set up the smart phone app without using the Mi-Token Intranet Provisioning Website

Note that images of smart phone screens are taken from Android; iPhone screens are very similar.

1. Go to the Apple iTunes or Google Play store and download the Mi-Token app.
2. Get in touch with your system administrators and ask for a smart phone token. They will send you an email containing a URL.
3. Launch the app.

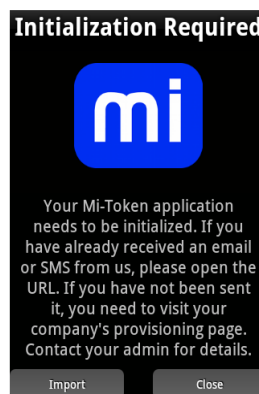


Figure 52. Mi-Token app initialization (Android)

You now have the choice of methods.

If your smart phone can receive emails

This method is known as the v4 method.

4. On the smart phone, receive the email, which will have content similar to this:
Please open this link on your mobile device:
[Set up smartphone token app](#)
5. Click the hyperlink. The smart phone downloads resources.



Figure 53. Mi-Token app downloading, and ready (Android)

When it is finished downloading, it displays a 6-digit token. If you requested a custom logo, this will now appear on the app.

If your smart phone cannot receive emails

This method is known as the v4 hybrid method.

4. On any device, receive the email, which will have content similar to this:
Please open this link on your mobile device:
[Set up smartphone token app](#)
5. Click the hyperlink. A web page opens, requesting an 8-digit code. This web page is the same as used for the Desktop Token, that is, Figure 34.
6. Press **Import** on the smart phone screen (Figure 58). The smart phone displays an 8-digit code.

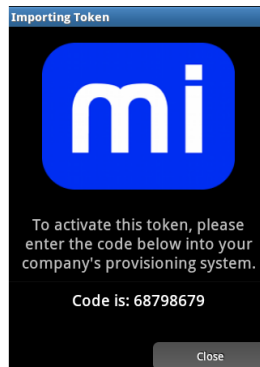


Figure 54. Mi-Token app activation code (Android)

7. Enter this code into the website and click **Close** on the smart phone.
The smart phone displays a 6-digit number.
The 6-digit number is the token which you must use, along with your password, to authenticate yourself when you log in remotely.
This 6-digit token is calculated by combining the fixed seed with the current clock time. Because the token depends on the current clock time, it changes periodically and has a limited life.

When you see the 6-digit token...

The smart phone app is now ready for use.

Your organization's servers and your smart phone now share certain secure information, known as a seed. In the future, when you try to log in, the server will, by an indirect process, verify this information and be 99.999% certain that it is you that is logging on.

Smart phone app with the Mi-Token Intranet Provisioning Website

You will need the Mi-Token Intranet Provisioning Website and your smart phone. Note that the Mi-Token Intranet Provisioning Website is only available on your organization's intranet.

There are two ways to set up the smart phone app; one requires your smart phone to be able to receive email (via webmail if necessary) and one does not.



To set up the smart phone app using the Mi-Token Intranet Provisioning Website

1. Browse to the Mi-Token Intranet Provisioning Website URL and log in. Click on the **Provision Smartphone Token** icon.

Mi-Token's Self Service Token Portal

Instructions

- Welcome to the Mi-Token Soft-Token deployment page
- Please confirm that your information is listed correctly. You may have an opportunity to change the information in the next step; if not, please contact your service desk.

[Log Out](#)

Check that your Windows user information is correct

Username: **Pat Smith (PatSmith)**

Email: **da@gmail.com**

Before we Begin

To successfully set up Mi-Token on your smartphone the following prerequisites apply:

- Data access (i.e. Internet) is required to download the Mi-Token application. Please check with your mobile network operator if you're unsure.
- You can deploy by email. Please check above that we have the correct email address and that you can receive emails from this address on your smartphone.
- If you experience difficulties, please contact the Customer Service Center at 1-877-724-8272.

[BACK](#) **Step 1 Prerequisites** **Step 2 PIN selection** **Step 3 Download token** [NEXT](#)

Figure 55. Mi-Token Intranet Provisioning Website

- Click **NEXT**.

Mi-Token's Self Service Token Portal

Instructions

- Your administrator has configured this Mi-Token instance to accept PINs for all soft-tokens.

[Log Out](#)

Setting a pin is required

PIN:

[BACK](#) **Step 1 Prerequisites** **Step 2 PIN selection** **Step 3 Download token** [NEXT](#)

Figure 56. Mi-Token Intranet Provisioning Website requesting a PIN

- Enter a PIN of your choosing. Despite the name, this PIN may contain alphanumeric characters.

Click **NEXT**.

Mi-Token's Self Service Token Portal

Instructions

- Open email or text message on your smartphone, click on "Set up Smartphone token app" and follow the instructions provided.

[Log Out](#)

Send a download link to your device

Email: **da@gmail.com**

Send link via Email
Email will go to da@gmail.com

[BACK](#) **Step 1 Prerequisites** **Step 2 PIN selection** **Step 3 Download token** [NEXT](#)

Figure 57. Mi-Token Intranet Provisioning Website about to send initialization link

The website offers to send a link via email.

4. Click **Send link via Email**.
5. Go to the Apple iTunes or Google Play store and download the Mi-Token app.
6. Launch the app.

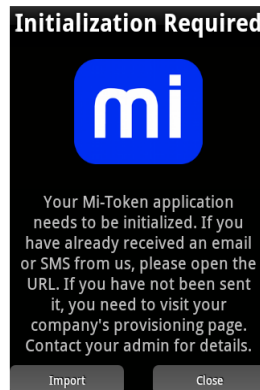


Figure 58. Mi-Token app initialization (Android)

You now have the choice of methods.

If your smart phone can receive emails

This method is known as the v4 method.

7. On the smart phone, receive the email, which will have content similar to this:

Please open this link on your mobile device:

[Set up smartphone token app](#)

The hyperlink will be quite long, and will start with the domain mobile.mi-token.com.

8. Click the hyperlink. The smart phone downloads resources.



Figure 59. Mi-Token app downloading, and ready (Android)

When it is finished downloading, it displays a 6-digit token. If you requested a custom logo, this will now appear on the app.

If your smart phone cannot receive emails

This method is known as the v4 hybrid method.

7. On any device, receive the email, which will have content similar to this:

Please open this link on your mobile device:

[Set up smartphone token app](#)

8. Click the hyperlink. A web page opens, requesting an 8-digit code.

9. Press **Import** on the smart phone screen (Figure 58). The smart phone displays an 8-digit code.

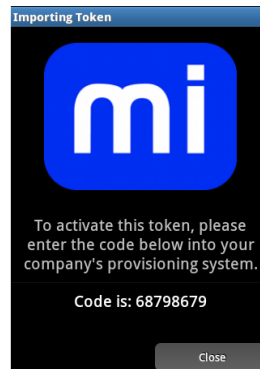


Figure 60. Mi-Token app activation code (Android)

10. Enter this code into the website and click **Close** on the smart phone.

The smart phone displays a 6-digit number.

The 6-digit number is the token which you must use, along with your password, to authenticate yourself when you log in remotely.

This 6-digit token is calculated by combining the fixed seed with the current clock time. Because the token depends on the current clock time, it changes periodically and has a limited life.

When you see the 6-digit token...

The smart phone app is now ready for use.

Your organization's servers and your smart phone now share certain secure information, known as a seed. In the future, when you try to log in, the server will, by an indirect process, verify this information and be 99.999% certain that it is you that is logging on.

Using the smart phone app

This is the procedure to follow when you need to authenticate yourself during a remote log in.

1. In the course of attempting to log in, your organization's portal or gateway system will ask you for a token. Launch the Smart phone app, either from the Windows Start menu or via the desktop icon.
2. Type into the authentication screen
 - your user name
 - your password
 - if your administrators have determined that it is required, your PIN
 - the 6-digit number from the smart phone app

You may need to concatenate the password, PIN and 6-digit number. Your administrators will advise.

3. Proceed with the login procedure.

Other actions with the smart phone app

The smart phone app has numerous options. To access them press the menu button.

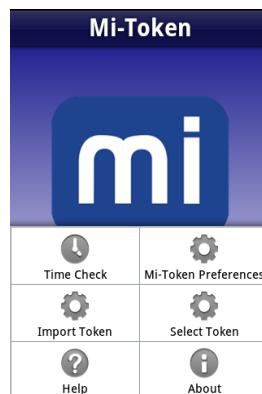


Figure 61. Smart phone app, showing the menu

Time check

Recall that the token is calculated from a seed and the current clock time. This means that if your computer clock deviates from the correct time, the token will not match with the server's. This option forces the smart phone app to check its time with Internet time servers (known as NTP servers).

Import Token

This option initiates a repeat of the *v4 hybrid* process, using an 8-digit code. You can use this option if the server loses synchronization with you.

Help

This option is intended to deliver helpful information.

Mi-Token Preferences

This option enables you to remove your identity from the smart phone app. You might use these functions if you are giving your smart phone to a colleague.

Select token

This option synchronizes the smart phone with a time server.

About

This option displays useful information about the Mi-Token product.

6 All-on-one-machine installation

The all-on-one-machine installation adds Mi-Token Reporting and the Mi-Token Intranet Provisioning Website feature, and, like the minimal installation, is deployed on a single machine.

It is straightforward to progress from a minimal to an all-on-one-machine installation.

You may choose to use the *Installation checklists* as an aid in working through the process.

6.1 Mi-Token Reporting

Mi-Token Reporting consists of three major components:

- An SQL Server database , for which you will need an ODBC driver.
- The Event Collector Service (sometimes referred to as just the Collector Service). This collects data from an NT event log and writes it to the SQL database .
- The Reporting website. This reads information from the database and processes it into a useful format.

These three components may be installed on the same machine or separate machines.

Installing the ODBC driver and Mi-Token Reporting

Note that you may use SQL Server browser service for Remote Instance discovery if you wish.



To install the ODBC driver and Mi-Token Reporting

1. Ensure that all prerequisites have been installed on the server. They are listed at *Prerequisites*.
2. Ensure that a database is present in SQL Server with name Mi-Token or MiToken. Mi-Token currently supports SQL server 2005, 2008, 2012 and 2014. The database may be on any accessible machine.
3. Configure the firewalls to permit:
 - HTTPS traffic, which is on port 443 by default
 - TCP traffic on the SQL Server port, which is 1433 by default
 - UDP traffic on port 1434, used by the SQL Server Browser service during Reporting setup only – this is optional

Refer to *Ports and protocols table*.

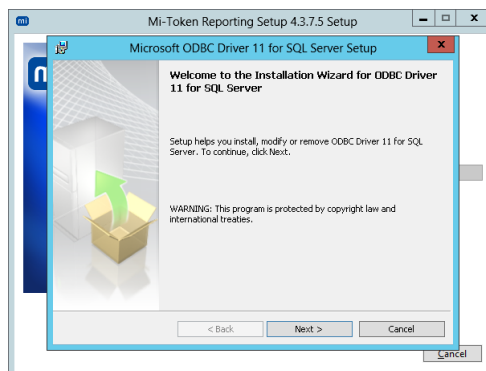
4. Ensure that you are logged in with an account that has local administrator and SQL Server administrator privileges.
5. Double-click the Mi-Token Reporting installer, downloaded under *Download the Mi-Token software*. Its name is Mi-Token Reporting Setup_64bit.exe or similar.



Figure 62. Reporting Setup welcome

6. Click **Install**.

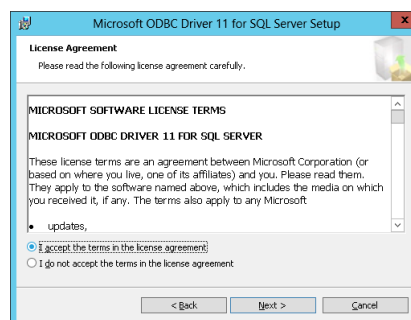
If an ODBC driver is not already present, the installer will install it.



(Standard Windows dialog box)

Figure 63. ODBC driver welcome dialog box

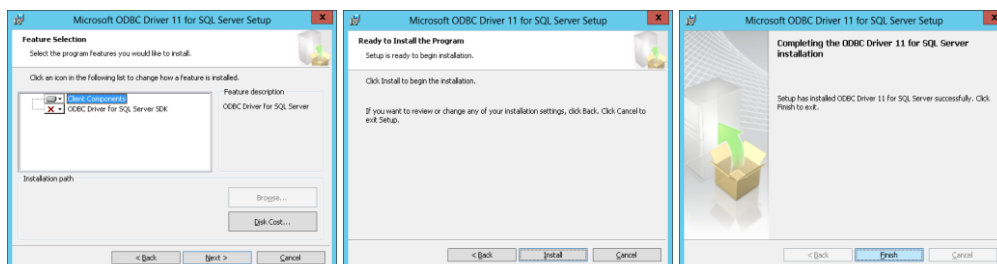
7. Click **Next>**.



(Standard Windows dialog box)

Figure 64. ODBC driver end-user license agreement

8. Read the end-user license agreement. If you accept the terms, proceed to install the ODBC driver.



(Standard Windows dialog boxes)

Figure 65. ODBC driver installation

When the ODBC driver is installed, the installer will proceed to Reporting Setup.

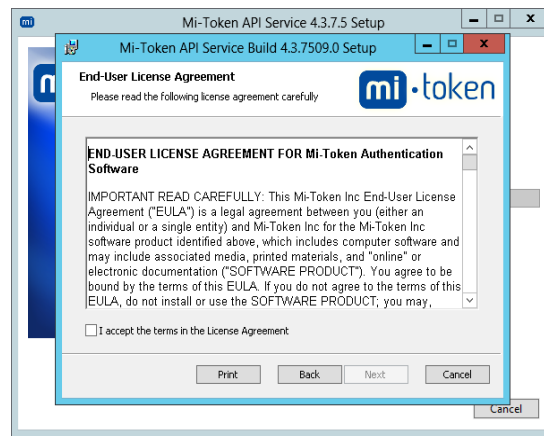


Figure 66. Reporting Setup end-user license agreement

9. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Install**.

The installation continues. The wizard completes. Click **Finish**.

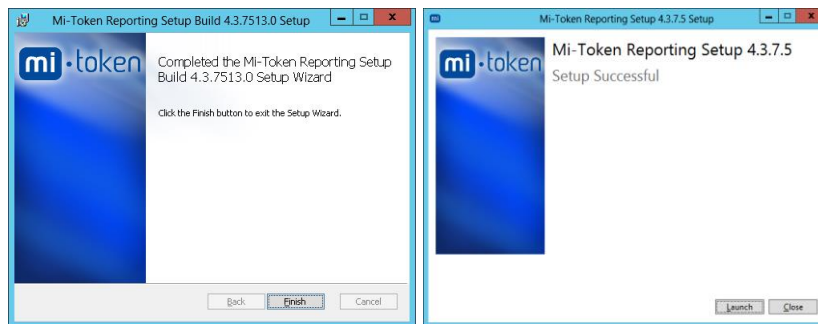


Figure 67. Reporting Setup wizard completed, Reporting setup successful

At this point you can launch Mi-Token Reporting by clicking **Launch**. However, to relaunch it later, use the Reporting Setup shortcut icon, created by the installer and accessible from the Windows logo key.

10. Click **Launch**.

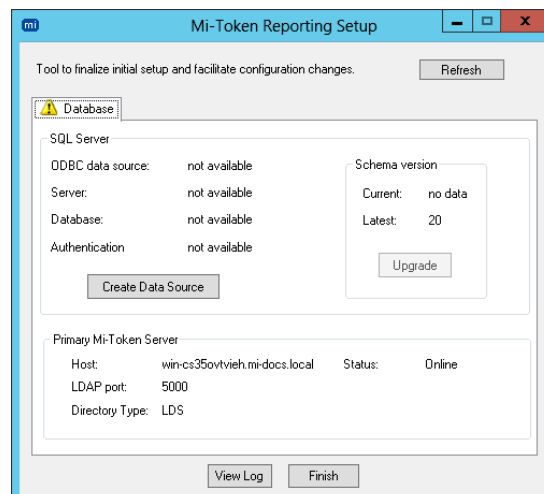


Figure 68. Reporting Setup tool

11. Click **Create Data Source**. The **New ODBC Data Source** dialog box opens.

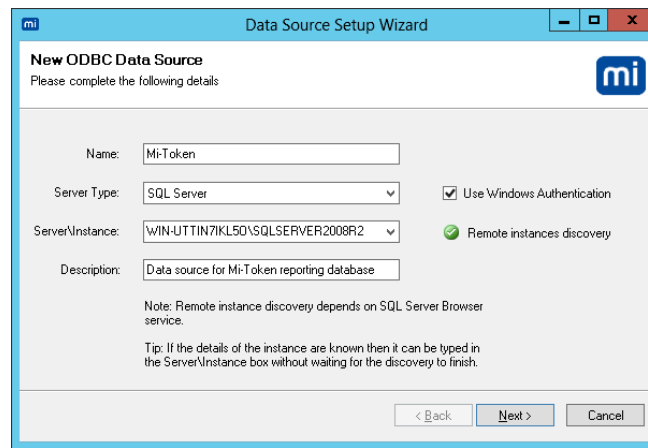


Figure 69. New ODBC Data Source

The tooltips on this dialog box are listed here for convenience:

Name

ODBC DSN to be used by Mi-Token Reporting. The characters '=' and ';' cannot be used.

Server Type

RDBMS type. Currently only SQL Server is supported.

Server\Instance

The name of the server hosting SQL Server separated by backslash from SQL Server instance name. For example: MyHost\MyInstance or 111.111.3.4\Sq123

The default instance name MSSQLSERVER is suppressed if found with only the server portion shown. If the server portion matches local computer name, then it is replaced with (local).

Description

Description for Mi-Token ODBC DSN.

Use Windows Authentication

Windows Authentication

Use credentials of the current user to connect to the database. At run-time the credentials of the NETWORK SERVICE account are used instead.

SQL Server Authentication

Always use username and password typed into Credentials Dialog displayed next.

Remote instances discovery

Once discovery finishes, the animated icon is replaced with green checkmark if remote instances are found, otherwise gray checkmark is used.

Note also the instructions at the bottom of the dialog box:

Note: Remote instance discovery depends on SQL Server Browser service.

Tip: If the details of the instance are known then it can be typed in the Server\Instance box without waiting for the discovery to finish.

If you choose to use Windows authentication but there is no SQL Server in the current domain, the installer will invite you to switch to SQL Server authentication.

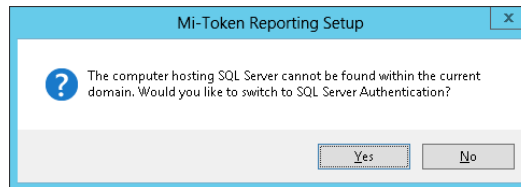


Figure 70. SQL Server cannot be found in the current domain

In this case, installer will uncheck the box on the **New ODBC data source** dialog box.

12. Select and connect to your database.

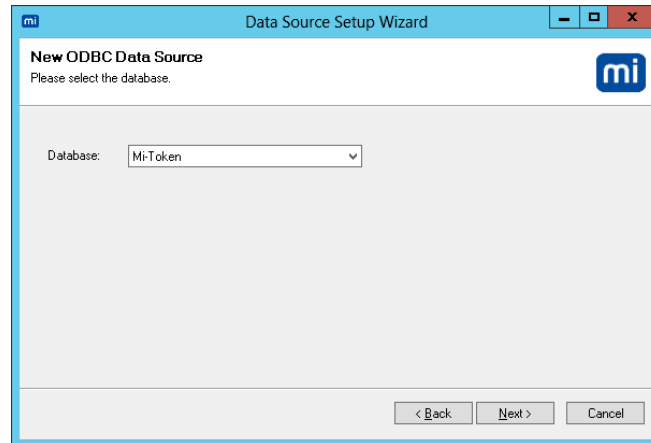


Figure 71. Select the database

13. Click **Next>** and complete the installation.



Figure 72. ODBC data source successfully installed

Configuring Mi-Token Reporting



To configure Mi-Token Reporting

1. Click **OK**. The installer restarts and when it does, the Reporting Setup dialog box now has three more tabs.

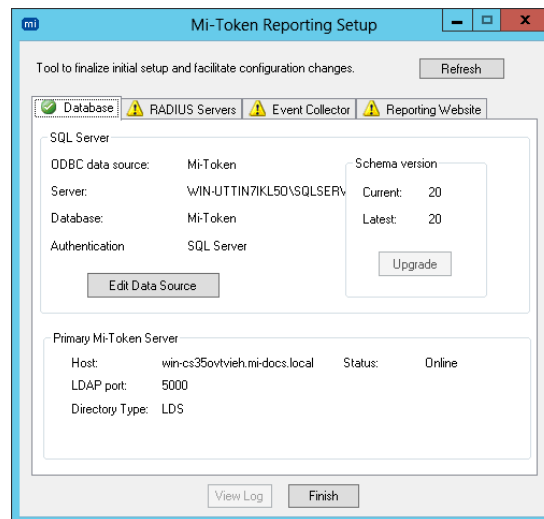


Figure 73. Reporting Setup dialog box with 4 tabs

- Inspect the Reporting Setup dialog box, **Database** tab. If the current version is not the latest, click **Upgrade** to bring the schema up to date. When successful, the current schema version will reflect the latest schema version.
- Register a new RADIUS server. To do this, select the **RADIUS Servers** tab, click **Add...** and fill in the details.

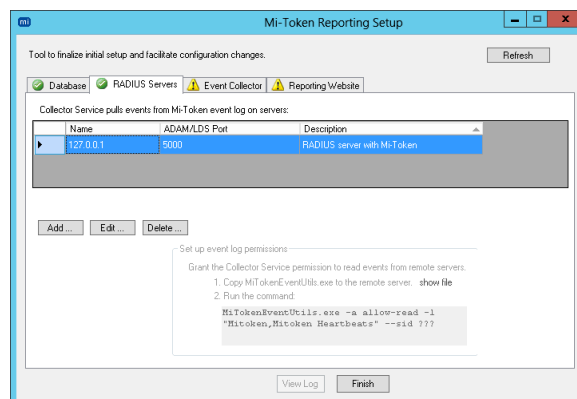


Figure 74. RADIUS Server tab: added a RADIUS server

By default, a new server grants permission to the Event Collector Service (which you will install in the next process by using the **Event Collector** tab) so that it can collect event messages – but only if the Event Collector Service is running on the same machine, which is assumed here in the context of an all-on-one-machine installation.

The material in the bottom part of the dialog box (**Set up event log permissions...**) is relevant to servers which are not on the same machine as the Event Collector Service. More information is presented in the context of a replica installation, under *Installing a replica authentication server*, and in particular, step 6.



To add, edit or remove RADIUS servers

- Add, edit or delete entries by using **Add...**, **Edit...** and **Delete...**.

Installing the Event Collector Service



To install the Event Collector Service

- Still on the same dialog box, go to the **Event Collector** tab.

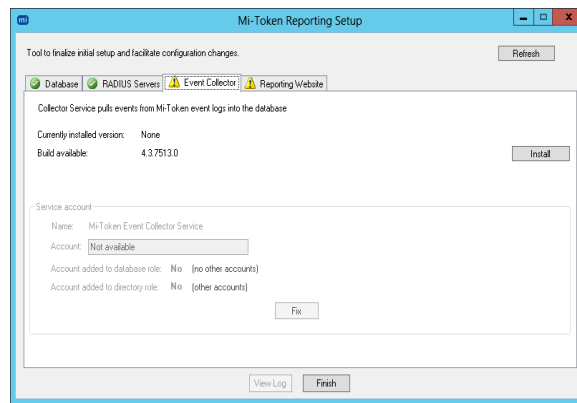


Figure 75. Reporting Setup – Event Collector tab

2. Click **Install**.



Figure 76. Event Collector Service installer

3. Click **Install**. The installation wizard starts.



Figure 77. Event Collector setup wizard

4. Click **Next**.

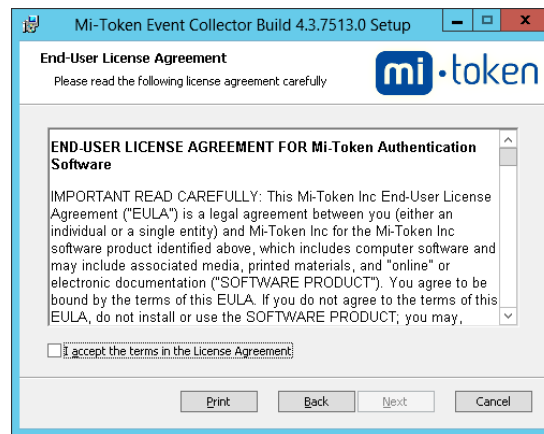


Figure 78. Event Collector end-user license agreement

5. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Next**.

The installation continues. When the wizard completes, you will see this dialog box.

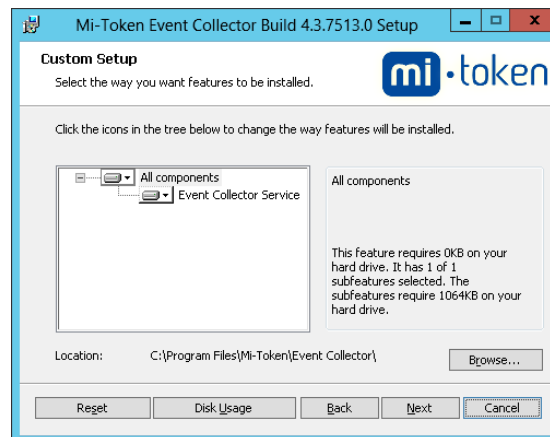



Figure 79. Event Collector installer, showing the installation options

In the central choice pane, click the drop-down box  next to **All components**.

6. Select **Entire feature will be installed on local hard drive**. Click **Next**.
7. Click **Install**. The installation proceeds and displays this dialog box.

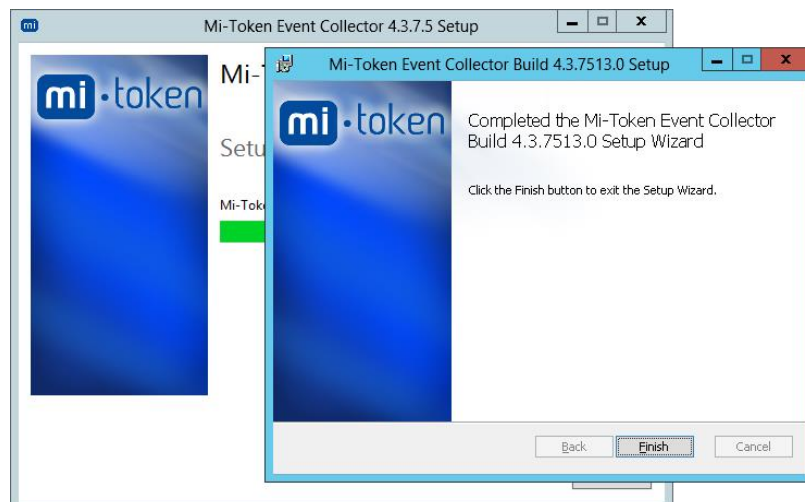


Figure 80. Event Collector installation wizard completed

8. Click **Finish**. Click **Close**.

Installing the Reporting website

The Reporting website uses HTTPS and therefore requires HTTPS binding for the IIS website, which in turn requires a certificate. The installer generates a self-signed certificate and places it into Windows certificate store. Then it examines IIS settings, specifically the default website bindings. If no HTTPS bindings are found, the installer creates one. You can edit the binding later on and replace the self-signed certificate with the one signed by your Enterprise Certificate Authority or by Root Certificate Authority.



To install the Reporting website

1. On the Reporting Setup dialog box, go to the **Reporting Website** tab and click **Install**.

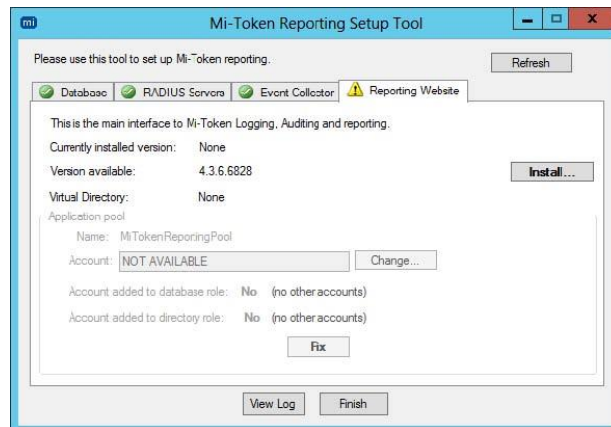


Figure 81. Install Reporting website

2. On the Mi-Token Reporting Website setup welcome dialog box, click **Install**.

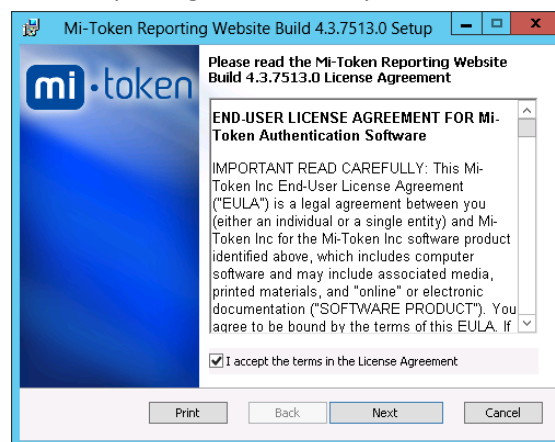


Figure 82. Reporting end-user license agreement

3. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Next**.

The installation proceeds and displays the IIS Settings dialog box.

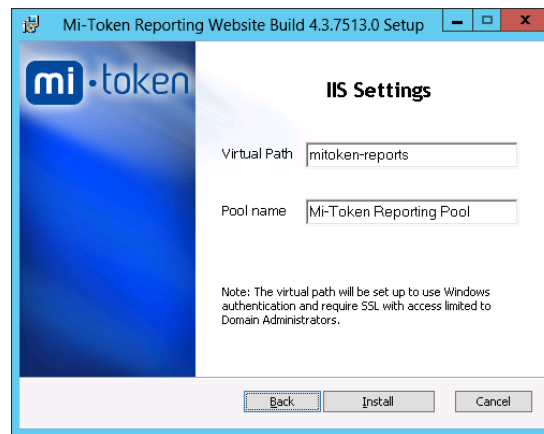


Figure 83. Reporting IIS Settings

Notice that access to the reports will be limited to domain administrators.

4. Click **Install** and proceed through the installation. When the installation is complete, you will see this dialog box.



Figure 84. Reporting installation successful

5. Click **Close**.
6. Optionally, check that you have an SSL certificate and that HTTPS bindings have been added to the IIS server.

Mi-Token Reporting is now set up and ready for use. Browse to <https://localhost/mitoken-reports>

Your report will look like Figure 85.

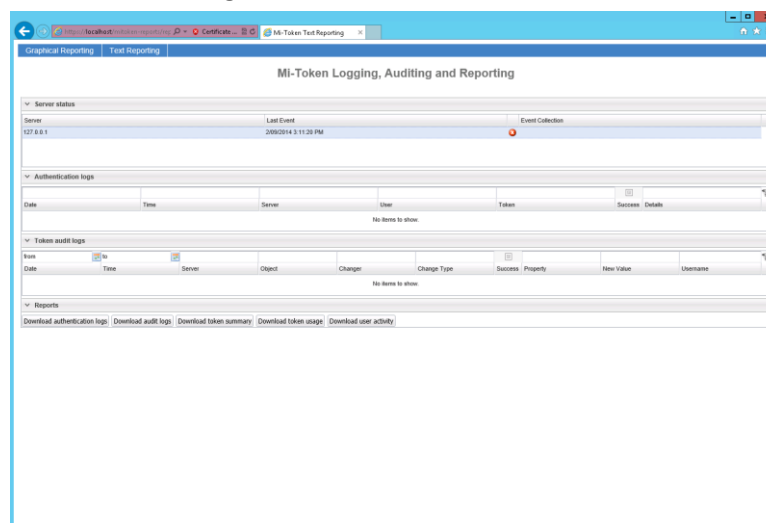


Figure 85. Sample Mi-Token Reporting website

6.2 Mi-Token Intranet Provisioning Website


Before you install the Mi-Token Intranet Provisioning Website, you must have an AD LDS instance running, and have run the MI-Token RADIUS plugin installer (or possibly the API installer) somewhere in the current domain.

The instructions here describe how to install a basic Intranet Provisioning Website. Advanced material is given under *Intranet Provisioning Website advanced topics*.

Installing the Mi-Token Intranet Provisioning Website

The Intranet Provisioning Website uses HTTPS and therefore requires HTTPS binding for the IIS website, which in turn requires a certificate. The installer generates a self-signed certificate and places it into Windows certificate store. Then it examines IIS settings, specifically the default website bindings. If no HTTPS bindings are found, the installer creates one. You can edit the binding later on and replace the self-signed certificate with the one signed by your Enterprise Certificate Authority or by Root Certificate Authority.

To install a Key Encryption Key

 **The Key Encryption Key is critical to your security, because, as the name suggests, it is used to encrypt other keys in transit. Your AD LDS installation contains, by default, a KEK and so, if you are performing an evaluation, you may use this one. However, the default KEK is not secret and so, if you proceed to a production deployment, you must obtain a secure KEK and install it.**

1. Obtain a Key Encryption Key (KEK) from Mi-Token. Store it in a convenient location.
2. From the Windows Start desktop, launch **Active Directory Users and Computers**. A **Tokens** node is visible in the tree in the left pane.
3. Right-click on the tokens node and select **Import....** An import wizard appears.
4. Browse to and select the Key Encryption Key (KEK), supplied by Mi-Token, Inc. Select **Next** and complete the wizard. The key will be imported.

To install the Mi-Token Intranet Provisioning Website

 **For security reasons, the website must be installed on an internally accessible web server only.**

1. Ensure that Internet Information Services (IIS) is installed. The website does not have to be installed on the same server running the AD LDS instance but it must reside in the same domain where AD LDS instance is found.
2. Double-click the Mi-Token Intranet Provisioning Website installer, downloaded under *Download the Mi-Token software*. Its name is Mi-Token Intranet Provisioning Website_64bit.exe or similar.

The default settings may be used throughout the install process.

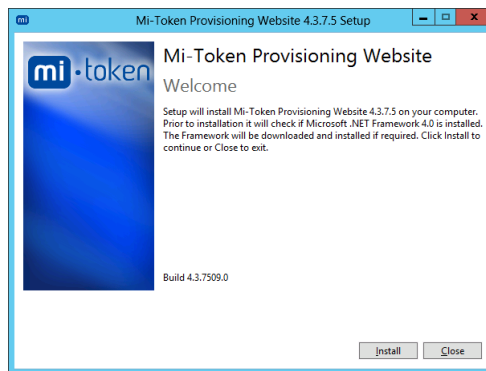


Figure 86. Mi-Token Intranet Provisioning Website welcome

3. Click **Install**.

The installer starts and displays the end-user license agreement.



Figure 87. Mi-Token Intranet Provisioning Website end-user license agreement

4. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Next**.

The installation continues.

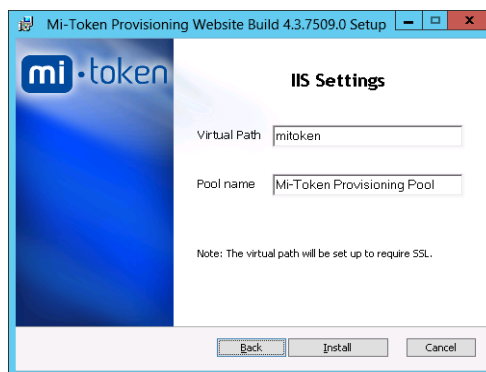


Figure 88. Mi-Token Intranet Provisioning Website IIS settings

5. Click **Install**. The installation continues. You will see this dialog box.

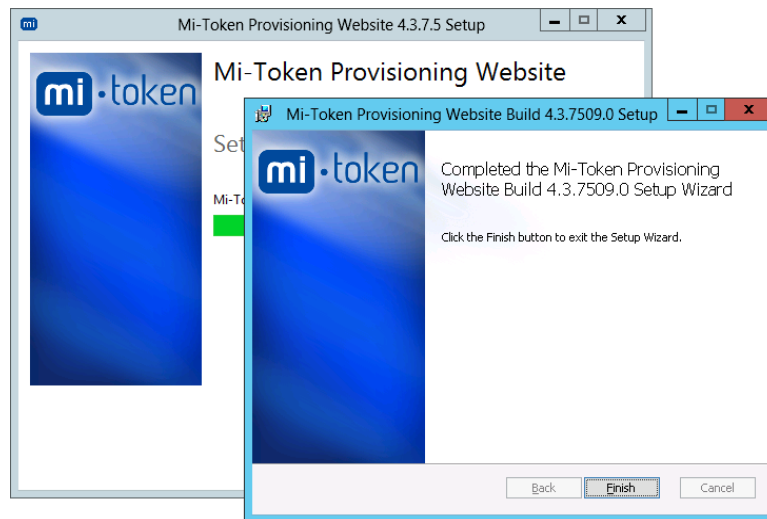


Figure 89. Mi-Token Intranet Provisioning Website wizard complete

6. Click **Finish**.

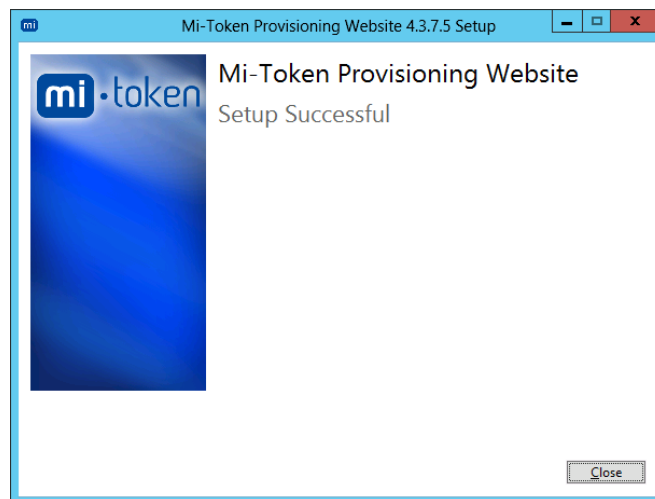


Figure 90. Mi-Token Intranet Provisioning Website setup successful

7. Click **Close**.
8. Browse to the website, which by default is `https://<host>/mitoken/`, where `<host>` is the name of your host.
9. You may see a page stating that the website does not have sufficient rights to access the AD LDS folder. It will also give a command to run in a command window. Run it with elevated privileges. The access right will then be granted to the website.
10. At this stage you may see a message saying that there is no deployment method enabled for the currently logged-on user. This means that the currently logged-on user does not have an email address and/or mobile phone number in Active Directory. For the website to work, the logged-on user must have an email address and/or mobile phone number configured in Active Directory.
11. You should now see the Mi-Token Intranet Provisioning Website and be able to log in. Follow the instructions on the page if you wish to provision a soft token.

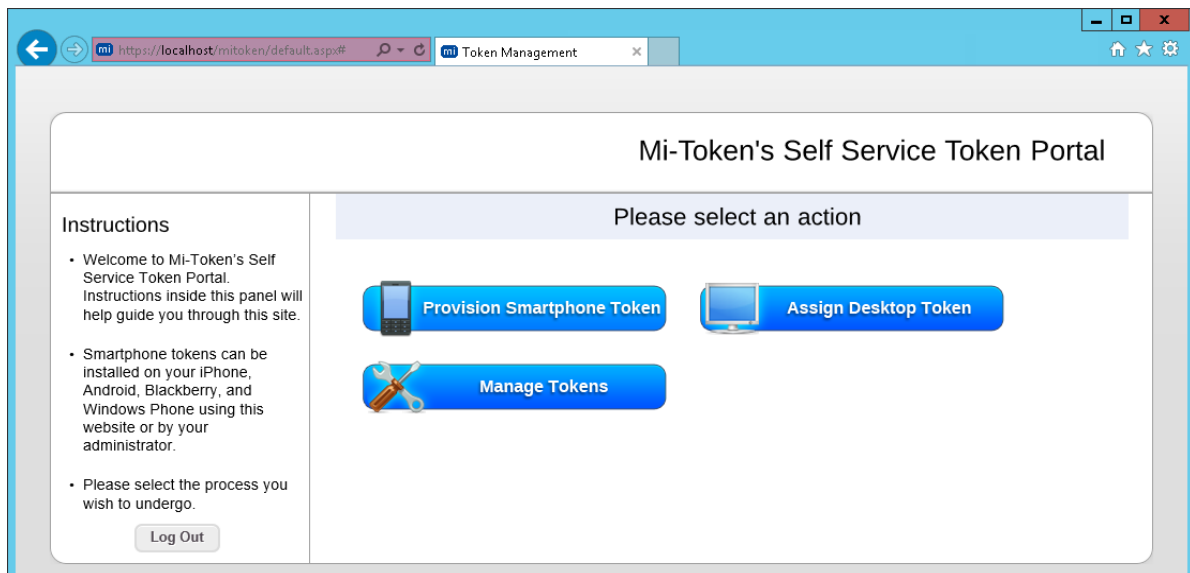


Figure 91. Mi-Token Intranet Provisioning Website

12. Optionally, check that you have an SSL certificate and that HTTPS bindings have been added to the IIS server.

You now have a functioning Intranet Provisioning Website. If you wish to familiarize yourself with it, you may proceed to do so.

Before publishing it for use in your company, you will probably need to configure it. For example, if you require the Assign Desktop Token feature, you must ensure that version 5 has been set in the `customer.settings.config` file. Configuration information is provided under *Intranet Provisioning Website advanced topics*.



Note also that if you chose to use the default Key Encryption Key and not to import one obtained from Mi-Token, you must do so before putting Mi-Token into production.

Publishing the Mi-Token Intranet Provisioning Website

You may now use the Mi-Token Intranet Provisioning Website to generate tokens, or just by way of testing.

After you have tested the system and are satisfied, you may also publish the link to this website to your users, so that they may provision their own mobile soft tokens.

Notes:

- Access to this website must be via your Intranet only.
- Remember to replace `localhost` or `127.0.0.1` with the true address of the computer the website is installed on.
- Publish the URL (with HTTPS).

End-user instructions

Instructions your end-users will follow to set up and use tokens are collected together in a single Chapter, *Mini-manual for end-users*. You will probably want to try them first.

6.3 Summary

You have now installed a Mi-Token 2-factor authentication system with substantially enhanced functionality. Not only can you now require your users to enter a token as part of the

authentication process, but you have made available to them a special-purpose website which enables them to assign their own soft tokens. You also have a powerful reporting tool.

7 Intranet Provisioning Website advanced topics

The advanced configuration of the Intranet Provisioning Website is done by modifying three configuration files

- `customer.settings.config`

The structure and syntax of this file is described immediately below under *The configuration file customer.settings.config*.

- `sensitive.settings.config`

The structure and syntax of this file is described under *The configuration file sensitive.settings.config*.

- `customer.SMTP.config`.

The structure and syntax of this file is self-explanatory.

7.1 Configuring the Intranet Provisioning Website



To configure the Intranet Provisioning Website

- 1 Browse to `C:\Program Files\Mi-Token\Intranet Provisioning Website\Config` where you will see six files. You may need to modify `customer.settings.config` and possibly `sensitive.settings.config` and `customer.SMTP.config` and you should become familiar with the structure and syntax of these.

For details concerning `customer.settings.config` and `sensitive.settings.config`, see *The configuration file customer.settings.config*. and *The configuration file sensitive.settings.config* respectively.

The `customer.SMTP.config` file contains information relating to your email infrastructure and is self-explanatory.

The other three files Template `customer.settings.config`, Template `sensitive.settings.config` and Template `customer.SMTP.config` are, on delivery, the same as `customer.settings.config`, `sensitive.settings.config` and `customer.SMTP.config` respectively, and may be useful for future reference.

- 2 Modify the files as required.

When you make a change to the configuration files, IIS will not immediately recognize the changes. You need to go through a process known as recycling before IIS recognizes the changes.

- 3 Launch IIS and navigate to the application pools.

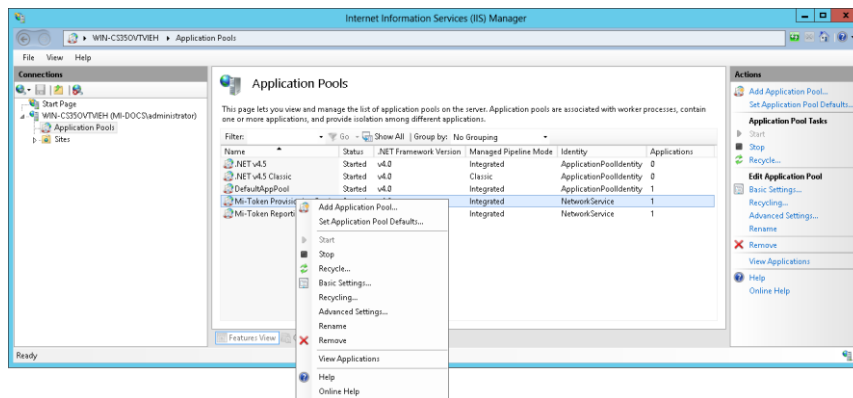


Figure 92. IIS, showing application pools

4. Right-click on Mi-Token Provisioning Pool. Select **Recycling...**
5. Right-click on Mi-Token Reporting Pool. Select **Recycling...**

7.2 Intranet Provisioning Website configuration files

The configuration file customer.settings.config

The customer.settings.config file is by default in C:\Program Files\Mi-Token\Intranet Provisioning Website\Config.

This section describes the customer.settings.config file in detail.

The configuration file is an XML file with a very limited repertoire of tags, as listed below.

Setting explanations are below items and are grouped by functions.

PINs

Create and require a PIN

Provide users the option to create and require a PIN after logging into the Mi-Token Intranet Provisioning Website.

```
<add key="Enable PIN" value = "false" />
```

Compulsory PIN

Enable compulsory creation and use of a PIN in addition to a username and password when logging into the Mi-Token Intranet Provisioning Website.

```
<add key="Require PIN" value = "false" />
```

- Cross-dependency: Enable PIN must be set **true**.

Numeric PINs

Force PINs to be numeric when PINs are enabled.

```
<add key="Numeric Password" value="false"/>
```

- Cross-dependency: Enable PIN must be set **true**.

PIN size

The minimum number of characters that can be used for the Mi-Token Intranet Provisioning Website PIN.

```
<add key="Token Min Pin Length" value="n"/>
```

The maximum number of characters that can be used for the Mi-Token Intranet Provisioning Website PIN.

```
<add key="Token Max Pin Length" value="n"/>
```

Tokens

Unassign tokens

The option to unassign your own tokens in the **Manage Tokens** page.

```
<add key="Enable Unassign" value="false" />
```

- Cross-dependency: Enable Management must be set **true**.

Token management

Enable the token management page on the Mi-Token Intranet Provisioning Website.

```
<add key="Enable Management" value="true" />
```

Back to homepage when a token is assigned

Redirect users back to the Mi-Token Intranet Provisioning Website homepage when a token is successfully assigned.

```
<add key="Back Home" value="true" />
```

Passcodes (or passwords) for soft tokens

Passcode usage rules

Force users to use a password when opening the soft-token (smart phone and tablet tokens).

```
<add key="Require Password" value="true" />
```

Disable passwords for soft tokens.

```
<add key="Disable Password" value="true" />
```

Force users to use a numeric password for soft tokens.

```
<add key="Use Numeric Password" value="true" />
```

- Cross-dependency: the Require Password function must be enabled.

Passcode size

The minimum number of characters for a soft token password.

```
<add key="Minimum Password Length" value="n" />
```

The maximum number of characters for a soft token password.

```
<add key="Maximum Password Length" value="n" />
```

Desktop token

Minimum number of characters that can be used for a desktop token password.

```
<add key="Desktop Password Length" value="n"/>
```

- Desktop tokens (soft tokens for Windows workstation OSs) require a locally stored password— sometimes known as a passcode — when opened. This option determines the minimum length for such a password or passcode.

SMS

SMS is used for Two-Phase Authentication and for sending the token download link.

Send links via SMS

Enable the option for soft-token (smart phone and tablet tokens) assigning links to be sent via SMS as well as email.

```
<add key="Enable SMS" value="false" />
```

- Prerequisite: If you wish to use this option, additional configuration information for SMTP or SMS server, or both, is needed. See below.

SMS body

```
<add key="SMS body" value="Please open: [URL]" />
```

- Keep the message as short as possible, as problems can arise with long SMS messages. The length limit for SMS is 160 characters.
- Mi-Token will replace [URL] with the Mi-Token download URL.
- Mi-Token examines the parameters provided to determine how to send the message, as follows.
 - If "SMS via Email" is set, Mi-Token sends an email to the provider for SMS via email.
 - If not, and a valid MessageMedia username and password are present, Mi-Token sends an SMS using MessageMedia.
 - If not, and a valid SMS Hosted customer id is present, Mi-Token sends an SMS using your hosted SMS provider.
 - If not, Mi-Token sends an SMS via SLI.

Send SMS via email

Address of an SMS provider which forwards an email as an SMS.

```
<!-- <add key="SMS via Email" value = "{0}@myprovider.com" /> -->
```

- The config file is delivered with this feature commented out; remove the comment characters `<!-- -->` to activate the feature.
- The value field must contain {0}, as shown in the example.
- Mi-Token constructs an email address by replacing {0} with the connecting user's cell phone number. It then sends an email to that address, with the download URL in the body of the email.
- This method can be used for sending the token download link.

SMS gateway host and port

```
<add key="smsGatewayHost" value = "host name" />
<add key="smsGatewayPort" value = "port" />
```

- If an SMS gateway host and port appear here, Mi-Token will use them for the SMTP server. If not, Mi-Token will obtain SMTP server information from `customer.SMTP.config`.

Edit phone number

Provide users the option to edit their phone number for soft-token assigning.

```
<add key="Phone number editable" value=true />
```

- Although this may be convenient in some cases, it can result in vulnerabilities. The config file is delivered with this feature commented out; remove the comment characters `<!-- -->` to enable it.

Email

Email content and structure

Structure and content of the email to contain a token download link: from address, from name, subject and body.

```
<add key="Email from address" value=soft-tokens@mi-token.com />
<add key="Email from name" value=IT Help Desk />
<add key="Email subject" value=Mt-Token security app - open on mobile device />
<add key="Email body" value="Please open this link on your mobile device: [URL]" />
```

- Replace [URL] with the correct URL.
- Cross-dependency: these four keys go together as a package.
- Further cross-dependency: if you are using email, you must configure the SMTP host/port in `customer.SMTP.config`.
- To disable soft-token assigning links sent via email in the Mi-Token Intranet Provisioning Website, comment out the functions listed above using `<!-- -->`.

Plain text or HTML text.

```
<add key="plain" value=true />
```

Edit email address option

Provide users the option to edit their email address for soft-token assigning.

```
<add key="Email editable" value=true />
```

- Although this may be convenient in some cases, it can result vulnerabilities. The config file is delivered with this feature commented out; remove the comment characters `<!-- -->` to enable it.

SSL

Enable the use of SSL with SMTP (used for soft-token assigning links sent via email).

```
<add key="SMTP enable SSL" value=false />
```

- In most cases, this value should be left as "false".

User credential requirements

Time limit

The number of days a user can log in with their with an AD password after a password reset.

```
<add key="Reset validity" value="n" />
```

- To disable this function, set the value to zero "0".

Credential requirement types

The credential requirements to log in to the Mi-Token Intranet Provisioning Website.

```
<add key="Authentication mode" value="mode"/>
```

- The value may be **domain**, **token**, **adaptive** or **mixed**.
- If the Authentication mode is **domain**, authentication is by username and password. Specify the AD server using a **domain** key. If the domain key is not set, it will be automatically determined as the domain of the computer the site is running on.

- If the Authentication mode is **token**, authentication is by username and token. Further, you must set the **API server** key. When using this option, users with no tokens assigned won't be able to log in to the Mi-Token Intranet Provisioning Website and an administrator will have to intervene.
- If the Authentication mode is **adaptive**, authentication is by domain auth (AD username and password) for users who don't have a token assigned, but by username and token for users who do have a token assigned.
- If the Authentication mode is **mixed**, authentication is by domain auth (AD username and password) only for users who don't have a token assigned and by domain auth with token auth for users who do have a token assigned.
- Cross-dependencies:
 - If the authentication mode is **domain**, you must set the **domain** key.
 - If, and only if, the authentication mode is not **domain**, you must set the **API server** key.

Authentication domain

```
<add key="domain" value="domain.name" />
```

- The config file is delivered with this feature commented out; remove the comment characters `<!-- -->` to enable it.
- Cross-dependency: only specify the domain key if the Authentication mode is **domain**.

API server key

Set the API server key

```
<add key="API server" value="server.name" />
```

- The config file is delivered with this feature commented out; remove the comment characters `<!-- -->` to enable it.
- Cross-dependency: only specify the API server key if the Authentication mode is not **domain**.

Version 4 and version 5

It is permissible to have both version 4 and version 5 enabled. In most cases, version 5 is used.

Enable version 4 settings for soft-tokens.

```
<add key="external URL" value="https://mobile.mi-token.com/4/" />
```

Enable version 5

```
<add key="v5 URL" value ="https://mobile.mi-token.com/5b/Default.aspx" />
```

- This option is required for Windows Phone 7 & 8). The config file is delivered with this feature commented out; remove the comment characters `<!-- -->` to enable it.

Proxy server

Proxy for outbound access from your server to the Internet.

```
<add key="proxyHost" value="<proxyHost>" />
```

```
<add key="proxyPort" value="<proxyPort>" />
```

```
<add key="proxyDomain" value="<proxyDomain>" />
```

```
<add key="proxyUser" value="<proxyUser>" />
```

- Substitute your values for the fields in `<angle brackets>`.
- Cross-dependency: these four keys go together as a package.

- The password is supplied in `sensitive.settings.config`. See *The configuration file sensitive.settings.config*.

The configuration file `sensitive.settings.config`

The `sensitive.settings.config` file is by default in `C:\Program Files\Mi-Token\Intranet Provisioning Website\Config`.

This section describes the `sensitive.settings.config` file in detail.

This file is similar in structure to `customer.settings.config`, but with just one key.

Proxy server

Password for the proxy server for outbound access from your server to the internet.

```
<add key="proxyPass" value = "password" />
```

- The other proxy settings are in `customer.settings.config`, and are described under *The configuration file customer.settings.config*.

7.3 Configuring an email address for the administrator



To configure an email address for the administrator

1. In Active Directory Users and Computers, navigate to your server and then to **Users**.
2. Double-click **administrator**. The **Properties** dialog box opens; find the email address on the **General** tab.
3. Update the email address. Click **OK**.

7.4 Tokens by SMS

If you send tokens by SMS, you will be dealing and interfacing with a service provider and will have to refer to that provider's documentation.

8 Full installation

A full installation includes the API Service and Active Directory Federation Services, and in addition usually includes multiple RADIUS servers deployed on different machines.

It is straightforward to progress from a minimal to a minimal to a full installation. An all-on-one-machine installation can be upgraded to a full one, but you may need to uninstall the Mi-Token Intranet Provisioning Website or Mi-Token Reporting or both and reinstall them on different machines.

To perform a full installation on multiple servers, first plan where the components are to be deployed. Then, if they are not installed already, install them in accordance with the instructions below and under *All-on-one-machine installation*.

You may choose to use the *Installation checklists* as an aid in working through the process.

8.1 Installing a replica authentication server

This is the procedure for installing a replica Mi-Token server, sometimes referred to as a replica Mi-Token instance or a replica RADIUS server. To be precise, this process will install, on a separate machine,

- a replica AD LDS, which will communicate and synchronize with the primary AD LDS
- the Mi-Token plugin to NPS

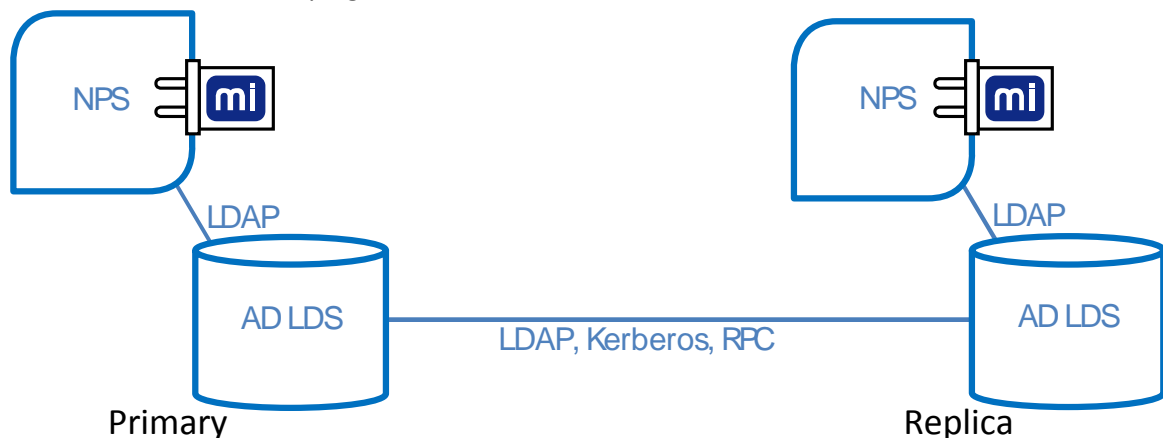


Figure 93. Primary and replica Mi-Token servers

At this point, both the primary Mi-Token instance and this replica will be able to perform authentication. Typically, you would install replicas to provide scalability, either because of geographic spread or because of extra load on the authentication function.

Note that the replica must be installed in the same Windows AD forest (preferably in same AD domain) as the primary Mi-Token server. Remember to check that the prerequisites are satisfied. In particular, it is critical that the firewall policy between the primary and replica servers complies with Microsoft requirements for AD LDS replication.

There is no effective limit to the number of replicas you may install.

Refer to *Ports and protocols table* for information on ports and protocols.



To install a replica authentication server

1. Ensure that you are logged in with an AD LDS administrator account that also has Domain Administrator rights.

- Run the Mi-Token RADIUS plugin executable, as when installing the primary RADIUS server. The install process starts the Mi-Token AD LDS configuration wizard.

Follow the procedure under *Authentication server* except that, at step 6, select **Create a replica of an existing Mi-Token instance on this server**.

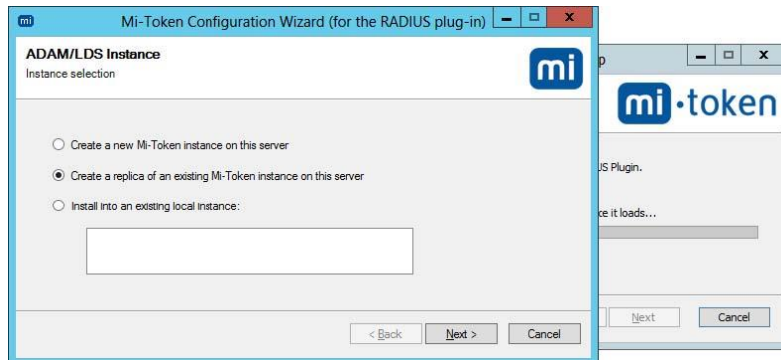


Figure 94. Create a replica

- Enter the details of the new AD LDS instance and click **Next>**.

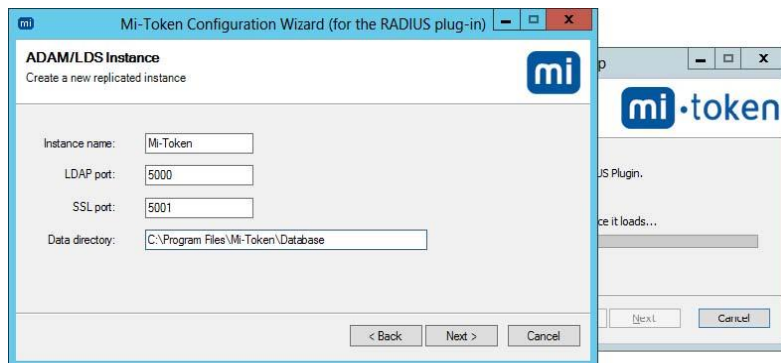


Figure 95. Replica AD LDS parameters

- Enter the details of the existing AD LDS instance.

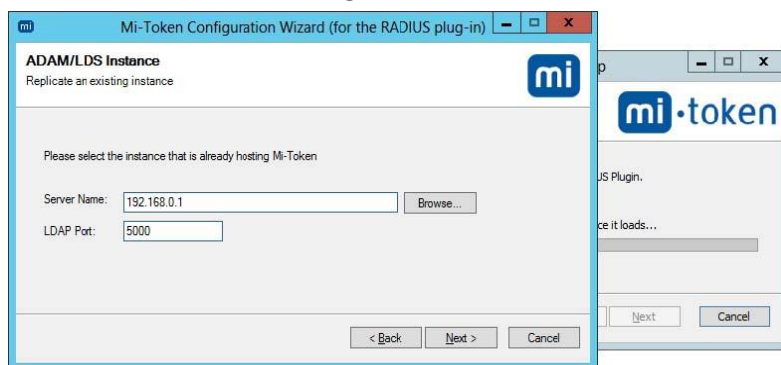


Figure 96. Replica: identify the existing instance

- Configure NPS as for the primary authentication server; see *Configuring the primary server*.

The primary and replica AD LDSs communicate and synchronize with each other.

Now recall from *Configuring Mi-Token Reporting* that a new server grants permission to the Event Collector Service so that it can collect event messages. This is only true if the server and the Event Collector Service are on the same machine. The replica just installed is on a different machine and so there is an extra task to be carried out, which is necessary to grant the Event Collector Service permission to read the information it needs, namely events from remote servers.

6. To achieve this, carry out the commands shown at the bottom of the Reporting Setup dialog box, **RADIUS Server** tab – see Figure 74, but do not copy the commands from Figure 74, because the installer generates a unique set of commands each time. Copy the commands from the dialog box on your own machine.
7. You may care to check that the AD LDSs are synchronizing. You could do this most easily just by observing whether the replica AD LDS becomes populated with the primary AD LDS's data. For a more detailed check, see the suggestions at *Troubleshooting replication*.

Check the event log and the NPS administrative console for help troubleshooting any errors or warnings. The installation process writes the logs in a file system, which can be used to identify the sequence of the installation process. If installation fails, these logs are very helpful and can be accessed from the shortcut link which appears on the installation dialog. Should you need technical support, you may be asked to forward the logs from this folder.

Because of the synchronization between the AD LDSs, the new replica NPS, associated with the new AD LDS, can perform authentication exactly as can the primary.

As a final note, the above has assumed that the replica NPS has the Mi-Token RADIUS plugin, but it is fully applicable to the case where the plugin is replaced by an API Service.

8.2 Installing the API Service

The Mi-Token API provides alternate administration and authentication channels for Mi-Token, on top of using the AD UI (Active Directory User Interface) to manage user-token assignments and RADIUS for authentication.

The Mi-Token API Service is an optional component of the Mi-Token solution and requires additional licensing over that of Mi-Token Enterprise Edition. Please contact sales@mi-token.com if your organization would like the Mi-Token Web API Service.



To install the API Service

1. Ensure that you are logged into the server with an account that has domain administrator privileges.
2. Check that all prerequisites are in place. They are listed at *Prerequisites*.
3. Double-click the **Mi-Token API service executable**, downloaded under *Download the Mi-Token software*. Its name is `Mi-Token API Service_64bit.exe` or similar.

The installation process starts a wizard. If any of the Mi-Token Enterprise Edition prerequisites are not installed, the installation wizard will alert you as to which prerequisites are missing and the installation process will not proceed.



Figure 97. API Service welcome dialog box

Note the instructions in the dialog box. In addition, if AD LDS is not present, the installer will stop and wait for AD LDS to be installed.

4. Click **Install**. The Mi-Token installer launches a wizard.

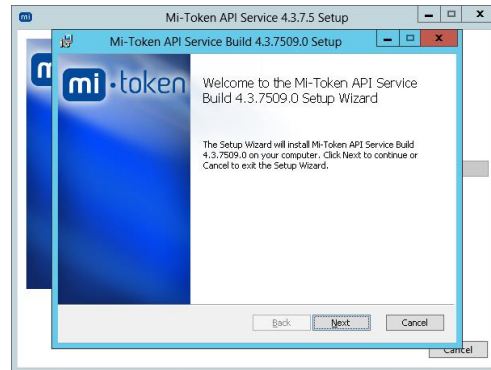


Figure 98. API Service setup progress

5. Click **Next**.

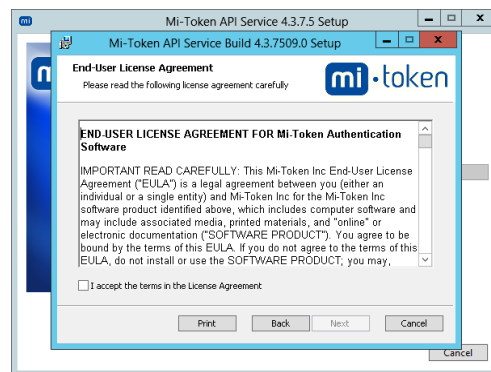


Figure 99. API Service end-user license agreement

6. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Next**.

The Custom Setup dialog box displays.

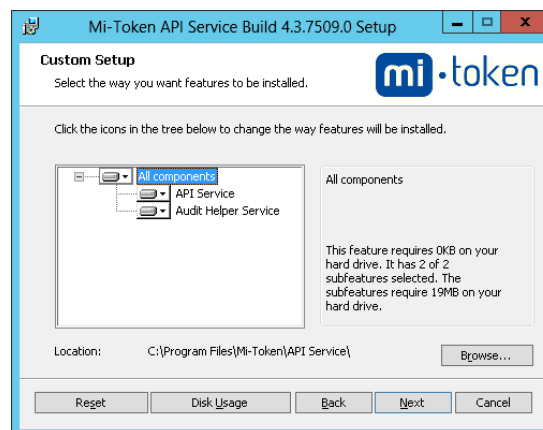



Figure 100. API Service Custom Setup

This dialog box offers you a default destination folder, and the option to change it. Mi-Token, Inc. recommends that you retain the default presented.

7. In the central choice pane, click the drop-down box  next to **All components**.

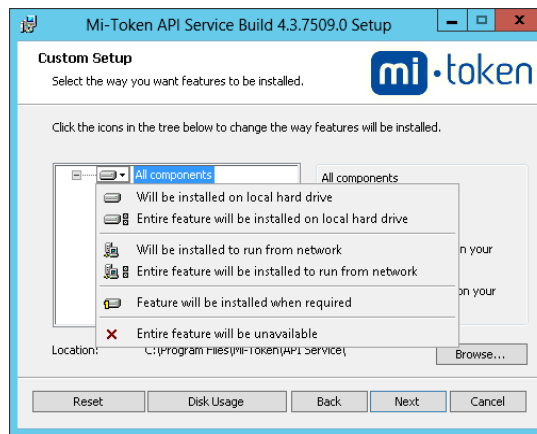


Figure 101. API Service Custom Setup, showing the installation options

8. Select ***Entire feature will be installed on local hard drive.***

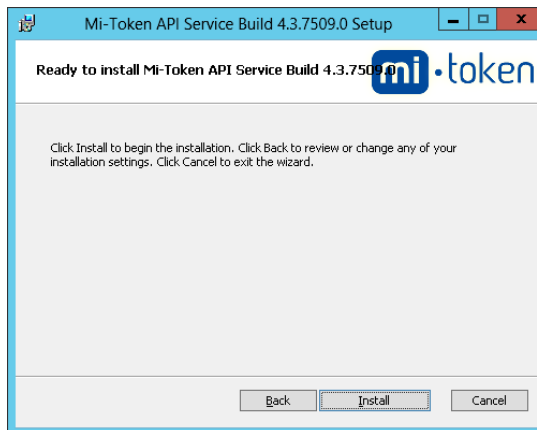


Figure 102. API Service Custom Setup, ready to install

9. Proceed with the installation.

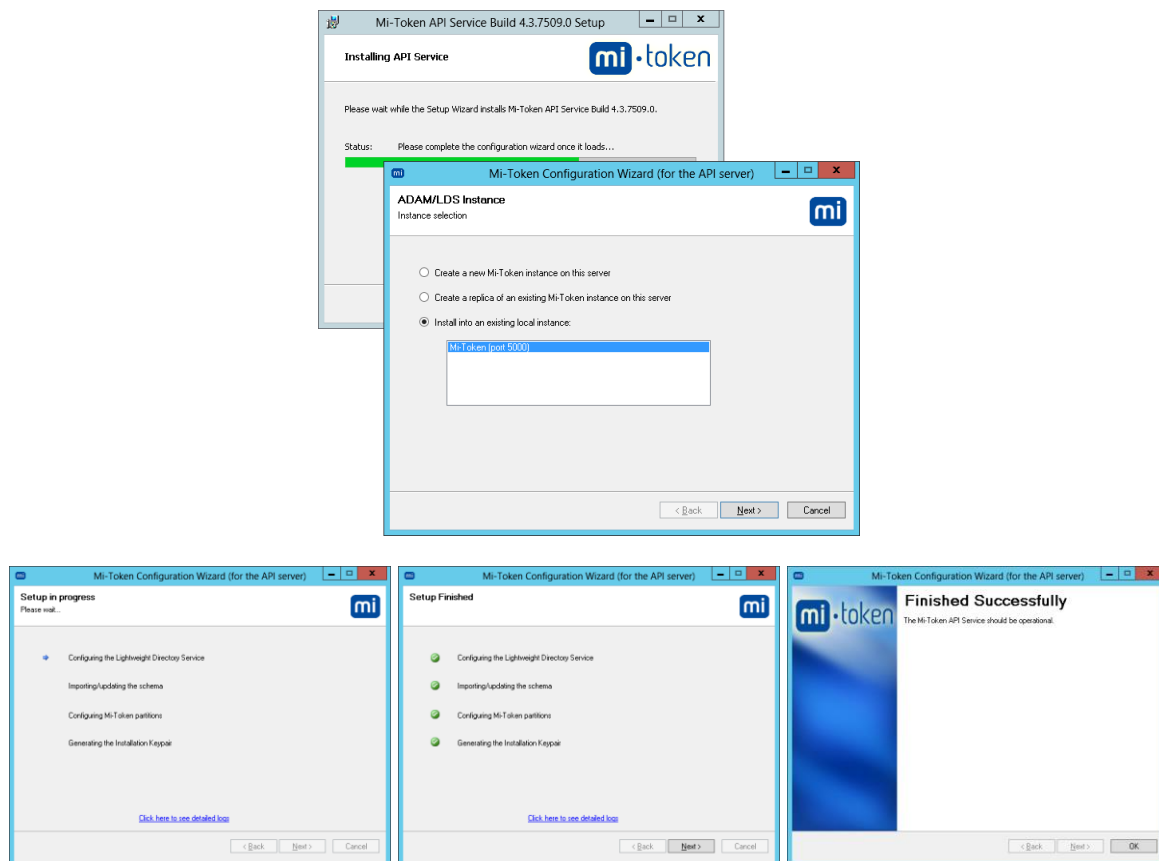


Figure 103. API Service Custom Setup installation progress

A certificate is generated...

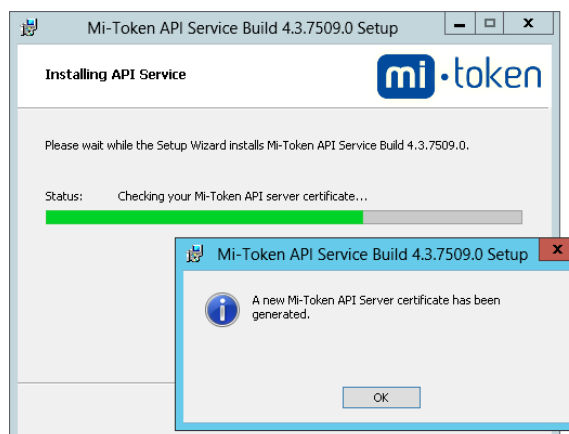


Figure 104. API Service Custom Setup certificate generated

And finally...

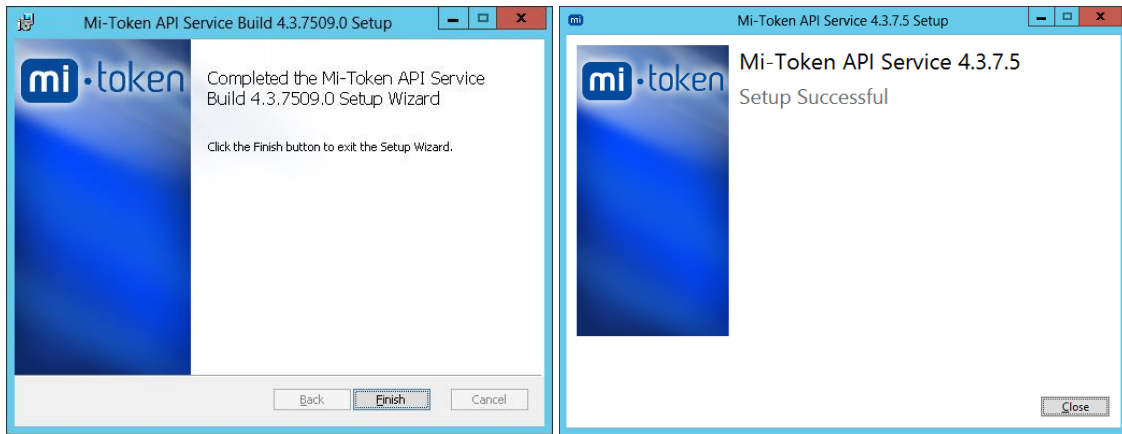


Figure 105. API Service setup completes

Configuring the HTTPS port

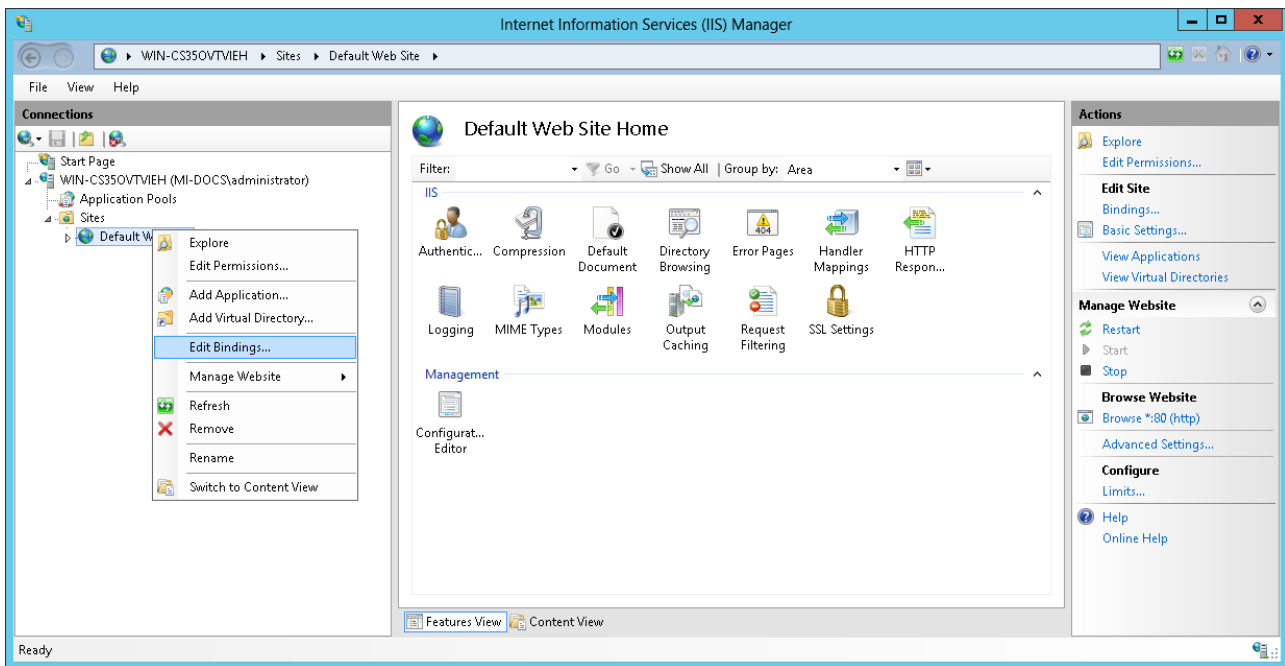


To configure the HTTPS port for the API Service

By way of background, the API Service is not served by IIS but from other Windows components. IIS's involvement in the API is that it retrieves the Mi-Token SSL certificate which is needed for HTTPS. This certificate is self-signed and so Mi-Token doesn't check it and if your IIS is serving some other website via HTTPS, you do not need the Mi-Token SSL certificate.

1. Open IIS and navigate to **Server Name > Sites > Default Web Site**.
2. Right-click on **Default Web Site**.

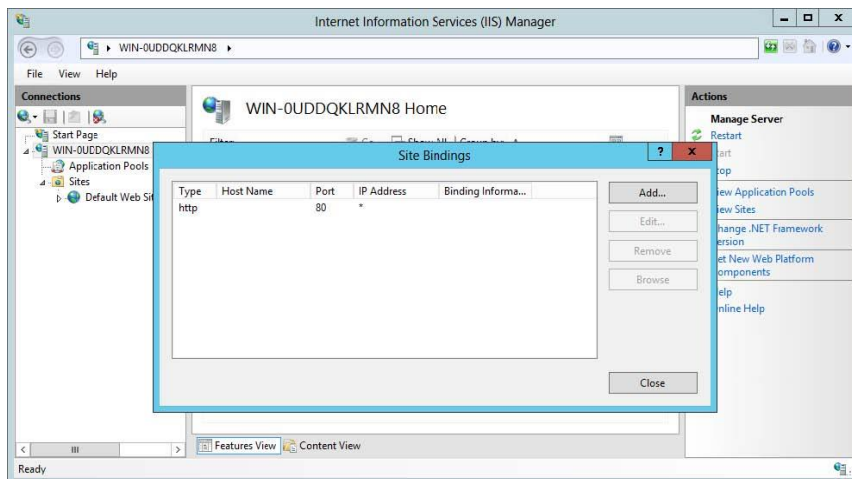
Note that Mi-Token uses **Default Web Site**. If you have other websites being served from **Default Web Site**, you must make other arrangements for them.



(Standard Windows dialog box)

Figure 106. IIS Manager – edit bindings

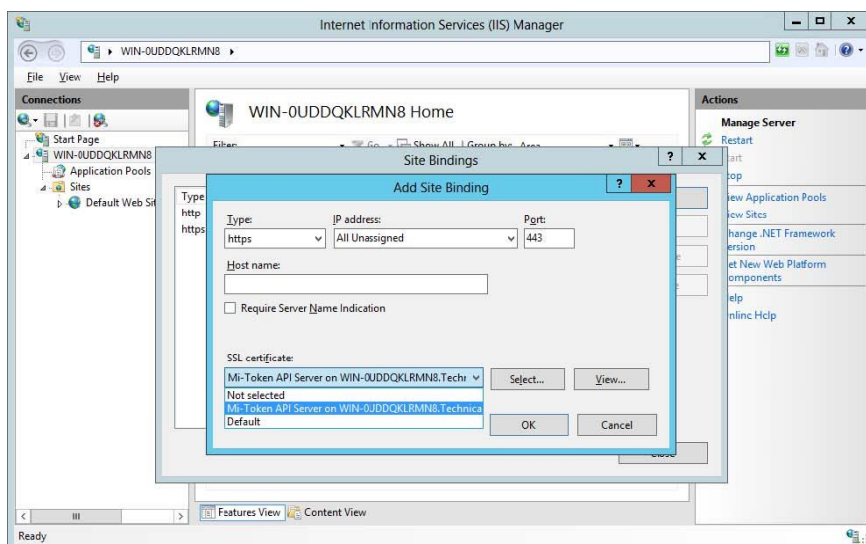
3. Click **Edit Bindings**.



(Standard Windows dialog box)

Figure 107. API install add binding

4. Click **Add...**



(Standard Windows dialog box)

Figure 108. API add site binding

5. Select Type as **https**, Port as **443**, IP Address as **All unassigned**.
Select the SSL certificate as **Mi-Token API Server**.
6. Click **OK**. Click **Close**.



To disable Windows Authentication

Windows Authentication must be disabled. If you have other web applications being served on the same server, you will need to make suitable arrangements.

- As above, open IIS and navigate to Server Name > **Sites** > **Default Web Site**.
- Double-click on **Authentication**. Ensure that **Windows Authentication** is disabled.

API Service is now ready for use.



To determine the base URL of the API

The method is just to export a client's configuration file. Apart from the base URL, this file will contain that client's key, which will thereby be exposed. You will probably prefer to choose a client that does not have **Management** privileges in order to avoid exposing the key for a management-privileged client.

- Choose a client and export its .cfg file as described under *API Clients tab*. The .cfg file contains the base URL.

Information relating to use of the URL can be found in *Mi-Token API GET/POST Documentation*.

8.3 Active Directory Federation Services



To install Active Directory Federation Services

- Ensure that you are logged into the server with an account that has domain administrator privileges. Installation cannot proceed without domain administrator privileges.
- Check that all prerequisites have been installed on the server. They are listed at *Prerequisites*.
- Double-click the **Active Directory Federation Services** installer, downloaded under *Download the Mi-Token software*. Its name is Mi-Token AD FS Integration_64bit.exe or similar.



Figure 109. AD FS welcome

- Click **Install**. The license agreement appears.



Figure 110. AD FS end-user license agreement

5. Read the end-user license agreement. If you accept the terms, place a checkmark in the box and click **Install**.

The installation continues.

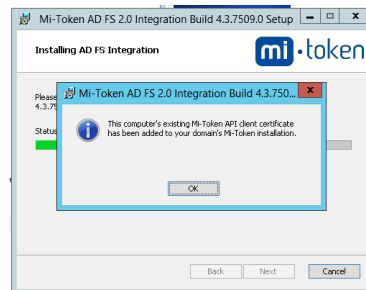


Figure 111. AD FS adds client certificate to the Mi-Token installation

6. When the installer reports that it has added the existing Mi-Token API client certificate to your domain's Mi-Token installation, click **OK**.

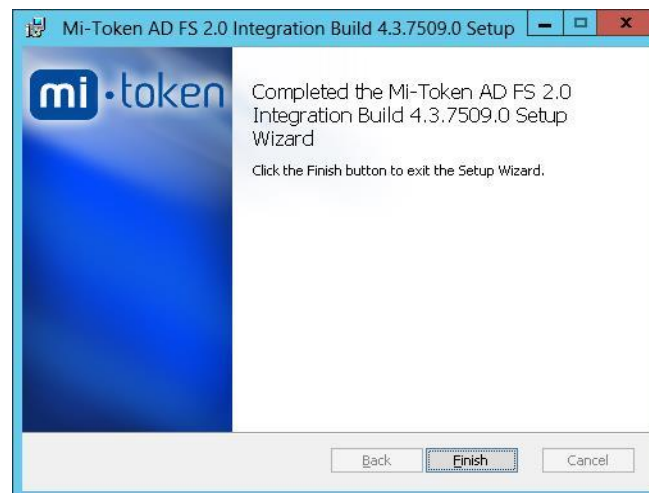


Figure 112. AD FS setup wizard completed

7. The wizard completes. Click **Finish**.



Figure 113. AD FS setup successful

The installer reports a successful setup.

8.4 Summary

You have now installed a Mi-Token 2-factor authentication system with full functionality, including a powerful API.

9 Licensing

Mi-Token's licensing model is easy to use and understand. Once a fresh installation of Mi-Token is completed, your installation is considered to be unlicensed. This can be remedied by activating Mi-Token.

LICENSING MODEL

Mi-Token implements a simple and cost-effective per-user licensing scheme. A single user license includes the assignment of any number of tokens. For example, Bob could have an LCD token, mobile soft token and Yubikey assigned to him, but these three token assignments are only considered to deplete a single user license, as they are all assigned to one individual user.

Licenses remain valid for a certain period of time, usually one, two, or three years initially and can be renewed for a further one or two year basis depending on your preferences.

OBTAINING ADDITIONAL MI-TOKEN USER LICENSES

To obtain additional Mi-Token user licenses, email your license request and details to sales@mi-token.com. Mi-Token will contact with you to verify your installation and will provide you with an upgraded Mi-Token license.

RENEWING YOUR MI-TOKEN LICENSE

When your license is due for renewal, Mi-Token will contact you with a quotation to renew.

9.1 Mi-Token licensing system

Mi-Token makes use of four different record types that contain data required to enable certain Mi-Token components to function correctly. These include:

Record type	Description
Seed files	These records contain the serial number and seed key for each individual hard token, LCD or YubiKey purchased. The hard token cannot be used with Mi-Token Enterprise Edition until the associated seed files are imported.
Licenses	This record contains the activation and deactivation date associated with the license as well as the number of individual users the license is valid for.
Soft token master key	Also referred to in this document as the Key Encryption Key. This record is used to enable the Mi-Token Intranet Provisioning Website to provision mobile soft tokens for users. It is also used if you use the feature of installing your own company logo in the Mi-Token smart phone app.
Activation pack	This record type is a combination of any number of the above records. We can combine these different records and provide them to you in an encrypted zip format, so that you may import all these records in but one individual action.

All record types are encrypted using your unique installation certificate before being sent to you. This ensures that the records can only be used by your organization and not by any third party. We use public/private (asymmetric) key encryption for this purpose.

9.2 Accessing your installation certificate and activating Mi-Token

During installation of Mi-Token a unique installation certificate is automatically generated. The certificate identifies your installation of Mi-Token Enterprise Edition and is required during activation and licensing. There are two parts to the installation certificate, the certificate itself and a verification string. While the certificate can be transmitted via the Internet as required, you should keep the verification string secure.



To access the installation certificate

1. Open Active Directory Users and Computers.
2. Right-click on the **Tokens** node and select **Properties**. A properties dialog box will appear.
3. Select the **Installation Info** tab.

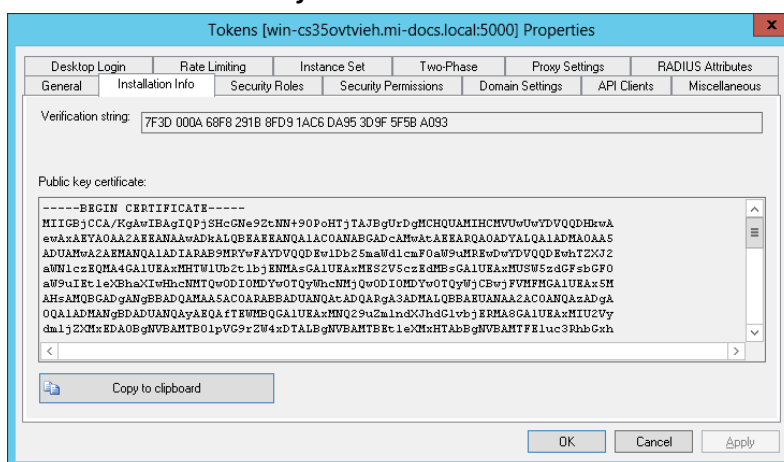


Figure 114. Installation Info tab, showing your installation certificate

4. Click **Copy to Clipboard**. The installation certificate contents are copied to the clipboard.
5. Paste this, without the verification string, into an email and send it to support@mi-token.com.
 - Specify which type of record you would like us to send back to you.
 - If you would like your company logo embedded in our smart phone app, include a graphic file. Mi-Token can accept most common graphic file formats for this purpose.

See *Mi-Token licensing system* for further information about record types.

Once you have sent your installation certificate, Mi-Token will contact you and confirm your verification string. This will ensure that the certificate has not been compromised during the transport process.

Once we have confirmed the verification string, we will use your installation certificate to securely encrypt the records mentioned above and will send them via email in the form of an activation pack for your installation of Mi-Token.

9.3 Importing license data

Records (Activation Pack, Seed Files, Licenses and Soft Token Master Keys) can be imported into your Mi-Token installation using this procedure.



To import license data

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
3. Click the **General** tab.

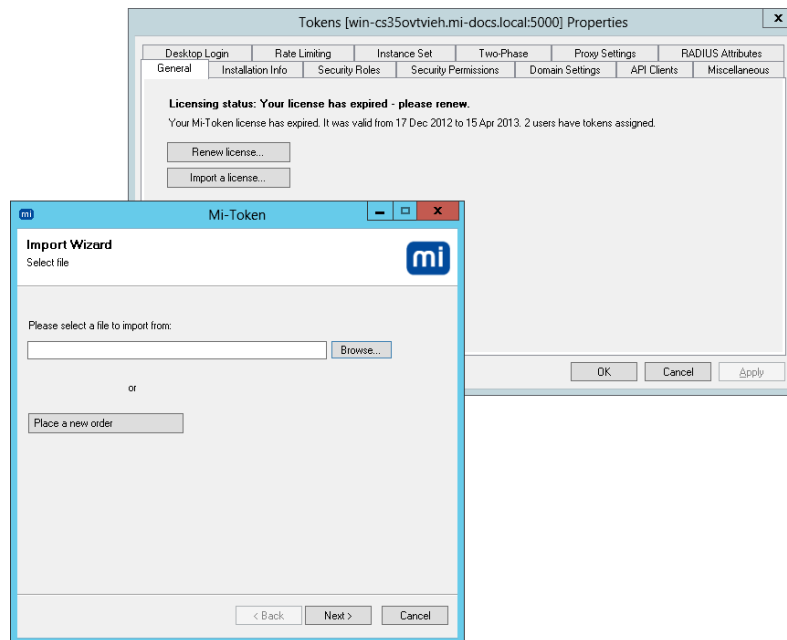


Figure 115. Importing license files

4. Click **Browse** and find the license file you wish to import. Click **Open**, click **Next**. The wizard will import the selected file. If the file is valid it will be added to your Mi-Token installation.

If you click **Place a new order**, Mi-Token opens a dialog box containing the same information as Figure 114, so that you can obtain a new license file. See *Accessing your installation certificate and activating Mi-Token*.

10 Management tools overview

Mi-Token provides an extensive set of management tools.

- *Active Directory Users and Computers*.
- *Active Directory Tokens Properties* is accessed via *Active Directory Users and Computers*.
- *Mi-Token UI Helper*.

11 Active Directory Users and Computers

The following section includes specific operational functions of the Mi-Token Enterprise Edition software for Administrators and Help-Desk/Token Operators.



To access the Mi-Token Enterprise Edition UI:

1. Open Active Directory Users and Computers. This is the dialog box shown in Figure 31.
2. Expand the **Tokens** node found in the tree on the left pane.

From here, you can access a large number of functions, some of which are

- Backup Mi-Token (see *Backup Mi-Token*)
- PINs: Set / remove PIN (see *Adding or resetting a token PIN*)
- Search for tokens (see *Searching for tokens*)
- Tokens: Assign, unassign users (see *Assigning users to tokens, Unassigning users from tokens*)
- Tokens: Auto-assignment (see *Auto-assignment*)
- Tokens: Delete (see *Deleting tokens*)
- Tokens: Disable and re-enable (see *Disabling and re-enabling tokens*)
- Tokens: Manually provision soft-tokens (see *Manual provisioning of soft-tokens*)
- Tokens: Organize (see *Organizing tokens*)
- Tokens: Properties (see *Token properties*)
- Tokens: Reset (see *Resetting tokens*)
- Tokens: Temporary token generate (see *Creating temporary tokens*)



Note that Active Directory users and groups assigned the Mi-Token Token Operators role do not have the same permissions as users and groups assigned to the Mi-Token Administrator role. See Security Permissions tab for further information regarding these roles.

11.1 Organizing tokens

In large token deployments, organizing tokens in the AD UI is essential. The basic organizational tool is the ability of administrators to organize tokens into **Containers**. Containers can be used to separate specific groups of tokens from the main token node. For instance, there can be a separate container for each department: HR, Marketing, Accounting and so on.



To set up a container

1. Open Active Directory Users and Computers.
2. Find the **Tokens** node in the left pane and right-click. From the menu, select **New > Container**. A dialog to enter the container name appears.
3. Type the container name in the **Name** text box and click **OK**. The container is created under the Tokens node.
4. You can now drag and drop tokens between containers. Mi-Token shows a verification dialog each time.

Containers may be nested; using Windows tools, you can apply security to containers so that they and the tokens they contain may be viewed and changed only by their respective administrators (although the domain administrator always has access to all tokens).

If a hard token is moved from one container to another, it retains its original security settings.

11.2 Searching for tokens

Some types of hardware tokens have visible identifier, usually in the form of a serial number printed or stamped on to the tokens themselves. Mi-Token makes it easy to identify tokens from within the AD UI plugin.



To search for LCD and other hard tokens by serial number

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node on the left pane and select **Search > Tokens by serial or YubiKey...** A dialog appears.

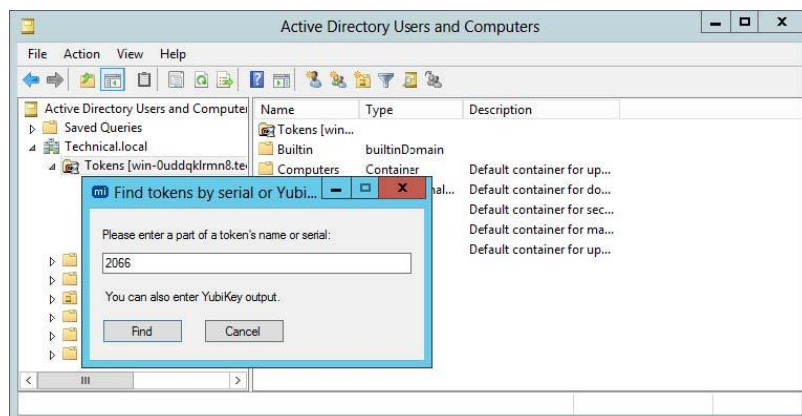


Figure 116. Search by Serial Number

3. Find the serial number on your token and enter it. Click **Find**. The right pane displays tokens matching the serial number.



To search for tokens by assigned username

1. Open Active Directory Users and Computers.
2. Right-click on the **Tokens** node in the left pane and select **Search > Tokens by users....** A dialog appears.
3. Type the username you are searching for. Press **OK**. The right pane displays all tokens assigned to that user.



Figure 117. Search by User ID



To search for a Yubikey via OTP output

1. Open Active Directory Users and Computers.
2. Right-click on the **Tokens** node in the left pane and hover over **Search**. Click **Tokens by Serial or YubiKey...**. A dialog box appears.
3. Insert the YubiKey into an available USB port, focus on the text box of the dialog box and press the YubiKey button. The right pane displays a token that matches that OTP output.

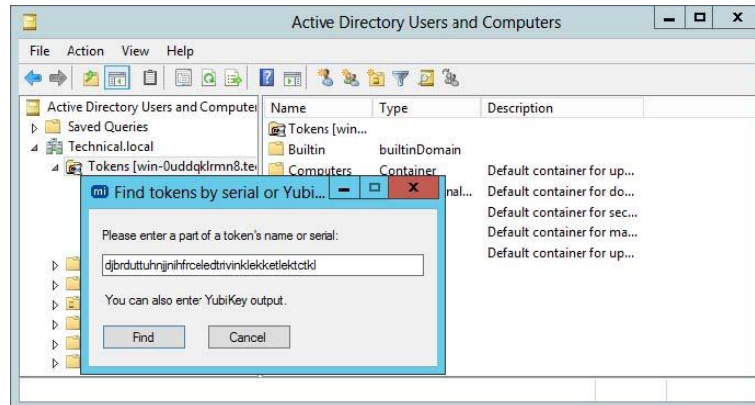


Figure 118. Search by YubiKey OTP

11.3 Assigning users to tokens

Help-Desk operators when necessary can assign tokens to users manually.



To assign a token to a user manually

1. Open Active Directory Users and Computers.
2. Open the **Tokens** node in the left pane. Right-click the tokens you wish to assign and click **Assign**. A dialog will appear.

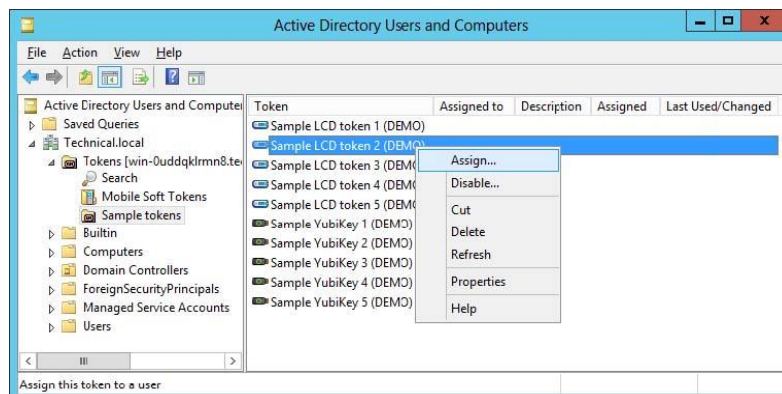


Figure 119. Assigning tokens

3. Enter the username you wish to assign to the token and click **OK**. The user will now be able to use their assigned token to authenticate. Each username can have multiple tokens assigned.

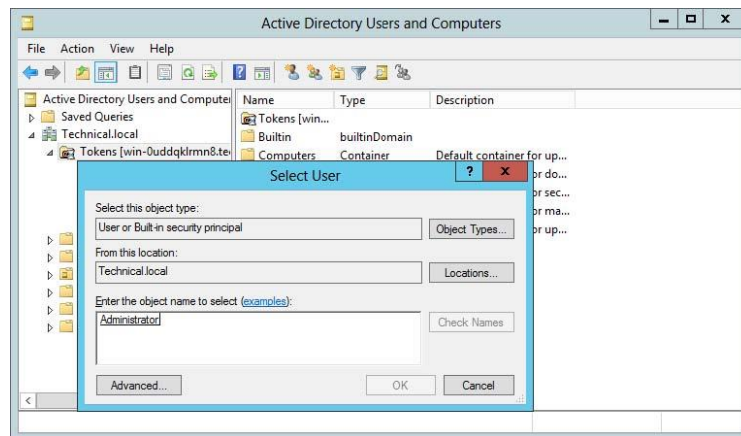


Figure 120. Assign token to user

11.4 Unassigning users from tokens

Help Desk operators can, when necessary, unassign tokens.



To unassign a token from a user manually

1. Open Active Directory Users and Computers.
2. Expand the **Tokens** node in the left pane and find the tokens you would like to unassign. Select those tokens and right-click the group of selected tokens. Click **Unassign**. A message box will appear.

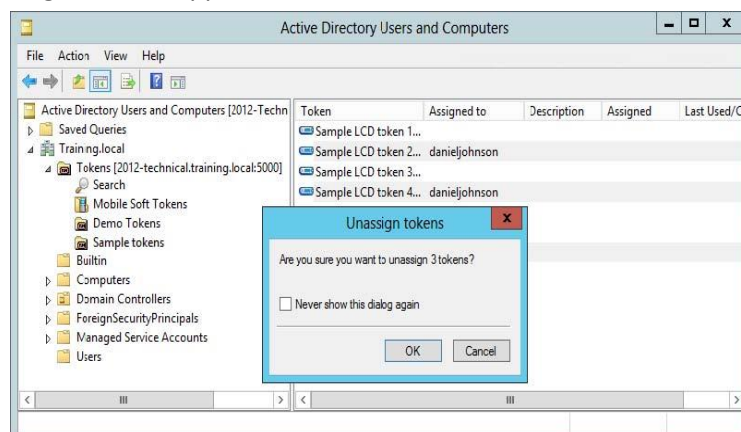


Figure 121. Unassign Tokens

3. Choose whether to never see a warning before unassigning again, or leave unchecked to warn you each time. Click **OK**. Selected tokens are now unassigned.

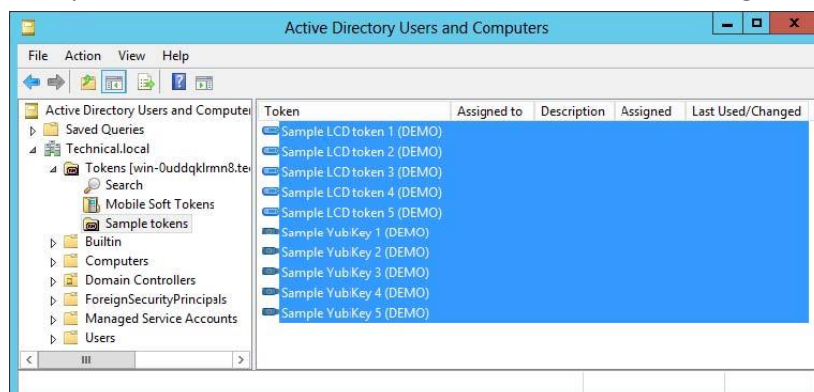


Figure 122. Tokens Unassigned

11.5 Token properties

Token operators can view and modify the token properties. Different types of tokens (LCD, YubiKey and so on) have a common set of properties except for a few differences. These properties are explained in next subsections. These properties can be accessed as follows:



To view and modify a token's properties

1. Open Active Directory Users and Computers.
2. Open the **Tokens** node found in the left pane.
3. Right-click on the token you want to set/view the properties of and click on **Properties**. A dialog appears containing a number of tabs depending on the type of token.

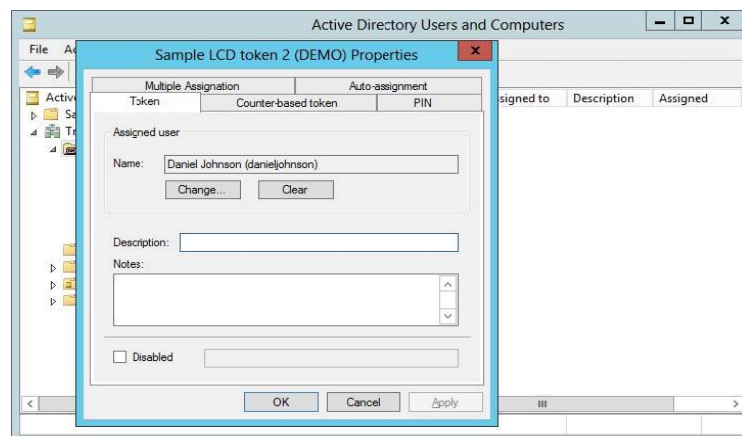


Figure 123. Token Properties

The available tabs are

- Token
- Counter-based token
- Time-based token
- PIN
- Multiple assignment
- Auto-assignment

Figure 123, as an example, only has five of these tabs.

Modifying token properties

You can store a description and notes about each token under the **Token** tab.



To modify a token's description and notes

4. Click on the **Token** tab inside the **Properties** dialog. This tab contains a portion for a description, notes and checkbox for disabling the token. See Figure 123 for a sample.
5. Enter the description and notes you would like in the appropriate text boxes. These fields are optional.
6. You may also disable the token if needed by checking the **Disable** checkbox.

Adding or resetting a token PIN

PINs are static secondary passwords placed before an OTP. For example, if a user's PIN is abcd and current OTP is 152362, the user will enter abcd152362 in the OTP field. Token operators can enable or disable PINs from **PIN** tab of the properties.



To manage PINs

- Click on the **PIN** tab inside the **Properties** dialog. This tab allows enabling and setting the PIN.

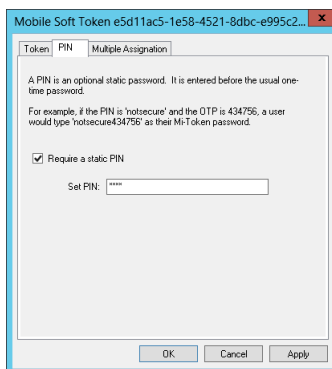



Figure 124. Token properties – PIN required

- Check the **Require a static PIN** checkbox to enable the **Set PIN** text box. Enter the PIN. It could be any combination of characters or numbers of any length.

Once the PIN is entered and the Properties are applied, you will notice a PIN token icon  (a small padlock icon) for the token that has a PIN assigned. If you right-click this token at this point, an option for resetting the PIN will appear.

Once any token has a PIN assigned, a **Set PIN...** option will appear in the right-click menu for all tokens, including those without PINs.

Resetting tokens

Event-based LCD tokens can be resynchronized.



To reset event-based tokens

- Click on the **Counter-based token** tab inside the **Properties** dialog. Hold the LCD token's button, the number followed by a C is the counter value (for example, C 1060).
- Enter the counter value in the textbox and click **OK**. Counter will be reset to a new value.

Time-based tokens can be resynchronized.



To reset time-based tokens

- Click on the **Time-based token** tab inside the **Properties** dialog. This tab allows you to reset the time.
- Click **Reset**, click **OK**. The counter is reset to a new time.

Multiple assignment

- Click on the **Multiple assignment** tab inside the **Properties** dialog. Press **Change...** to open a dialog which can accept another user to be assigned to the token.

Auto-assignment

This feature is described on the dialog box:

A YubiKey auto-assignment will enable automatic assignment of a token to the first user to authenticate with a valid OTP, provided that user has no other assigned hard tokens. This can significantly assist in provisioning tokens since they can be simply handed out.

Note that Mi-Token doesn't currently check the user's Windows password before auto-assigning. This is because in many environments it won't be provided in RADIUS requests. If checking the Windows password is important, please make sure it gets checked by the VPN device before the OTP.

Note then also that you can configure multiple tokens for auto-assignment in one operation.



To access auto-assignment

1. Open Active Directory Users and Computers.
2. Open the **Tokens** node found in the left pane.
3. Select the tokens you want to configure for auto-assignment and right-click. Select **Properties**. If you have selected more than one token, the **Properties** dialog has just one tab, **Auto-assignment**. If there are multiple tabs, select the **Auto-assignment** tab.

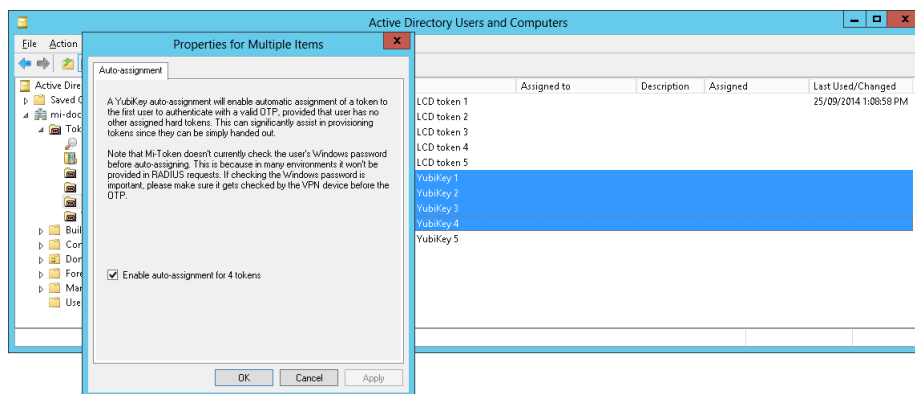


Figure 125. Auto-assignment tab

4. To select auto-assignment, place a check mark in the check box. Click **Apply**, click **OK**.

11.6 Manual provisioning of soft-tokens

If you have not installed the Mi-Token Intranet Provisioning Website, or if a user does not have access to it, you can provision users with soft-tokens manually.



To manually provision a soft token to a user

1. Open Active Directory Users and Computers.
2. Navigate to the **Tokens** node in the left pane under your server.
3. Right-click on the **Mobile Soft-Tokens** container in the right pane and select **Generate soft-token**. A dialog box appears.
4. Enter the AD username you wish to create a soft-token for and click **OK**. A dialog box appears with the new soft-token activation link.

This is the link to send to the user. Note the **Copy to clipboard** button, provided for convenience.

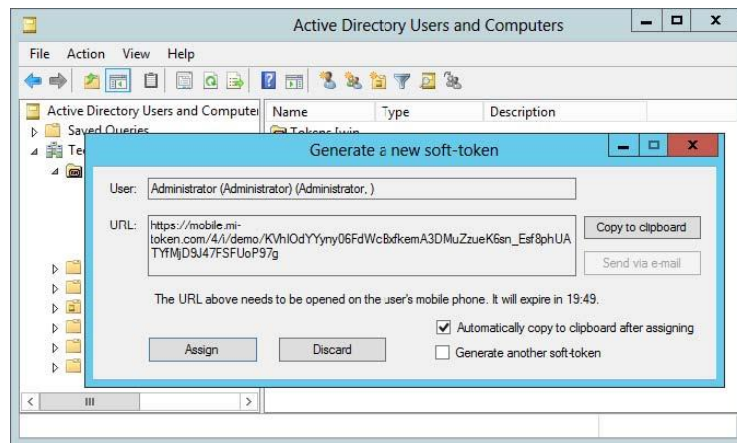


Figure 126. Provision soft token

- Click **Assign** to confirm the token activation or click **Discard** to not assign the soft-token. If you confirm assigning of the soft-token, copy the link to clipboard and send it to the user to activate the token. If you discard the soft-token, the URL will be invalid.
- Send the link to the user immediately by any convenient means, normally SMS or email, with a warning that it will expire after 20 minutes.

11.7 Disabling and re-enabling tokens

Tokens imported into Mi-Token are enabled by default.

When you disable a token, it remains assigned to a user if it has been previously assigned.



To disable a token from use

- Open Active Directory Users and Computers.
- Open the **Tokens** node in the left pane. Right-click the token you want to disable. Select **Disable**. A dialog will appear.
- Enter the reason for disabling the token and click **OK**. The selected token will be disabled and can no longer be used for authentication requests. Disabled tokens will appear as a disabled token icon, (note the small x).

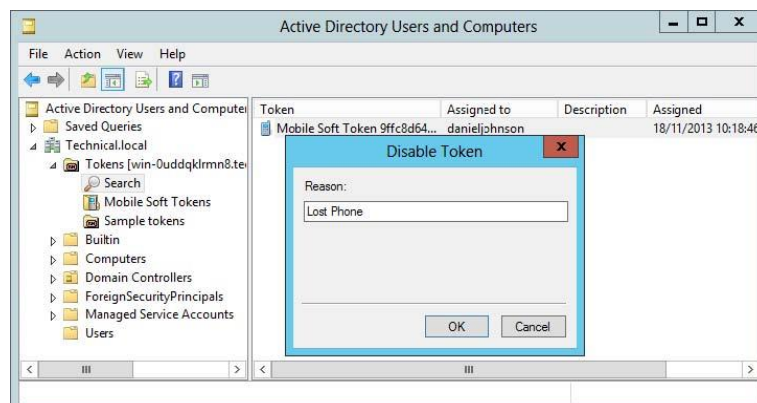


Figure 127. Disable a token



To re-enable a token so that it can be used by a user

- Open Active Directory Users and Computers.
- Open the **Tokens** node in the left pane and select the token you want to re-enable.

3. Right-click on the token, and select **Enable**. The selected token is now re-enabled and can be used by users to authenticate.

11.8 Deleting tokens

Deleting a token is dangerous and should not be undertaken under normal circumstances. It will be difficult to restore the token if you delete it. In almost all cases the preferred option is to unassign or disable it. However, it is possible to delete a token from the AD LDS database.



To delete a token

1. Open Active Directory Users and Computers.
2. Open the **Tokens** node in the left pane and select the token you want to delete.
3. Right-click the token, and select **Delete**. A dialog confirming the deletion will open.
4. Click **YES** to delete the token.



Restoring a token once it is deleted will be difficult.

11.9 Creating temporary tokens

Temporary tokens are static access codes that have an expiry time (for example, 8 hours or 7 days). The expiry time is global: the same expiry time applies to all your temporary tokens.

You may only generate temporary tokens if you have enabled them – see *Temporary Tokens*, where you can also set the token validity time limits.



To create a temporary token

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node and click on **Generate Temp-Token**. The **Select User** dialog appears.
3. Select the user you would like to assign a temporary token to. An alert will appear.

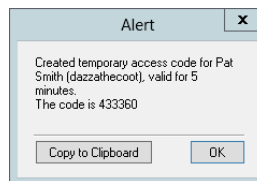


Figure 128. Confirmation of temporary token

Take care to accurately send the token to the appropriate user. The **Copy to Clipboard** button can be used to copy the code and subsequently send it via email.



Once the Alert dialog box is closed, the temporary token code is irretrievable. Make sure to press **Copy to Clipboard** and send the code via email to the appropriate user before closing the alert dialog box.

11.10 Backup Mi-Token

Mi-Token is highly secure software and because of this backups are more limited than they otherwise could be. The primary way to back up Mi-Token is to set up a replica server which you can restore from later. Another way of backing up Mi-Token is to take regular backups of

the Mi-Token database. This database can only be restored on the same machine as the backup was taken from.

The Microsoft website has procedures for backing up and restoring your AD LDS databases. The default location of your AD LDS file for Mi-Token is C:\Program Files\Mi-Token\Database.

Although the database can only be restored on the same Mi-Token instance it was backed up from it is still highly advisable to keep the backup secure and encrypted.

If you are running Mi-Token in a virtual machine then taking regular snapshots of the machine should allow you to keep Mi-Token backed up in case of failure.

11.11 Properties dialog box



To view user properties

1. Open Active Directory Users and Computers.
2. Navigate to the **Users** node and right-click on the user of interest. This dialog box appears.

(Standard Windows dialog box)

Figure 129. Properties dialog box

This is a standard Windows dialog box. For information, consult Microsoft documentation.

12 Active Directory Tokens Properties dialog box

The Active Directory Tokens Properties dialog box has 13 tabs relating to different areas: API Settings, Rate Limiting, Instance Set, Two-Phase, Proxy Settings, RADIUS Attributes, General, Installation Info, Security Roles, Security Permissions, Domain Settings, API Clients, Miscellaneous. They are covered in the sub-sections below.

Some important functions:

- Certificates: Import and export installation certificates (see *API Clients tab*)
- Domains: Configure an additional domain, add a new partition, reassign roles (see *Domain Settings tab*)
- Groups: set up overrides for group members (see *Group Settings*).
- License files: import license files (see *General tab*)
- Seed files: Import seed files (see *Importing license data*)
- Proxy RADIUS: Configure proxy RADIUS server support (see *Proxy Settings tab*)
- Roles: Add and remove roles, modify assignments (see *Security Roles tab*)
- Roles: Modify permissions (see *Security Permissions tab*)
- Temporary tokens: Enable and configure temporary tokens (see *Temporary Tokens*)
- Tokens: Limit the number and type of tokens that can be assigned to one user (see *Token limits*)
- Version number (see *General tab*)

For information on Credential Provider and Two-Phase authentication, refer to the *Mi-Token Enterprise Edition Add-ins* manual.

12.1 General tab

Most of the **General** tab is described under *Importing license data*.



To find the version number you are currently running

- Look in the bottom left-hand corner of the **General** tab.

12.2 Installation Info tab

The **Installation Info** tab is described under *Accessing your installation certificate and activating Mi-Token*.

12.3 Security Roles tab

This tab enables you to set up and manage roles. Manage the permissions assigned to the roles on the *Security Permissions tab*.

In order to make Mi-Token more securely administrable, a configurable security policy has been developed allowing for custom permissions for security roles. These roles are defined within Mi-Token and Active Directory users and groups can be assigned to these roles using the Microsoft Management Console.

AD Users or Groups assigned the Mi-Token Enterprise Edition Administrator role have full access to all features by default.

AD Users or Groups assigned the Mi-Token Enterprise Edition Roles have configurable access to the following features:

- Import license/seed files
- Modify containers
- Delete tokens
- Assign / un-assign tokens
- Generate soft tokens
- Enable / disable tokens
- Set / remove PIN
- Auto-assignment
- View tokens
- Modify roles / permissions



Always ensure that there is at least one Active Directory user or group assigned to the Administrator role. Failure to do so may result in the Mi-Token Enterprise Edition installation becoming unusable. In the unlikely event that this occurs, contact support@mi-token.com.



To modify assignments for the Mi-Token roles

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node found in the left pane and select **Properties**.
3. Click the **Security Roles** tab. This tab has controls for creating security roles and adding members to those roles.
4. Select the role on the left and click on it. Below the **Members of __ Role** pane, click **Add...**.
5. Select an Active Directory group or user who will be assigned this Mi-Token role. Click **OK**.
6. The **Select User or Group** dialog displays. Make your changes and click **OK**. If necessary, use the **Advanced...** button, which offers a search facility.

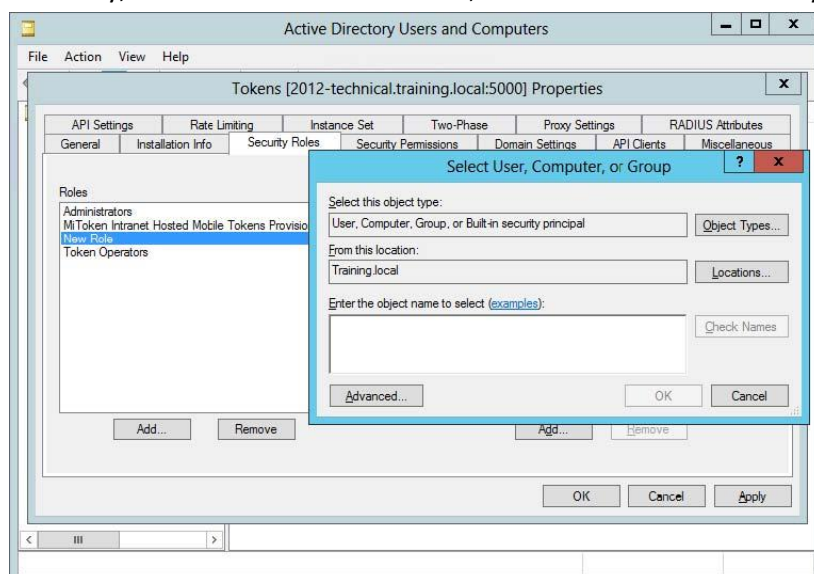


Figure 130. Adding a token operator

- When focus returns to the **Security Roles** tab, the user or group will be added to the selected Mi-Token role.



To add and remove roles

- Open **Active Directory Users and Computers**.
- Right-click the **Tokens** node found in the left pane and select **Properties**.
- Click the **Security Roles** tab. This tab has controls for creating security roles and adding members to those roles.
- Below the **Roles** pane, click **Add...** to add a new role and **Remove** to remove one.

12.4 Security Permissions tab

The **Security Roles** tab enables you to set up and manage roles. Manage the permissions assigned to the roles on this tab.



To modify permissions for the Mi-Token roles

- Open Active Directory Users and Computers.
- Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
- Click the **Security Permissions** tab. This tab has controls for modifying permissions to roles.

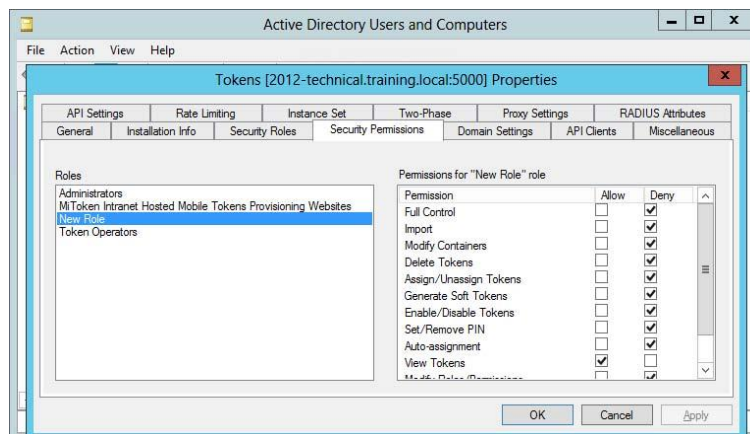


Figure 131. Modifying Role Permissions

- Click the role on the left. In the **Permissions for __ Role** pane, adjust the check boxes for **Allow** and **Deny** under each task.
- Click **OK**.

12.5 Domain Settings tab

Mi-Token comes with options for configuring Mi-Token two-factor authentication support for multiple domains. All domains for a single Mi-Token Enterprise Edition instance must be part of the same forest. Multiple domain support is a standard feature of Mi-Token and is available out of the box. For domains other than the domain the Mi-Token Enterprise Edition server was installed into, Mi-Token must be enabled for each additional domain.

The usual configuration is to have a domain mapped to each partition.

Mi-Token permits you, via this tab, to create partitions and map domains to them.

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
3. Select the **Domain Settings** tab. Right-click on a domain to configure its Mi-Token settings.

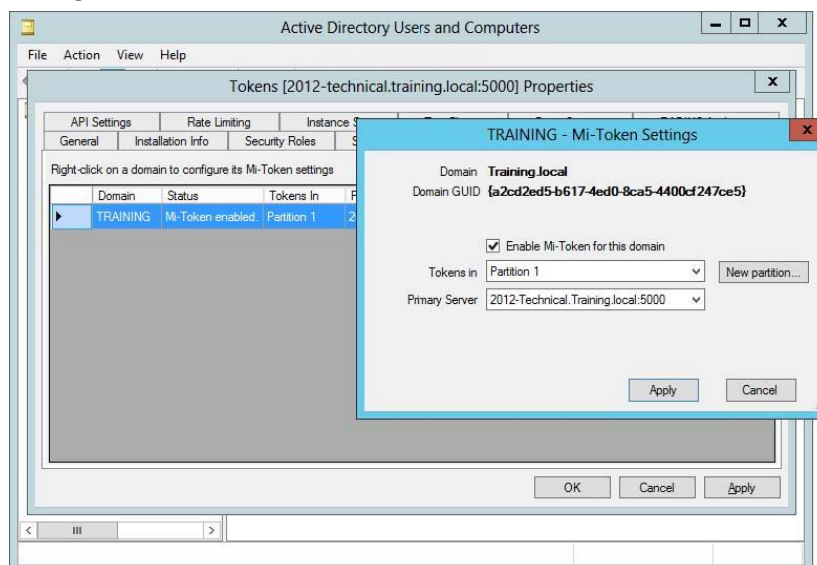


Figure 132. Domain Settings tab

To enable Mi-Token support for a selected domain

4. Check **Enable Mi-Token for this domain**.
5. Choose a partition and a primary server from the drop-downs.
6. Click **Apply**.

To add a new partition

4. Click **New partition....**
5. Enter the partition name when prompted.
6. Click **OK**, click **Apply**.

To redesignate the primary and replica servers

4. Select your primary server from the **Primary Server** drop-down.

If another server is configured as primary, it will observe the change and set its own status to Replica. This applies to other servers which may be inactive: they will set their own status to Replica when they come online.

5. Click **Apply**.

12.6 API Clients tab

Mi-Token's .NET API requires the configuration of client SSL certificates.



To manage clients

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
3. Select the **API Clients** tab.

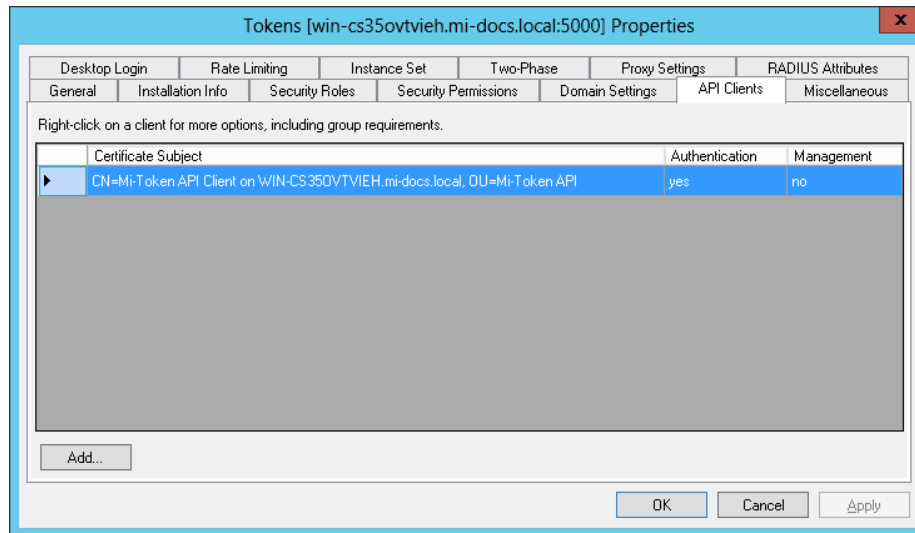


Figure 133. API Clients tab

This tab lists information relating to each configured API client.

Certificate Subject

The name of an API client.

Authentication

The client may perform the API authentication operation Verify.

Management

The client may perform the API management operations Assign, CreateSoftToken, Delete, List, Unassign, Disable, Enable.

Right-click

Numerous functions can be performed on an existing client by right-clicking on the client. The options presented are

- **Groups...** launches the **Group Settings** dialog box, described under *Group Settings*.
- **Settings...** launches the **New API client** dialog box, shown as Figure 134, allowing you to change settings.
- **Export**. Exports details of the client in a .cfg file.
- **Delete**. Deletes the entry.



To create a new client or partition

4. Click **Add...**

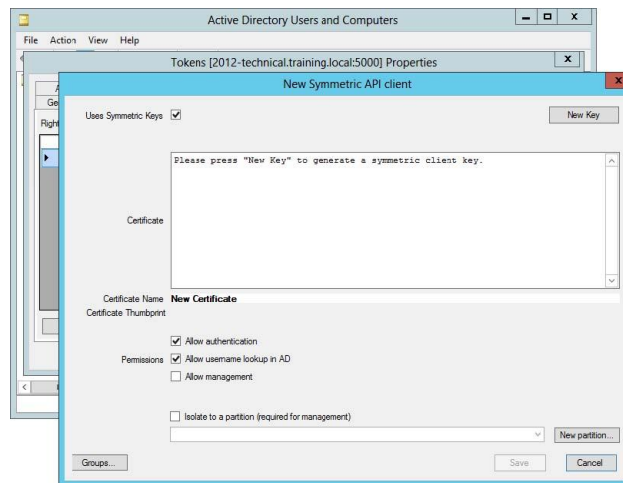


Figure 134. New API client dialog box

New Key

Click to generate a key.

Allow authentication, Allow management

These checkboxes refer to **Authentication** and **Management** on the **API Clients** tab itself.

Allow username lookup in AD

The API client may perform the Verify function, which involves looking up usernames in the AD.

New partition

The **New partition** button enables you to create a new AD partition. It will have the same schema as the existing one and will be empty.

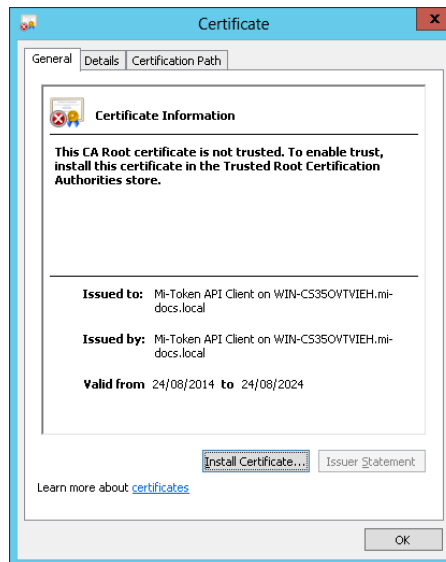
Groups

The **Groups** button launches the **Group Settings** dialog box, described under *Group Settings*.



To access SSL certificate details

4. Right-click on a client and select **View Certificate...** from the drop-down.



(Standard Windows dialog box)

Figure 135. View certificate

**To import SSL certificates (not keys)**

4. Press **Install Certificate...** on the **General** tab, which launches a wizard.

**To export SSL certificates (not keys)**

4. Press **Copy to File...** on the **Details** tab, which launches a wizard.

For further information, refer to Microsoft documentation.

12.7 Miscellaneous tab

The Miscellaneous tab offers several functions.

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
3. Select the **Miscellaneous** tab.

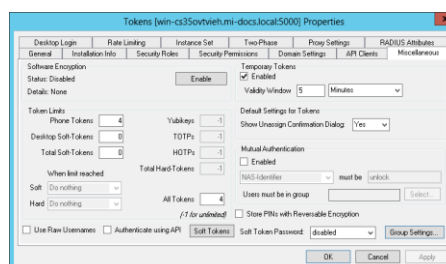


Figure 136. User interface dialog box, Miscellaneous tab

Software encryption

Enable this to indicate that encryption is to be performed in software on the server.

4. Click **Apply** to save the settings.

Token limits

Mi-Token offers the option of limiting the number and type of tokens that can be assigned to one user.

Here you can

- Set limits on the numbers of tokens per user. -1 indicates that there is no limit.
- Specify the action when the limit is reached – to be implemented in the future.

5. Click **Apply** to save the settings.

Temporary Tokens

Temporary tokens are static access codes that have an expiry time. The expiry time is global: the same expiry time applies to all your temporary tokens.

Here you can

- Enable and disable the ability to create temporary tokens.
- Set the token validity time limits, to the desired number of minutes, hours or days, for example, 8 hours or 7 days.



To enable/disable temporary tokens

4. In the **Temporary Tokens** section, enable temporary tokens by checking the box. Then you can define the time for which you would like the temporary tokens to be valid.
5. Click **Apply** to save the settings.
6. Completely close Active Directory Users and Computers. Then reopen it for further use.

For information on creating a temporary token. See *Creating temporary tokens*.

Use Raw Usernames

Check if AD is to use raw names instead of GUIDs.

Authenticate using API

Self-explanatory.

Store PINs with Reversible Encryption

If checked, PINs are reversibly encrypted; otherwise they are hashed.

Soft Token Password

Select whether the password (or passcode) requirement is disabled, required or optional when the Desktop Token is launched.

Group Settings

The group settings features allow you to set up special overriding treatment for members of your Active Directory groups.

If you press **Group Settings...**, a dialog box opens.

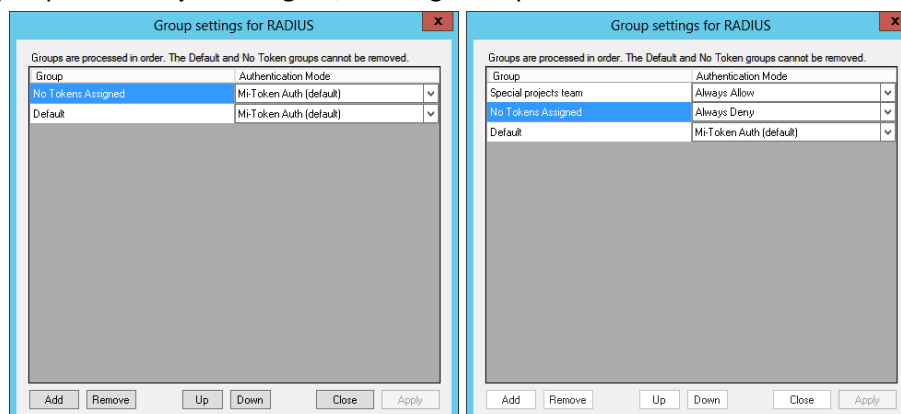


Figure 137. The Group Settings dialog box, as installed and example in use

Group, Authentication Mode

For each group you specify an **Authentication Mode**.

- **Always Allow**. Members of the group are always allowed entry, irrespective of the credentials presented.
- **Always Deny**. Members of the group are always denied entry, irrespective of the credentials presented.
- **Mi-Token Auth**. Membership of this group is irrelevant to authentication.

Any individual could be a member of no group, or one or more groups and the rules listed below determine how Mi-Token will handle group memberships.

The **Group Settings** dialog box shows a list of the Active Directory groups which have been notified to Mi-Token. This includes two “groups” which do not reflect real groups in your Active Directory, but are created by Mi-Token. They are known as pseudo-groups and are called **No Tokens Assigned** and **Default**, as shown in Figure 137.

Every group in the list in Figure 137 has a priority. The groups are arranged in the list in priority order with the lowest at the bottom and the highest at the top. Mi-Token works through the priority list to determine whether to give special treatment to members of the various groups.

The **Default** pseudo-group is the least specific and is always at the bottom of the list. It contains everybody.

No Tokens Assigned is the second-least specific and is always second from the bottom of the list. As the name suggests, it contains all persons who have no token assigned.

Your groups are always above the pseudo-groups and you determine their relative priorities by using the **Up** and **Down** buttons. Mi-Token recommends that you arrange your groups so that the less specific ones have lower priority and are lower in the list.

As mentioned, each group, including the pseudo-groups, is assigned an authentication mode, **Always Allow**, **Always Deny** or **Mi-Token Auth**, from a drop-down list.

When a user attempts to connect, Mi-Token applies these business rules:

- The **No-Token Bypass** feature overrides the group settings. If **No-Token Bypass** is set and the connecting user has no tokens assigned, group settings do not apply and the user is immediately authenticated. For more information, see *No-Token Bypass*.
- Mi-Token makes use of the groups and priorities in Figure 137 by working up the list from the bottom and attempting to match the connecting user with a group, **ignoring** entries that are set **Mi-Token Auth**.

The first group tried will be the pseudo-group **Default**, which will always result in a match unless **Default** is set **No-Token Bypass**. The second group tried will be the **No Tokens Assigned** pseudo-group, and this will be followed by any groups you have set up, such as the group in the example dialog box, **Special projects team**.

- When the comparison process is complete, it applies the setting, **Always Allow** or **Always Deny**, indicated by the **last** match.
- If there is no match, access is determined by the other system settings – see *To create or edit a connection request policy*.

In the case of the example dialog box shown in Figure 137, suppose a member of the **Special projects team** group tries to connect. Providing that user has no tokens, he or she will match two of the groups shown, namely **Special projects team** and **No Tokens Assigned**. (The **Default** group is ignored because of the setting **Mi-Token Auth**.) The outcome is that Mi-Token applies the last match working upwards, that is, **Special projects team**, and it will allow access.



To add a group

- Click **Add**. A dialog box opens to allow you to search for AD objects to add.



To remove a group

- Select a group and click **Remove**.



To change an authentication mode in Group Settings

- Use the drop-down to select **Always Allow**, **Always Deny** or **Mi-Token Auth**.

Usage note: Recall that if a group has its Authentication Mode set to **Mi-Token Auth**, that group does not participate in the authentication process. Using this Authentication Mode, you can set up groups which may have no immediate significance but will be needed in the future: assign them as **Mi-Token Auth** and Mi-token will ignore them.

12.8 Rate Limiting tab

This function allows you to place limits on the frequency with which a user may attempt to log in unsuccessfully. The function only operates if you set **Rate Limiting** in the UI Helper – see *Rate Limiting enable and disable*.

- Open Active Directory Users and Computers.
- Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
- Click the **Rate Limiting** tab.

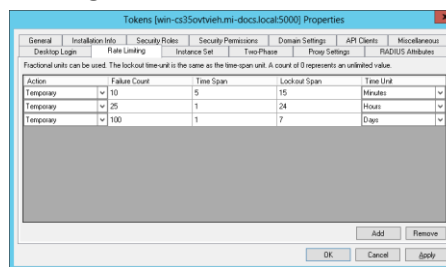


Figure 138. Rate Limiting tab

For each row, Time Unit (Seconds, Minutes, Hours, Days or Weeks) applies to Time Span and Lockout Span. In the top row of Figure 138 for example, the Time Span is 5 minutes and the Lockout Span is 15 minutes. If a user attempts 10 unsuccessful authentications in 5 minutes, he or she is locked out for 15 minutes. Each row applies in turn.

The Action may be set to Temporary or Permanent. If it is Permanent, this overrides the Time Span, being a permanent lockout of that user.



To add or remove a row on the Rate Limiting tab

- Click **Add** or **Remove**.

12.9 Instance Set tab

Reserved for future use.

12.10 Proxy Settings tab

Mi-Token can be configured to forward failed requests (Legacy two-factor authentication system requests) to another RADIUS Server. This feature is for easy migration from other two-factor authentication systems.



To configure proxy RADIUS server support:

1. Open **Active Directory Users and Computers**.
2. Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
3. Select the **Proxy Settings** tab. Click **Add** and Check the **Enabled** box.

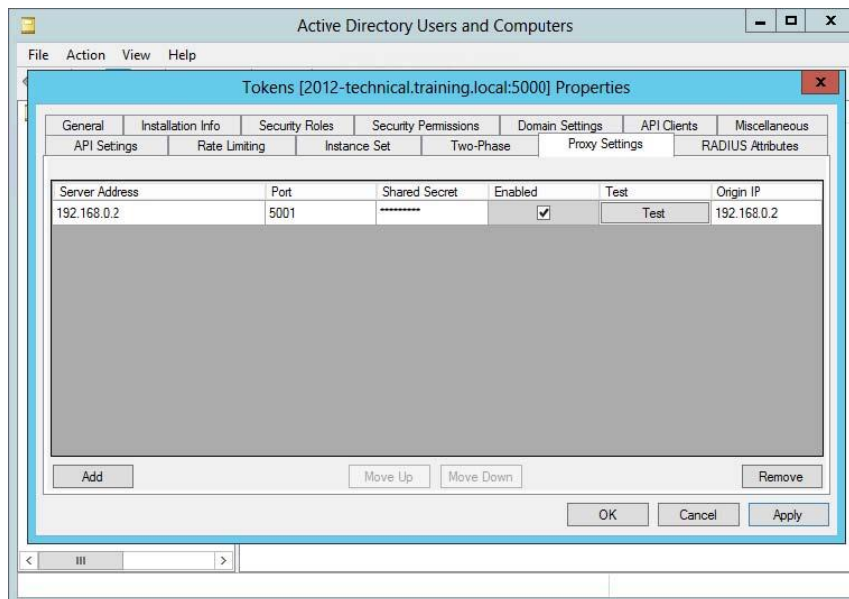


Figure 139. Configure proxy RADIUS server

4. Enter the **Server Address** (that is, IP address), **Port** and **Shared Secret** of the RADIUS server you wish to forward to.
5. You can test this server using the built-in Mi-Token RADIUS Tester. Launch **RADIUS Tester** either by pressing the Windows logo key or from its exe in the default location: C:\Program Files\Mi-Token\RADIUS Tester. See *Testing RADIUS server installation and configuration*.
6. Click **OK**.

12.11 RADIUS Attributes tab

1. Open Active Directory Users and Computers.
2. Right-click the **Tokens** node found in the tree in the left pane and select **Properties**.
3. Click the **RADIUS Attributes** tab.

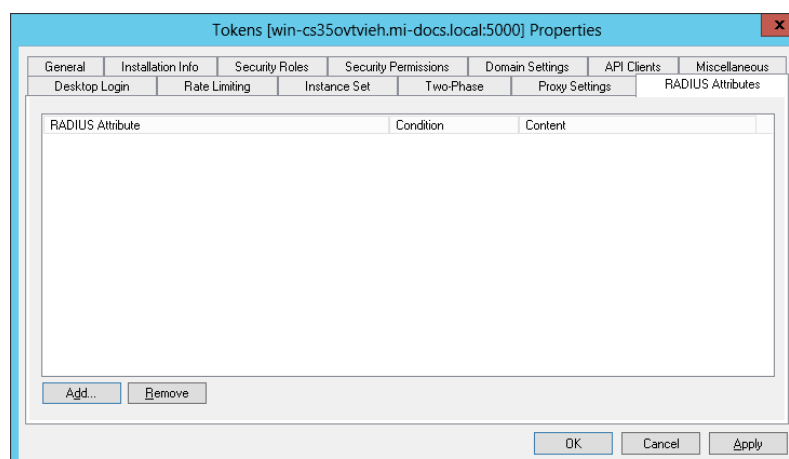


Figure 140. RADIUS attributes tab

For details, consult RADIUS documentation.

13 Mi-Token UI Helper

The UI Helper offers such facilities as

- No-Token Bypass
- Required Windows group
- Rate Limiting

Some of the features are described in the installation procedures under *Configuring the primary server*.



To access the UI Helper

1. Launch **Administration UI Quick-Start** and select the **RADIUS plug-in management** tab. (See Figure 20.)
2. Click **Launch**.

13.1 Required Windows group



To set a Windows group

1. Launch **Administration UI Quick-Start** and select the **RADIUS plug-in management** tab. Click **Launch**. This launches the UI Helper.

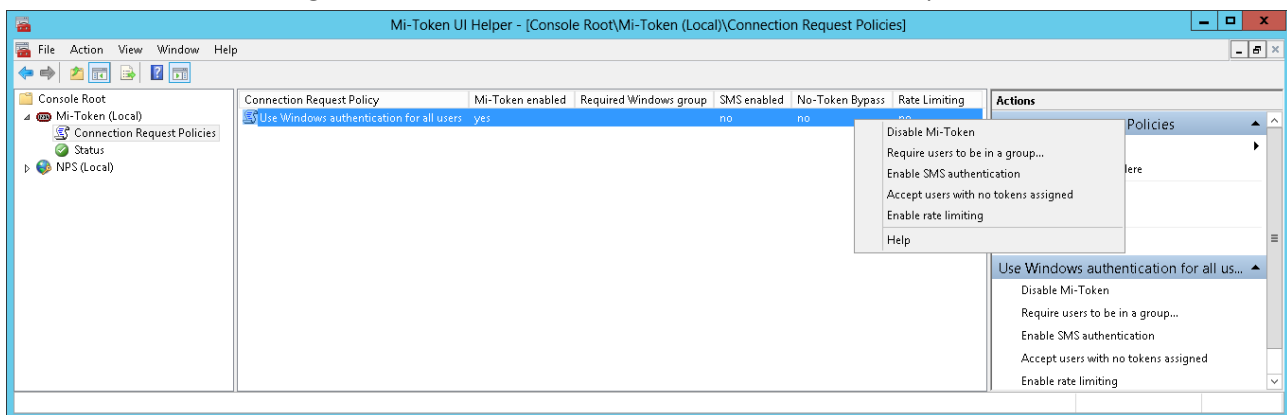


Figure 141. UI Helper showing a connection request policy

2. In the left pane, navigate to **Mi-Tokens (local) > Connection Request Policies**. Notice the Required Windows group column.

CONNECTION REQUEST POLICIES IN MI-TOKEN AND NPS

Recall the relationship of the Mi-Token plugin to the NPS, as depicted in, for example, Figure 3. Both components, Mi-Token and NPS, have their **own set** of Connection Request Policies. Both sets of policies are accessible from the UI Helper (and NPS's policies are also accessible from NPS's own user interface).

This can result in confusion, particularly with respect to groups, because groups can be set in both components.

When a user attempts to connect, NPS first interrogates the Mi-Token plugin. If the plugin denies access, the user does not connect. If the plugin allows access, NPS applies its own criteria.

13.2 No-Token Bypass

If **No-Token Bypass** is set, users who do not have any tokens will be permitted to authenticate. This overrides group settings – see *Group Settings*.

This setting would typically be used when an organization is deploying tokens for the first time. There can be a degree of confusion and non-compliance among the user community and you could set this option during a transition period.



To set No-Token Bypass

1. Launch **Administration UI Quick-Start** and select the **RADIUS plug-in management** tab. Click **Launch**. This launches the UI Helper.
2. In the left pane, navigate to **Mi-Tokens (local) > Connection Request Policies**. Notice the No-Token Bypass column.
3. In the left pane, right-click on the policy concerned.
4. In the drop-down, select **Accept** (or **Reject**) **users with no tokens assigned**.

13.3 Rate Limiting enable and disable

If **Rate Limiting** is set, the rate limiting feature is active – see *Rate Limiting tab*.



To set Rate Limiting

1. Launch **Administration UI Quick-Start** and select the **RADIUS plug-in management** tab. Click **Launch**. This launches the UI Helper – see Figure 141.
2. In the left pane, navigate to **Mi-Tokens (local) > Connection Request Policies**. Notice the Rate Limiting column.
3. In the left pane, right-click on the policy concerned.
4. In the drop-down, select **Enable** (or **Disable**) **rate limiting**.

14 Troubleshooting

This troubleshooting guide contains several suggestions for helping administrators overcome installation or operating issues regarding the implementation of Mi-Token Enterprise Edition.

- ⓘ *Mi-Token Inc. does not provide direct support for the variety of SSL VPN devices with which our customers typically integrate Mi-Token. However we can provide general support for configuring a RADIUS protocol/client.*

Additional support can be provided by Mi-Token upon request and may be subject to additional fees.

Upon ordering of Mi-Token Enterprise Edition, you will be issued with an installation certificate, which may be requested during any support call regarding Mi-Token.

14.1 General troubleshooting hints

Common issues which may prevent the successful installation or management of Mi-Token include:

- The system prerequisites set out in this administration guide have not been met.
- The account used to install the software does not have the required domain permissions.
- Firewall permissions are incorrectly set.
- The RADIUS shared secrets on the plugin and SSL VPN device (or other authentication end-point) do not match.
- NPS has been incorrectly configured.
- IIS is not installed or is not up-to-date.
- For soft-tokens, authentication wasn't correctly configured in IIS for the Mi-Token Intranet Provisioning Website.
- For Mi-Token Reporting, no database is installed, or the database is incorrectly configured.
- For soft-token deployment, SMTP settings and permissions are not correctly set.
- The relevant Mi-Token license has been incorrectly imported, not imported at all, or has expired.
- Particularly if you have recently upgraded your system, check that the various components have the same version and build numbers.

Please check these before issuing a support request.

14.2 Troubleshooting user authentication

General troubleshooting suggestions:

- The Windows Event log is a very useful tool. Please check both the Mi-Token (Authentication) and the System logs to identify errors with user authentication.
- Check Mi-Token Reporting for any authentication errors.
- Ensure that PAP is enabled in the NPS policy.
- Ensure that the RADIUS shared secrets on the NPS server and the remote-access device are the same.

- Ensure that the user has remote-access permissions (**Active Directory user properties** > Dial-in tab > **Allow access**), or that NPS is configured to grant access regardless of said permissions.
- If authentication is successful with the Mi-Token RADIUS PAP testing tool but not with your remote access appliance check that the device supports long passwords and/or shared secrets as some appliances are known to truncate passwords/secondary passwords and/or shared secrets which will cause authentication to fail.

Symptom: Event ID 33 – A token has been assigned to a same user and the token app has been successfully installed on the user’s mobile device, but the token authentication fails locally, with a message in the event viewer stating that the concerned user has no 2FA tokens.

This can happen if two RADIUS servers are installed, both configured as primary. Reconfigure (with reinstallation as necessary) so that one is the primary and the other is a replica server.

Symptom: Tokens are available on all servers but during the process of assigning a token to a user, the user mobile issues a message stating that the instance is not yet registered on mobile.mi-token.com.

Your Key encryption Key could be corrupt. Please get in touch with Mi-Token.

Symptom: The authentication process does not appear to recognize the connecting user’s group membership.

Check that there is no conflict between the group memberships as defined in NPS and in the Mi-Token plugin. Refer to Connection Request Policies in Mi-Token and NPS.

14.3 Troubleshooting RADIUS plugin failure

General troubleshooting suggestions:

- Check that the RADIUS client’s IP address and shared secret are correctly configured.
- Be aware of DNS names resolving to unexpected IPv6 or IPv4 addresses.
- Check that the Mi-Token AD LDS service has started. e.g. Windows Start > **Administrative Tools** > **Services**.
- Check that NPS services have started.
- Check the Mi-Token RADIUS snap-in extension’s status node for plugin heartbeats within NPS.
- Check the event log (Application, System, and Mi-Token) for errors.
- Run `dsdbutil.exe` to list instances to obtain the LDAP port used by the Mi-Token AD LDS instance. Connect to that port via the Microsoft Support Tool `ldp.exe`, and verify that it’s working as expected.
- Ensure that the RADIUS plugin’s registry entries contain references to the correct AD LDS port.
- Check firewall permissions if there are intervening firewalls between the Mi-Token Enterprise Edition server and the remote access device or between the Mi-Token Enterprise Edition server and any referenced domain controllers.

14.4 Troubleshooting replication

If you have difficulty with replication, we suggest you run the following commands.

(Suppose that the names of the two servers are DC01 and DC02.)

On server DC01...

```
ping DC02.test.local
dcdiag /s:localhost:5000
dcdiag /s:DC02.test.local:5000
dcdiag /s:DC02.test.local
repadmin /bind /s:DC02.test.local:5000
```

On server DC02...

```
ping DC01.test.local
dcdiag /s:localhost:5000
dcdiag /s:DC01.test.local:5000
dcdiag /s:DC01.test.local
repadmin /bind /s:DC01.test.local:5000
```

This should indicate whether the issue is at the networking level.

14.5 Troubleshooting missing audit logs

General troubleshooting suggestions:

- Restart the Mi-Token AD LDS service and check its event log to ensure has the privileges required to generate audits. If it is lacking those privileges, give the Generate Audit Logs privilege to the appropriate service account.
- Ensure that Directory Access audit event logs are appearing in the Security event log.
- Ensure that the Mi-Token Audit Helper service is running.
- Ensure that the Mi-Token Audit Helper service is placing processed security event logs into the Mi-Token event log.
- If you have recently changed the audit policies, make sure that you have updated with **gpupdate**.

14.6 Troubleshooting the Mi-Token Intranet Provisioning Website

Installing the Mi-Token Intranet Provisioning Website

Symptom: The installer exits immediately with the following message:

INSTALLATION INCOMPLETE

A: The installer was interrupted before the Mi-Token Intranet Provisioning Website could be installed.

This problem is related specifically to Windows Server 2008 and 2012 and IIS 7.

The IIS 6 Management Compatibility component must be installed for the installation to be successful. You can install it via server manager in the role services section of IIS. Then restart the installer and try again.

Symptom: When browsing to the website you receive a warning:

ERROR LOADING ENCRYPTION KEY FROM ADAM/LDS DATABASE

The website will instruct you to run a command in an elevated command window. If you run the command you receive another error message:

RUNNING WEB APPLICATIONS RUNNING UNDER AN APPLICATIONPOOLIDENTITY ACCOUNT (DEFAULT IN IIS 7.5) IS NOT YET SUPPORTED.

A: You will have to switch the identity that the application pool is running under. If you are having this issue, it will be ApplicationPoolIdentity. We recommend changing it to NetworkService.

Once this is done you will have to refresh the website as it will provide you with a different command to run.

Running the Mi-Token Intranet Provisioning Website

General troubleshooting suggestions:

- Ensure you have the ASP.NET IIS role service component installed.
- Ensure you have installed either the Windows Authentication or Digest Authentication IIS role service components.
- The website must be able to serve static content, ensure the Static Content IIS role service component is installed.
- The server's time must be correct for you to successfully set up and authenticate soft tokens. You can view the server's current time (in the GMT time zone) by viewing the Mi-Token NPS MMC snap-in. You'll find this snap-in under the NPS management admin tool. The server's GMT time can be found with a Google search for the current GMT, or by reference to a website such as www.timeanddate.com.

14.7 FAQs

Q: Is there a cost associated with the replica server capability?

A: When an authentication server (NPS with Mi-Token RADIUS plugin or API Server) is installed, it needs an AD LDS instance, either the primary or a replica (the installers provide the option to designate an instance as a primary or a replica). Typically the first to be installed becomes the primary in the given Active Directory domain, while subsequent installations become replicas. The replica(s) and the primary instance exchange data using Microsoft AD LDS replication technology, and there is no extra cost attached to this functionality. Further details are available from this link: <http://technet.microsoft.com/en-au/library/cc770465.aspx> and in this manual under Installing a replica authentication server.

Having multiple AD LDS instances makes for scalability (provided a load-balancing solution utilizing several Microsoft NPS or Mi-Token API servers is in place) and also contributes to reliable data storage with the Mi-Token database distributed between several automatically replicating locations.

Q: Mi-Token has its own AD LDS as a directory instance to store all token related information. Does Mi-Token use the existing enterprise AD to store all token related information? What will be the impact to the existing enterprise AD if it is allowed?

A: No. Mi-Token always uses AD LDS.

Q: Can Mi-Token be installed on shared servers with other applications? What should be considered when using Mi-Token on shared servers?

A: Yes it does, but please consider making sure the Mi-Token data is kept extremely secure. For example, we would not recommend installing Mi-Token on a terminal server to which general users have access.

Q: Can Mi-Token be installed on a member server of a domain?

A: Yes. Mi-Token can be installed on a member server of a domain.

Q: Does Mi-Token work on both VM and traditional standalone server hardware?

A: Yes.

Q: Which server will be used to host the soft-token software for mobile phones to download?

A: the soft-token software and user provisioning page is hosted on an IIS server. However, Mi-Token can also provide a hosted server for soft-token provision.

Q: Does this server need to be in Demilitarized Zone (DMZ)?

A: Yes it does, and it needs an SSL certificate.

Q: Does the soft-token server need to be a member server of the AD domain supporting Mi-Token or can it be a standalone server?

A: It can/should be standalone. This will help maintain the integrity of the solution.

Q: Is the soft-token provisioning server, which provides the users with the soft-token provisioning page, a domain server on the internal network?

A: Yes.

Q: Is there any relationship of the standalone DMZ server (hosted by Mi-Token) that stores the software for cell phones to download and the Mi-Token Intranet Provisioning Website?

A: Yes, there is a relationship between the two. Both servers shared a cryptographic secret (the KEK) but do not communicate directly at all. The KEK is used to encrypt the URL that users go to on their mobile phones.

Q: How is a specific URL for a specific user to download the software established on the DMZ server? Is this URL one-time URL?

A: This URL is generated by the internal server by encrypting the token secret using the KEK. The URL is indeed one-time and also has a time window for the user to activate the token (the internal server also embeds the current time into the URL).

Q: Are the policies and configuration of connections for RADIUS clients centrally stored or do you need to configure them individually on each Mi-Token server?

A: The RADIUS client configurations are stored within NPS, which (unlike AD) doesn't store configurations centrally. However, NPS does allow import/exports of its configurations. This makes setting up of multiple Mi-Token servers the correct connection request policies quite easy.

Q: Does Mi-Token use RADIUS accounting, or will all user access logs depend on NPS logs?

A: Mi-Token can use RADIUS accounting, because NPS supports RADIUS accounting. Mi-Token also has its own logs in addition to the NPS user access logs.

Q: If a RADIUS client does not have the third login field for the OTP or cannot use separate authentication servers for token and uid/password authentication, will you have to use the same AD for Mi-Token and uid/password authentication?

A: Yes, although optionally Mi-Token can have its own static PIN so you won't have to use the AD password.

Q: If Mi-Token is installed on an existing NPS server that is currently supporting one-factor user authentication (uid/password), does it require all existing NPS RADIUS clients to immediately use two-factor authentication or is there a migration configuration?

A: Mi-Token once installed is initially disabled, and won't disrupt your existing NPS RADIUS clients. To enable Mi-Token you will need to create a new connection request policy, and enable Mi-Token for that policy.

Q: Is it possible to restrict the user group that an administrator can view and assign tokens to?

A: Yes, but only if the user group in question is a domain. If it is necessary to have different groups in the one domain, containers may provide a solution, at least for hard tokens, by delegating privileges to separate administrators for each group. However, the domain administrator will still have access to all tokens.

14.8 Additional support

For additional support, please contact support@mi-token.com

You may be asked to quote your customer reference number found on your Mi-Token installation certificate.

15 Installation checklists

If convenient, you can print this list and check off the items as they are done.

15.1 Information to be collected

- Mi-Token Reporting to be deployed?
- Mi-Token Intranet Provisioning Website to be installed?
- SMTP server needed?
If so, note the parameters
- SMS gateway needed?
If so, note the parameters
- Planning (*Administrative and infrastructure requirements*).
 - Instance name
 - LDAP port (default 5000)
 - SSL port (default 5001)
 - AD LDS database administrator individual or group name.
- Planning for RADIUS (see step 5, page 37). Each client requires a friendly name, address and shared secret
- Firewall configuration considerations
 - RADIUS authentication (UDP 1812)
 - Between management PCs and RADIUS servers:
 - AD LDS LDAP ports (TCP 5000 by default)
 - Between replicating RADIUS servers:
 - AD LDS LDAP ports (TCP 5000 by default)
 - RPC endpoint mapper (TCP 135)
 - A set of replication ports (2 configurable ports, TCP)
- End-user device allows entry of two passwords or only one?

Req'd	Done

--	--

15.2 Required facilities

- Windows 2012 (64-bit) with Network Policy Server
- Active Directory and Active Directory Lightweight Directory Services correctly installed and configured.
- Domain Name Services correctly installed and configured.
- Suitable version of Internet Information Server available
- Firewall rule-set configurations planned, implemented and tested. Refer to *Ports and protocols table*.
- SQL Server 2005, 2008 or 2008 R2

Req'd	Done
x	
x	
x	
x	
x	
x	

15.3 Activities

These are the activities involved in installing Mi-Token Enterprise Edition once all the prerequisites are installed on the target server.

This list, and the manual as a whole, set out the steps in a convenient order but in fact the order is very flexible.

- Mi-Token software downloaded and extracted

Req'd	Done
x	

Components to be installed

- Primary RADIUS server installed (required unless authentication is via API)
- Primary RADIUS server tested
- UI installed
- Mi-Token Intranet Provisioning Website installed – optional
- API server installed
- AD Federation Services installed
- Mi-Token Reporting installed
- Replica server or servers installed
- Replica server or servers tested

x	
x	
x	

16 Upgrading

Mi-Token recommends you keep your Mi-Token software up to date, including AD LDS, and keeping in mind that the AD LDS schema changes from time to time. In broad outline, the upgrade procedure is

- Back up AD LDS first.
- Ensure that either the RADIUS installer or the API installer is the first installer to be run. These installers are the ones which upgrade the AD LDS schema.
- Run the rest of the installers.

More detailed upgrade notes will be provided.

16.1 Updating the Mi-Token RADIUS plugin and AD LDS database

It is recommended that when updating the RADIUS plugin you update the replica server first, if you have a replica server.



To upgrade the Mi-Token RADIUS plugin

1. Make sure you are logged into the server with a Domain Administrator account.
2. Run the Mi-Token RADIUS plugin installer. This starts a wizard.
3. Progress through the wizard, allowing all components to be installed.
4. The wizard will bring up the option of either creating a new AD LDS instance or using an existing one (if present). Select the existing instance – it should be selected by default if found. The installer will start to upgrade AD LDS instance. Make sure a Global Catalog Server is contactable otherwise the upgrade will fail.
5. The installer will start to upgrade the instance by loading the new schema and updating the data. The AD LDS configuration wizard will be completed.
6. You will be returned to the RADIUS installer, it will stop and start NPS. RADIUS plugin upgrade is complete.

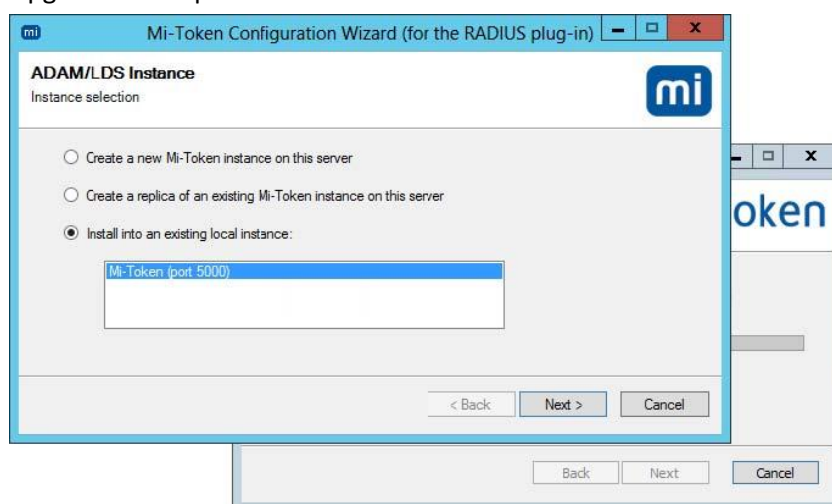


Figure 142. Upgrade RADIUS plugin

Continue reading if you have a replica server, otherwise the RADIUS Plugin upgrade is complete.

1. At this stage you should have a fully upgraded Mi-Token replica server, it is important at this stage to confirm that it is working.
2. Log on to your primary Mi-Token server, go to services (services.msc). Stop the NPS service.
3. Log on to your VPN or other remote access device. The authentication request will be sent to the newly upgraded replica server.
4. Confirm that the authentication was successful via the device and the event viewer logs on the replica machine.
5. If the authentication was successful, complete steps 1 to 6 (under *To upgrade the Mi-Token RADIUS plugin*) for your primary Mi-Token server. You should have two completely upgraded Mi-Token servers at this stage.



To upgrade Mi-Token (Active Directory UI)

1. Run the Mi-Token Active Directory UI installer.
2. There are no configuration options; the installer will upgrade the Active Directory UI. Upgrade is complete.

17 About Mi-Token

Mi-Token was originally designed specifically for two-factor authentication use within the banking industry.

Since then, Mi-Token has established itself as an independent product, and now has more than a million end-users across leading banks and enterprises.

Based in the US and Australia, Mi-Token is focused on creating innovative solutions that deliver the world's best security in the most efficient fashion possible.

Mi-Token is rapidly expanding, with an increasing presence in the international market.

Mi-Token is a proud OATH member.

For more information about Mi-Token, please contact sales@mi-token.com

Contact information

USA (Head-Office):

Mi-Token Inc., 13812 Research Boulevard Suite B-1 Austin TX 78750, United States

US Phone: +1 (512) 992-0158

APAC (Research and Development):

Mi-Token Pty. Ltd., Level 1, 27 Atchison Street St Leonards, NSW 2065, Australia.

APAC Phone: +61 (02) 9002 5562

For all other regions or general enquiries, please direct your email to sales@mi-token.com