Product Guide
Revision A

McAfee One Time Password 4.1.0
COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscope, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
# Contents

## 1 Introduction

## Deployment

### 2 Deployment

- Supported user databases
- Supported protocols
- McAfee OTP Client software development kit (SDK)
- Intel® Identity Protection Technology (Intel IPT)
- Deployment checklist

### 3 Installation and start-up

- Requirements
- Install McAfee OTP
- The McAfee OTP dashboard
- Enable the dashboard feature
- Start or stop McAfee OTP
- Start and Stop McAfee OTP on a Windows-based computer
- Start and stop McAfee OTP on a UNIX, Linux, or Mac OS X-based computer
- Introducing the configuration console
- Select pane
- Mouse functions

## Integration

### 4 Integration

- Integration modules
- VPN/RADIUS access
- Programming APIs

## OATH integration

### 5 OATH integration

- Check the requirements
- Portable Symmetric Key Container format
- Key format in user databases

## Configuration and use

### 6 Configuring McAfee OTP server, RADIUS object, and databases

- Configuration checklist
- Configure the Server object type
  - Server Settings
  - Mobile Numbers
  - Onetime Password Options
- Client Settings
  - Encryption
  - Options

McAfee One Time Password 4.1.0  Product Guide
7 Configuring the Clients object type

Create a client ..................................... 47
Delete a client ...................................... 48
Duplicate a client .................................. 48
Create a RADIUS client ............................. 48
  Advanced .................................. 48
  RADIUS Options ............................... 50
  Prefetch OTP Options ............................ 50
  User Database ................................ 51
  Other options ................................ 51
Create a Native client ............................. 51
  Advanced — Native Client Name Detection 52
  Options .................................. 52
  User Database ................................ 52
  Other options ................................ 52
Create a Web services client ........................ 53
  Options .................................. 53
  User Database ................................ 53
  Other Options ................................ 53

8 Configuring the Delivery Method object type

Enable a delivery method type ........................ 55
Configure the SMS Gateway delivery method .............. 56
  General Settings and Proxy areas ..................... 56
  Location .................................. 57
  Configuration and Status ........................... 57
  Advanced .................................. 57
Configure the HTTP delivery method ....................... 57
  Headers or Template file .......................... 57
  Authentication ................................ 58
  Proxy ................................... 58
  Other Settings ................................ 58
Configure the Extended HTTP delivery method ............. 58
  Headers or Template file .......................... 59
  Authentication and Proxy ........................... 60
  Other Settings ................................ 60
Configure the SMTP delivery method ....................... 61
  SMTP Host ................................. 61
  Authentication ................................ 61
  SMTP Options ................................ 61
Configure the Netsize delivery method ..................... 62
  Communication ................................ 62
  Authentication ............................... 63
9 Configuring the Misc object type

Configure the Expired Password Notification settings ............................................ 69
Expired Password Notification ..................................................................................... 69
Configure the OATH settings ......................................................................................... 70
HOTP ............................................................................................................................. 70
TOTP ............................................................................................................................... 70
General OATH Settings ................................................................................................. 70
Automatic OATH Enrollment ......................................................................................... 71
Configure the Prefetch OTP options ............................................................................. 71
Configure the Unlock User Accounts options ............................................................... 72
Configure the AES Encryption options ......................................................................... 72
General Settings ........................................................................................................... 73
Advanced Settings ......................................................................................................... 73
Test encryption and decryption ...................................................................................... 74
Configure the Embedded HTTP Server Options ........................................................... 74
Configure a cluster ......................................................................................................... 74
Configure Enrollment ..................................................................................................... 75
Configure the enrollment methods .............................................................................. 75
Configure the Pledge Enrollment options ..................................................................... 76
Configure text message and email enrollment ............................................................... 78
Configure OATH token enrollment .............................................................................. 78
Configure Intel IPT Enrollment ..................................................................................... 78
Configure the Web Manager options ........................................................................... 79
Authentication settings ................................................................................................. 79
Other ............................................................................................................................. 80
Enable the Self Service tool .......................................................................................... 80
Self Service Configuration settings ............................................................................. 80
Secret Question and Answer (Q/A) .............................................................................. 81
Lockout ........................................................................................................................... 82
Information for Self Service .......................................................................................... 82
Configure the Yubico options ....................................................................................... 83

10 Logs, Alerting, and Licensing overview

Configure the Logs object type ...................................................................................... 85
Log Files .......................................................................................................................... 85
Other Settings ............................................................................................................... 86
Configure the Alerts object type ................................................................................... 86
Alert Configuration ......................................................................................................... 86
Configure the Licenses object type ................................................................................. 87
License Information ........................................................................................................ 87

11 Getting information

McAfee OTP monitor ...................................................................................................... 89
Logging features ............................................................................................................. 89
Introduction

McAfee® One Time Password (McAfee OTP) adds a layer of security that protects applications and systems with strong, multi-factor authentication. It combines user name and password authentication with a one-time password as a second authentication method to protect the authentication process and the "key" to an organization’s applications and systems.

After McAfee OTP verifies a user name and password against a defined user store, it sends the user a one-time password. The user enters the one-time password and is authenticated to the application or system only after McAfee OTP verifies the entered password.

McAfee OTP generates and distributes one-time passwords to users by email, text message to a mobile phone, and voice to a mobile telephone or landline.

Types of one-time password tokens

McAfee OTP supports hardware and software tokens that generate one-time passwords using the HOTP (RFC 4226), the TOTP algorithm (RFC 6238), and OATH OCRA standards. In addition, McAfee offers McAfee® Pledge Software Token that, when installed on a mobile device, generates one-time passwords using the OATH standard.

Deliver one-time passwords to RADIUS and non-RADIUS systems

McAfee OTP can be integrated with applications and systems through integration modules and protocols. For example, McAfee OTP can be integrated with most VPN services using the RADIUS protocol. Since McAfee OTP can act as a RADIUS server, most VPN/RADIUS-aware products can be
integrated without any installation. Configuring the McAfee OTP and the VPN/RADIUS product completes the integration. Refer to mcafee.nordicedge.com/integrations for the integration modules that are available.

Figure 1-1  McAfee OTP architecture
Deployment

Install McAfee OTP, deploy it within your network, and integrate it with RADIUS and non-RADIUS systems at your site to provide them with strong two-factor authentication.
Deployment
Deployment

This section describes the options for planning your McAfee OTP product deployment. When you have completed this section, you should be ready to install the McAfee OTP product, set up communications between McAfee OTP and the SMS gateway and McAfee Pledge, integrate with the OATH algorithm, and configure clusters.

Contents
- Supported user databases
- Supported protocols
- McAfee OTP Client software development kit (SDK)
- Intel Identity Protection Technology (Intel IPT)
- Deployment checklist

Supported user databases

McAfee OTP supports these user stores.

- LDAP, including:
  - Sun Directory Server
  - Microsoft Active Directory
  - Novell eDirectory
- SQL through JDBC or ODBC, including:
  - Oracle
  - Microsoft SQL Server
  - MySQL

Other user stores are supported through APIs.

Supported protocols

McAfee OTP supports these protocols.

- LDAP
- SMTP
- HTTP/HTTPS
- Web Services/SOAP
- SMPP
- CIMD2
McAfee OTP Client software development kit (SDK)

Use the Java Client API to integrate McAfee OTP with applications that do not include integration modules.

For information about downloading COM and .NET APIs, go to the McAfee Technical Support ServicePortal.

For information about integrating Microsoft .NET applications using the Java Client API, go to mcafee.nordicedge.com/integrations.

Intel® Identity Protection Technology (Intel IPT)

Use the Intel Identity Protection Technology (Intel IPT) feature to store the OATH key on the chipset of supported devices to prevent malware or hacking from compromising the credentials. With the Intel IPT chipset on a device, a user enrolls for a profile in the same way, but the OATH key is stored on the device chipset.

Requirements

Verify that the device (smartphone or computer) satisfies these requirements.

• An Intel IPT chipset (check http://ipt.intel.com/Home/devices-with-intel-ipt) for a list of supported devices

• The Intel IPT software installed on the hardware or mobile device

The Intel IPT software is either already installed on a Microsoft Windows device, or can be downloaded from a link supplied by Intel.

See also

Create templates on page 103
Configure Intel IPT Enrollment on page 78

Deployment checklist

Prepare your environment before you install McAfee OTP and McAfee Pledge.

Pre-deployment considerations

Before you begin your deployment gather the following items and information:

• Installers for McAfee OTP and the OTPRemoteConfig tool.

• A license file in XML format with a valid McAfee SMS section if you want to register for that service

• LDAP attributes for each McAfee OTP option that you want to implement

• A McAfee OTP user proxy with proper access rights to LDAP attributes

• Communication between the McAfee OTP host and LDAP store or between the McAfee OTP host and protected systems is verified
• A Pledge Profile Service customer account exists
• Test user accounts and groups exist

**McAfee OTP server communication**

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure McAfee OTP queries your LDAP or JDBC user store using default TCP ports 389 for LDAP, and 636 for secure LDAP (LDAPS).</td>
<td></td>
</tr>
<tr>
<td>McAfee OTP must be able to communicate inbound with selected RADIUS ports. The default is 1645.</td>
<td></td>
</tr>
<tr>
<td>- UDP high port numbers are used for RADIUS communication between McAfee OTP and the RADIUS client.</td>
<td></td>
</tr>
<tr>
<td>Configure McAfee OTP to send one-time passwords to the SMS service over HTTPS on TCP port 443.</td>
<td></td>
</tr>
<tr>
<td>Set up integration modules to send requests to McAfee OTP using TCP port 3100. RADIUS modules must send requests using UDP port 1645 or 1812.</td>
<td></td>
</tr>
<tr>
<td>These port numbers are the default values and can be customized.</td>
<td></td>
</tr>
</tbody>
</table>

**McAfee SMS Gateway communication**

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound communication outbound with otpnordicedge.net and otp.nordicedge.com via HTTPS/TCP port 443.</td>
<td></td>
</tr>
<tr>
<td>Valid McAfee OTP license with SMS included</td>
<td></td>
</tr>
<tr>
<td>- The license is valid for 1000 users and will expire at the given date. The software uses the license file to create an SMS gateway user account with the user name mcafeese-31323.</td>
<td></td>
</tr>
<tr>
<td>Valid SMS gateway account</td>
<td></td>
</tr>
</tbody>
</table>

**McAfee Pledge communication**

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid McAfee OTP license</td>
<td></td>
</tr>
<tr>
<td>A Pledge Profile Service customer account</td>
<td></td>
</tr>
<tr>
<td>A Pledge Profile Service user account</td>
<td></td>
</tr>
<tr>
<td>A Pledge Web service account</td>
<td></td>
</tr>
<tr>
<td>Pledge clients must have access to pledge-api.nordicedge.com via on 443</td>
<td></td>
</tr>
<tr>
<td>Pledge Enrollment web application must have access to pledge-api.nordicedge.com on port 443</td>
<td></td>
</tr>
<tr>
<td>Administrator workstation has access to pledge.nordicedge.com on port 443 to access Pledge Profile Services</td>
<td></td>
</tr>
</tbody>
</table>
Installation and start-up

Review the requirements and instructions to download and install McAfee OTP on a Microsoft Windows platform and get started with the McAfee OTP configuration console.

Contents
- Requirements
- Install McAfee OTP
- The McAfee OTP dashboard
- Start or stop McAfee OTP
- Introducing the configuration console

Requirements

To install and operate McAfee OTP on a Windows platform, the system must meet the following minimum requirements.

Hardware server or virtual machine (VM)
- McAfee OTP is software that you install on any server in your internal network or DMZ.
- Use any modern hardware server or a virtual machine running on top of a modern hardware server as the installation platform.
- The hardware server must have a static IP address configured.
- If you configure McAfee OTP using DNS names, the server must be able to contact DNS servers.

Operating system
- You can install McAfee OTP on any operating system that supports Java Virtual Machine (Java VM) version 1.6 or later, including:
  - Microsoft Windows 2003 R2
  - Microsoft Windows 2008 R2
  - Linux
  - Sun Solaris
  - IBM AIX
  - Mac OS X
- You can install McAfee OTP on both 32-bit and 64-bit operating systems.

Software

When registering and downloading the software, select the version of the installer that correctly corresponds to your operating system platform.
Install McAfee OTP

The process to install McAfee OTP on a Microsoft Windows-based computer is similar to that on other operating system platforms. For platforms other than Microsoft Windows, you can install McAfee OTP in GUI or console mode.

**Before you begin**

Download the McAfee OTP installation application. To install McAfee OTP, you must have administrator permissions and a valid license file. If you are unsure of your status, use the Run as administrator option when you begin the installation process.

**Task**

1. Double-click the McAfee OTP installation program.
   The Introduction opens.

2. Click Next.
   The McAfee OTP License Agreement opens.

3. Read the license agreement, select the I accept the terms of the License Agreement option, then click Next.
   The Database Drivers step opens.

4. Read the Database Drivers license information, then select the checkbox to accept the terms and click Next.
   The Select Install Set step opens.

5. Select an installation option, then click Next.
   The Choose Install Folder step opens.

6. Specify an installation folder, or accept the default value, then click Next.
   You must install McAfee OTP in a folder that does not contain a previous installation of McAfee OTP. If a warning message displays regarding the installation folder you chose, click Previous to specify a new folder or rename the existing folder.

   The Select License File step opens.

7. Specify the location of the license file that you received from McAfee, then click Next.
   The Install Windows Service step opens.

8. Select the Install Windows Service checkbox, then click Next.
   The Choose Link Folder step opens.

9. Specify where to create shortcuts to the software, then click Next.
   The shortcuts are identified by a product icon. You click the icon to manually start the McAfee OTP.

   The Pre-Installation Summary opens.

10. Review the Pre-Installation Summary, then click Install.
    The Install Complete step opens.

11. Click Next.
    The Start the OTP Server step opens.
To start McAfee OTP, select Yes, then click Done.

The installer closes and McAfee OTP opens.

The McAfee OTP dashboard

McAfee OTP can be configured to display a dashboard of information for administrators to check system health and start enabled McAfee OTP web applications.

After you enable the feature in McAfee OTP, you can access the dashboard from https://<IPaddress>:<port_number>/

The default port number is 8080. If that port is already used, you can specify a different port.

From the dashboard, you can:

- Use the Health section to get quick system information, such as the number of used licenses, and the number of locked accounts since the last system restart. Click More health info to get complete details.

- Start enabled McAfee OTP applications, such as:
  - Web Manager
  - Enrollment
  - Self Service
  - Web Services

- Access a link to the latest product documentation.

- Connect to the McAfee technical support portal.

- Browse additional step-by-step guides documentation.

- Start Pledge Profile Service.
Table 3-1  One-time password Health statistics

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total OTPs</td>
<td>The number of one-time passwords sent</td>
</tr>
<tr>
<td>Successful OTPs</td>
<td>The number of one-time passwords that resulted in a successful logon</td>
</tr>
<tr>
<td>Failed OTPs</td>
<td>The number of one-time passwords that resulted in a failed logon</td>
</tr>
<tr>
<td>Unfetched OTPs</td>
<td>The number of one-time passwords that were not used</td>
</tr>
<tr>
<td>Expired OTPs</td>
<td>The number of one-time passwords that expired before they were used</td>
</tr>
<tr>
<td>RADIUS packets sent</td>
<td>All the RADIUS packets that McAfee OTP sends</td>
</tr>
<tr>
<td>RADIUS packets received</td>
<td>All the RADIUS packets that McAfee OTP receives</td>
</tr>
<tr>
<td>Number of licenses</td>
<td>The total number of licenses available</td>
</tr>
<tr>
<td>Used licenses</td>
<td>The number of licenses currently in use</td>
</tr>
<tr>
<td>Active connections</td>
<td>The number of active connections with client systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Successful connections</td>
<td>The number of successful connections with client systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Failed connections</td>
<td>The number of failed connections with client systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Encrypted requests</td>
<td>The number of encrypted requests from client systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Unencrypted requests</td>
<td>The number of unencrypted requests from client systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Rejected unencrypted requests</td>
<td>The number of unencrypted requests from client systems that McAfee OTP protects that were rejected</td>
</tr>
<tr>
<td>Successful logins</td>
<td>the number of successful logons to systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Failed logins</td>
<td>The number of failed logons to systems that McAfee OTP protects</td>
</tr>
<tr>
<td>Locked accounts</td>
<td>The number of accounts that were locked because of failed authentication</td>
</tr>
</tbody>
</table>

Enable the dashboard feature

Configure McAfee OTP to display dashboard information.

Before you begin
The Embedded HTTP Service must be enabled and running.

Task
1  In the select pane, expand the Misc object type, then select Embedded HTTP Server.
2  Click Enable OTP Dashboard.
3  Go to https://<OTPIPaddress>:<port_number>/ to open the dashboard.

The dashboard displays system health information and provides access to product documentation and starts enabled McAfee OTP and Pledge applications.
Start or stop McAfee OTP

McAfee OTP supports Microsoft Windows Server 2003, 2008, UNIX, Linux, and Mac OS X operating systems.

McAfee recommends that you stop McAfee OTP by clicking Shutdown on the McAfee OTP monitor. For this option, the monitor must be enabled.

Contents

- Start and Stop McAfee OTP on a Windows-based computer
- Start and stop McAfee OTP on a UNIX, Linux, or Mac OS X-based computer

Start and Stop McAfee OTP on a Windows-based computer

To start and stop McAfee OTP on Windows-based computer, use the following options.

- Start and stop McAfee OTP using Microsoft Windows Services.
- Start McAfee OTP by running the following program file, which is located in the installation directory: OTPServer.exe.
- Stop McAfee OTP by clicking Shutdown on the monitor.

Start and stop McAfee OTP on a UNIX, Linux, or Mac OS X-based computer

To start and stop McAfee OTP on a UNIX, Linux, or Mac OS X-based computer, use the following options.

- Start McAfee OTP by running the OTPServer program file in the background using the following UNIX command: OTPServer &.
- Stop McAfee OTP by using the UNIX kill command.
- Stop McAfee OTP by clicking Shutdown on the monitor.

Introducing the configuration console

Use the configuration console to perform all configuration tasks.

Use one of the following methods to start the McAfee OTP configuration console:

- Start McAfee OTP, then click Configuration to start the internal McAfee OTP configuration console — this method provides all configuration options.
- Shut down McAfee OTP. Go to the McAfee One Time Password installation directory and select OTPConfigurator.exe — this method allows you to configure McAfee OTP settings and view settings. McAfee OTP services and applications cannot be started using this configuration console.
- Go to the McAfee OTP directory in program files and launch OTPRemoteConfig — this method allows you to configure McAfee OTP remotely. Use this tool when McAfee OTP runs as a service on Microsoft Windows or when McAfee OTP is installed on UNIX without a user interface. McAfee OTP services and applications cannot be started using this configuration console and connections to databases cannot be tested. The test buttons test the connection between the workstation on which you are working and the remote systems to which McAfee OTP is connected.

To open McAfee OTP software and configuration options, click the McAfee OTP product icon that is created when McAfee OTP is installed.
### Option | Definition
--- | ---
**Menu bar** | Creates configuration objects, updates functions, and accesses Help.

**Select pane (left)** | Provides the option to select, create, configure, delete, or view an object type.

**Configuration pane (right)** | Provides the option to view the configuration options of an object selected in the select pane.

**Save Config** | Saves the configuration to the otp.properties file in the installation directory.

**Close** | Closes the administration console.

---

### Select pane

Select the type of object to create, configure, delete, or view it.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>Configure the McAfee OTP.</td>
</tr>
<tr>
<td><strong>RADIUS</strong></td>
<td>Configure McAfee OTP as a RADIUS server for McAfee OTP RADIUS clients.</td>
</tr>
<tr>
<td><strong>Logs</strong></td>
<td>Configure logging and the log files.</td>
</tr>
<tr>
<td><strong>Alerts</strong></td>
<td>Configure error messages and alerts that can be sent to a list of administrators using text message or email.</td>
</tr>
<tr>
<td><strong>Licenses</strong></td>
<td>Manage McAfee OTP licenses.</td>
</tr>
<tr>
<td><strong>Databases</strong></td>
<td>Configure connections to user stores.</td>
</tr>
<tr>
<td><strong>Clients</strong></td>
<td>Configure McAfee OTP clients.</td>
</tr>
<tr>
<td><strong>Delivery Methods</strong></td>
<td>Configure and enable one or more of these delivery methods.</td>
</tr>
<tr>
<td>• CIMD2</td>
<td>• McAfee Voice</td>
</tr>
<tr>
<td>• Concurrent Sender</td>
<td>• Prefetch Detection</td>
</tr>
<tr>
<td>• Extended HTTP</td>
<td>• SMPP</td>
</tr>
<tr>
<td>• HTTP</td>
<td>• SMTP</td>
</tr>
<tr>
<td>• NetSize</td>
<td>• UCP File</td>
</tr>
<tr>
<td>• McAfee SMS</td>
<td></td>
</tr>
<tr>
<td><strong>Misc</strong></td>
<td>Configure these objects:</td>
</tr>
<tr>
<td>• Embedded HTTP Server</td>
<td>• Self Service</td>
</tr>
<tr>
<td>• Cluster Configuration</td>
<td>• Unlock User Accounts</td>
</tr>
<tr>
<td>• Enrollment</td>
<td>• Web Manager</td>
</tr>
<tr>
<td>• Expired Password Notification</td>
<td>• AES Encryption</td>
</tr>
<tr>
<td>• OATH Configuration</td>
<td>• Yubico</td>
</tr>
<tr>
<td>• Prefetch Proxy Config</td>
<td></td>
</tr>
</tbody>
</table>
Mouse functions
The configuration console supports these mouse functions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tooltips</td>
<td>Provides context-sensitive help.</td>
</tr>
<tr>
<td>Mouse left-click</td>
<td>Allows you to view and select menu items on the menu bar, expand and select object types in the select pane, and open, close, minimize, and resize windows.</td>
</tr>
<tr>
<td>Mouse right-click</td>
<td>Provides a context menu for a selected object type in the select pane.</td>
</tr>
</tbody>
</table>
Installation and start-up
Introducing the configuration console
Integration

You can integrate McAfee OTP with Apache Reverse Proxy and Web Server, Citrix, Microsoft Internet Information Services (IIS), Microsoft Outlook Web Access, Microsoft Outlook Web App, and Novell GroupWise WebAccess. You can integrate systems that contain a challenge response such as Cisco, Check Point, F5, Blue Coat, and Juniper by configuring them to work with McAfee OTP. Other applications can be integrated with McAfee OTP using APIs or web services.

Using Java, COM, .NET, and PHP Client APIs, you can write custom integration modules for your applications. By using the Client APIs, you can add strong authentication to your custom applications.

Contents
- Integration modules
- VPN/RADIUS access
- Programming APIs

Integration modules

McAfee OTP supports these integration modules.

| Apache         | Apache Reverse Proxy Server  
|                | Apache Web Server 1.3/2.0  
| CA             | SiteMinder r6  
|                | SiteMinder r12  
| Citrix         | Citrix Access Gateway 4.2  
|                | Citrix Access Gateway 4.5  
|                | Citrix Access Gateway 5.X VPX  
|                | Citrix Presentation Server 4.6  
|                | Citrix Web Interface 4.0/4.2  
|                | Citrix Web Interface 4.5  
|                | Citrix Web Interface 5.4  
|                | Citrix XenApp Server 5.1  
|                | Citrix XenApp Server 5.2/5.3  
| IBM            | Lotus Domino (Apache Proxy)  

### Microsoft
- Internet Security and Acceleration (ISA) Server 2006
- Forefront Threat Management Gateway (TMG) 2010
- Internet Information Services (IIS) 6.0
- Internet Information Services (IIS) 7.x — Custom AD Membership Provider - ASP.NET
- Outlook Web Access 2003
- Outlook Web Access 2007
- Outlook Web App 2010
- Outlook Web App 2013
- SharePoint 2007 AD Membership Provider - ASP.NET
- SharePoint 2010 AD Membership Provider - ASP.NET
- Internet Information Services (IIS) — Custom AD Membership Provider - ASP.NET
- EPiServer AD Membership Provider — ASP.NET
- EPiServer SQL Membership Provider — ASP.NET

### Novell
- IChain 2.3
- GroupWise WebAccess 6
- GroupWise WebAccess 7

### VPN/RADIUS access
McAfee OTP acts as a RADIUS server to support most VPNs and other RADIUS-aware applications.

McAfee recommends that the VPN/RADIUS application support the RADIUS challenge-response standard.

These vendors provide RADIUS systems that have been tested with McAfee OTP and approved:
- Cisco
- Check Point
- F5
- Juniper
- Palo Alto
- AppGate

With the RADIUS challenge-response standard, you can use all McAfee OTP authentication methods. Without the standard, you can use the Pledge software token and all OATH tokens.

### Programming APIs
McAfee OTP can be integrated with custom applications through its Java, COM, and .NET APIs.
OATH integration

OATH is an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication. OATH offers these algorithm types that are supported by McAfee OTP:

- HOTP — An HMAC-based One Time Password algorithm. For more information, view the HOTP: An HMAC-Based One-Time Password Algorithm memo.
- TOTP — Time-based One Time Password algorithm. For more information, view the TOTP: Time-Based One-Time Password Algorithm memo.

Contents
- Check the requirements
- Portable Symmetric Key Container format
- Key format in user databases

Check the requirements
For a successful integration, verify that the following algorithm requirements are met.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| OATH HOTP | - McAfee OTP requires the OATH key to be stored as a user object attribute in the LDAP or SQL user database.  
- McAfee OTP 3.0 and later supports any OATH HOTP-compliant device.  
- When generating one-time passwords, McAfee® Software Token Pledge 1.0 uses the OATH HOTP algorithm.  
- If using OATH HOTP, McAfee OTP requires write access to the attribute or field where the key and counter are stored. |
| OATH TOTP | - McAfee OTP requires the OATH key to be stored as a user object attribute in the LDAP or SQL user database.  
- McAfee OTP 3.0.10285 and later supports any OATH TOTP-compliant device.  
- Since the counter does not have to be updated, only read access is required.  
- A time source (such as NTP) must be configured on the server running McAfee OTP to synchronize with the TOTP devices. |

Portable Symmetric Key Container format
The Portable Symmetric Key Container (PSKC) (RFC 6030) format is supported to import OATH keys into the McAfee OTP keystore.
Key format in user databases

This section describes the key format used to verify one-time passwords in the HOTP and TOTP formats in the user database.

**HOTP format**

When verifying the HOTP one-time password from the user object in the user database, the `key_in_hex:counter_in_decimal` format is used.

For example, f6d1a039ca13da1b5359e0b8f8e740c11a92509:29123

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key_in_hex</td>
<td>The HOTP key in hexadecimal format is 20 characters.</td>
</tr>
<tr>
<td>counter_in_decimal</td>
<td>The HOTP counter value that is increases after each successful one-time password verification. This value must be stored in decimal form. McAfee OTP automatically decrypts and encrypts the value.</td>
</tr>
</tbody>
</table>

**TOTP format**

When verifying the TOTP one-time password from the user object in the user database, the `TOTP:keysizer_1 | 256 | 512:key_in_hex:time_adjustment:timesteps_in seconds: otplength6 | 8` format is used.

For example, TOTP:1:28C2799CD7AE7596BC4C908BD4DF2B969170D9F:0:60:6

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTP</td>
<td>A static identifier for the TOTP algorithm.</td>
</tr>
<tr>
<td>keysizer_1</td>
<td>256</td>
</tr>
<tr>
<td>time_adjustment</td>
<td>The Unix time to start counting step steps. Usually this value is set to 0, Unix epoch.</td>
</tr>
<tr>
<td>timestamps_in seconds</td>
<td>McAfee recommends 30 seconds, but this value can differ depending on TOTP vendors.</td>
</tr>
<tr>
<td>otplength6</td>
<td>8</td>
</tr>
</tbody>
</table>
Configuration and use

Use the McAfee OTP configuration console to set up the McAfee OTP server, databases, and clients. Specify the type of methods you want to use to deliver one-time passwords to your users.

Chapter 6  Configuring McAfee OTP server, RADIUS object, and databases
Chapter 7  Configuring the Clients object type
Chapter 8  Configuring the Delivery Method object type
Chapter 9  Configuring the Misc object type
Chapter 10 Logs, Alerting, and Licensing overview
Chapter 11 Getting information
Configuring McAfee OTP server, RADIUS object, and databases

Configure the settings to manage and maintain McAfee OTP.

Contents

- Configuration checklist
- Configure the Server object type
- Configure the RADIUS object type
- Configure the Databases object type

Configuration checklist

To ensure successful configuration and use of your McAfee OTP product, ensure that you take these minimum actions on the objects relevant to your installation in the McAfee OTP configuration console.

Check that a valid license file is in the License directory. McAfee OTP configuration is saved into the otp.properties file in the installation directory.

McAfee OTP server configuration

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run all McAfee OTP options using the Run as administrator option on Microsoft Windows computers.</td>
<td></td>
</tr>
</tbody>
</table>

If configuration changes are not saved into the otp.properties file, check the file access permissions.

RADIUS

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>The McAfee OTP server RADIUS port configuration matches the RADIUS client configuration that is protected.</td>
<td></td>
</tr>
<tr>
<td>The shared secret is identical on McAfee OTP and the RADIUS client.</td>
<td></td>
</tr>
<tr>
<td>Outbound UDP high ports are opened from McAfee OTP to the RADIUS client.</td>
<td></td>
</tr>
</tbody>
</table>

Databases

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clicking the Test button returns a positive result.</td>
<td></td>
</tr>
<tr>
<td>The RADIUS shared secret is the same on both systems and that it is not too long or contains illegal characters.</td>
<td></td>
</tr>
</tbody>
</table>
## Client

### Workflow step

The **Client Name Detection** option is enabled when necessary.

The **Client Name Detection** value is used by McAfee OTP to differentiate applications calls asking McAfee OTP to perform various operations (APIs) like authenticating users, data lookup (mobile phone numbers, email address, OATH key for example), or writing data like the Pledge Enrollment.

Ideally, there should be one client per application to make it easier to troubleshoot, but the same client can be used by different applications or purposes.

The client object is associated to the correct database object.

The selected optional RADIUS attributes are not already used by McAfee OTP and match the configuration of the RADIUS client that is protected.

---

## McAfee SMS delivery

### Workflow step

A test one-time password can be sent from the McAfee SMS gateway and received by a mobile phone.

The Debug option is selected.

---

## McAfee Pledge

If Pledge Enrollments stops working suddenly, it might be that the Pledge Profile Services account exceeded the maximum number of licenses. The error message on the Pledge Profile Service webpage resembles "No results from web service! Error: Failed to create a Pledge Profile"

### Workflow step

Pledge Enrollment is enabled.

The embedded HTTP server is started.

The database to authenticate users and store their OATH keys is correct. That is, the selected attribute is a string type, its minimum length is 60 characters, and is multi-value to store multiple profiles.

There is a native client that represents Pledge Enrollment in the clients section.

https://necs.nordicedge.se/PLEDGESession/SessionService can be reached from a browser that is running on the same host as McAfee OTP.

The Pledge for Desktop option is enabled in Pledge Profile Services to authorize users to receive one-time passwords on their computer.

Pledge clients can download a static test profile if they can't download a Pledge profile ID.

Check whether failed Pledge ID attempts are occurring before or after the TTL period.

---

The Pledge Enrollment URL for users is similar to https://x.x.x.x:8080/PledgeEnrollment/enroll.jsp. The mixture of uppercase and lowercase characters in the URL makes it harder for intruders.
Web Manager

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>The database chosen to perform administrative tasks is correct.</td>
<td></td>
</tr>
<tr>
<td>Databases are configured with the LDAP DN and not administrator@company.</td>
<td></td>
</tr>
<tr>
<td>Administrative groups and users are chosen from the user store.</td>
<td></td>
</tr>
<tr>
<td>There is a native client that represents Web Manager in the clients section.</td>
<td></td>
</tr>
<tr>
<td>The native client has name detection enabled.</td>
<td></td>
</tr>
<tr>
<td>A corresponding OATH client is created for OATH tokens administration.</td>
<td></td>
</tr>
<tr>
<td>The OATH token client has name detection enabled.</td>
<td></td>
</tr>
<tr>
<td>The OATH token client is connected to an OATH database type.</td>
<td></td>
</tr>
</tbody>
</table>

Configure the Server object type

Use the configuration pane to configure the Server object type settings.

**Task**

1. In the select pane, select the Server object type.
   
   Server configuration options open in the configuration pane.

2. In the configuration pane, configure the remaining settings.

**Server Settings**

The following settings are located in the Server Settings area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Specifies the port number that Native and remote McAfee OTP clients use when connecting to the McAfee OTP. <strong>Default:</strong> 3100</td>
</tr>
<tr>
<td>Bind to IP Address</td>
<td>Specifies the IP address of the server on which the McAfee OTP is installed.</td>
</tr>
<tr>
<td>All</td>
<td>Selecting this checkbox specifies that the McAfee OTP accepts connections from McAfee OTP clients on all IP addresses assigned to the host server's system.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Specifies the number of milliseconds that the connection between the McAfee OTP client and the McAfee OTP can be idle before the session times out.</td>
</tr>
</tbody>
</table>

- A zero value specifies that there is no timeout.
Mobile Numbers

The following settings are located in the Mobile Numbers area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Mobile Number</td>
<td>Selecting this checkbox specifies checking the mobile number for non-numeric characters and removing them, including spaces.</td>
</tr>
<tr>
<td></td>
<td>This setting does not remove the “+” character from mobile numbers.</td>
</tr>
<tr>
<td>Default Country Prefix</td>
<td>Specifies removing any leading zeros and then adding the default country prefix that you provide.</td>
</tr>
<tr>
<td></td>
<td>This setting is only available when the Check Mobile Number checkbox is selected.</td>
</tr>
</tbody>
</table>

Onetime Password Options

The following settings are located in the Onetime Password Options area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTP Length</td>
<td>Specifies the length of the one-time password in number of characters.</td>
</tr>
<tr>
<td>OTP Valid Time</td>
<td>Specifies how long in minutes the one-time password is valid. A zero value specifies that one-time password is valid indefinitely.</td>
</tr>
<tr>
<td>OTP Retries</td>
<td>Specifies the number of times that the user can attempt to log on within the same session after entering the one-time password incorrectly, that is, McAfee OTP does not send a new one-time password. A zero value disables this function.</td>
</tr>
<tr>
<td>Retry Message</td>
<td>Specifies the message that the user receives after entering an incorrect one-time password.</td>
</tr>
<tr>
<td>Regenerate Timeout</td>
<td>Specifies the time in seconds required between McAfee OTP requests. This setting is designed to prevent users from requesting multiple one-time passwords in quick succession.</td>
</tr>
<tr>
<td>Composition</td>
<td>Select one of these options to specify the set of characters allowed in a one-time password:</td>
</tr>
<tr>
<td></td>
<td>• Digits (0–9)</td>
</tr>
<tr>
<td></td>
<td>• Letters &amp; Digits (A–Z, a–z, 0–9)</td>
</tr>
<tr>
<td></td>
<td>• Custom Characters — Specifies a custom set of letters and digits.  Letters are case sensitive.  To disable this requirement, set the timeout value to zero.</td>
</tr>
</tbody>
</table>
**Client Settings**

The following settings are located in the **Client Settings** area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Clients Are Allowed</td>
<td>Selecting this checkbox specifies that all McAfee OTP clients are allowed to use McAfee OTP Server.</td>
</tr>
<tr>
<td>Allowed Clients</td>
<td>Specifies a comma-separated list of IP addresses corresponding to the McAfee OTP clients that are allowed to use McAfee OTP.</td>
</tr>
<tr>
<td></td>
<td>This setting is only available when not all clients are allowed.</td>
</tr>
<tr>
<td>Allow remote configuration</td>
<td>Selecting this checkbox allows remote configuration of McAfee OTP.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Specifies the password that is required for remote configuration of McAfee OTP.</td>
</tr>
<tr>
<td></td>
<td>This setting is only available when remote configuration is allowed.</td>
</tr>
</tbody>
</table>

**Encryption**

The following settings are located in the **Encryption** area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>No encryption</td>
<td>Selecting this option specifies that messages between the McAfee OTP client and McAfee OTP are not encrypted.</td>
</tr>
<tr>
<td>Encryption if Client does encryption</td>
<td>Selecting this option specifies that messages between the McAfee OTP client and McAfee OTP are encrypted if the McAfee OTP client supports encryption.</td>
</tr>
<tr>
<td>Always encryption</td>
<td>Selecting this option specifies that messages between the McAfee OTP client and McAfee OTP are always encrypted.</td>
</tr>
<tr>
<td></td>
<td>McAfee OTP rejects messages from the McAfee OTP client that are not encrypted.</td>
</tr>
</tbody>
</table>

**Options**

The following settings are located in the **Options** area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Monitor</td>
<td>Select this checkbox to start the statistics monitor when the McAfee OTP starts.</td>
</tr>
<tr>
<td>Debug</td>
<td>Select this checkbox to display the output of the Debug function on the console.</td>
</tr>
<tr>
<td>Use Secure Random</td>
<td>Select this checkbox to use the FIPS-compliant java.security.SecureRandom algorithm when generating the one-time password for the user.</td>
</tr>
</tbody>
</table>
Global Options
The following settings are located in the Global Options area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent SQL Injection Attacks</td>
<td>Selecting this checkbox specifies that all user names and passwords are checked for the following patterns found in SQL statements: ' , ”, or, select, drop, --, insert. If any of these patterns are found, user authentication is denied.</td>
</tr>
<tr>
<td>Use Whitelist</td>
<td>Selecting this checkbox specifies that McAfee OTP only accepts characters in user names and passwords that are defined in a whitelist. To define the whitelist for SQL databases, you can use a regular expression or a list of characters.</td>
</tr>
<tr>
<td>Is RegEx</td>
<td>Selecting this checkbox allows you to define the whitelist for SQL databases using a regular expression. This option is only available when the Use whitelist checkbox is selected.</td>
</tr>
<tr>
<td>Test</td>
<td>Using this field, you can verify characters against the whitelist configured for SQL databases. This field is only available when the Use whitelist checkbox is selected.</td>
</tr>
<tr>
<td>Prevent LDAP Injection Attacks</td>
<td>Selecting this checkbox specifies that all user names are checked for the following characters: *, (, ), &amp;. If any of these characters are found, user authentication is denied.</td>
</tr>
<tr>
<td>LDAP follow referrals</td>
<td>Selecting this checkbox specifies that McAfee OTP automatically follows a referral to another LDAP directory, which is provided when a directory tree is distributed over multiple LDAP servers.</td>
</tr>
<tr>
<td>LDAP idle reconnect</td>
<td>Specifies the number of minutes that an LDAP connection can be idle before McAfee OTP forces a reconnection. A zero value disables forced reconnection.</td>
</tr>
<tr>
<td>Set System Charset</td>
<td>Selecting this checkbox allows you to specify a system character set other than UTF-8, the default. All McAfee OTP clients must be configured for the character set that you specify.</td>
</tr>
</tbody>
</table>

Configure the RADIUS object type
Use the configuration pane to configure the RADIUS object type settings.

Task
1. In the select pane, select the RADIUS object type.
2. In the configuration pane, configure the remaining settings.
RADIUS Server Settings

The following settings are located in the RADIUS Server Settings area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RADIUS</td>
<td>Selecting this checkbox enables McAfee OTP as a RADIUS server.</td>
</tr>
<tr>
<td>Port number</td>
<td>Specifies the port number that McAfee OTP Native clients use when connecting to McAfee OTP configured as a RADIUS server. Default: 1645</td>
</tr>
<tr>
<td>Bind to IP Address</td>
<td>Specifies the IP address of the server on which McAfee OTP is installed and configured as a RADIUS server.</td>
</tr>
<tr>
<td>All</td>
<td>Selecting this checkbox specifies that McAfee OTP configured as a RADIUS server accepts connections from McAfee OTP Native clients on all IP addresses assigned to the host server’s system.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the number of milliseconds that the connection between the McAfee OTP client and McAfee OTP can be idle before the RADIUS session times out. A zero value specifies that there is no timeout.</td>
</tr>
<tr>
<td>Debug Packets</td>
<td>Selecting this checkbox writes the output of the Debug function to the McAfee OTP console and log file.</td>
</tr>
<tr>
<td>Restart RADIUS Server</td>
<td>Selecting this checkbox restarts McAfee OTP each time that you update and save the RADIUS server configuration.</td>
</tr>
</tbody>
</table>

Additional Ports

The following settings are located in the Additional Ports area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Selecting this checkbox configures McAfee OTP to listen on more than one port.</td>
</tr>
<tr>
<td>Port number</td>
<td>Specifies an additional port number on which McAfee OTP listens.</td>
</tr>
<tr>
<td>Used by Client</td>
<td>Specifies the McAfee OTP client that is assigned to the specified port number.</td>
</tr>
</tbody>
</table>

Configure the Databases object type

The Databases object type contains configuration details that allow McAfee OTP to connect to a user store, read information from the user store, and authenticate users.

Contents

- Create a database
- Delete a database
- Duplicate a database
- Create an LDAP database
- Create an SQL database
- Create a RADIUS Forward database
Create a database group

Create a database
Create and add a database for connections to user stores.

Task
1 To create a database, choose from these options:
   - In the select pane, right-click the Databases object type, then select the New Database type from the context menu.
   - In the select pane, select the Databases object type, then select the New Database type on the configuration pane.
2 In the Database Display Name field, specify a unique, meaningful name.
3 In the configuration pane, configure the remaining settings.

Delete a database
Delete a database that is no longer needed.

You can also access the database actions through the File menu on the menu bar.

Task
1 In the select pane, navigate to the database.
2 Right-click the database and select Delete from the context menu.

Duplicate a database
Duplicate an existing database.

You can also access the database actions through the File menu on the menu bar.

Task
1 In the select pane, navigate to the database.
2 Right-click the database and select Duplicate Database from the context menu.
3 In the Database Display Name field, specify a unique, meaningful name.
4 In the configuration pane, configure the remaining settings.

Create an LDAP database
Create an LDAP database using the following steps.

Task
1 To select the LDAP database type, use one of these options:
   - In the select pane, right-click the Databases object type, then select the New LDAP database type from the context menu.
   - In the select pane, select the Databases object type, then select the New LDAP database type on the configuration pane.
2. To configure the new LDAP database for use with tokens based on the Open Authentication (OATH) HOTP or TOTP standard, select the **Uses HOTP or TOTP (OATH)** checkbox.

   Selecting this checkbox modifies the available settings in the Account Settings, Onetime Password Prefetch, and PIN code areas on the configuration pane.

   Select this checkbox when configuring the new LDAP database for use with Pledge, the McAfee software token.

3. On the configuration pane, configure the remaining settings.

### Host Settings

Use the configuration pane to configure the settings in the **Host Settings** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Host Address** | Specify the IP address or DNS name of the LDAP server.  
      - For multiple LDAP servers (replicas), separate the host addresses with a space character. |
| **Port number** | Specify the port number of the LDAP server.  
      - **Default**: 389 (LDAP) or 636 (LDAPS). |
| **SSL** | Select this checkbox to specify that the SSL protocol is used when communicating over a network.  
      - **SSL is an acronym for Secure Sockets Layer.** |
| **TLS** | Select this checkbox to specify that the TLS protocol is used when communicating over a network.  
      - **TLS is an acronym for Transport Layer Security.** |
| **Admin DN** | Specify the Distinguished Name (DN) of an administrative user that has read and write access to the Account Disable attribute for all user accounts.  
      - An Active Directory (AD) search using LDAP requires the DN and password of a privileged user. If the DN is not specified, McAfee OTP connects to the LDAP server using an anonymous bind. |
| **Password** | Specify the password of an administrative user that has read and write access to the Account Disable attribute for all user accounts. |
| **Test Connection** | Test the connection to the LDAP server.  
      - **This feature cannot be used with the OTP Remote Configuration tool.** |
Search Settings

Use the configuration pane to configure the settings in the Search Settings area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base DN</td>
<td>Specifies the location in the directory tree from which McAfee OTP searches for users.</td>
</tr>
</tbody>
</table>
| Scope         | Specifies the scope of the directory search:  
  - BASE — Search the Base DN only.  
  - ONE — Search the BASE DN and one level below.  
  - SUB — Search the Base DN and all levels below. |
| No of Connections | Specifies the maximum number of connections that McAfee OTP can have to the LDAP server. |
| Filter Start  | Specifies the beginning of the search filter.                               |
| Filter End    | Specifies the end of the search filter.                                    |
| Samples       | Click this button to allow the selection of a sample search that populates the Filter Start and Filter End fields with values.  
  Samples are available for Microsoft Active Directory, Novell eDirectory, and an LDAP directory. |
| Test LDAP Authentication | Test the authentication for LDAP.                                           |

Search Filters — LDAP Examples

Configure search filters that return users based on specified user attributes, or membership in specified user groups. For example, you can search for users whose mobile attribute is empty, and send those users one-time passwords by email instead of text message.

```
Filter Start = "(&(cn="
Filter End = "){objectclass=user}(mobile=*))"
Filter = "(&(cn=<username>)(objectclass=user)(mobile=*))"
```

Or you can search for all users who are members of the SMS OTP delivery method group.

```
Filter Start = "(& (cn="
Filter End = "){objectclass=user}(memberOf=CN=OTP-SMS-users,DC=company, DC=local))"
Filter = "(& (cn=<username>)){objectclass=user}(memberOf=CN=OTP-SMS-users,
(memberOf=CN=OTP-SMS-users,
DC=company,DC=local))"
```
Account Settings (HOTP/TOTP Disabled)
Use the configuration pane to configure the settings in the Account Settings area when the Uses HOTP or TOTP (OATH) checkbox is not selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTP Attribute</td>
<td>Specify the LDAP attribute that McAfee OTP uses to look up an email address, instant messaging address, or mobile phone number.</td>
</tr>
<tr>
<td></td>
<td>To specify multiple attributes, separate them with commas.</td>
</tr>
<tr>
<td>Accept Pwd change</td>
<td>Select this checkbox to allow Active Directory users to log in with the account option user must change password at next logon enabled.</td>
</tr>
<tr>
<td>Login Retries</td>
<td>Specify the maximum number of incorrect passwords that users can provide before the user’s account is locked.</td>
</tr>
<tr>
<td></td>
<td>Specifying a value for this field enables the lock user function. If you do not specify a value for this field, there is no limit to the number of incorrect passwords that users can provide. Locked accounts are automatically unlocked after a specified time period that you configure.</td>
</tr>
<tr>
<td>Locked Attribute</td>
<td>Specify the LDAP attribute that McAfee OTP reads to determine whether the user account is locked.</td>
</tr>
<tr>
<td></td>
<td>When the number of login retries exceeds the maximum, McAfee OTP sets the Locked Attribute to the Locked Value.</td>
</tr>
<tr>
<td>Locked Value</td>
<td>Specify the value of the Locked Attribute when the user account is locked.</td>
</tr>
<tr>
<td></td>
<td>When the number of login retries exceeds the maximum, McAfee OTP sets the Locked Attribute to the Locked Value.</td>
</tr>
<tr>
<td>Disable OTP Attribute</td>
<td>Specify the LDAP attribute that McAfee OTP reads to determine whether the user can log in without authenticating with a one-time password.</td>
</tr>
<tr>
<td>Disable OTP Value</td>
<td>Specify the value of the Disable OTP Attribute when authentication with a one-time password is not required.</td>
</tr>
<tr>
<td>Not</td>
<td>Select this checkbox to specify that authentication with a one-time password is not required when the Disable OTP Attribute is not set to the Disable OTP Value. Checkbox options include:</td>
</tr>
<tr>
<td></td>
<td>• Deselected — The value of the Disable OTP Attribute is the same as the value that you specify for the Disable OTP Value setting.</td>
</tr>
<tr>
<td></td>
<td>• Selected — The value of the Disable OTP Attribute is not the same as the value that you specify for the Disable OTP Value setting.</td>
</tr>
</tbody>
</table>

See also
Configure the Unlock User Accounts options on page 72

Account Settings (HOTP/TOTP Enabled)
Use the configuration pane to configure the settings in the Account Settings area when the Uses HOTP or TOTP (OATH) checkbox is selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OATH Key</td>
<td>Specifies the LDAP attribute that McAfee OTP uses to read and store the user’s OATH key.</td>
</tr>
<tr>
<td>Accept Pwd change</td>
<td>Select this checkbox to allow Active Directory users to log in with the account option user must change password at next logon enabled.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Login Retries</td>
<td>Specify the maximum number of incorrect passwords that users can provide before the user’s account is locked. Specify a value for this field enables the lock user function. If you do not specify a value for this field, there is no limit to the number of incorrect passwords that users can provide. Locked accounts are automatically unlocked after a time period that you configure.</td>
</tr>
<tr>
<td>Locked Attribute</td>
<td>Specify the LDAP attribute that McAfee OTP reads to determine whether the user account is locked.</td>
</tr>
<tr>
<td></td>
<td>When the number of login retries exceeds the maximum, McAfee OTP sets the Locked Attribute to the Locked Value.</td>
</tr>
<tr>
<td>Locked Value</td>
<td>Specify the value of the Locked Attribute when the user account is locked.</td>
</tr>
<tr>
<td></td>
<td>When the number of login retries exceeds the maximum, McAfee OTP sets the Locked Attribute to the Locked Value.</td>
</tr>
<tr>
<td>Time drift attribute (TOTP)</td>
<td>Specifies the LDAP attribute which stores a time drift value for TOTP tokens.</td>
</tr>
<tr>
<td></td>
<td>Data Type: String</td>
</tr>
</tbody>
</table>

**See also**

*Configure the Unlock User Accounts options on page 72*

**Onetime Password Prefetch**

Allow users to obtain a configurable number of one-time passwords in advance.

Onetime Password Prefetch is useful when mobile phone coverage is an issue, or to generate emergency one-time passwords, using the McAfee OTP Web Manager, when users lose or forget a mobile device. McAfee OTP can also be configured to send a new set of prefetch one-time passwords to the user each time all of the passwords are used.

Users prefetch one-time passwords through a web server that is configured with the McAfee OTP Prefetch web application. Users log on to the web application, request prefetch one-time passwords, and are sent to a mobile phone number or email address.

Click **Configure Prefetch OTP** to configure the settings for Onetime Password Prefetch.

The Onetime Password Prefetch options are only available when the Enable OTP Prefetch checkbox is selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefetch OTP Attribute</td>
<td>Select the attribute that contains the McAfee OTP prefetch string.</td>
</tr>
<tr>
<td>Enable LDAP Filter</td>
<td>(Optional) Specify an LDAP filter to allow users to use prefetch one-time passwords.</td>
</tr>
<tr>
<td>Maximum No of Prefetch OTPs</td>
<td>Specify the maximum number of prefetch one-time passwords that can be sent to a user at one time.</td>
</tr>
<tr>
<td>Must be used in order</td>
<td>Select this checkbox to specify that the prefetch one-time passwords must be used in order.</td>
</tr>
<tr>
<td></td>
<td>This option is global and applies to all user databases.</td>
</tr>
<tr>
<td>OTP Length</td>
<td>Specify the length of each prefetch one-time password in characters.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatically send new Prefetch OTPs when last OTP is used</td>
<td>Select this checkbox to specify that a new set of prefetch one-time passwords is automatically sent to users when the last password from the previous set is used.</td>
</tr>
</tbody>
</table>
| Message to user                             | Specify the message sent to users that includes the prefetched one-time password. McAfee OTP replaces the tag $$OTP$$ with the one-time password. If you omit the tag from the message, McAfee OTP appends the one-time password to the end of the message.  

  > This option is global and applies to all user databases. |
| Message Delivery                            | Specify whether to send a set of prefetch one-time passwords in one message, or multiple messages.                                                                                                         |
| Allow administration creation of Prefetch OTP | Select this checkbox to allow administrators to create prefetch one-time passwords for any user.                                                                                                          

  > Deselecting this checkbox limits requests for prefetch one-time passwords to users themselves. |
| Administrator Database                       | Specify the McAfee OTP database to use when authenticating the administrator or group of administrators that can create prefetch one-time passwords for users.                                                   |
| Allowed IP Addresses                         | Specify a comma-separated list of client IP addresses from which an administrator can create prefetch one-time passwords.                                                                                   |

**PIN Code**

Use PINs to add a layer of security to the one-time password process.

When prompted for a one-time password, users must first enter the PIN, then the one-time password without a space separating the two strings.

For example, if the PIN is 1234, and the one-time password is OTPOTP, the resulting string is 1234OTPOTP.

Users and technical support create PINs using the McAfee OTP Web Manager.

The PIN configuration options include hashed PIN. McAfee OTP supports these hash algorithms:

- SHA1
- Secure SHA256 (SSHA256)

SHA is an acronym for Secure Hash Algorithm. The Secure SHA256 algorithm is also known as the Salted SHA256 algorithm.

To configure the PIN settings, click Configure PIN Code.

  > The PIN configuration options are only available when the Enable PIN Code checkbox is selected.
### Configuring McAfee OTP server, RADIUS object, and databases

Configure the Databases object type

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select LDAP attribute for the PIN code</td>
<td>Select the attribute where the PIN is stored.</td>
</tr>
<tr>
<td></td>
<td>The PIN must be stored in the same attribute in the LDAP database as in the McAfee OTP database. If you leave the attribute setting empty, McAfee OTP accepts the one-time password without the PIN.</td>
</tr>
<tr>
<td>Show advanced hashed PIN code options (Global)</td>
<td>Select this checkbox to enable hashed PINs.</td>
</tr>
<tr>
<td></td>
<td>All hashed PIN options are global and apply to all user databases.</td>
</tr>
<tr>
<td>Digest Charset</td>
<td>Specify the character set used by the user store where the hashed PINs are saved.</td>
</tr>
<tr>
<td>Default</td>
<td>ISO–8859–1</td>
</tr>
<tr>
<td></td>
<td>This setting is only available when configuring hashed PINs.</td>
</tr>
<tr>
<td>Hashed value format</td>
<td>Choose one of these formats to use when reading hashed PINs:</td>
</tr>
<tr>
<td></td>
<td>• Base64</td>
</tr>
<tr>
<td></td>
<td>• Hexadecimal</td>
</tr>
<tr>
<td></td>
<td>This setting is only available when configuring hashed PINs.</td>
</tr>
</tbody>
</table>

### Advanced options

Use the configuration pane to configure the settings in the Advanced options area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Databasehandler</td>
<td>Select this checkbox to allow the extension of the database handler with your own Java class. In the field that opens, specify a Java class name that extends se.nordicedge.radius.DBHandler.</td>
</tr>
</tbody>
</table>

### Create an SQL database

Create an SQL database using the following steps.

#### Task

1. To select the SQL database type, use one of these options:
   - In the select pane, right-click the Databases object type, then select the New SQL database type from the context menu.
   - In the select pane, right-click the Databases object type, then select the New SQL database type on the configuration pane.

2. In the Database Display Name field, specify a unique, meaningful name.
3 To configure the new SQL database for use with tokens based on the Open Authentication (OATH) HOTP or TOTP standard, select the Uses HOTP or TOTP (OATH) checkbox.

Select this checkbox to modify the available settings in the SQL Queries area on the configuration pane.

Select this checkbox when configuring the new SQL database for use with Pledge, the McAfee software token installed on a mobile device.

4 On the configuration pane, configure the remaining settings.

### JDBC/ODBC Settings

Use the configuration pane to configure the settings in the JDBC/ODBC Settings area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver Manager</td>
<td>Specify the Driver Manager using JDBC syntax.</td>
</tr>
<tr>
<td></td>
<td><strong>ODBC example:</strong> sun.jdbc.odbc.JdbcOdbcDriver</td>
</tr>
<tr>
<td></td>
<td><strong>MySQL example:</strong> com.mysql.jdbc.Driver</td>
</tr>
<tr>
<td>Database URL</td>
<td>Specify the Database URL of the JDBC/ODBC database.</td>
</tr>
<tr>
<td></td>
<td><strong>ODBC example:</strong> jdbc:odbc:Databasename</td>
</tr>
<tr>
<td></td>
<td><strong>MySQL example:</strong> jdbc:mysql://Ipaddress:portnr:/dbname</td>
</tr>
<tr>
<td>Samples</td>
<td>Provides sample settings for the Driver Manager and Database URL fields.</td>
</tr>
<tr>
<td>Username</td>
<td>Specify the user name for the JDBC/ODBC database.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password for the JDBC/ODBC database.</td>
</tr>
<tr>
<td>No of conns</td>
<td>Specify the number of concurrent database connections in the connection pool available to McAfee OTP.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Test the database connection.</td>
</tr>
</tbody>
</table>

### SQL Queries (HOTP/TOTP Disabled)

Use the configuration pane to configure the settings in the SQL Queries area when the Uses HOTP or TOTP (OATH) checkbox is not selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>Specify the SQL query used for authentication, which must return the user name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> SELECT NAME FROM UserDB WHERE NAME='$$NAME$$' AND PASSWORD='$$PASSWORD$$'</td>
</tr>
<tr>
<td>OTP Field</td>
<td>Specify the SQL query that retrieves the mobile phone number or email address from the user’s account.</td>
</tr>
<tr>
<td></td>
<td>In the query, use the $$NAME$$ tag for the user name.</td>
</tr>
<tr>
<td>Login Retries</td>
<td>Specify the maximum number of incorrect passwords that users can provide before the user’s account is locked.</td>
</tr>
<tr>
<td></td>
<td>Specify a value for this field to enable the lock user function. If a value for this field is not specified, there is no limit to the number of incorrect passwords that users can provide. Locked accounts are automatically unlocked after a time period that you configure.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get Locked (Get Disabled)</td>
<td>Specify the SQL query that reads whether the user account is locked.</td>
</tr>
<tr>
<td></td>
<td>Use the $$NAME$$ tag for the user name in the SQL query.</td>
</tr>
<tr>
<td><strong>Example</strong>: SELECT disabled FROM users WHERE name='$$NAME$$' AND disabled='TRUE'</td>
<td></td>
</tr>
<tr>
<td>Set Locked (Set Disabled)</td>
<td>Specify the SQL query to execute when the maximum number of Login Retries is exceeded.</td>
</tr>
<tr>
<td></td>
<td>Use the $$NAME$$ tag for the user name in the SQL query.</td>
</tr>
<tr>
<td><strong>Example</strong>: UPDATE users SET disabled='TRUE' WHERE name='$$NAME$$'</td>
<td></td>
</tr>
<tr>
<td>Get Disable OTP</td>
<td>Specify the SQL query that determines whether the user can log in without a one-time password.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: SELECT skipotpflag UserTable WHERE name='$$NAME$$'</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a value for this field, authentication with a one-time password is always required.</td>
</tr>
<tr>
<td>Test Authentication</td>
<td>Test the authentication.</td>
</tr>
</tbody>
</table>

**See also**

Configure the Unlock User Accounts options on page 72

**SQL Queries (HOTP/TOTP Enabled)**

Use the configuration pane to configure the settings in the SQL Queries area when the Uses HOTP or TOTP (OATH) checkbox is selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>Specify the SQL query used for authentication, which must return the user name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: SELECT NAME FROM UserDB WHERE NAME='$$NAME$$' AND PASSWORD='$$PASSWORD$$'</td>
</tr>
<tr>
<td>Get OATHKey</td>
<td>Specify the SQL query that retrieves the OATH key from the user’s account.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: SELECT OATHKey FROM UserDB WHERE NAME='$$NAME$$'</td>
</tr>
<tr>
<td>Set OATHKey</td>
<td>Specify the SQL query that sets the OATH key in the user’s account.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: UPDATE users SET OATHKey ='$$KEY$$' WHERE name='$$NAME$$'</td>
</tr>
<tr>
<td>Login Retries</td>
<td>Specify the maximum number of incorrect passwords that users can provide before the user’s account is locked.</td>
</tr>
<tr>
<td></td>
<td>Specify a value for this field to enable the lock user function. If a value for this field is not specified, there is no limit to the number of incorrect passwords that users can provide. Locked accounts are automatically unlocked after a time period that you configure.</td>
</tr>
<tr>
<td>Get Locked (Get Disabled)</td>
<td>Specify the SQL query that reads whether the user account is locked.</td>
</tr>
<tr>
<td></td>
<td>Use the $$NAME$$ tag for the user name in the SQL query.</td>
</tr>
<tr>
<td><strong>Example</strong>: SELECT disabled FROM users WHERE name='$$NAME$$' AND disabled='TRUE'</td>
<td></td>
</tr>
</tbody>
</table>
### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Locked (Set Disabled)</td>
<td>Specify the SQL query to execute when the maximum number of login retries is exceeded.</td>
</tr>
<tr>
<td></td>
<td>Use the $$NAME$$ tag for the user name in the SQL query.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> UPDATE users SET disabled='TRUE' WHERE name='$$NAME$$'</td>
</tr>
<tr>
<td>Test Authentication</td>
<td>Test the authentication.</td>
</tr>
</tbody>
</table>

See also

*Configure the Unlock User Accounts options on page 72*

### Onetime Password Prefetch

The SQL database **Onetime Password Prefetch** settings are the same as the LDAP database.

See also

*Onetime Password Prefetch on page 40*

### PIN code

The SQL database **PIN code** settings are the same as the LDAP database.

See also

*PIN Code on page 41*

### Advanced options

The SQL database **Advanced options** settings are the same as the LDAP database.

See also

*Advanced options on page 42*

### Create a RADIUS Forward database

Use a RADIUS Forward database to allow McAfee OTP to pass through and forward RADIUS requests to a third-party RADIUS Server, which supports RSA SecurID and SafeWord tokens.

#### Task

1. To select the **RADIUS Forward** database type, use one of these options:
   - In the select pane, right-click the **Databases** object type, then select the **New RADIUS Forward** database type from the context menu.
   - In the select pane, right-click the **Databases** object type, then select the **New RADIUS Forward** database type in the configuration pane.
2. In the **Database Display Name** field, specify a unique, meaningful name.
3. Click **Add RADIUS Server**, then specify the IP address and port number of the RADIUS server. McAfee OTP uses this information when forwarding requests to the server.
4 (Optional) To remove a RADIUS server, select it, then click Remove RADIUS Server.

5 On the configuration pane, configure the remaining options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>Specify the secret shared by the McAfee OTP server and the RADIUS server.</td>
</tr>
<tr>
<td>Forward additional RADIUS</td>
<td>Specify whether the McAfee OTP server forwards additional RADIUS attributes to the other RADIUS server.</td>
</tr>
<tr>
<td>attributes</td>
<td></td>
</tr>
<tr>
<td>Test RADIUS request</td>
<td>Test authentication to the selected RADIUS server.</td>
</tr>
</tbody>
</table>

**Create a database group**

Configure multiple McAfee OTP databases as a group.

Database groups can include LDAP, JDBC, and RADIUS Forward databases, or a combination.

When databases are configured as a group, McAfee OTP searches them in the order that they are listed on the configuration pane. When a matching user name and password are found in a specified database for a specified user, McAfee OTP uses that database for that user.

- LDAP and JDBC databases must be configured before they can be added to a database group.

**Task**

1 To select the **Database group** database type, use one of these options:
   - In the select pane, right-click the **Databases** object type, then select the **Database Group** database type from the context menu.
   - In the select pane, right-click the **Databases** object type, then select the **Database Group** database type in the configuration pane.

2 In the **Database Display Name** field, specify a unique, meaningful name.

3 In the **Database Group Settings** area, click **Add Database**, then select one or more databases.

4 Click **Up** and **Down** to position the selected databases in the list.

5 (Optional) To remove a database from the database group, click **Remove Database**.
Configuring the Clients object type

McAfee OTP uses McAfee OTP client objects to manage connections to McAfee OTP clients. These McAfee OTP clients are supported:

- **RADIUS** — Use the RADIUS challenge-response protocol to communicate with McAfee OTP. **Examples:** Firewall and VPN (BlueCoat, Cisco, Citrix, F5, and Juniper)
- **Native** — Communicate with McAfee OTP using the API that it provides. **Examples:** CA SiteMinder, Microsoft Outlook Web Access, Microsoft SharePoint, and Novell GroupWise Web Access.
- **Web services** — Use SOAP-based web services implemented through an API to communicate with McAfee OTP.

See also

Contents
- Create a client
- Delete a client
- Duplicate a client
- Create a RADIUS client
- Create a Native client
- Create a Web services client

Create a client

Create a McAfee OTP client object to manage connections to McAfee OTP clients.

Task

1. To create a client, choose from these options:
   - In the select pane, right-click the Clients object type, then select the New Client type from the context menu.
   - In the select pane, select the Clients object type, then select the New Client type in the configuration pane.

2. In the Client Display Name field, specify a unique, meaningful name.

3. In the configuration pane, configure the remaining settings.
Delete a client
Delete a client that is no longer needed.

Task
1. In the select pane, navigate to the client.
2. Right-click the client, and select Delete from the context menu.

Duplicate a client
Duplicate an existing client.

Task
1. In the select pane, navigate to the client.
2. Right-click the client and select Duplicate Client from the context menu.
3. In the Client Display Name field, specify a unique, meaningful name.
4. In the configuration pane, configure the remaining settings.

Create a RADIUS client
Create a RADIUS client using the following steps.

Task
1. To select the RADIUS client type, use one of these options:
   • In the select pane, right-click the Clients object type, then select the New RADIUS client type from the context menu.
   • In the select pane, right-click the Clients object type, then select the New RADIUS client type in the configuration pane.
2. In the Client Display Name field, specify a unique, meaningful name.
3. In the Client IP Address field, specify the IP address of the RADIUS client.
   • Do not specify a DNS name.
   • You can specify multiple IP addresses by using a wildcard character, such as “*”.
4. In the configuration pane, configure the remaining settings.

Advanced
Click Advanced to configure the RADIUS client settings.

Contents
- RADIUS Client Attribute Detection
- Listen on RADIUS Ports
- Encoding
- RADIUS Reject Error Messages
**RADIUS Client Attribute Detection**

Specify a different client configuration and database for each user group at the same IP address, differentiate between user groups, such as employees, partners, and customers, and enable different authentication methods for each user group at the same IP address.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Attribute Detection</td>
<td>Specifies whether the RADIUS attribute detection feature is enabled.</td>
</tr>
<tr>
<td>RADIUS attribute number</td>
<td>Specifies a RADIUS attribute by number.</td>
</tr>
<tr>
<td>RADIUS attribute value</td>
<td>Specifies a value for the selected RADIUS attribute.</td>
</tr>
<tr>
<td>Match type</td>
<td>Specifies whether the match must be exact.</td>
</tr>
<tr>
<td>Match case</td>
<td>Specifies whether the match is case sensitive.</td>
</tr>
</tbody>
</table>

**Listen on RADIUS Ports**

Specify the RADIUS port numbers on which McAfee OTP listens.

> The **Listen on RADIUS Ports** settings are only available when McAfee OTP is configured as a RADIUS server, and **Additional Ports** are enabled in the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen on ALL available port numbers</td>
<td>Specify whether McAfee OTP listens on all RADIUS port numbers.</td>
</tr>
<tr>
<td>Selected ports</td>
<td>Specify one or more RADIUS port numbers on which McAfee OTP listens.</td>
</tr>
</tbody>
</table>

**Encoding**

Use the configuration pane to configure the settings in the **Encoding Settings** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charset encoding</td>
<td>Specifies a system character set.</td>
</tr>
</tbody>
</table>

> The RADIUS standard uses UTF-8 encoding to transform packet data to strings.

**RADIUS Reject Error Messages**

Configure user error messages that are sent when authentication fails.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Auth/Error</td>
<td>Specify the message that is sent when the user fails to authenticate or a system error occurs.</td>
</tr>
</tbody>
</table>

> • This message is sent by RADIUS attribute 18.  
> • To disable this message, leave this field blank.

| Failed OTP | Specifies a message that is sent when the user's one-time password fails. |

> • This message is sent by RADIUS attribute 18.  
> • To disable this message, leave this field blank.
## RADIUS Options

Use the configuration pane to configure the settings in the **RADIUS Options** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Specify the RADIUS client’s shared secret. The RADIUS client and the RADIUS client application must have the same shared secret.</td>
</tr>
<tr>
<td><strong>Supports RADIUS Access-Challenge</strong></td>
<td>Select this checkbox to specify that the RADIUS client supports the RADIUS challenge-response protocol.</td>
</tr>
<tr>
<td><strong>Response Message</strong></td>
<td>Specify the message that is sent to the RADIUS client for prompting the user to enter a one-time password. This field is only available when the RADIUS client supports the challenge-response protocol.</td>
</tr>
<tr>
<td><strong>Allow multiple user requests</strong></td>
<td>Select this checkbox to allow a user to request one-time passwords from multiple RADIUS endpoints. This setting is useful when single users are requesting one-time passwords from redundant VPN servers. This field is only available when the RADIUS client does not support the challenge-response protocol.</td>
</tr>
<tr>
<td><strong>Auth. Server IP Address</strong></td>
<td>Specify the IP address of the RADIUS client, VPN, or firewall. This field is only available when the RADIUS client does not support the challenge-response protocol.</td>
</tr>
</tbody>
</table>

## Prefetch OTP Options

Use the **Prefetch OTP Options** for RADIUS clients that do not support the challenge-response protocol.

The **Prefetch OTP Options** are only available when the RADIUS client is configured to use only prefetch one-time passwords.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use ONLY OATH OTP or Prefetch OTPs</strong></td>
<td>Select this checkbox to specify using only OATH tokens or prefetch one-time passwords. This checkbox is only available when the RADIUS client does not support the challenge-response protocol.</td>
</tr>
<tr>
<td><strong>Require Password AND Prefetch OTP</strong></td>
<td>Specify that users must enter a string which is the concatenation of the database password and the one-time password. This setting is only available when prefetch one-time passwords are enabled. Example: dbpassword012345</td>
</tr>
<tr>
<td><strong>Generate Prefetch OTP if none exists</strong></td>
<td>When users log on with user name and password, specify the ability to generate prefetch one-time passwords if none exist. This setting is only available when prefetch one-time passwords are enabled.</td>
</tr>
</tbody>
</table>
User Database
From the User Database drop-down list, select one of the configured databases for the RADIUS client to use.

See also
Configure the Databases object type on page 35

Other options
Use the configuration pane to configure the settings in the Other options area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses external OTP API</td>
<td>Select this checkbox to specify that the external code using the API generates and verifies the one-time password instead of McAfee OTP. Type the Java class name that implements the interface in the field that opens: se.nordicedge.interfaces.OTPVerificationHandler</td>
</tr>
<tr>
<td>Uses external OTP API</td>
<td>Click Radius Attributes to specify attributes that are sent following successful authentication. In the interface that opens, add each attribute and attribute number to the attribute list. Attribute values include: • Static Value • Login Name • UserDN • external code • User Attribute</td>
</tr>
<tr>
<td>Force OTP Delivery Method</td>
<td>Select a delivery method from the drop-down list. This setting overrides the McAfee OTP default, which uses the delivery methods in the order they are configured by the administrator.</td>
</tr>
</tbody>
</table>

Create a Native client
Create a Native OTP client using the following steps.

Task
1 To select the Native client type, use one of these options:
   • In the select pane, right-click the Clients object type, then select the New Native client type from the context menu.
   • In the select pane, right-click the Clients object type, then select the New Native client type in the configuration pane.

2 In the Client Display Name field, specify a unique, meaningful name.
   Example: CA SiteMinder.

3 In the Client IP Address field, specify the IP address of the Native client.
   • Do not specify a DNS name.
   • You can specify multiple IP addresses by using a wildcard character, such as “*”.

4 In the configuration pane, configure the remaining settings.
Advanced — Native Client Name Detection

McAfee OTP uses the name of the integration module to differentiate between user groups at the same IP address, and applies a different client configuration and database to each one.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Name Detection</td>
<td>Select this checkbox to enable the Native Client Name Detection feature, and enable different authentication methods for each user group at the same IP address.</td>
</tr>
<tr>
<td>Client Name</td>
<td>Specify the client name used by the integration module.</td>
</tr>
</tbody>
</table>

**Options**

Use the configuration pane to configure the settings in the **Options** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept User Lookup only</td>
<td>Select this checkbox to allow McAfee OTP to look up users based on user name only, issue one-time passwords, and enable authentication with a one-time password instead of user name and password. The password field can be empty.</td>
</tr>
<tr>
<td>Client Name</td>
<td>Specify the client name used by the integration module. This field is available when Accept User Lookup only is selected.</td>
</tr>
</tbody>
</table>

**User Database**

From the User Database drop-down list, select one of the configured databases for the Native client to use.

**See also**

*Configure the Databases object type on page 35*

**Other options**

Use the configuration pane to configure the settings in the **Other options** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses external OTP API</td>
<td>Select this checkbox to specify that the external code using the API generates and verifies the one-time password instead of McAfee OTP Server. Type the Java class name that implements the interface in the field that opens: se.nordicedge.interfaces.OTPVerificationHandler</td>
</tr>
<tr>
<td>Force OTP Delivery Method</td>
<td>Select an McAfee OTP delivery method from the drop-down list. This setting overrides the McAfee OTP default, which uses the delivery methods in the order they are configured by the administrator.</td>
</tr>
</tbody>
</table>
Create a Web services client

Create a Web services client using the following steps.

**Task**

1. To select the Web services client type, use one of these options:
   - In the select pane, right-click the Clients object type, then select the New Web services client type from the context menu.
   - In the select pane, right-click the Clients object type, then select the New Web services client type in the configuration pane.

2. In the WS Client Name field, specify a unique, meaningful name.
   - The name must correspond to the client name in the client’s web services requests.

3. In the WS Client Password field, specify a password for the Web services client.

4. In the configuration pane, configure the remaining settings.

**Options**

Use the configuration pane to configure the settings in the Options area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept User Lookup only</td>
<td>Select this checkbox to allow McAfee OTP to look up users based on user name only and issue one-time passwords, and enable authentication with a one-time password instead of user name and password.</td>
</tr>
<tr>
<td></td>
<td>The password field can be empty.</td>
</tr>
</tbody>
</table>

**User Database**

From the User Database drop-down list, select one of the configured databases for the Web services client to use.

**See also**

*Configure the Databases object type on page 35*

**Other Options**

Use the configuration pane to configure the settings in the Other Options area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses external OTP API</td>
<td>Selecting this checkbox specifies that the external code using the API generates and verifies the one-time password instead of McAfee OTP. Type the Java class name that implements the interface in the field that opens: se.nordicedge.interfaces.OTPVerificationHandler</td>
</tr>
<tr>
<td>Force OTP Delivery Method</td>
<td>Selects an McAfee OTP delivery method from the drop-down list of configured methods for McAfee OTP to use.</td>
</tr>
<tr>
<td></td>
<td>This setting overrides the McAfee OTP default, which uses the delivery methods in the order they are configured by the administrator.</td>
</tr>
</tbody>
</table>
Configuring the Clients object type
Create a Web services client
Configuring the Delivery Method object type

Configure one or more methods for McAfee OTP to use to deliver one-time passwords. These options are available:
- **Show all** — Displays all delivery method types.
- **Show enabled** — Displays enabled delivery method types only.
- **Show disabled** — Displays disabled delivery method types only.

Contents
- Enable a delivery method type
- Configure the SMS Gateway delivery method
- Configure the HTTP delivery method
- Configure the Extended HTTP delivery method
- Configure the SMTP delivery method
- Configure the Netsize delivery method
- Configure the Concurrent Sender delivery method
- Configure the SMPP delivery method
- Configure the CIMD2 delivery method
- Configure the UCP File delivery method
- Configure the Prefetch Detection delivery method
- Configure McAfee Voice delivery method

Enable a delivery method type

Enable a delivery method type for McAfee OTP to use to deliver one-time passwords.

**Task**
1. In the select pane, right-click the Delivery Method object type, then select the Delivery object type.
2. In the configuration pane, enable the Delivery object type.
3. To change the order the delivery method types are used, right-click the Delivery method type, then select Move up or Move down.
Configure the SMS Gateway delivery method

McAfee SMS module is a plug-in that delivers one-time passwords to users using the McAfee SMS Gateway. The module provides status controls, usage statistics, and automatic failover for lapses in SMS service.

**Task**
1. In the select pane, expand the **Delivery Methods** object type, then select **McAfee SMS**.
2. In the configuration pane, select the **Enable McAfee SMS Gateway** checkbox.
3. Configure the remaining settings.

**General Settings and Proxy areas**

Use the configuration pane to configure the settings in the **General Settings** and **Proxy** areas.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Specify the user name for the McAfee SMS service.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password for the McAfee SMS service.</td>
</tr>
<tr>
<td>Flash SMS</td>
<td>Select this checkbox to allow McAfee SMS service to send Flash SMS messages to a mobile phone.</td>
</tr>
<tr>
<td>Message</td>
<td>Specify the one-time password message sent to mobile phones. <strong>In the message, the one-time password replaces the $$OTP$$ tag. If the tag is omitted, the one-time password appends to the end of the message.</strong></td>
</tr>
<tr>
<td>Enable HTTP proxy server</td>
<td>Select this checkbox to enable support for an HTTP proxy server. <strong>This setting is required when McAfee OTP is installed on a server that cannot access the Internet without going through an HTTP proxy.</strong></td>
</tr>
<tr>
<td>Server</td>
<td>Specify the DNS name or IP address of the HTTP proxy server. <strong>This field is only available when the HTTP proxy server is enabled.</strong></td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port number of the HTTP proxy server. <strong>This field is only available when the HTTP proxy server is enabled.</strong></td>
</tr>
<tr>
<td>Disable PF SMS Status</td>
<td>Select this checkbox to send a message to the McAfee SMS Gateway disabling SMS status control for users that have prefetch one-time passwords stored in the user database, reducing the waiting time for these passwords.</td>
</tr>
<tr>
<td>Username in accounting file</td>
<td>Select this checkbox to include the user name in the McAfee OTP log accounting file. <strong>If you are not using the accounting file, you can ignore this setting.</strong></td>
</tr>
<tr>
<td>Validate SSL Certificates</td>
<td>Select this checkbox to enable SSL certificate validation.</td>
</tr>
</tbody>
</table>
Location
Select the geographic area that corresponds to your location.

Configuration and Status
To configure the settings in the Configuration and Status area, click Request a demo account.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>Send a test SMS message to a mobile phone through McAfee SMS Gateway.</td>
</tr>
<tr>
<td>Update Config</td>
<td>Manually update the configuration for the McAfee SMS Gateway service.</td>
</tr>
<tr>
<td>Debug</td>
<td>Write SMS debug information to the log files.</td>
</tr>
</tbody>
</table>

Advanced
Click Advanced to open the following settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable max Limit</td>
<td>Set thresholds for SMS delivery.</td>
</tr>
<tr>
<td>Max SMS per user per day</td>
<td>Maximum number of SMS messages that each user can send in one day.</td>
</tr>
<tr>
<td>Max SMS total per day</td>
<td>Total number of SMS messages that all users can send in one day.</td>
</tr>
</tbody>
</table>

Configure the HTTP delivery method
Send one-time passwords using the HTTP or HTTPS protocol to an SMS provider.

Task
1. In the select pane, expand the Delivery Methods object type, then select HTTP.
2. In the configuration pane, select the Enable HTTP checkbox.
3. Configure the remaining settings.
   - For more information, contact your SMS provider.

Headers or Template file
Use the configuration pane to configure the settings in the Headers or Template file area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Header</td>
<td>The name of the HTTP header corresponding to the user’s mobile phone number or email address.</td>
</tr>
<tr>
<td>OTP Header</td>
<td>The name of the HTTP header corresponding to the one-time password.</td>
</tr>
<tr>
<td>Headers in Query String</td>
<td>Include HTTP headers in the query string as GET parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>?USER=070112233&amp;CHALLENGE=123456</td>
</tr>
<tr>
<td>Template file</td>
<td>Name of the template file that replaces HTTP headers.</td>
</tr>
</tbody>
</table>

- The template file must contain the following two tags: $$IDENTITY$$ and $$CHALLENGE$$.
- To use headers only, leave this field blank.
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Accept SSL</td>
<td>Allows McAfee OTP to automatically trust SSL certificates received over HTTPS.</td>
</tr>
<tr>
<td>Debug</td>
<td>Enables logging of HTTP messages.</td>
</tr>
</tbody>
</table>

**Authentication**

Use the configuration pane to configure the settings in the Authentication area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HTTP Authentication</td>
<td>Enables HTTP authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>User name required for HTTP authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Password required for HTTP authentication.</td>
</tr>
</tbody>
</table>

**Proxy**

Use the configuration pane to configure the settings in the Proxy area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Proxy Server</td>
<td>Enable HTTP requests and responses through a proxy server.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>DNS name of the proxy server.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>Port number of the proxy server.</td>
</tr>
</tbody>
</table>

**Other Settings**

Use the configuration pane to configure the settings in the Other Settings area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Type</td>
<td>Content type of HTTP email messages using the MIME standard.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: application/x-www-form-urlencoded</td>
</tr>
<tr>
<td>HTTP(S) URL</td>
<td>URL where the one-time password is posted.</td>
</tr>
<tr>
<td>Success String</td>
<td>The string that the HTTP server sends to McAfee OTP when the one-time password is posted successfully.</td>
</tr>
</tbody>
</table>

**Configure the Extended HTTP delivery method**

The Extended HTTP delivery method offers more configuration options than the HTTP delivery method.

**Task**

1. In the select pane, expand the Delivery Methods object type, then select Extended HTTP.
2. In the configuration pane, select the Enable Extended HTTP Sender checkbox.
3. Configure the remaining settings.
### Headers or Template file

Use the configuration pane to configure the settings in the **Headers or Template file** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Header</td>
<td>The name of the HTTP header corresponding to the user's mobile phone number or email address.</td>
</tr>
<tr>
<td>OTP Header</td>
<td>The name of the HTTP header corresponding to the one-time password.</td>
</tr>
<tr>
<td>Remove leading +</td>
<td>Removes the leading “+” character from mobile phone numbers.</td>
</tr>
<tr>
<td>Replace + with 00</td>
<td>Removes the leading “+” character from mobile phone numbers, and replaces it with two zeros.</td>
</tr>
</tbody>
</table>
| Template File   | The name of the template file that replaces HTTP headers. The template file must contain the following two tags: $$IDENTITY$$ and $$CHALLENGE$$.  
|                 | To use headers only, leave this field blank.                              |
| Edit            | Allows you to edit the template file.                                     |
| Auto-Accept SSL Certificates | Allows McAfee OTP to automatically trust SSL certificates received over HTTPS. |
| Debug           | Enables logging of HTTP messages.                                         |
| Use GET         | Specifies GET as the HTTP method in place of POST.                        |
Authentication and Proxy

Use the configuration pane to configure the settings in the Authentication and Proxy area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Proxy Server | Enables HTTP requests and responses through a proxy server.  
• Proxy Server — The DNS name of the proxy server.  
   - This field opens when the proxy server is enabled.  
• Proxy Port — The port number of the proxy server.  
   - This field opens when the proxy server is enabled. |
| HTTP Auth  | Enables HTTP authentication.  
• Username — The user name required for authentication.  
   - This field opens when HTTP authentication is enabled.  
• Password — The password required for authentication.  
   - This field opens when HTTP authentication is enabled. |
| Client Cert | Enables certificate authentication.  
• PKCS12 file — The full path name to the certificate file.  
   - This field opens when certificate authentication is enabled.  
• Password — The password required to decrypt the certificate file.  
   - This field opens when certificate authentication is enabled.  
   | Certificate authentication requires HTTPS. |

Other Settings

Use the configuration pane to configure the settings in the Other Settings area.

McAfee OTP uses the URLs in the order that you specify them. If one URL fails, McAfee OTP fails over to the last working URL.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Content Type      | The content type of HTTP email messages using the MIME standard.  
   Default: application/x-www-form-urlencoded |
| HTTP(/S) URL 1    | The first of three URLs where McAfee OTP can post the one-time password. |
| HTTP(/S) URL 2    | The second of three URLs where McAfee OTP can post the one-time password. |
| HTTP(/S) URL 3    | The third of three URLs where McAfee OTP can post the one-time password. |
| Success String    | The string that the HTTP server sends to McAfee OTP when the one-time password is posted successfully. Without this string, McAfee OTP continues processing as though the post failed.  
   Default: application/x-www-form-urlencoded |
| Set SOAP Action request header | Adds a SOAP Action header field to the HTTP request. |
Configure the SMTP delivery method

Send one-time passwords using the SMTP protocol.

- SMTP is an acronym for Simple Message Transfer Protocol.
- McAfee OTP sends all messages containing the “@” character to users by SMTP.

**Task**

1. In the select pane, expand the Delivery Methods object type, and select **SMTP**.
2. In the configuration pane, select the **Enable SMTP** checkbox.
3. Configure the remaining settings.

**SMTP Host**

Use the configuration pane to configure the settings in the SMTP Host area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Host</td>
<td>The IP address or DNS name of the SMTP host.</td>
</tr>
<tr>
<td>Mime Encoding</td>
<td>The MIME encoding for messages delivered by the SMTP method.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number of the SMTP host.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>Use the SSL or TLS protocol.</td>
</tr>
<tr>
<td>Force TLS</td>
<td>Use TLS, not SSL.</td>
</tr>
</tbody>
</table>

**Authentication**

Use the configuration pane to configure the settings in the Authentication area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SMTP Auth</td>
<td>Enables SMTP authentication.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name required for SMTP authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required for SMTP authentication.</td>
</tr>
</tbody>
</table>

**SMTP Options**

Use the configuration pane to configure the settings in the SMTP Options area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail sender address</td>
<td>The address of the email sender.</td>
</tr>
<tr>
<td>Mail To Address</td>
<td>The address of the email recipient.</td>
</tr>
<tr>
<td>Mail address</td>
<td>Use the user’s email address as the recipient’s address, and disable the Mail To Address field.</td>
</tr>
</tbody>
</table>
### Configure the Netsize delivery method

Send one-time passwords using the Netsize SMS Gateway.

A Netsize account is required.

#### Task
1. In the select pane, expand the Delivery Methods object type, and select Netsize.
2. In the configuration pane, select the Enable Netsize checkbox.
3. Configure the remaining settings.

#### Communication

Use the configuration pane to configure the settings in the Communication area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Gateway</td>
<td>Specifies the IP address or DNS name of the Netsize SMS Gateway.</td>
</tr>
<tr>
<td>Port nr</td>
<td>Specifies the port number of the Netsize SMS Gateway.</td>
</tr>
</tbody>
</table>
Authentication
Use the configuration pane to configure the settings in the Authentication area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Specifies the user name required for authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password required for authentication.</td>
</tr>
</tbody>
</table>

Message
Use the configuration pane to configure the settings in the Message area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Specifies the message to send to the mobile phone that includes the one-time password. McAfee OTP replaces the $OTP$ tag in the message with the one-time password. If the tag is omitted from the message, McAfee OTP appends the one-time password to the end of the message.</td>
</tr>
</tbody>
</table>

Consulting the Browse button opens the editor.

Endpoint Settings
Use the configuration pane to configure the settings in the Endpoint Settings area.

Use these available settings:

- Sending (MT)
- Receive (MO)
- Notification (SR)

Consult your Netsize customer service representative for more information.

Options
Use the configuration pane to configure the settings in the Options area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>Selecting this checkbox enables debugging of Netsize packets in the console or log files.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Selecting this checkbox enables encryption. This function requires coordination between McAfee OTP and the Netsize SMS Gateway. Consult your Netsize customer service representative for more information.</td>
</tr>
</tbody>
</table>
| Message Type | Specifies the presentation of the message on the mobile phone. Select one of the following options:  
- Immediate Display (Flash)  
- Stored on Mobile phone  
- Stored on SIM-card |
Configure the Concurrent Sender delivery method

Simultaneously send one-time passwords using two or more delivery methods.

**Task**
1. In the select pane, expand the **Delivery Methods** object type, and select **Concurrent Sender**.
2. In the configuration pane, select the **Enable Concurrent Sender** checkbox.
3. From the **Add Method** drop-down list, select the delivery method, then click **Add**.
   - The method is added to the **Sending methods** list.
4. (Optional) To remove a delivery method from the **Sending methods** list, select the delivery method, then click **Delete**.

Configure the SMPP delivery method

Send one-time passwords using the SMPP protocol.

```
| SMPP is an acronym for Short Message Peer-to-Peer. |
```

**Task**
1. In the select pane, expand the **Delivery Methods** object type, and select **SMPP**.
2. In the configuration pane, select the **Enable SMPP** checkbox.
3. Configure the remaining settings.

Configure the CIMD2 delivery method

Send one-time passwords using the proprietary Nokia CIMD2 protocol.

**Task**
1. In the select pane, expand the **Delivery Methods** object type, then select **CIMD2**.
2. In the configuration pane, select the **Enable CIMD2** checkbox.
3. Configure the remaining settings.

Configure the UCP File delivery method

Create one UCP file for each one-time password. Use this method when one-time passwords are processed by modem software, and then sent by text message to users.

```
| UCP is an acronym for Uniformity Correction Parameters. |
```
**Task**

1. In the select pane, expand the **Delivery Methods** object type, then select **UCP File**.
2. In the configuration pane, select the **Enable UCP File** checkbox.
3. Configure the remaining settings.

**UCP File Options**

Use the configuration pane to configure the settings in the **UCP File Options** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Directory to drop file</td>
<td>Specifies the directory where one-time passwords are stored, each password in a separate UCP file.</td>
</tr>
<tr>
<td>Filename starts with</td>
<td>Specifies a string that occurs at the beginning of each file name. <strong>Example:</strong> ucp</td>
</tr>
<tr>
<td>Filename ends with</td>
<td>Specifies a string that occurs at the end of each file name. <strong>Example:</strong> .txt</td>
</tr>
<tr>
<td>Template File</td>
<td>Specifies the name of the template file that provides the text contained in every UCP file. The text includes a variable which is replaced by the one-time password.</td>
</tr>
<tr>
<td>Control+New Line (0D 0A)</td>
<td>Selecting this checkbox adds line breaks to the UCP file.</td>
</tr>
<tr>
<td>File character set</td>
<td>Specifies the character encoding for the UCP file. <strong>Example:</strong> ISO–8859–1</td>
</tr>
</tbody>
</table>

**Configure the Prefetch Detection delivery method**

Detect if users are using only prefetch one-time passwords. This delivery method is useful when some, but not all, users are using only prefetch one-time passwords. When the **Prefetch Detection** delivery method is configured and selected, McAfee OTP checks the McAfee OTP attribute. If the attribute is set to a value that you configure, only prefetch one-time passwords are used. In this case, McAfee OTP does not send a one-time password by any delivery method.

**Task**

1. In the select pane, expand the **Delivery Methods** object type, then select **Prefetch Detection**.
2. In the configuration pane, select the **Enable Prefetch Detection** checkbox.
3. In the **OTP Attribute detection** field, type the value of the OTP attribute when **prefetch one-time passwords only** is true. **Example:** PF-ONLY
Configure McAfee Voice delivery method

McAfee OTP can be set up to deliver a one-time password to land-line or mobile phones using voice technology in various languages when a user is unable to see a one-time password.

**Before you begin**
You must have a license with SMS activated to set up the McAfee Voice delivery method. Check the license file (OTP with SMS) for when it expires.

Register to use the voice service. McAfee OTP contacts the message service to verify credentials and then populates some fields automatically.

McAfee Voice delivers one-time passwords of five digits. If your server configuration is set up to deliver six-digit passwords, or passwords made up of letters and digits, configure the one-time password length and composition in **OTP Configuration | Server**.

**Task**

1. In the McAfee OTP configuration console, expand **Delivery Methods** and select **Enable McAfee Voice**.

2. To sign up to use voice technology to deliver passwords, click **Register for Voice Service**.
   
   You only need to do this once.

   The system checks your license file and populates the user name and password fields automatically.

3. Select **Enable HTTP proxy server** and add the proxy server IP address and port number if you connect to the Internet through a proxy server.

4. By default, the following options are already selected:
   - **Username in accounting file** — Records the name of the user who requested a one-time password and successful logon to the **OTP access log file**.
   - **Disable PF SMS status** — Prevents McAfee OTP from authenticating with McAfee Voice because the password was already created.
   - **Validate SSL Certificates** — Checks the SSL certificates of the messaging gateway and denies access of the SSL certificates do not match.

5. Set up the location of your McAfee messaging gateway.
   a. Select the location of your nearest McAfee messaging gateway server.
   b. Click **Test** to verify the connection.
      
      A dialog box opens.
   c. Add your telephone number (mobile or landline).
      
      McAfee OTP delivers a voice one-time password.
   d. Click **Update Config** if you change the location of the messaging gateway.
   e. Select **Debug** to have McAfee Voice information added to the McAfee OTP log file.

6. Click **Language Settings** to specify the language you want to use the one-time password.
English (US) is selected by default.

a Specify whether you want to use the language code from the user attribute and type the attribute name in your user object that you have configured to store the language code. To use this feature, you need to have set up an attribute in your user object that stores your language code.

b Specify whether you want McAfee OTP to check the telephone number for a language code if no code is stored in an attribute.

c Select the default language to deliver the password if no other method is available.

You can have all three of these options selected. If one fails, McAfee OTP tries another of the options.

7 Click OK to save the language settings.

8 Click Save Config to save the configuration changes.
Configuring the Misc object type

The Misc object type includes the following miscellaneous configuration types.

Contents

- Configure the Expired Password Notification settings
- Configure the OATH settings
- Configure the Prefetch OTP options
- Configure the Unlock User Accounts options
- Configure the AES Encryption options
- Configure the Embedded HTTP Server Options
- Configure a cluster
- Configure Enrollment
- Configure the Web Manager options
- Enable the Self Service tool
- Configure the Yubico options

Configure the Expired Password Notification settings

Use the configuration pane to configure the settings in the Expired Password Notification area.

Task

1. In the select pane, expand the Misc object type, then select Expired Password Notification.
2. In the configuration pane, select the Enable Expired Password Notification checkbox.
3. Configure the remaining settings.

Expired Password Notification

Use the configuration pane to configure the settings in the Expired Password Notification area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| User attributes to send message to | Specifies a comma-separated list of attributes, each one storing an email address or mobile phone number where the expired password notification can be sent.  
**Example**: mail, mobile |
| Message to the user           | Specifies the message that is sent to the user when the user's password has expired.                                                       |
| Method to send notification with | Selects the delivery method to use when sending the expired password notification to users.                                              |
Configure the OATH settings

McAfee OTP supports the OATH HOTP and TOTP hardware tokens used by Pledge and other OATH software tokens.

**Task**

1. In the select pane, expand the Misc object type, then select OATH Configuration.
2. Configure the remaining settings.

**HOTP**

Use the Oath Configuration pane to configure the settings in the HOTP area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Key and counter</td>
<td>Selecting this checkbox specifies whether the HOTP key and counter are encrypted in the database.</td>
</tr>
<tr>
<td>Validation LookAhead Value</td>
<td>Specifies the number of unused one-time passwords the user can generate with the OATH device before the device is out-of-sync and needs to be resynchronized.</td>
</tr>
<tr>
<td>OTP Length</td>
<td>Selects the length of the one-time password.</td>
</tr>
<tr>
<td>Truncation value</td>
<td>Specifies an offset value for OATH devices.</td>
</tr>
<tr>
<td></td>
<td><em>A value of –1 specifies variable truncation. Do not modify this value.</em></td>
</tr>
</tbody>
</table>

**TOTP**

Use the configuration pane to configure the settings on the TOTP area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept time drift</td>
<td>Selecting this checkbox allows McAfee OTP to accept the preceding, current, or succeeding one-time password instead of only the current one-time password to compensate for time drift.</td>
</tr>
<tr>
<td>Anti-replay check</td>
<td>Selecting this checkbox specifies that each one-time password is only valid once in a specified time frame set by the software token, usually 30 or 60 seconds.</td>
</tr>
<tr>
<td>Encrypt Key value</td>
<td>Selecting this checkbox specifies that the TOTP key is encrypted in the database.</td>
</tr>
<tr>
<td>Max Out of Synch Time Steps</td>
<td>Specifies the maximum number of time steps that an OATH device can be out-of sync with McAfee OTP. The time step is set by the OATH device, for example, 30 seconds.</td>
</tr>
</tbody>
</table>

**General OATH Settings**

The following settings can be configured for both HOTP and TOTP tokens.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin code placement</td>
<td>Selects whether the user enters the PIN before or after the HOTP/TOTP token when a PIN is used.</td>
</tr>
<tr>
<td>Accept OATH Token Identifier</td>
<td>Selecting this checkbox adds support for software tokens that send a token identifier in addition to a one-time password.</td>
</tr>
<tr>
<td>Enable Automatic Enrollment (Class A - OATH Token Identifier)</td>
<td>Selecting this checkbox specifies whether the automatic enrollment process retrieves the OATH key and counter from the keyfile and uses the OATH token identifier to store them in the user database.</td>
</tr>
</tbody>
</table>
**Automatic OATH Enrollment**

The Automatic Oath Enrollment settings are only available when the Accept OATH Token Identifier and Enable Automatic Enrollment checkboxes are selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key storage database</td>
<td>Selects the database containing the keys and token identifier.</td>
</tr>
<tr>
<td>Check SQL Database</td>
<td>Tests whether the TOKENDB database and tokens table exist in the selected SQL database. If they do not exist, click Yes to create them.</td>
</tr>
<tr>
<td>Object DN</td>
<td>Selects an LDAP object in which to store the keys.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Selects an LDAP attribute in which to store the keys.</td>
</tr>
<tr>
<td>Upload keyfile to database</td>
<td>Clicking this button uploads the keys from the keyfile to the selected database. The keyfile must be a PSKC (RFC 6030) file or contain comma-separated or semicolon separated keys.</td>
</tr>
<tr>
<td>Allow multiple token assignments</td>
<td>Selecting this checkbox accepts a user that has one OATH token and wants to enroll for a second token.</td>
</tr>
<tr>
<td>Encrypt keys in keystorage database</td>
<td>Selecting this checkbox specifies that the keys in the keystore are encrypted. If AES is configured, the keys are encrypted using AES encryption. However, you must configure AES encryption before you import the keyfile.</td>
</tr>
</tbody>
</table>

**Advanced automatic OATH enrollment**

Some LDAP databases limit the number of keys per object to 1,000. To overcome this limitation, you can configure multiple LDAP objects and attributes for storing OATH keys on the Advanced Configuration dialog box. To open the dialog box, click Advanced in the Automatic OATH Enrollment area in configuration pane.

**Configure the Prefetch OTP options**

Configure how prefetch one-time passwords are delivered to the user. McAfee OTP can send prefetch one-time passwords by any configured McAfee OTP delivery method or by forwarding them to another McAfee OTP server.

**Task**

1. In the select pane, expand the Misc object type, then select Prefetch Proxy Config.

2. To send all prefetch one-time passwords to another McAfee OTP server, select the Proxy Sending of Prefetch OTPs checkbox in the configuration pane.
3. Type the IP address and port number of the proxy server (separated by a colon).
   
   To specify multiple proxy servers, use a comma to separate each IP address-port number pair.

4. From the Force Sending Prefetch OTP with Method drop-down list, select the McAfee OTP delivery method to use when sending prefetch one-time passwords.
   
   Only configured McAfee OTP delivery methods are available.

**Configure the Unlock User Accounts options**

Configure how many minutes user accounts are locked before the server automatically unlocks them, and specify different values for the first and second lockout. The Unlock function is used together with the OTP Databases object settings — Login Retries, Locked Attribute, and Locked Value — to manage access to McAfee OTP user accounts.

**Task**

1. In the select pane, expand the Misc object type, then select Unlock User Accounts.

2. In the configuration pane, configure the remaining settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlock Accounts after First Lockout</td>
<td>Specifies in minutes how long user accounts are locked when they are locked for the first time.</td>
</tr>
<tr>
<td>Unlock Accounts after Second Lockout</td>
<td>Specifies in minutes how long user accounts are locked when they are locked for the second time.</td>
</tr>
<tr>
<td>Reset Value</td>
<td>Specifies the value to write to the Locked Attribute in the McAfee OTP database when the user account is unlocked. If you do not specify a value for this setting, McAfee OTP sets the value of the Locked Attribute to empty.</td>
</tr>
</tbody>
</table>

**Configure the AES Encryption options**

McAfee OTP supports AES encryption and decryption. Using AES, McAfee OTP can store OATH keys and other sensitive information encrypted in McAfee OTP databases.

**Task**

1. In the select pane, expand the Misc object type, then select AES Encryption.

2. In the configuration pane, select the Enable AES Encryption checkbox.

3. Configure the remaining settings.

**Tasks**

- General Settings on page 73
  Specify the attributes for McAfee OTP to encrypt.
General Settings
Specify the attributes for McAfee OTP to encrypt.

Task
1. In the General Settings area, click Add.
2. In the configuration pane corresponding to the database, select the External Database handler checkbox, and type ext.aes in the field that opens.
3. Click Save Config.

Advanced Settings
Use the configuration pane to configure the settings in the Advanced Settings area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AES Key</strong></td>
<td>Specifies the key to use for AES encryption and decryption:</td>
</tr>
<tr>
<td></td>
<td>• To specify a 128-bit key, provide a string of 32 characters.</td>
</tr>
<tr>
<td></td>
<td>• To specify a 256-bit key, provide a string of 64 characters.</td>
</tr>
<tr>
<td></td>
<td>Do not modify the AES key in a production environment. All data encrypted</td>
</tr>
<tr>
<td></td>
<td>with the key that you erase can no longer be decrypted or recovered.</td>
</tr>
<tr>
<td><strong>Key size</strong></td>
<td>Selects a key size from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• 128</td>
</tr>
<tr>
<td></td>
<td>• 192</td>
</tr>
<tr>
<td></td>
<td>• 256</td>
</tr>
<tr>
<td><strong>Units</strong>:</td>
<td>bits</td>
</tr>
<tr>
<td><strong>AES prefix</strong></td>
<td>Specifies the encryption format of an encrypted value. The prefix is added</td>
</tr>
<tr>
<td></td>
<td>to the front of the value.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: {AES}</td>
</tr>
<tr>
<td><strong>Key type format</strong></td>
<td>Selects a format for the AES key: hex (hexadecimal) or Base64.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: hex</td>
</tr>
<tr>
<td><strong>Data format</strong></td>
<td>Selects a format for the encrypted data: hex (hexadecimal) or Base64.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: hex</td>
</tr>
<tr>
<td><strong>Use CBC</strong></td>
<td>Selecting this checkbox enables cipher-block chaining (CBC).</td>
</tr>
<tr>
<td><strong>IV (CBC)</strong></td>
<td>Specifies the initialization vector required to implement CBC.</td>
</tr>
<tr>
<td></td>
<td>The initialization vector must be specified in hexadecimal format and be</td>
</tr>
<tr>
<td></td>
<td>32 characters in length (16 bytes).</td>
</tr>
<tr>
<td><strong>Lock</strong></td>
<td>Locks and unlocks the AES settings.</td>
</tr>
<tr>
<td></td>
<td>Locking the settings protects them from being changed unintentionally.</td>
</tr>
</tbody>
</table>
**Test encryption and decryption**

Use the configuration pane to configure the settings in the Test encryption & decryption area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Specifies a value to encrypt or decrypt with the AES key that you configured. For the test, specify a value that is as long as or longer than the AES key.</td>
</tr>
<tr>
<td>Result</td>
<td>Clicking Encrypt or Decrypt displays the encryption or decryption result, respectively.</td>
</tr>
</tbody>
</table>

**Configure the Embedded HTTP Server Options**

McAfee OTP includes an embedded HTTP server, which is used for Pledge Enrollment, Web Manager, and other web applications.

**Task**

1. In the select pane, expand the Misc object type, then select Embedded HTTP Server.
2. In the configuration pane, select the Enable Embedded HTTP Server checkbox.
3. Configure the remaining settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Specifies the port number of the embedded HTTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 8080</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Selecting this checkbox enables SSL for the HTTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: Selected</td>
</tr>
<tr>
<td>SSL Options - PKCS12 file</td>
<td>Selects the P12 certificate file used by the SSL protocol.</td>
</tr>
<tr>
<td>SSL Options - PKCS Password</td>
<td>Specifies the password that protects the P12 certificate file.</td>
</tr>
<tr>
<td>Enable AJP</td>
<td>Enables the AJP option for the Apache front end.</td>
</tr>
</tbody>
</table>

*Note: Enable AJP is an acronym for Apache JServ Protocol.*

**Enable OTP Dashboard**

Enable the dashboard to see system health statistics and launch enabled applications.

The embedded HTTP server reads the configuration settings each time it starts. Therefore, McAfee OTP must be restarted for the new settings to take effect. If McAfee OTP is started manually, and not as a service, you can restart the embedded HTTP server using the start-stop button located on the configuration pane.

**Configure a cluster**

Set up a cluster of McAfee OTP servers where all servers in the cluster share memory and state to provide instant failover capability.

**Task**

1. In the select pane, expand the Misc object type, then select Cluster Configuration.
2. In the Cluster Configuration pane, type the name of the cluster.
Specify a password for the administrators to manage the cluster. The default password is nepass.

Configure the remaining settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster port</td>
<td>Choose a port that is not already used, such as port 5701.</td>
</tr>
<tr>
<td>Enable TCP/IP Cluster</td>
<td>Select to create a cluster of McAfee OTP servers.</td>
</tr>
<tr>
<td>Members in cluster</td>
<td>Shows the IP addresses of the servers that are in the cluster.</td>
</tr>
<tr>
<td>Add member</td>
<td>Click to add a server as a member of a cluster. To do so, enter its IP address.</td>
</tr>
</tbody>
</table>

Restart McAfee OTP.

Configuration data is saved into a file called hazelcast.xml stored in the McAfee OTP root directory.

See also

McAfee OTP redundancy on page 92

---

Configure Enrollment

Enable the methods of enrollment that you want to make available to your users and start the Enrollment website.

Modules

The following methods of enrollment are available:

- Pledge enrollment
- SMS/Email enrollment
- OATH Token enrollment
- Intel IPT Enrollment

Configure the enrollment methods

Set up which methods of enrollment you want to use.

Before you begin

You must know the name of the user object attribute in your directory where your group membership attributes details are stored.

Create a native client so that McAfee OTP knows where to authenticate the users that are associated with a known OATH database. The client must have Enable name detection selected. McAfee recommends you name the client to reflect enrollment.

Task

1. In the select pane, expand the Misc object type, then select Enrollment.
2. Select Enable Enrollment.
3. Select the native client that you set up for enrollment.
4. Select Require OTP authentication to enforce users to go through two-factor authentication when they enroll.
5 Select Administrator role settings to select the attribute name of the user object attribute where the group membership details are stored, and the group that has been created for the administrator role.

6 In Modules, click the enrollment method that you want to set up: Pledge, SMS/Email enrollment, OATH Token Enrollment, or Web IPT Enrollment.

The settings page for the enrollment method that you want to set up is displayed.

Configure the Pledge Enrollment options
Using the Pledge Enrollment web application, users can easily download a Pledge profile, which includes an HOTP key, PIN settings, and customized user interface settings. Using the web services interface that is integrated with Pledge Profile Service, administrators can customize the PIN requirements and user interface.

Before you begin
A client for Pledge Enrollment must be set up in McAfee OTP so that McAfee OTP knows where to store the OATH key that it gets from Pledge Enrollment Service.

From Pledge Profile Service you must gather the Pledge customer ID, the Pledge customer password, and the template ID of the template you want to use. If you want to use more than one type of template, you must create a McAfee OTP installation for each template.

If you don't have a customized template created, you can use the default template.

The user store that you want to enroll with the Pledge system must be set up and authenticating correctly with McAfee OTP.

Set up the email or text message email delivery methods (Delivery Methods | McAfee SMS or Delivery Methods | SMTP) if you want your users to receive profile IDs on their smartphone or to their email account when enrollment is performed by an administrator.

Task
1 In the select pane, expand the Misc object type, then select Pledge enrollment.
2 In the configuration pane, select the Enable Pledge Enrollment checkbox.
3 In Pledge Enrollment Settings, add the following information:
   • The customer ID that you copied from Pledge Profile Service
   • The customer password
   • The profile template ID
   • Select the client you set up for the Pledge Enrollment application
   • Select the user key action you want:
     • Allow multiple user keys to allow your users to have an OATH key for multiple devices
     • Prevent overwrite of existing user keys to have the same OATH key to generate one-time passwords.
   • Specify the OATH key attribute where the Pledge OATH keys are stored.
   • Select Profile download notifications to specify whether you send a user their profile ID by email or text message.

Your users can now enroll with the Pledge Enrollment Service. Give the Enrollment URL to your users. When they log on, they need to select the Pledge option.
### Tasks

- **Connect a user store with Pledge Enrollment on page 77**
  
  A database in McAfee OTP must be configured to work with the Pledge Enrollment Service to store the OATH keys generated by Pledge Profile Service.

### Connect a user store with Pledge Enrollment

A database in McAfee OTP must be configured to work with the Pledge Enrollment Service to store the OATH keys generated by Pledge Profile Service.

**Before you begin**

The user store that you want to enroll with the Pledge system must be set up and functioning correctly.

To enable McAfee OTP to authenticate users that request profiles using the Pledge Enrollment Service, you must have a database configured for OATH. Only one store can be associated with each Pledge client. If you have multiple user stores, you must have a McAfee OTP installation for each one.

Connecting other user stores to Pledge Enrollment follows slightly different steps. This task is based on an Active Directory installation.

**Task**

1. Start McAfee OTP, and select **Configuration**.
2. Select **Databases**, then click **LDAP database**.
3. Type a display name for the database such as Pledge Enrollment database.
   
   The display name is used to locate the database in the list of databases.
4. Enter the IP address of the Active Directory server. Keep the default port number.
5. Enter the Admin DN user name and password, then click **Test Connection**.
6. In **Search Settings**, enter the details for the Base DN where McAfee OTP looks for user objects in the Active Directory.
7. Click **Samples** to set Active Directory as the search filter.
8. In the **OATH Key** field, choose an attribute that is not currently used in the target Active Directory domain and ensure that it has the following properties:
   - **String type**
   - **Multiple value**
   - **Unlimited length**
9. Click **OK**.
Configure text message and email enrollment
Enable your users to receive their one-time passwords by text message or email message.

**Task**
1. In the select pane, expand the Misc object type, then select Enrollment.
2. Select Enable Enrollment.
3. Select SMS/Email enrollment.
4. Select the user database object where McAfee OTP can find information about the user attributes.
5. In Email Settings, enable email enrollment so that your users receive their one-time passwords by email.
6. Select the attribute where you want McAfee OTP to find the email address of your user.
7. Select Allow users to change their email address to enable the users to set another email address to use for enrollment.
8. In SMS settings, if you want to allow users to receive their one-time passwords by text message, select Enable SMS enrollment.
9. Specify in which attribute to find the mobile number in the directory.
10. Select Allow users to change the mobile phone number to enable users to set another phone number to use for enrollment.
11. Click Done.

Configure OATH token enrollment
Enable your users to receive their one-time passwords by OATH token.

**Task**
1. In the select pane, expand the Misc object type, then select Enrollment.
2. Select Enable Enrollment.
3. Select OATH Token enrollment.
4. Click Enable OATH Token enrollment.
5. From the drop-down menu, select the client that you want to use, then click Done.

Configure Intel IPT Enrollment
Set up the enrollment feature to enable one-time passwords to be installed on a device with an Intel IPT chipset.

**Before you begin**
The device must contain the Intel IPT chipset and have Intel IPT software installed.

To check whether the device is enabled for the Intel IPT feature, check [ipt.intel.com/Home/devices-with-intel-ipt](ipt.intel.com/Home/devices-with-intel-ipt) The software is either installed already on the device, or can be downloaded from the Intel website.

McAfee OTP must be running correctly and have the Pledge Enrollment application enabled.
In Pledge Profile Service, there must be customer account and customer ID and password already set up, and a valid template that supports Intel IPT created.

You could have more than one template set up in Pledge Profile Service; for example, one for pledge enrollment and one for Intel IPT.

**Task**

1. In the select pane, expand the Misc object type, then select Enable Web IPT Enrollment.

2. In the configuration pane, select the Enable Web IPT Enrollment checkbox.

3. Copy the template ID from Pledge Profile Service and paste it in to the enrollment page.

4. Click Done.

Your users can now enroll for Intel IPT.

Give the Enrollment URL to your users. When they log on, they need to select the Intel IPT option.

**See also**

Templates page on page 98
Create templates on page 103

---

**Configure the Web Manager options**

McAfee OTP includes a tool to manage administrative tasks for users. Using the tool, administrators and help desk personnel can manage day-to-day tasks such as adding and changing PINs, assigning and resynchronizing tokens, and creating emergency one-time passwords.

**Before you begin**

To use the Emergency OTP feature, you must enable and configure the Onetime Password Prefetch option on your database.

**Task**

1. In the select pane, expand the Misc object type, then select Web Manager.

2. In the configuration pane, select the Enable Web Manager checkbox.

3. Select the LDAP database that you want to use from the drop-down menu.

4. Click Select administrators to specify the people who you want to administer the Web Manager application.

5. Configure the options in the Authentication and Other sections.

**Authentication settings**

Use the configuration pane to configure the settings in the Authentication area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client for authentication</td>
<td>Specifies the McAfee OTP client used by the Web Manager to authenticate administrators.</td>
</tr>
<tr>
<td>Enable OTP protection</td>
<td>Select this checkbox to require one-time password authentication.</td>
</tr>
</tbody>
</table>
Other
Use the configuration pane to configure the settings in the Other area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile attribute</td>
<td>Specifies the LDAP attribute that stores the mobile number.</td>
</tr>
<tr>
<td>PIN code attribute</td>
<td>Specifies the LDAP attribute that stores the PIN. A PIN is used with a one-time password to increase the security in the authentication process.</td>
</tr>
<tr>
<td>Client for OATH</td>
<td>Selects the McAfee OTP client used by the Web Manager to resynchronize tokens and verify the identity of users. Select a McAfee OTP client that is connected to a McAfee OTP database with OATH enabled.</td>
</tr>
<tr>
<td>Launch Web Manager</td>
<td>Opens the Web Manager interface in your web browser.</td>
</tr>
</tbody>
</table>

Enable the Self Service tool
McAfee OTP includes a Self Service tool to let users reset their own password, update their mobile numbers, manage secret question and answers, and generate a PIN. Users log on to their accounts using a user name and password. If a user forgets their password, they can use a one-time password, or answer a preconfigured question.

Task
1. In the select pane, expand the Misc, then select Self Service.
2. In the configuration pane, select the Enable Self Service checkbox.
3. Configure the remaining settings.

Self Service Configuration settings
Use the Self Service configuration pane to configure the settings in the Configuration area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP database</td>
<td>Selects a configured LDAP database from the drop-down list. Self Service connects to this database to collect and/or update attribute information.</td>
</tr>
<tr>
<td>Mobile attribute</td>
<td>Specifies the LDAP attribute that stores the user’s mobile phone number. Click Editable to allow your users to update their mobile number themselves through the Self Service tool.</td>
</tr>
<tr>
<td>Mail attribute</td>
<td>Specifies the LDAP attribute that stores the user’s mail address.</td>
</tr>
<tr>
<td>PIN Code attribute</td>
<td>Specifies the LDAP attribute that stores the user’s PIN. If the PIN is configured for the LDAP database, but a value is not entered on the configuration pane, the value for the LDAP database will be used. If a PIN attribute value is not configured for the LDAP Database, McAfee OTP database, or the Web Manager configuration pane, the web form for Self Service does not appear.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display name attribute</td>
<td>Specifies the LDAP attribute that stores the user’s display name.</td>
</tr>
<tr>
<td>Client for OTP authentication</td>
<td>The client specified in McAfee OTP used to authenticate users who will access Self Service.</td>
</tr>
<tr>
<td>Password reset settings</td>
<td>Specifies these options:</td>
</tr>
<tr>
<td></td>
<td>• Minimum password length.</td>
</tr>
<tr>
<td></td>
<td>• Maximum password length.</td>
</tr>
<tr>
<td></td>
<td>• Password policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> A-Z:1</td>
</tr>
<tr>
<td></td>
<td>This policy generates a password that contains:</td>
</tr>
<tr>
<td></td>
<td>• At least one character between A–Z</td>
</tr>
<tr>
<td></td>
<td>• At least one character between a–z</td>
</tr>
<tr>
<td></td>
<td>• At least one digit between 0–9</td>
</tr>
<tr>
<td></td>
<td>• Optional characters are # and @</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> A-Z:2</td>
</tr>
<tr>
<td></td>
<td>This policy generates a password that contains:</td>
</tr>
<tr>
<td></td>
<td>• At least one character between A–Z</td>
</tr>
<tr>
<td></td>
<td>• At least one digit between 0–9</td>
</tr>
<tr>
<td></td>
<td>• Optional characters are # and @</td>
</tr>
</tbody>
</table>

### Secret Question and Answer (Q/A)

Use the configuration pane to configure the settings in the **Secret Question and Answer (Q/A)** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Secret Question and Answer (Q/A)</td>
<td>Select the checkbox to activate this feature. When a user logs on, this feature is manageable in the Manage Q and A web form.</td>
</tr>
<tr>
<td>Total number of questions</td>
<td>The number of configured questions and answers the question bank holds for each user.</td>
</tr>
<tr>
<td>Prompted number of questions</td>
<td>The number of questions a user is prompted if they forget their login password. For example, if a user has configured five questions in the question bank, but configured two prompted number of questions, only two random questions are required an answer to successfully log on.</td>
</tr>
<tr>
<td>Answer all questions</td>
<td>Answer all questions checked, the user is prompted to answer only two questions, even if the question bank contains five questions.</td>
</tr>
<tr>
<td>Allow custom questions</td>
<td>Allows the user to create their own questions.</td>
</tr>
<tr>
<td>Q/A attribute</td>
<td>Holds the question and answer information.</td>
</tr>
<tr>
<td></td>
<td><strong>This value is encrypted.</strong></td>
</tr>
</tbody>
</table>
Lockout

Use the configuration pane to configure the settings in the Lockout area. If a user attempts to log on and uses an incorrect password for a specified number of times, Self Service locks out the user from their account.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of tries</td>
<td>Number of user login attempts that are allowed when an incorrect password is used.</td>
</tr>
<tr>
<td>Lockout time (minutes)</td>
<td>Amount of time a user is locked out of their account.</td>
</tr>
<tr>
<td>Lockout attribute</td>
<td>Holds the lockout time value.</td>
</tr>
<tr>
<td>Launch Self Service and Launch Forgot Password button</td>
<td>Opens the Self Service interface in your web browser.</td>
</tr>
</tbody>
</table>

- Any change to the Self Service configuration page needs McAfee OTP to be restarted.
- The Launch button is only available when the administration console is started from the McAfee OTP monitor. If the Launch button is not available, you can access the Self Service application by entering a URL with this format in your browser’s address bar:
  - https://OTPServeripaddress:portnumber/selfservice
  - https://OTPServeripaddress:portnumber/selfservice/module/selfservice/jsp/forgot.jsp

Information for Self Service

Change default question of Secret Question and Answers

The default questions are stored in this file system:

drive:\pathtoMcAfeerootfolder\McAfee\OTPServer3\im4otp\webapps\selfservice\WEB-INF\classes\module\selfservice

The questions are stored in questionbank.txt. When changes are saved to this file, save the file as UTF-8 with the same format.

Change PIN Code length

Open DSEditor.properties and search for this parameter:

drive:\pathtoMcAfeerootfolder\McAfee\OTPServer3\im4otp\webapps\selfservice\WEB-INF\NEIDMgmt\IM4OTP.PINCODE.LENGTH=4

Disable OTP as an option for forgotten password

Open DSEditor.properties and search for this parameter:

drive:\pathtoMcAfeerootfolder\McAfee\OTPServer3\im4otp\webapps\selfservice\WEB-INF\NEIDMgmt

Change this setting to false:

PWDRESET_ALLOW_OTP=true

Enable Help menu
Open DSEditor.properties and look for this parameter:

```
drive:\pathtoMcAfeerootfolder
\McAfee\OTPServer3\im4otp\webapps\selfservice\WEB-INF\NEIDMgmt
DISPLAY_HELP_LINK=true
EXTERNAL_HELP_LINK=http://www.mcafee.com
```

**Enable/Disable Language as an option**

Open DSEditor.properties and search for this parameter:

```
drive:\pathtoMcAfeerootfolder
\McAfee\OTPServer3\im4otp\webapps\selfservice\WEB-INF\NEIDMgmt
DISPLAY_LANGUAGE=true
```

---

**Configure the Yubico options**

To integrate the Yubico YubiKey Validation Server, which provides McAfee OTP validation and management services through web services APIs, use the configuration pane to configure the Yubico options.

**Task**

1. In the select pane, expand the Misc object type, then select Yubico.
2. In the configuration pane, select the Enable Yubico checkbox.
3. Configure the remaining settings.
Configuring the Misc object type
Configure the Yubico options
Configure the Logs object type

Using the configuration pane, configure the Logs object type settings.

**Task**

1. In the select pane, select the Logs object type.
   
   Logs configuration options open in the configuration pane.

2. In the configuration pane, configure the remaining settings.

**Log Files**

The following settings are located in the Log Files area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| System Log File | Specifies the name and location of the log file that stores all debugging information.  
|                 |   ▪ To disable logging to a system file, leave this field blank.              |
|                 |   ▪ For information about extending the McAfee OTP logging API with more logging destinations, go to the McAfee KnowledgeBase. |
| Accounting file | Specifies the name of the log file that stores all successful user authentication events.  
|                 |   ▪ To disable logging to an accounting file, leave this field blank.         |
| Roll Accounting File Now | Clicking this button rolls the current log file, and opens a new log file. |
| Loglevel        | Specifies one of the following log levels:  
|                 |   • Trace  
|                 |   • Debug  
|                 |   • Info   
|                 |   • Warn   
|                 |   • Error   
|                 |   • Fatal   
|                 | **Default:** Debug                                                        |
### Logs, Alerting, and Licensing overview

Configure the Alerts object type

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max logfile size</strong></td>
<td>Specifies the maximum size that a log file can reach before it is rolled, and a new log file is opened.</td>
</tr>
<tr>
<td></td>
<td>When a log file is rolled, it is saved as a back-up file.</td>
</tr>
<tr>
<td><strong>Units:</strong> Kilobytes (KB)</td>
<td></td>
</tr>
<tr>
<td><strong>Default:</strong> 5000</td>
<td></td>
</tr>
</tbody>
</table>

- **Max backup index**

  Specifies the maximum number of back-up log files that can be saved before McAfee OTP removes the oldest file.
  
  **Default:** 100
  
  **Examples:** Saving 100 logging files, each file 5000 KB in size, requires 500 megabytes (MB) of disk space.

- **Append session number**

  Selecting this checkbox adds session numbers to the log file.
  
  **Default:** Selected

- **External Log Handler**

  (Optional) Specifies a Java class name that implements the following interface:
  
  ```java
  se.nordicedge.interface.OTPlogging
  ```

  - To use an external log handler, specify a value for this setting.
  - To use the default log handler, leave this field blank.
  - For the new setting to take effect, restart McAfee OTP.

- **Check for config changes every:**

  Specify the frequency for how often you want McAfee OTP to check for configuration changes.

- **Check classpath during startup**

  Check whether the content of the lib file directory has been changed.

### Other Settings

The following settings are located in the **Other Settings** area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check for config changes every</strong></td>
<td>Specifies a time interval in seconds for checking the McAfee OTP configuration file for changes.</td>
</tr>
<tr>
<td></td>
<td>To disable this function, set the time interval to zero.</td>
</tr>
</tbody>
</table>

- **Check classpath during startup**

  Selecting this checkbox specifies that McAfee OTP reads changes in the lib directory during startup.

---

### Configure the Alerts object type

Use the configuration pane to configure the **Alerts** object type settings.

**Task**

1. In the select pane, select the **Alerts** object type.

   Server configuration options open in the configuration pane.
2 Select the Enable Alerts checkbox.

3 In the configuration pane, configure the remaining settings.

**Alert Configuration**

The following settings are located in the Alert Configuration area on the configuration pane.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Use Method   | Selects the McAfee OTP delivery method that triggers the first alert from the drop-down list.  
Default: All  

The McAfee OTP delivery methods must be configured before they are available in the drop-down list. |
| Alert events | Select one of these checkboxes to specify which errors trigger alerts:  
• RADIUS errors  
• User database errors  
• Sending OTP errors  
• Other errors  
Default: All |
| Message Prefix | Specifies a prefix that is added to each alert message. |
| Recipients   | Specifies the email address or mobile phone number of each alert recipient.  
Entered one email address or mobile phone number per line |
| Test         | Click Test to output a test alert. |

**Configure the Licenses object type**

Use the configuration pane to configure the License object type settings.

The new license system supports multiple license files. For example, you can have in the licenses directory one license file that supports 50 users and another license file that supports 100 users, totaling registered licenses for 150 users.

- Since the license system for McAfee OTP V3 is new and not compatible with V2, you need to obtain new license files from McAfee to upgrade.
- For more information, go to the McAfee Technical Support ServicePortal.

**Task**

1 Copy the new license file to the license directory.  
The license file name must end with the file name extension .dat or .xml.

2 In the select pane, select the Licenses object type.
3 In the configuration pane, click **Detect New**.

4 In the **Registered Licenses** field, verify that the value is updated to include the number of licenses in the new license file.

**License Information**

Use the configuration pane to configure the settings in the **License Information** area.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Licenses</td>
<td>Displays the number of licenses specified in the license files.</td>
</tr>
<tr>
<td>Detect new</td>
<td>Click this button to check for new licenses in the license directory and update the value in the <strong>Registered Licenses</strong> field.</td>
</tr>
<tr>
<td>Used Licenses</td>
<td>Displays the number of registered licenses used by current users.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clicking this button resets the value in the <strong>Used Licenses</strong> field to zero.</td>
</tr>
<tr>
<td>Unused Licenses</td>
<td>Displays the number of registered licenses available to new users.</td>
</tr>
<tr>
<td>Counter started</td>
<td>Displays the date and time that the license counter was started.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Clicking this button refreshes the information displayed in the <strong>License Information</strong> area on the configuration pane.</td>
</tr>
</tbody>
</table>
Getting information

Enable the monitor and log features in McAfee OTP to get information about system events and statistics.

McAfee OTP monitor

To enable the McAfee OTP monitor, select the Server object type in the select pane. In the Options area in the configuration pane, select the Enable Monitor checkbox. If this checkbox is selected, the monitor opens when McAfee OTP starts.

The monitor requires GUI support.

Use the following monitor options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Clicking this option opens the administration console. Select and configure these object types:</td>
</tr>
<tr>
<td></td>
<td>• Server</td>
</tr>
<tr>
<td></td>
<td>• RADIUS</td>
</tr>
<tr>
<td></td>
<td>• Logs</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Licenses</td>
</tr>
<tr>
<td></td>
<td>• Databases</td>
</tr>
<tr>
<td></td>
<td>• Clients</td>
</tr>
<tr>
<td></td>
<td>• Delivery Methods</td>
</tr>
<tr>
<td></td>
<td>• Misc</td>
</tr>
<tr>
<td>Show Details</td>
<td>Clicking this option displays the server statistics.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Clicking this option shuts down McAfee OTP.</td>
</tr>
</tbody>
</table>

Logging features

McAfee OTP contains standard event logs stored in its Logs folder. You can also retrieve additional event information regarding the server itself by a log properties file to the McAfee OTP root folder.
Set up additional McAfee OTP server logging

Add a log4j.properties file to the root directory and configure it to report McAfee OTP events not already reported in the standard McAfee OTP log files, such as Tomcat events.

Task
1. Create a log4j.properties file and add it to the McAfee OTP root folder.
2. Edit the log4j.properties file to log server-specific events:

   log4j.appender.LOCALHOST=org.apache.log4j.RollingFileAppender
   log4j.appender.LOCALHOST.layout=org.apache.log4j.PatternLayout
   log4j.appender.LOCALHOST.MaxFileSize=50KB
   log4j.appender.LOCALHOST.MaxBackupIndex=10
   log4j.appender.LOCALHOST.layout.ConversionPattern=%d{ISO8601}: %p: % m%n
   log4j.appender.LOCALHOST.File=logs/tomcat.log
   log4j.logger.org.apache.catalina.core.ContainerBase=DEBUG, LOCALHOST
Configuring a cluster

Configure McAfee OTP in a cluster.

Contents
- McAfee OTP cluster requirements
- McAfee OTP redundancy
- Configure McAfee OTP redundancy
- Configure the VPN Gateway or application with multiple McAfee OTP servers
- Test the McAfee OTP cluster
- McAfee OTP cluster configuration

McAfee OTP cluster requirements
To configure a cluster, the following minimum requirements must be met.
- Two configured McAfee OTP servers
- McAfee OTP configured with SMS and/or Pledge
McAfee OTP redundancy

McAfee OTP supports full active-active clusters to allow users to log on with two-factor authentication to any of the McAfee OTP servers within the same cluster.

For example, when a user authenticates with a user name and password with McAfee OTP server 1, then the user receives and enters the one-time password to the McAfee OTP server 2 for verification.

Figure A-1  McAfee OTP redundancy

Configure McAfee OTP redundancy

To configure a cluster, each McAfee OTP server must point to all other McAfee OTP servers. For this example:

- McAfee OTP server 1 points to McAfee OTP server 2.
- McAfee OTP server 2 points to McAfee OTP server 1.

Task

1. Configure McAfee OTP server 1.
   a. Open and edit C:\Program Files\McAfee\OTP\hazelcast.xml.
      If using UNIX/Linux, open and edit /opt/McAfee/OTP/hazelcast.xml.
   b. Change tcp-ip enabled to true.
   c. Change interface to the IP address of McAfee OTP server 2.
      In this case 192.168.92.183.
   d. Save and close the file.
   e. Restart McAfee OTP server 1.
2 Configure McAfee OTP server 2.
   a Open and edit C:\Program Files\McAfee\OTP\hazelcast.xml.
      If using UNIX/Linux, open and edit /opt/McAfee/OTP/hazelcast.xml.
   b Change tcp-ip enabled to true.
   c Change interface to the IP address of McAfee OTP server 2.
      In this case 192.168.92.238.
   d Save and close the file.
   e Restart McAfee OTP server 2.
      For more information about cluster configuration, go to the Hazelcast webpage.

McAfee OTP server 1 and 2 appear as a cluster.

Configure the VPN Gateway or application with multiple McAfee OTP servers

Configure the VPN Gateway or application to the McAfee OTP cluster.
In the following scenario, the McAfee OTP web test application is used to demonstrate how to configure two McAfee OTP servers with redundancy.

Task
1 Open the configuration for McAfee OTP web test application: C:\inetpub\wwwroot\OTPServerWebTestApp\Web.config

2 Type the IP addresses to McAfee OTP server 1 and 2.
   In this case 192.168.92.238:3100;192.168.92.183:3100

3 Save and close the file.
4 Restart the IIS server.

Test the McAfee OTP cluster

Test and verify the active-active cluster configuration.

Task
1 Go to the OTP Web Test App.
2 Type the user name and password.
3 Select SMS or Pledge, then click Login.
   The OTPServer.exe window appears.
4 Shut down McAfee OTP server 1.
5 On the OTP Web Test App - Custom Login page, type the one-time password, then click Verify. The Welcome to the OTP Protected Web Test App Site message and OTPServer.exe window appear.

6 Verify that the McAfee OTP server 2 successfully verified the one-time password.

**McAfee OTP cluster configuration**

The group name and password option can be used to create separate clusters. For example, McAfee OTP server production and McAfee OTP server test.

```
<group>
  <name>ne-otp-prod</name>
  <password>SecretPassword</password>
</group>
```

With the tcp-ip option, you can configure one or many McAfee OTP servers, specific ports or if a range of IP addresses for McAfee OTP in the cluster.

```
<tcp-ip enabled="true">
  <hostname>otpserver1.domainlocal</hostname>
  <hostname>otpserver2.domainlocal</hostname>
  <hostname>otpserver3.domainlocal:1980</hostname>
  <interface>192.168.1.21</interface>
  <interface>192.168.1.0-7</interface>
</tcp-ip>
```
The McAfee Pledge system

The McAfee Pledge system provides a secure, two-factor authentication method for users to log on to applications.

Contents
- About the McAfee Pledge system
- Pledge Profile Service
- Pledge Enrollment
- McAfee Pledge Software Token

About the McAfee Pledge system

The McAfee Pledge system consists of these components:

- Pledge Profile Service — A web service that administrators use to configure and customize Pledge corporate profiles, which include logos, background pictures, colors, PIN settings, and contact information. Pledge corporate profiles provide the template for Pledge user profiles used by Pledge Software Token clients.

- Pledge Enrollment — A service that automates the delivery of Pledge user profiles to user devices.

- Pledge Software Token client — Installed on user devices with which they will download the Pledge profile onto their smartphone or computer and subsequently be able to generate one-time passwords based on the OATH algorithm.
How Pledge works

<table>
<thead>
<tr>
<th>Reference</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Pledge Enrollment, the user enrolls in Pledge.</td>
</tr>
<tr>
<td>2</td>
<td>Pledge Enrollment sends a request for McAfee OTP to check the user's credentials.</td>
</tr>
<tr>
<td>3</td>
<td>McAfee OTP verifies the user's credentials.</td>
</tr>
<tr>
<td>4</td>
<td>Pledge Enrollment sends a web service request to the Pledge Profile Service.</td>
</tr>
</tbody>
</table>
| 5         | Pledge Profile Service performs these actions:  
|           | • Generates a random symmetric key and corresponding counter  
|           | • Packages the Pledge corporate profile into a .zip file  
|           | • Generates a unique Pledge profile ID  
|           | • Combines the preceding information into an XML message for the user to download  
|           | • Sends the ID and OATH key to Pledge Enrollment  
|           | • Stores the information for the length of time you specify for the user to download the profile |
| 6         | Pledge Enrollment sends the OATH key and counter to McAfee OTP. |
| 7         | McAfee OTP saves the key in the configured database. |
| 8         | Pledge Enrollment sends the Pledge profile ID to the user or administrator. On a supported device, the user starts the Pledge Software Token client application, then clicks +, and enters the Pledge profile ID. |
| 9         | To download the Pledge user profile, which includes the Pledge corporate profile, OATH key, and Pledge profile ID, the Pledge Software Token client application contacts Pledge Profile Service through an HTTPS connection. |
| 10        | Pledge Profile Service sends the corresponding Pledge user profile, flags the Pledge profile ID, and removes the OATH key. |
Pledge ID numbers

Customer ID — The customer ID is assigned when you add the customer account.

Client ID — The client ID identifies the device you downloaded the profile for. It remains constant while a new profile ID is created each time you create a profile.

Profile ID — The profile ID is randomly generated by Pledge Profile Service and is an activation code. The profile ID is discarded as soon as it is downloaded.

The generated OATH key is stored in the user store, and is not stored in Pledge Profile Service once it is downloaded.

Your smartphone or computer receives an ID. The next time you download a profile, you get a new profile ID, but the client ID remains the same because the client ID is linked to the device rather than the profile.

Pledge Profile Service

McAfee Pledge Profile Service is a web-based system to manage your company profile data and the way your user's one-time passwords are generated. Your company profile can include images (like background, logo, icon, and button), background color, text color, PIN length, signing URL (optional), and support contact information. You can also use Pledge Profile Service to verify Pledge licensing information.

Pledge corporate profiles provide the template for Pledge user profiles used by Pledge clients.

McAfee hosts the Pledge Profile Service in the cloud for you to:

- Create one or more Pledge profiles for your organization or for groups of users.
- Set up the way the profile appears on users' smartphones or computer.
- Set your policy for one-time password generation.

You can install the Pledge Software Token on computers for users who, for example, do not have the use of a smartphone.

When you first log on to Pledge Profile Service, you must create a user account for yourself that will enable you to create a customer account for your organization. After this account is created, you can add other administrators who can manage your company profiles and settings using Pledge Profile Service.

Profiles contain cryptographic keys to create one-time passwords. The profile ID is also known as a session in the Pledge Profile Service. It is used to download a unique profile to each user's device.

Themes page

Themes define how your profiles appear to your users' smartphone or desktop. Use the Themes feature to add your own corporate images and colors. You can create multiple themes for your organization and associate them with various templates for groups of users.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the theme.</td>
</tr>
<tr>
<td>Display icon image</td>
<td>The icon that you want to display on the smartphone or computer.</td>
</tr>
<tr>
<td>Text color</td>
<td>The color of the one-time password on the device.</td>
</tr>
</tbody>
</table>
### Option | Definition
--- | ---
**Button text color** | The color of the text on the *Generate one-time password* button.

**Button pressed text color** | The color of the text on the *Generate one-time password* button when it is pressed.

**Background color** | Choose whether to have a background color or a background image.

**Animation** | Defines the way that the one-time password is revealed to the user after they click *Generate one-time password*.
- **Scratch** — Reveals the one-time password in a way similar to scratching out the numbers of a lottery ticket.
- **Airport** — The one-time password is revealed in a similar way to flight details changing in an airport.

**Background image** | Use as the background image display on the device.

**Logotype image** | Select from a logo image you added.

**Button background image** | Choose from images you added to have this image appear on the *Generate one-time password* image.

**Pledge preview** | Displays how your theme will appear on user devices as you add the image types.

### Templates page
Using the themes you created, you can create templates for individual user groups, and specify the way that template group generates their one-time passwords.

### Option | Definition
--- | ---
**Name** | A unique name for the template.

**Make public** | Deselected by default. Do not enable the template until you are satisfied that it works the way you want it to.

**Allowed client types** | Click *Any* to have McAfee OTP allow all the mobile phone client types listed to request profiles, as well as any not listed. Or, select only the client types that you want to support.
- If you only want to support devices that contain an Intel IPT chipset, select *IPT browser plug-in*.

**Allow Pledge Desktop** | Enable the template to be downloaded on computers if, for example, a user does not have access to a smartphone.

**Lock type** | Choose from:
- **1 PIN** — Requires users to enter a second PIN to access the Pledge Software Token client application
- **2 NONE** — Users can access the Pledge Software Token client after they have provided correct authentication to log on to their device

- McAfee recommends that you use the PIN option.

**Validity periods** | Set the length of time, in days, that you want these users to be able to generate one-time passwords before they have to re-enroll for a new profile.
- Leave the field blank for an unlimited validity period.
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max time before download</td>
<td>The maximum length, in minutes, of time between a user enrolling for a Pledge profile and downloading the profile onto their device. Leave the field blank to have the validity period forever.</td>
</tr>
<tr>
<td></td>
<td>McAfee recommends that you leave adequate time for a user to download their profile, such as two hours, before it becomes unavailable.</td>
</tr>
<tr>
<td>Keytype</td>
<td>Choose the type of OATH algorithm that is used to generate one-time passwords:</td>
</tr>
<tr>
<td></td>
<td>• HOTP — Event-based algorithm</td>
</tr>
<tr>
<td></td>
<td>• TOTP — Time-based algorithm. Select this option to set up the Intel IPT feature and choose from one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• IPT only — stores the Pledge OATH key on the chipset of a device that contains an Intel IPT chipset</td>
</tr>
<tr>
<td></td>
<td>• Supported — stores the Pledge OATH key on the chipset or the Pledge file system</td>
</tr>
<tr>
<td></td>
<td>• Not supported — stores the Pledge OATH key in the Pledge file system</td>
</tr>
<tr>
<td></td>
<td>You can have more than one template set up and configure one that supports Intel IPT.</td>
</tr>
<tr>
<td></td>
<td>• OCRA — Challenge response algorithm</td>
</tr>
<tr>
<td>OTP Length</td>
<td>The length of the generated one-time password that the user receives. It must be six or eight characters.</td>
</tr>
<tr>
<td>Theme</td>
<td>Select from the themes you created.</td>
</tr>
<tr>
<td>Support</td>
<td>Specify the information that you want to be available on user phones or computers so they can get technical support at your company if they have an issue with their Pledge installation.</td>
</tr>
</tbody>
</table>

**Sessions page**

See information about currently active profiles or create a profile session to visualize how a profile looks on a device using the templates you created.

A session is a currently active profile that has been requested. It lasts as long as the user is logged on using the profile session, or until the profile ID expires because the user did not download it.

To find that a user has successfully enrolled, you see it listed in the Sessions list. The OATH key is not stored on Pledge Profile Service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Add the user name.</td>
</tr>
<tr>
<td>Template</td>
<td>Select the currently active template.</td>
</tr>
<tr>
<td>Client ID</td>
<td>This field can be left blank. It is populated when you create the session.</td>
</tr>
<tr>
<td>Profile key</td>
<td>This field can be left blank. It is populated when you create the session.</td>
</tr>
<tr>
<td>Button text</td>
<td>This field can be left blank. It is populated when you create the session.</td>
</tr>
<tr>
<td>Session valid from /</td>
<td>This field can be left blank. It is populated when you create the session.</td>
</tr>
<tr>
<td>Session valid until</td>
<td></td>
</tr>
<tr>
<td>Profile valid from /</td>
<td>This field can be left blank. It is populated when you create the session.</td>
</tr>
<tr>
<td>Profile valid until</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create</td>
<td>Click to create the session. The session will display on the Sessions page. You can find sessions by user name and the date that it expires.</td>
</tr>
<tr>
<td>Actions</td>
<td>For each session listed on the Sessions page.</td>
</tr>
<tr>
<td></td>
<td>• Details — Shows the profile ID, whether the profile has been downloaded, the profile key (only for profiles that have not been downloaded), the length of time the profile is valid, and the length of time that the user's profile is valid.</td>
</tr>
<tr>
<td></td>
<td>• Download — Click to download active templates. Templates that have expired cannot be downloaded.</td>
</tr>
<tr>
<td></td>
<td>• Delete — Remove a session from the list.</td>
</tr>
</tbody>
</table>

### Settings page

Change information related to your customer account.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the customer account you created when you first logged on to the Pledge Profile Service.</td>
</tr>
<tr>
<td>Contact email address</td>
<td>The email address associated with the person who created the customer account.</td>
</tr>
<tr>
<td>Customer ID</td>
<td>A unique identification number associated with the customer account.</td>
</tr>
<tr>
<td>Create new password</td>
<td>Create a password for the customer account.</td>
</tr>
<tr>
<td></td>
<td>You cannot choose the password.</td>
</tr>
<tr>
<td>Key enrollment</td>
<td>This option is not supported in McAfee OTP 4.0.</td>
</tr>
<tr>
<td>PKI</td>
<td>This option is not supported in McAfee OTP 4.0.</td>
</tr>
<tr>
<td>Administrators</td>
<td>Add the email addresses of Pledge Profile Service administrators who you want to be able to access the administrator-level features available in the Pledge Profile Service. The administrators you add must be registered in Pledge Profile Service to administer the customer account.</td>
</tr>
<tr>
<td></td>
<td>To use this feature, the administrator must already have a user account that uses their email address as a user name.</td>
</tr>
</tbody>
</table>

### Create a user account

To use the services offered by Pledge to have your users generate one-time passwords on their smartphone or computer, you must register with Pledge Profile Service. The first time you register with Pledge Profile Service, you must create a user account from which you create a customer account. Use this process to create other user accounts who can administer Pledge after the customer account is set up.

- The user is unable to use Pledge until they have activated the user account with Pledge Profile Service and had their email address verified.

**Task**

1. Go to the URL for Pledge Profile Service [https://pledge.nordicedge.com](https://pledge.nordicedge.com).
2. On the Welcome to Pledge Profile Services page, type your email address and a password. Create a strong password containing at least one uppercase character, one numeric character, and be at least eight characters.
3 Click Sign in.

Sends an email to verify the email address.

4 Either click the link in the message or copy and paste the long code into the Pledge Profile Service logon page.

   If this is the first time you log on to Pledge Profile Service, you must create a customer account.

Create a customer account
When you create a user account as an administrator, create a customer account for your company.

   Before you begin
   Ensure that your user account is set up.

After your user account is successfully created, you can add further administrators to manage it using the Settings page in Pledge Profile Service.

Task
1 Open the email message sent to the administrator you specified when you set up the user account.
2 Type the user account email address and click Login.
3 Either click the registration link or copy the code in the registration message to open Pledge Profile Service.
4 On the User Registration page, agree to the license, then click Next.
   The user account is created.
5 On the Create Customer Account page, add the company name that you want to use for the customer account.
6 On Customer Account Registration, make a note of the password and click Next.
   This is the only time you see this password. If you lose the password, use the Forgot Password? feature on the Pledge Profile Service logon page.
   Your Pledge profile and customer account are created.
7 Click Done.
   The Customer home page for your company is displayed.

Your customer account details are added to the Settings page in Pledge Profile Service.

Create a user account password
Request a new password for your user account to replace a lost password.
When you create your customer account, you are given a password associated with that account. This is the only time that you see your customer account password for the Pledge system. If you can't remember your password, you must generate a new password using the Forgot Password? feature.

   The password is automatically generated at random and cannot be configured.
**Task**

1. Go to the URL for Pledge Profile Service [https://pledge.nordicedge.com](https://pledge.nordicedge.com).
2. Click the **Forgot password?** link.
3. Enter the email address associated with the user account.
4. Click **Reset**.
   
   A password code is sent to that email account.
5. Either click the link or copy the verification code into the **Password Reset** code field and click **Next**.
6. Enter the email address and password and click **Next**.
   
   A one-time password is sent.
7. Enter the one-time password that you received.

   Pledge Profile Service opens.

A new password is sent to your customer account email address.

**Customize a corporate template overview**

Using Pledge Profile Service, you can create and customize a corporate template with your company background, logo, icon, button, background color, and text color. You can also set the PIN length and the length of time the template is available.

- Add images such as logos and background colors.
- Create themes from images you have uploaded to Pledge Profile Service.
- Set up the way you want this template to behave.

**See also**

- *Add your own images on page 102*
- *Create templates on page 103*
- *Create a sample Pledge profile on page 104*

**Add your own images**

Create your own company themes by adding a selection of images that compile the corporate template that appears on your user devices.

- McAfee recommends that you add several versions of each image that you can compile into a template that looks the way you want it to on your users’ devices. Follow the sizing guidelines for each image type.

**Task**

1. In Pledge Profile Service, select **Themes**.
2. Click **Add image**.
3 Type a unique name for the image.
   You might find that you have to add several images for each image type while you check how your
   profile appears best. Make sure you name each image in a way that makes it easy to identify from
   the image list.

4 Select the type of image that you want to add.
   Template image sizes for .psd and .png image formats are available.

5 Click Add.

   You return to the Themes page and the image you added is available in the list of images.

Create templates
Using the themes you created, you can apply themes to one or more specific user-group templates.

**Before you begin**
Have correctly sized images available in your themes.

**Task**
1 In Pledge Profile Service, select Templates.

2 Click Create new Template.

3 In Name, type a name for the group that enables you to identify it easily.

4 Select Allow Pledge Desktop to enable the Pledge Software Token client to download this template onto
   this user groups’ computer.

5 In Lock type, specify whether you want this group of users to have to type a PIN to access the Pledge
   Software Token client application to generate a one-time password token.
   McAfee recommends that you set this option to PIN.

6 In Validity period, specify the length of time, in days, that users in this group are enrolled with the
   Pledge system before they have to re-enroll.

7 In Download period, specify the length of time, in minutes, between the user enrolling with the Pledge
   service and downloading the Pledge profile to their device.

8 In Keytype, select which type of OATH algorithm you want to generate the one-time password tokens
   for this template.
   To set up the Web IPT feature:
   a Select TOTP as the keytype.
   b Select one of the following options:
      • IPT only — stores the Pledge OATH key on the chipset of an IPT-enabled device
      • Supported — stores the Pledge OATH key on the chipset or the Pledge file system
      • Not supported — stores the Pledge OATH key in the Pledge file system

9 In OTP Length, specify six or eight characters for the one-time passwords generated for this
   template.

10 Select the corporate theme you want to apply to this group.
11 Add details of your technical support team to appear on user's devices to enable them to get help on Pledge-related issues.

12 Click Save changes.

On an existing template, you can select the client types that you want to support. Click Any to have McAfee OTP check all the client types listed or unlisted.

Create a sample Pledge profile
Create a sample profile to visualize the way a profile looks on a device using a template you created.

Task
1 In Pledge Profile Service, open the Sessions page.
2 Click Create New Session to see the Create new Session page.
3 Add the user name and select the currently active template.
   You do not need to add other information. The feature populates the information for you.
4 Click Done to return to the Sessions page.
   The session appears in the list of sessions.

Pledge Enrollment
The McAfee Pledge Enrollment service enables the delivery of user profiles to user devices.
Users can enroll themselves, or get enrolled by Pledge administrators.

The Pledge Enrollment service is embedded into McAfee OTP, but can also be downloaded and installed separately into a DMZ solution.

To enable McAfee OTP to authenticate users requesting profiles from their smartphones or desktop, you must have your user stores configured with the OATH attribute.

You must use an attribute that is not already used.

Contents

- Requirements
  - Enroll users for Pledge profile IDs as an administrator

Requirements
Verify that the following requirements are met to complete enrollment and successfully use the McAfee Pledge system.

Pledge connections

- The Pledge Software Token client application must have access to pledge-api.nordicedge.com on port 443 to download profiles from Pledge Profile Service.
- The Pledge Enrollment service must have access to pledge-api.nordicedge.com on port 443 to make a web service connection to Pledge Profile Service.
- The administrator workstation must have access to pledge.nordicedge.com on port 443 to log on to Pledge Profile Service.

Supported mobile phone platforms
- Apple iPhone
- Google Android
- Microsoft Windows Phone

**Enroll users for Pledge profile IDs as an administrator**
Administrators can enroll a unique Pledge profile ID for users.

**Before you begin**
Verify the user has the Pledge Software Token client installed on a supported device.

**Task**
1. Go to the URL for the McAfee OTP Enrollment service http://<OTPipaddress>:<portnumber>/Enroll.
   - By default, the port number is 8080. If you have enabled SSL, you will have an https URL.
   - Click **Settings | Languages** and select your language.
   - The software stores the language you selected for use with other McAfee OTP web services.
   - In the **User name** field, type the administrator user name.
   - In the **Password** field, type the administrator password and click **Sign In**.
   - Click **Pledge Admin**, then select **Enroll User**.
   - Type the user name of the person you want to enroll and click **Enroll**.
     A Pledge profile ID appears that the user must download onto their device.

2. Give the user the profile ID, or scan the QR code with their smartphone, or click **Send activation link** and type the user’s mobile phone number.
   - If you gave the user the profile ID, from the Pledge Software Token client application, they must click **Get a profile**.
   - Type the unique profile ID and click **Continue**.
   - Type the PIN if necessary, then click **Continue**.

3. To test the profile, ask the user for the one-time password.

---

**McAfee Pledge Software Token**
Use the McAfee® Pledge Software Token to download profiles onto either your smartphone or computer.

**How the Pledge Software Token works**
- When you enroll with Pledge Enrollment, the enrollment service verifies your user credentials.
- Pledge Enrollment sends an ID to you to enter into the Pledge Software Token.

After a profile has been downloaded to your device, you can generate a one-time password.
From the Pledge Software Token, you can manage your PIN and get support information.
Installing a Pledge profile on your smartphone or computer

Use Pledge Enrollment to enroll with the Pledge Software Token client application, then download a profile onto your smartphone or computer.

Pledge profiles on smartphones

Verify that your platform is supported, then install a Pledge profile on your smartphone.

Supported smartphone platforms

You can install the McAfee Pledge Software Token client application on these smartphone platforms.

- Apple iPhone
- Google Android
- Microsoft Windows Phone

The Pledge Software Token client application can support multiple Pledge profiles on a single mobile device.

Install Pledge Software Token on a smartphone

Install the Pledge Software Token on your smartphone to be able to generate one-time passwords.

Before you begin

You need a profile ID. Either enroll with the Pledge Enrollment service to receive a Pledge profile ID yourself, or use an ID that your administrator gives you.

Task

1. Download the Pledge Software Token client application onto your smartphone from your mobile phone provider's online store.
2. Click +.
3. Type or paste the profile ID and click Continue.
4. Type the PIN and click Continue.

The Pledge profile is installed on your smartphone ready to generate one-time passwords.
Pledge profiles on computers
Verify that your platform is supported, then install a Pledge profile on your computer.

Supported computer platforms
McAfee Pledge Software Token client application can run on computers for platforms that support the Java Runtime Environment (JRE) 5.0 or higher.

- Microsoft Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Apple Mac OS X
- Linux 32-bit and 64-bit operating systems
- Any UNIX platforms

Install Pledge Software Token on a computer
The process to install the Pledge Software Token client application onto a computer is similar across all supported platforms.

This example is based on the procedure to install the Pledge Software Token client application onto a computer running one of the supported Microsoft Windows operating systems.

Task
1. Go to the URL given to you by your administrator to download the Pledge Software Token client application.
2. Select the required platform, then click Download.
3. Double-click the installation file to start the installation.
4. Click Run to accept the security warning and start the Pledge Software Token installation wizard.
5. Define installation settings:
   a. On the Introduction page, read the instructions, then click Next.
   b. Select the installation folder.
   c. Specify where you want Pledge icons to appear, for example, in the Start menu or desktop.
   d. Read the installation summary, then click Install.
6. Choose whether to start the Pledge Software Token client application now, then click Next.
7. Click Done to close the installation wizard.

Using the McAfee Pledge Software Token client application
After the Pledge Software Token client application is installed, it can be used to generate one-time passwords and manage the user profile.

Contents
- Generate a one-time password
- Manage your PIN
- Add a master password for extra profile security
**Generate a one-time password**
Use your smartphone or computer to generate a one-time password to access specified applications securely.

### Before you begin
Created a user profile to generate a one-time password.

### Task
1. Start the Pledge Software Token client application.
2. Click **Generate one-time password**.
3. Enter a PIN if necessary.
   The PIN decrypts the key and the one-time password is revealed. You might have to "scrape" the screen to reveal the password similar to revealing numbers on a lottery ticket.
4. Enter the one-time password into the application.

### Manage your PIN
Your administrator might specify that you need a PIN to access the Pledge Software Token client application. You set the PIN when you first create your Pledge profile.

You can add or change a PIN associated with a profile from within the profile settings.

### Task
1. Start the Pledge Software Token client application.
2. Select a Pledge profile, then click the **Details** icon in the lower-right corner of the application.
   Depending on the profile configuration, you are asked whether you want to add or change a PIN.
3. Select the option. If the profile is locked already, enter the original PIN, then click **OK**.
4. Type the new PIN, then type it again to confirm it, then click **OK**.
   The profile is locked.

### Add a master password for extra profile security
You can protect your profile using a PIN, or use a PIN and a master password to add an extra layer of security when you run Pledge on your computer.

Your administrator will specify whether you need a PIN to access the Pledge Software Token client application.

> McAfee recommends that you change your PIN and master password regularly.

### Task
1. Start the Pledge Software Token client application.
2. Click the Tools icon to open the **Tools** options, then click **Master Password**.
3. Click **Set password** to add or edit the master password.
4. Type the new password, then type it again to confirm it.
   Use strong password techniques to ensure that your profile is kept more securely.

5. Click OK to set the master password.

   To remove a master password, click Remove password.

Next time you start the Pledge Software Token client application, you will be asked to enter your master password.
The McAfee Pledge system
McAfee Pledge Software Token
McAfee OTP web-based services

Enroll for a Pledge profile, and use the Web Manager and Self Service web-based applications as an end user.

Contents
- Self Service
- Web Manager

Self Service

McAfee OTP includes a Self Service tool to let users reset their own password, manage secret question and answers, update their mobile numbers, and generate a PIN.

Users log on with a user name and password. If a user forgets their password, they can use their user name and one-time password, or answer a preregistered question.

Users can choose to view the Self Service site in various languages.

Log on to Self Service

Log on to the Self Service website and change the language you view the application in.

Task
1. Go to the URL https://<OTP_server_name>/selfservice/.
2. Click Settings | Language to change the language you selected.
   
   The software stores the language you selected for use by other McAfee OTP web services.
3. Enter your user name and password.
   
   If you forget your password, go to https://<OTP_server_name>/selfservice/module/selfservice/jsp/forgot.jsp and enter your user name and a one-time password.
### Management pages for self-administration

A user has three forms to choose from, depending on the configuration of their solution.

<table>
<thead>
<tr>
<th>Form</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Information</td>
<td>Update mobile telephone numbers, reset user passwords, and verify user information such as email address.</td>
</tr>
<tr>
<td>Secret Question and Answers</td>
<td>Allows users to configure their questions and answers. Displayed if the Secret Question and Answers feature is enabled.</td>
</tr>
<tr>
<td>PIN Code</td>
<td>Generates a PIN. If this form does not appear, a value is not configured for the PIN.</td>
</tr>
</tbody>
</table>

### Web Manager

McAfee OTP includes a tool to manage administrative tasks for users.

Using the Web Manager tool, administrators, and technical support can manage day-to-day tasks such as adding and changing PINs, assigning and resynchronizing tokens, and creating emergency one-time passwords.

Users can choose to view the Self Service and Web Manager websites in a variety of languages.

### Login page with username and password

https://<OTPiaddress>:<OTPortnumber>/webmanager. Port 8080 is used by default.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Click to view the Web Manager in the language you view your browser in. The software stores the language you selected for use with other McAfee OTP web services.</td>
</tr>
<tr>
<td>Manager User view</td>
<td>Search for users. To edit a user, double-click or right-click a user in the result set.</td>
</tr>
<tr>
<td>General Information</td>
<td>When editing a user, use these options:</td>
</tr>
<tr>
<td></td>
<td>• Disable one-time password protection — Allow a user to log on using their standard logon details, without one-time password authentication.</td>
</tr>
<tr>
<td></td>
<td>• Account locked by OTP — View whether the users account is locked.</td>
</tr>
<tr>
<td></td>
<td>• User Identity Verification — Verify whether users have OATH-tokens or PIN verification enabled.</td>
</tr>
<tr>
<td></td>
<td>• Mobile number — Change mobile number.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Manage Tokens     | Manages hardware tokens for users who need to have a hardware token assigned to them, or whose token has become unsynchronized with the token information held in the user object.  

You can specify a margin of unsynchronized tokens before the users account is prevented from logging on.  
Click **Assign token**, then choose an unassigned token ID from the list of tokens. Click the **Assign** link and select the user who you want to associate with this token. The user object is updated with the token.  
**Resynchronize OTP:**  
- **Enter first OTP** — Ask the user to generate a one-time password and enter it here.  
- **Enter second OTP** — Ask the user to generate a second one-time password and enter it here.  
- Click **Sync** to resynchronize the one-time password counters. |
| Emergency OTP     | When two-factor authentication is enabled, the user is asked for a one-time password. If the user forgot or lost their mobile device, they are unable to log on. To log on, you can create an emergency one-time password that you can give them for one use.  
Enable and configure the prefetch option your database object to be able to set up emergency one-time passwords. |
| PIN Code          | Generates a PIN for a user who has forgotten their PIN. |
Index

.NET integration 24

A
add master password
  Pledge Software Token Client 108
AES Encryption options 72–74
  Advanced Settings 73
  General Settings 73
  Test encryption and decryption 74
AES Encryption options, Misc object type 72
  Advanced Settings 73
  General Settings 73
  Test encryption and decryption 74
Alerts object type 86
  Alert Configuration 87
API
  integration 24
  Java 12

C
CIMD2 delivery method 64
CIMD2 delivery method, Delivery Method object type 64
Citrix
  integration modules 23
Client Software Development Kit (SDK) 12
Clients object type 47–53
  create 47
  delete 48
  duplicate 48
  RADIUS client 48
cluster
  active-active 92
  configuration requirements 91
  configure 91, 94
  configure using configuration console 74
  redundancy 92
  redundancy configuration 92, 93
  test configuration 93
  two-factor authentication 92
COM integration 24
computer platforms
  supported 107
Concurrent Sender delivery method 64
Concurrent Sender delivery method, Delivery Method object type 64
  configuration
    configuration console 19
  configuration checklist
    client 29
    databases 29
    McAfee OTP server 29
    McAfee Pledge 29
    McAfee SMS delivery 29
    RADIUS 29
    Web Manager 29
  configuration console
    elements 19
    internal 19
    mouse functions 21
    remote 19
    select pane 20
    tooltips 21
  configuration pane 19
  configure, Alerts object type
    Alert Configuration 87
  configure, Clients object type
    create 47
    delete 48
    duplicate 48
    Native client 51, 52
    RADIUS client 48–51
    Web services client 53
  configure, Databases object type
    create 36
    Database group 46
    delete 36
    duplicate 36
    LDAP 37–42
    RADIUS Forward database 45
    SQL 42–45
  configure, Delivery Method object type 55
    CIMD2 delivery method 64
    Concurrent Sender delivery method 64
    enable 55
    Extended HTTP delivery method 58–60
    HTTP delivery method 57, 58
    Netsize delivery method 62, 63
configure, Delivery Method object type 55 (continued)
  Prefetch Detection delivery method 65
  SMPP delivery method 64
  SMS Gateway delivery method 56–58
  SMTP delivery method 61
  UCP File delivery method 64, 65
configure, Licenses object type
  License Information 88
configure, Logs object type
  Log Files 85
  Other Settings 86
configure, McAfee OTP 29
  Alerts object type 86, 87
  Clients object type 47–53
  Databases object type 35–46
  Delivery Method object type 55–65
  Licenses object type 87, 88
  Logs object type 85, 86
  Misc object type 69–74, 76, 79–83, 111, 112
  RADIUS object type 34, 35
  Server object type 31–34
configure, Misc object type 69
  Admin Guide 80
  AES Encryption options 72–74
  Embedded HTTP Server Options 74
  Expired Password Notification settings 69
  Oath settings 70, 71
  OATH settings 70, 71
  Pledge Enrollment options 76
  Prefetch OTP options 71
  Self Service 80–82, 111, 112
  Unlock User Accounts options 72
  User Guide 111, 112
  Web Manager options 79, 80
  Yubico options 83
configure, RADIUS object type 34
  Additional Ports 35
  RADIUS Server Settings 35
configure, Server object type
  Client Settings 33
  Encryption 33
  Mobile Numbers 32
  Onetime Password Options 32
  Options 33
create, Databases object type
  LDAP 36

Databases object type, LDAP
  Account Settings (HOTP/TOTP Disabled) 39
  Account Settings (HOTP/TOTP Enabled) 39
  Advanced options 42
  create 36
  Host Settings 37
  Onetime Password Prefetch 40
  PIN Code 41
  Search Settings 38
Databases object type, RADIUS Forward database 45
Databases object type, SQL 42
  Advanced options 45
  JDBC/ODBC Settings 43
  Onetime Password Prefetch 45
  PIN code 45
  SQL Queries (HOTP/TOTP Disabled) 43
  SQL Queries (HOTP/TOTP Enabled) 44
Delivery Method object type 55–65
  enable 55
deployment
  checklist 12, 29
deployment considerations, McAfee OTP server 12
deployment considerations, McAfee SMS Gateway 12
deployment considerations, Pledge 12
details
  PIN 108
download
  client application to computer 107
  client application to smartphone 106

E
Embedded HTTP Server Options 74
Embedded HTTP Server Options, Misc object type 74
Expired Password Notification settings 69
  Expired Password Notification 69
Expired Password Notification settings, Misc object type 69
  Expired Password Notification 69
Extended HTTP delivery method 58–60
  Authentication and Proxy 60
  Headers or Template File 59
  Other Settings 60
Extended HTTP delivery method, Delivery Method object type 58
  Authentication and Proxy 60
  Headers or Template File 59
  Other Settings 60

G
generate one-time password 108

H
hardware
  requirements 15
HOTP keys 26
HTTP delivery method 57, 58
  Authentication 58
  Headers or Template file 57
HTTP delivery method, Delivery Method object type 57
  Authentication 58
  Headers or Template file 57

I
install, McAfee OTP 15
  requirements 15
  Windows-based computer 16
installation
  on a computer 107
  on a smartphone 106
integration
  APIs 24
  integration modules 23
  integration modules, McAfee OTP 23
  internal configuration console 19

J
Java
  API 12
  Java integration 24

L
LDAP
  supported user stores 11
  LDAP database 36
    Account Settings (HOTP/TOTP Disabled) 39
    Account Settings (HOTP/TOTP Enabled) 39
    Advanced options 42
    Host Settings 37
    Onetime Password Prefetch 40
    PIN Code 41
    Search Settings 38
Licenses object type 87
  License Information 88
Logs object type 85
  Log Files 85
  Other Settings 86

M
maintenance, McAfee OTP
  McAfee OTP monitor 89
manage your PIN
  Pledge Software Token Client 108
master password
  profile security 108
McAfee OTP
  configure 29
  install on a Windows-based computer 16
  installation 15
McAfee OTP (continued)
  installation requirements 15
  start 19
  start on a Linux-based computer 19
  start on a Mac OS X-based computer 19
  start on a UNIX-based computer 19
  stop 19
  stop on a Linux-based computer 19
  stop on a Mac OS X-based computer 19
  stop on a UNIX-based computer 19
McAfee OTP server configuration checks 29
  menu bar 19
Microsoft
  integration modules 23
Misc object type 69–74, 76, 79–83, 111, 112
  mouse functions 21

N
Native client 51, 52
  Advanced — Native Client Name Detection 52
    Options 52
    Other options 52
    User Database 52
Native client, Clients object type 51
  Advanced — Native Client Name Detection 52
    Options 52
    Other options 52
    User Database 52
Netsize delivery method 62, 63
  Authentication 63
  Communication 62
  Endpoint Settings 63
  Message 63
  Options 63
Netsize delivery method, Delivery Method object type 62
  Authentication 63
  Communication 62
  Endpoint Settings 63
  Message 63
  Options 63

O
Oath settings 70, 71
  Automatic OATH Enrollment 71
  General OATH Settings 70
  HOTP 70
  TOTP 70
OATH settings 70, 71
  Advanced automatic OATH enrollment 71
OATH settings, Misc object type 70
  Advanced automatic OATH enrollment 71
Oath, Misc object type
  Automatic OATH Enrollment 71
  General OATH Settings 70
  HOTP 70
  TOTP 70
one-time password
  generate 108
operating system
  requirements 15

P
platforms
  computer 107
  smartphone 106
Pledge 95
  about 95
  Pledge Enrollment 104
  Pledge Profile Factory 97
Pledge Enrollment
  administrator 105
  requirements 104
Pledge Enrollment options 76, 79
Pledge Enrollment options, Misc object type 76
Pledge Software Token Client
  add master password 108
  generate one-time password 108
  installation on computer 107
  installation on smartphone 106
  manage your PIN 108
  supported computer platforms 107
  supported smartphone platforms 106
  update your PIN 108
Prefetch Detection delivery method 65
Prefetch Detection delivery method, Delivery Method object type 65
Prefetch OTP options 71
Prefetch OTP options, Misc object type 71
profile
  add a PIN 108
  install on a computer 107
  install on a smartphone 106
  password 108
protocols
  supported 11

R
RADIUS
  access 24
  RADIUS checks 29
RADIUS client 48–51 (continued)
  Prefetch OTP Options 50
  RADIUS Client Attribute Detection 49
  RADIUS Options 50
  RADIUS Reject Error Messages 49
  User Database 51
RADIUS client, Clients object type
  Advanced settings 48
  Encoding 49
  Listen on RADIUS Ports 49
  Other options 51
  Prefetch OTP Options 50
  RADIUS Client Attribute Detection 49
  RADIUS Options 50
  RADIUS Reject Error Messages 49
  User Database 51
RADIUS Forward database 45
RADIUS object type 34
  Additional Ports 35
  RADIUS Server Settings 35
remote configuration console 19
requirements
  hardware and virtual machine 15
  operating system 15
  software 15
  virtual machine 15

S
security
  add a PIN 108
  profile password 108
select pane 19, 20
Self Service 80–82, 111, 112
  Configuration settings 80
  Information) 82
  Lockout) 82
  Log on page with username and password) 111
  Management pages for self administration 112
  Secret Question and Answer (Q/A) 81
Self Service, Misc object type 80, 111
  Admin Guide 80
  Configuration settings 80
  Information) 82
  Lockout) 82
  Log on page with username and password) 111
  Management pages for self administration 112
  Secret Question and Answer (Q/A) 81
  User Guide 111
Server object type 31
  Client Settings 33
  Encryption 33
  Global Options 34
  Mobile Numbers 32
  Onetime Password Options 32
Server object type 31 (continued)
  Options 33
  Smartphone Settings 31
smartphone platforms supported 106
SMPP delivery method 64
SMPP delivery method, Delivery Method object type 64
SMS Gateway delivery method 56–58
  Advanceds 57
  Configuration and Status 57
  General Settings and Proxy 56
  Location 57
  Other Settings 58
  Proxy 58
SMS Gateway delivery method, Delivery Method object type 56
  Advanced 57
  Configuration and Status 57
  General Settings and Proxy 56
  Location 57
  Other Settings 58
  Proxy 58
SMTP delivery method 61
  Authentication 61
  SMTP Host 61
  SMTP Options 61
SMTP delivery method, Delivery Method object type 61
  Authentication 61
  SMTP Host 61
  SMTP Options 61
software requirements 15
SQL
  supported user stores 11
SQL database 42
  Advanced options 45
  JDBC/ODBC Settings 43
  OneTime Password Prefetch 45
  PIN code 45
  SQL Queries (HOTP/OTP Disabled) 43
  SQL Queries (HOTP/OTP Enabled) 44
supported platforms
  computer 107
  smartphone 106
supported protocols 11
supported user databases 11

T
Tools
  master password 108
tooltips 21
TOTP 26

U
UCP File delivery method 64, 65
  UCP File Options 65
UCP File delivery method, Delivery Method object type 64
  UCP File Options 65
Unlock User Accounts options 72
Unlock User Accounts options, Misc object type 72
update your PIN
  Pledge Software Token Client 108
user interface 19
user stores supported 11

V
virtual machine requirements 15
VPN access 24

W
Web Manager 112
Web Manager options 79, 80
  Authentication settings 79
  Other settings 80
Web Manager options, Misc object type 79
  Authentication settings 79
  Other settings 80
Web Manager, Misc object type 112
  User Guide 112
Web service client, Clients object type
  Options 53
  Other Options 53
  User Database 53
Web services client 53
  Options 53
  Other Options 53
  User Database 53
Web services client, Clients object type 53

Y
Yubico 83
Yubico options, Misc object type 83