# Document Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Description</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>001US</td>
<td>McAfee® One Time Password Server Administration Guide V3.1</td>
<td>October 2012</td>
</tr>
</tbody>
</table>
## Contents

1.0 **Terms and Acronyms** ........................................................................................................ 9
   1.1 Useful Terms .................................................................................................................. 9
   1.2 Useful Acronyms ......................................................................................................... 10

2.0 **Overview** .................................................................................................................. 13
   2.1 Supported Operating Systems ..................................................................................... 14
   2.2 User Database Support ............................................................................................... 15
   2.3 Protocol Support ........................................................................................................ 15
   2.4 OTP Client Software Development Kit (SDK) ............................................................. 15

3.0 **What's New** ............................................................................................................... 17
   3.1 What's New in V3 ....................................................................................................... 17
   3.2 What's New in V3.1 .................................................................................................... 18

4.0 **McAfee® OTP Server Features** ................................................................................. 19

5.0 **Integration Overview** ................................................................................................ 21
   5.1 Integration Modules ..................................................................................................... 22
   5.2 VPN/RADIUS Access .............................................................................................. 23
   5.3 Programming APIs .................................................................................................... 23

6.0 **Installation** ................................................................................................................ 25
   6.1 Installation Requirements ......................................................................................... 25
   6.2 Install McAfee® OTP Server on Windows ................................................................... 26

7.0 **Administration Console** ........................................................................................... 37
   7.1 Select Pane ................................................................................................................ 38
   7.2 Other Features .......................................................................................................... 39

8.0 **Configuration Overview** ............................................................................................ 41

9.0 **Configuring the Server Object Type** ......................................................................... 43
   9.1 Server Settings .......................................................................................................... 44
   9.2 Mobile Numbers ....................................................................................................... 44
   9.3 One-time Password Options ...................................................................................... 44
   9.4 Client Settings .......................................................................................................... 45
   9.5 Encryption ................................................................................................................ 46
   9.6 Options ..................................................................................................................... 46
   9.7 Global Options .......................................................................................................... 46

10.0 **Configuring the RADIUS Object Type** .................................................................... 49
   10.1 RADIUS Server Settings ....................................................................................... 50
   10.2 Additional Ports ....................................................................................................... 50

11.0 **Logs** .......................................................................................................................... 51
   11.1 Log Files ................................................................................................................ 52
   11.2 Other Settings ......................................................................................................... 52

12.0 **Alerts** ....................................................................................................................... 53
   12.1 Alert Configuration .................................................................................................. 54

13.0 **Licenses** .................................................................................................................... 55
   13.1 License Information ............................................................................................... 56

14.0 **Configuring the Databases Object Type** ................................................................. 57
   14.1 The OATH Database Option .................................................................................... 57
   14.2 Creating an LDAP Database .................................................................................... 58
14.2.1 Host Settings .................................................................................................. 59
14.2.2 Search Settings ............................................................................................ 59
14.2.3 Account Settings (HOTP/TOTP Disabled) ....................................................... 60
14.2.4 Account Settings (HOTP/TOTP Enabled) ....................................................... 61
14.2.5 One-time Password Prefetch ....................................................................... 62
14.2.6 PIN Code ..................................................................................................... 63
14.2.7 Advanced Options ....................................................................................... 64
14.3 Creating a SQL Database ................................................................................... 65
14.3.1 JDBC/ODBC Settings ............................................................................... 66
14.3.2 SQL Queries (HOTP/TOTP Disabled) ........................................................... 66
14.3.3 SQL Queries (HOTP/TOTP Enabled) ............................................................ 67
14.3.4 One-time Password Prefetch ....................................................................... 67
14.3.5 PIN Code ..................................................................................................... 67
14.3.6 Advanced Options ....................................................................................... 68
14.4 Creating a RADIUS Forward Database .......................................................... 68
14.5 Creating a Database Group ............................................................................... 69

15.0 Configuring the Clients Object Type ............................................................... 71
15.1 Creating a RADIUS Client ............................................................................... 72
15.1.1 Advanced Options ....................................................................................... 73
15.1.2 RADIUS Options ....................................................................................... 74
15.1.3 User Database ............................................................................................. 74
15.1.4 Other Options ............................................................................................. 75
15.1.5 Prefetch OTP Options ................................................................................ 75
15.2 Creating a Native Client .................................................................................. 76
15.2.1 Advanced — Native Client Name Detection ............................................... 77
15.2.2 Options ....................................................................................................... 77
15.2.3 User Database ............................................................................................. 77
15.2.4 Other Options ............................................................................................. 77
15.3 Creating a Web Services Client ...................................................................... 78
15.3.1 Options ....................................................................................................... 79
15.3.2 User Database ............................................................................................. 79
15.3.3 Other Options ............................................................................................. 79

16.0 Configuring the Delivery Methods Object Type ............................................. 81
16.1 McAfee® SMS Gateway .................................................................................. 82
16.1.1 General Settings and Proxy Areas ............................................................... 83
16.1.2 Location ...................................................................................................... 83
16.1.3 Configuration and Status .......................................................................... 84
16.1.4 Advanced ................................................................................................... 84
16.2 HTTP ............................................................................................................... 85
16.2.1 Headers or Template File .......................................................................... 86
16.2.2 Authentication ............................................................................................ 86
16.2.3 Proxy .......................................................................................................... 86
16.2.4 Other Settings ............................................................................................. 87
16.3 Extended HTTP .............................................................................................. 88
16.3.1 Headers or Template File .......................................................................... 89
16.3.2 Authentication and Proxy ......................................................................... 90
16.3.3 Other Settings ............................................................................................. 91
16.4 SMTP ............................................................................................................... 92
16.4.1 SMTP Host ................................................................................................. 93
16.4.2 Authentication ............................................................................................ 93
16.4.3 SMTP Options ........................................................................................... 94
16.5 Netsize ............................................................................................................. 95
16.5.1 Communication .......................................................................................... 95
16.5.2 Authentication ........................................................................................... 96
16.5.3 Message ............................................................................................... 96
16.5.4 Endpoint Settings .................................................................................. 96
16.5.5 Options .................................................................................................. 96
16.6 Concurrent Sender ............................................................................................ 97
16.7 Instant Messaging ............................................................................................. 98
  16.7.1 The User Prefix Feature ........................................................................... 98
  16.7.2 Skype ................................................................................................... 99
  16.7.3 Microsoft Live (MSN) ............................................................................. 100
  16.7.4 Jabber (Google Talk) ............................................................................ 101
16.8 SMPP ............................................................................................................. 102
16.9 CIMD2 .......................................................................................................... 103
16.10 UCP File ...................................................................................................... 104
  16.10.1 UCP File Options .................................................................................. 105

17.0 Misc ....................................................................................................................... 107
  17.1 Expired Password Notification ................................................................ 108
    17.1.1 Expired Password Notification ................................................................ 108
  17.2 OATH Configuration ...................................................................................... 109
    17.2.1 HOTP .................................................................................................. 110
    17.2.2 TOTP .................................................................................................. 110
    17.2.3 General OATH Settings .......................................................................... 110
    17.2.4 Automatic OATH Enrollment .................................................................. 111
    17.2.5 Advanced Automatic OATH Enrollment ................................................... 112
  17.3 Prefetch Proxy Config ....................................................................................... 113
  17.4 AES Encryption ............................................................................................... 114
    17.4.1 General Settings .................................................................................. 114
    17.4.2 Advanced Settings ................................................................................ 115
    17.4.3 Test Encryption and Decryption ............................................................ 115
  17.5 Embedded HTTP Server .................................................................................. 116
  17.6 Pledge Enrollment ........................................................................................... 117
  17.7 Web Manager .................................................................................................. 118
  17.8 Yubico ........................................................................................................... 119

18.0 Starting and Stopping McAfee® OTP Server .......................................................... 121
  18.1 Starting and Stopping on Windows .................................................................. 121
  18.2 Starting and Stopping on UNIX ................................................................. 121

19.0 The McAfee® OTP Server Monitor ....................................................................... 123
  19.1 McAfee® OTP Server Statistics .................................................................. 124
    19.1.1 Sending One-time Passwords .............................................................. 125
    19.1.2 One-time Passwords ............................................................................. 125
    19.1.3 RADIUS .............................................................................................. 125
    19.1.4 Licenses ............................................................................................... 125
    19.1.5 Connections ........................................................................................ 126
    19.1.6 Encryption ........................................................................................... 126
    19.1.7 User Database Authentication ............................................................... 126

20.0 On-demand Services ............................................................................................. 127
1.0 Terms and Acronyms

Administrators of McAfee® One Time Password Server (McAfee® OTP Server) need to know many of the following terms and acronyms.

1.1 Useful Terms

This section includes many of the terms referenced in this guide.

**Authentication**
Authentication is the process of verifying that users are who they assert they are.

**Authorization**
Authorization is the process of deciding what resources users can access based on who they are and what permissions they have.

**JDBC**
Java Database Connectivity (JDBC) is an application program interface (API) specification for connecting programs written in Java to the data in popular databases.

**ODBC**
Open Database Connectivity (ODBC) is an open standard application programming interface (API) for accessing a database.

**LDAP**
Lightweight Directory Access Protocol (LDAP) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP).

**OATH**
Open Authentication (OATH) is an open standard that enables strong authentication for devices from multiple vendors. McAfee® OTP Server provides support for tokens that use the OATH HOTP and TOTP standards.

**RADIUS**
Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol and software that enables remote access servers to communicate with a central server for the purpose of authenticating dial-in users and authorizing their access to the requested system or service.

**OTP Client**
A native OTP client communicates with McAfee® OTP Server through an API.

**OTP Service**
Instead of installing McAfee® OTP Server, customers access the OTP service on-demand through web services.
**Pledge**

Pledge is an OTP client that is installed on a mobile device. Using the OATH standards HOTP (RFC 4226) and TOTP (RFC 6238), Pledge converts the mobile device into a security token.

### 1.2 Useful Acronyms

This section includes many of the acronyms referenced in this guide.

- **AES**
  - Advanced Encryption Standard

- **AJP**
  - Apache JServ Protocol

- **API**
  - Application Programming Interface

- **CBC**
  - Cipher-block Chaining

- **CIMD**
  - Computer Interface Message Distribution

- **DN**
  - Distinguished Name

- **DNS**
  - Domain Name System

- **HOTP**
  - HMAC-based One Time Password algorithm

- **HTTP**
  - Hypertext Transfer Protocol

- **HTTPS**
  - Secure Hypertext Transfer Protocol

- **IM**
  - Instant Messaging

- **IV**
  - Initialization Vector

- **JDBC**
  - Java Database Connectivity

- **JVM**
  - Java Virtual Machine

- **LDAP**
  - Lightweight Directory Access Protocol

- **LDAPS**
  - Secure Lightweight Directory Access Protocol
Terms and Acronyms

MD5
Message Digest Algorithm

MIME
Multipurpose Internet Mail Extensions

OATH
Initiative for Open Authentication

ODBC
Open Database Connectivity

OTP
One Time Password

PSKC
Portable Symmetric Key Container

RADIUS
Remote Authentication Dial in User System

RFC
Request for Comments

SDK
Software Development Kit

SHA
Secure Hash Algorithm

SMPP
Short Message Peer-to-Peer

SMS
Short Message Service

SMTP
Simple Message Transfer Protocol

SOAP
Simple Object Access Protocol

SQL
Structured Query Language

SSHA
Salted Secure Hash Algorithm

SSL
Secure Sockets Layer

TCP
Transmission Control Protocol

TLS
Transport Layer Security
Terms and Acronyms

**TOTP**
Time-based One Time Password algorithm

**UCP**
Uniformity Correction Parameters

**UDP**
User Datagram Protocol

**VM**
Virtual Machine

**VPN**
Virtual Private Network
2.0 Overview

McAfee® One Time Password Server (McAfee® OTP Server) adds an extra layer of security that is flexible and efficient to implement and that protects applications and systems with strong, multi-factor authentication. For example, combining user name and password authentication with one-time password as the second authentication method on a mobile device protects the authentication process and the "key" to an organization's applications and systems.

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

McAfee® OTP Server generates and distributes one-time passwords to end users by a variety of methods, including email, Short Message Service (SMS) to a mobile phone, and Instant Messaging (IM) services such as Google* Talk*, Microsoft* MSN* Messenger*, and Skype*.

McAfee® OTP Server supports token devices that generate one-time passwords using the HOTP (RFC 4226) and TOTP (RFC 6238) OATH standards. In addition, McAfee® offers Pledge, an OTP client that when installed on a mobile device generates one-time passwords using the OATH standard.

You can integrate McAfee® OTP Server with applications and systems that support RADIUS. You can also integrate McAfee® OTP Server using one of the many native integration modules that McAfee® provides. Integration modules exist for Apache* Reverse Proxy and Web Server*, Citrix*, Microsoft IIS*, Microsoft Outlook Web Access*, Novell* GroupWise WebAccess*, VPN (including Cisco*, Check Point*, F5*, Blue Coat*, and Juniper*), and more. Other applications can be integrated with McAfee® OTP Server using APIs or web services.

**Note:** RADIUS is an acronym for Remote Authentication Dial in User System.
2.1 Supported Operating Systems

McAfee® OTP Server supports any operating system that has support for Java* Virtual Machine* (JVM) version 1.6 or higher. For example, McAfee® OTP Server supports 32-bit and 64-bit versions of the following operating systems:

- Microsoft Windows Server 2003/2008* R2 and earlier
- Linux*
- Sun* Solaris*
- IBM* AIX*
- Apple* MAC OS X*
2.2 User Database Support

McAfee® OTP Server supports the following user stores:

- LDAP (including Sun* Directory Server*, Microsoft Active Directory*, and Novell* eDirectory*)
- SQL through JDBC or ODBC (including Oracle*, Microsoft SQL Server*, and MySQL*)

Note: Other user stores are supported through APIs.

2.3 Protocol Support

McAfee® OTP Server supports the following protocols:

- LDAP
- HTTP/HTTPS
- SMPP
- SMTP
- Web Services/SOAP
- NetSize
- CIMD2
- Instant Messaging (including Google Talk, Microsoft MSN Messenger, and Skype)

2.4 OTP Client Software Development Kit (SDK)

You can use the Java Client API to integrate McAfee® OTP Server with applications for which there is no integration module. For information about downloading the COM*/.NET* APIs, visit https://mysupport.mcafee.com.

For information about integrating Microsoft .NET applications using the Java Client API, visit the following link:

https://kc.mcafee.com/corporate/index?page=content&id=KB76374
What's New

3.0 What’s New

This chapter details what’s new in McAfee® OTP Server V3 and V3.1.

3.1 What’s New in V3

The following features have been improved or added in McAfee® OTP Server V3:

- **Configuration Interface** — The functionality and logic of the configuration interface have been improved, making configuration of McAfee® OTP Server easier.

- **Identity Manager** — McAfee® OTP Server is now shipped with a preconfigured version of the Identity Manager Portal installed on the Apache Tomcat® server. Administrators and help desk personnel can use the Portal to manage user information in user stores (databases). End users can also use the Portal to update information in their accounts.

- **Pledge Enrollment** — Using a web application installed on the Tomcat server, end users follow an easy, step-by-step Pledge Enrollment process that downloads a Pledge Profile which includes an HOTP key. Using a web services interface that is integrated with the Profile Factory, administrators can customize the Pledge Profile. **Note:** For more information about Pledge Enrollment, see the step-by-step guide on implementing Pledge Enrollment to McAfee® OTP Server.

- **Expired Password Notification** — McAfee® OTP Server detects when a password expires and then notifies end users.

- **RADIUS Attribute Detection** — McAfee® OTP Server can recognize different connections from the same RADIUS client based on the request type and RADIUS attributes.

- **RADIUS Forward** — RADIUS Forward is a new database type, which McAfee® OTP Server can use to pass through and forward a RADIUS request to another RADIUS server. In addition to supporting integration with other RADIUS servers, RADIUS Forward supports RSA SecurID and SafeWord tokens as well as the migration of legacy tokens.

- **Yubico YubiKey** — McAfee® OTP Server supports the one-time password that YubiKey generates in OATH-HOTP mode using the standard RFC 4226 HOTP algorithm and encrypts using the AES algorithm. McAfee® OTP Server has added support for the Yubico validation server through web services and stores AES keys locally in a SQL database or LDAP directory. Keys are easily imported and stored, supporting automatic OTP enrollment. **Note:** AES is an acronym for Advanced Encryption Standard.

- **Multiple RADIUS UDP Ports** — You can configure the McAfee® OTP Server RADIUS module to listen on multiple UDP ports. This enhancement supports the assignment of clients to specific ports.
• External OTP Creation and Verification — McAfee® OTP Server supports any algorithm that creates and verifies one-time passwords through an API.

• Native OTP Client Names — McAfee® OTP Server supports native clients through an API. McAfee® OTP Server now supports multiple native clients at one IP address by allowing you to assign a name to each client’s integration module. In this way, each client can be separately configured in McAfee® OTP Server.

### 3.2 What’s New in V3.1

The following features have been improved or added in McAfee® OTP Server V3.1:

• **New OTP Client Type** — McAfee® OTP Server supports a new OTP client type through an API for any application or system using SOAP-based web services. For more information, see the McAfee® OTP Server guide to the Web Service Client API (SOAP).

• **OTP Delivery Method Configuration** — You can now configure the OTP delivery method at the OTP client level. This feature overrides the automatic delivery method selection.

• **Hashed PIN Codes** — McAfee® OTP Server supports the following hash functions applied to a PIN code: MD5, SHS, and SSHA.

• **Custom RADIUS Reject Messages** — You can customize the messages returned when authentication fails, a system error occurs, or a one-time password is entered incorrectly.

• **TOTP Anti-replay Check** — The McAfee® OTP Server keeps track of the one-time passwords used. For each TOTP device, the anti-replay check feature restricts one-time password use to once during a specified time interval.

• **Maximum Steps to Sync TOTP Device** — You can configure the maximum number of steps end users are allowed to sync a TOTP device with the McAfee® OTP Server during a specified time interval.

• **OTP Retry Function** — The OTP retry function allows end users to easily reenter the one-time password after failing to enter the password correctly the first time.

• **API to Sync OATH HOTP/TOTP Devices** — Using a new API, you can sync OATH HOTP/TOTP devices by sending two one-time passwords in sequence. For more information, visit the following link:
  https://kc.mcafee.com/corporate/index?page=content&id=KB76278

• **Multiple OATH Key Support for SQL Databases** — McAfee® OTP Server now provides multiple OATH key support for SQL databases.
McAfee® OTP Server Features

4.0 McAfee® OTP Server Features

McAfee® OTP Server has the following features:

**SMS and Email Delivery of One-time Passwords**
McAfee® OTP Server delivers one-time passwords using SMS and email, providing two-factor authentication for end users who want remote access to applications.

**McAfee® Short Message Service Module (McAfee® SMS Module)**
The McAfee® SMS Module is a plug-in that delivers one-time passwords using the McAfee® SMS Gateway. The module is easy to set up and provides status controls, usage statistics, and automatic failover for lapses in SMS service.

**A Trial Account Is Created for You on McAfee® SMS Gateway**
When you install a new version of the McAfee® OTP Server, a trial account is automatically created for you on the McAfee® SMS Gateway. You can later replace the trial account with a production account or other method of SMS delivery.

**LDAP User Stores**
You can use any LDAP-compliant directory service to look up users and user attributes. McAfee® OTP Server does not require proprietary user stores.

**SQL User Stores**
You can use any JDBC-compliant database to look up users and user attributes. McAfee® OTP Server does not require proprietary user stores.

**Multiple User Stores**
For each OTP client, there is no limit on the number of user stores that can be added. For example, you can add multiple user stores for failover. However, when one set of users is saved in two different user stores, configure SMS delivery for the users in one store and email delivery for users in the other store.

**Test Tool**
The Test Tool is a stand-alone application that you can use to test the McAfee® OTP Server. Use this tool to test whether the user store is configured correctly and the one-time password distribution plug-in is working as expected. The Test Tool supports the OTP native API and RADIUS protocol.

**Remote Configuration**
You can use the API to read and set the McAfee® OTP Server configuration from a remote client. This API function is ideal for bundled applications, servers with limited access, and graphical interfaces.

**Pledge**
Pledge is an OTP client that you download and install on a mobile device. Pledge provides strong authentication by generating one-time passwords using the OATH algorithm. Pledge supports multiple platforms, including iPhone®, Android®, Windows Mobile®, and any mobile phone that supports Java Platform, Micro Edition® (Java ME).
OATH Support
McAfee® OTP Server supports tokens based on the OATH HOTP/TOTP standard.

Alerts
You can configure McAfee® OTP Server to send error messages and alerts to one or more administrators using SMS or email.

Easy Configuration
You can configure McAfee® OTP Server, including a full user store, SMS delivery, and application integration, in less than one day.

Java, COM, and .NET APIs
Using APIs, you can create custom integration modules for your applications.

Plug-in Interface
Using the plug-in interface, you can write a custom OTP distribution plug-in.

Custom User Store Handler
If the user stores have special requirements, advanced users can write a custom database handler that overrides the internal database handler.

PIN Codes for One-time Passwords
Using this feature, you can add a PIN code to the one-time password for added protection. PIN codes are stored in the user directory.

Prefetch One-time Passwords
The Prefetch feature allows end users and administrators to store one-time passwords when there is no mobile coverage. For example, one-time passwords can be stored as text in a mobile or email account or printed on cards or paper. This feature is controlled by a web administration application.

Failover User Stores and OTP Servers
You can configure user stores in groups for failover. All client integrations can be configured for multiple OTP Servers.

RADIUS Support
McAfee® OTP Server can act as a RADIUS server to support any RADIUS-aware application. Most VPN solutions have RADIUS support, including Cisco, Check Point, AppGate®, and Juniper.

Integration Modules

Platform Independence
McAfee® OTP Server can be run on any Java-compliant platform, including Windows, Linux, Solaris, HP-UX®, and Mac OS X.

Session Data
McAfee® OTP Server can store both persistent and one-time session data. This feature supports single sign-on.

User Attributes
Using APIs, you can retrieve any available user attribute from the directory service.
5.0 Integration Overview

McAfee® OTP Server can be integrated with applications and systems through integration modules. For example, McAfee® OTP Server can be integrated with most VPN services using a RADIUS integration module. Because McAfee® OTP Server can act as a RADIUS server, most VPN/RADIUS-aware products can be integrated without any installation. Configuring the McAfee® OTP Server and the VPN/RADIUS product completes the integration.

Using Java, COM, and .NET 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. Or you can integrate custom applications by accessing the hosted OTP service version of the product on-demand through web services.
### 5.1 Integration Modules

McAfee® OTP Server supports the integration modules in the following table:

<table>
<thead>
<tr>
<th>Module</th>
<th>Integration Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apache</strong></td>
<td>Apache Reverse Proxy Server</td>
</tr>
<tr>
<td></td>
<td>Apache Web Server 1.3/2.0</td>
</tr>
<tr>
<td>CA</td>
<td>SiteMinder</td>
</tr>
<tr>
<td><strong>Citrix</strong></td>
<td>Citrix Access Gateway 4.2</td>
</tr>
<tr>
<td></td>
<td>Citrix Access Gateway 4.5</td>
</tr>
<tr>
<td></td>
<td>Citrix Access Gateway 5.X VPX</td>
</tr>
<tr>
<td></td>
<td>Citrix Access Gateway Enterprise Edition (NetScaler VPX)</td>
</tr>
<tr>
<td></td>
<td>Citrix Presentation Server 4.6</td>
</tr>
<tr>
<td></td>
<td>Citrix Web Interface 4.0/4.2</td>
</tr>
<tr>
<td></td>
<td>Citrix Web Interface 4.5</td>
</tr>
<tr>
<td></td>
<td>Citrix Web Interface 5.4</td>
</tr>
<tr>
<td></td>
<td>Citrix XenApp Server 5.1</td>
</tr>
<tr>
<td></td>
<td>Citrix XenApp Server 5.2/5.3</td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>Lotus Domino* (Apache Proxy)</td>
</tr>
<tr>
<td><strong>Microsoft</strong></td>
<td>ISA Server 2006</td>
</tr>
<tr>
<td></td>
<td>TMG 2010</td>
</tr>
<tr>
<td></td>
<td>UAG 2010</td>
</tr>
<tr>
<td></td>
<td>IIS 6.0</td>
</tr>
<tr>
<td></td>
<td>IIS 7.x - IIS Custom AD Membership Provider - ASP.NET</td>
</tr>
<tr>
<td></td>
<td>Outlook Web Access 2003</td>
</tr>
<tr>
<td></td>
<td>Outlook Web Access 2007</td>
</tr>
<tr>
<td></td>
<td>SharePoint 2007 AD Membership Provider - ASP.NET</td>
</tr>
<tr>
<td></td>
<td>SharePoint 2010 AD Membership Provider - ASP.NET</td>
</tr>
<tr>
<td></td>
<td>IIS Custom AD Membership Provider - ASP.NET</td>
</tr>
<tr>
<td></td>
<td>EPiServer AD Membership Provider - ASP.NET</td>
</tr>
<tr>
<td></td>
<td>EPiServer SQL Membership Provider - ASP.NET</td>
</tr>
<tr>
<td><strong>Novell</strong></td>
<td>IChain* 2.3</td>
</tr>
<tr>
<td></td>
<td>Novell Access Manager*</td>
</tr>
<tr>
<td></td>
<td>GroupWise WebAccess 6</td>
</tr>
<tr>
<td></td>
<td>GroupWise WebAccess 7</td>
</tr>
</tbody>
</table>

**Note:** For information about new and updated integration modules and configuration guides, visit [https://mysupport.mcafee.com](https://mysupport.mcafee.com).
Integration Overview

5.2 VPN/RADIUS Access

McAfee® OTP Server can act as a RADIUS server to support most VPNs and other RADIUS-aware applications. For the best integration, we recommend that the VPN/RADIUS application support the RADIUS challenge/response standard.

The following list shows some of the vendors that have been tested and approved:

- Cisco
- Check Point
- F5
- Juniper
- Palo Alto*
- AppGate

5.3 Programming APIs

McAfee® OTP Server can be integrated with custom applications through its Java, COM, and .NET APIs.
Integration Overview
6.0 Installation

This chapter includes requirements and instructions for installing McAfee® OTP Server on a Windows platform.

6.1 Installation Requirements

The requirements for installing McAfee® OTP Server are:

Hardware Server or Virtual Machine (VM)
- The McAfee® OTP Server is software that you install on any server in your internal network or DMZ.
- You can 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 an IP address configured.
- If you configure the McAfee® OTP Server using DNS names, then the hardware server must be able to contact DNS servers.

Operating System
- You can install McAfee® OTP Server on any operating system that supports Java Virtual Machine (Java VM) version 1.6 or higher, including Microsoft Windows (2003/2008 R2 and earlier versions), Linux, Sun Solaris, IBM AIX, MAC OS X.
- You can install McAfee® OTP Server on both 32-bit and 64-bit operating systems.

Communication
- The McAfee® OTP Server queries your LDAP or JDBC user store using default TCP ports 389 for LDAP and 636 for secure LDAP (LDAPS).
- Integration modules must send requests to McAfee® OTP Server using TCP port 3100. RADIUS modules must send requests using UDP port 1645 or 1812.
- To use McAfee® SMS Module, configure the McAfee® OTP Server to send one-time passwords to the SMS service over HTTPS on TCP port 443.

Software
- When registering and downloading the software, select the version of the installer that correctly corresponds to your operating system platform.
6.2 Install McAfee® OTP Server on Windows

You can use the installation process on Windows as a guide for how installation is done on other operating system platforms. For each operating system platform, there are two versions of the installer. In one version, the software is bundled with Java; in the other version, it is not. In the following procedure, the software is bundled with Java, which is the recommended version.

To install McAfee® OTP Server on Windows

1. Start the installation program: otp3install.exe.
   The Introduction opens.

2. Click Next.
   The License Agreement step opens.
3. Read the license agreement, select the **I accept the terms of the License Agreement** option, and click **Next**. The Select Install Set step opens.
4. Select the **Full Installation** or **Remote Configuration Only** option, and click **Next**.

The Choose Install Folder step opens.
Installation

5. Specify an installation folder, or accept the default value, and click **Next**. The Select License File step opens.
6. Specify the location of the license.dat file that you received from McAfee®, and click **Next**.

The Install Windows Service step opens.
Installation

7. To install the software as a Windows service, select the **Install Windows Service** check box, and click **Next**. The Choose Link Folder step opens.
8. Specify where you want the installer to create shortcuts to the software, and click Next. The shortcuts are identified by a product icon. You click the icon to manually start the McAfee® OTP Server. The Pre-Installation Summary opens.
9. Review the Pre-Installation Summary, and click **Install**.
The Install Complete step opens.
10. Click **Next**.
   The Start the OTP Server step opens.
11. To start the McAfee® OTP Server, select the **Yes** option, and click **Done**. The installer closes, and the McAfee® OTP Server opens.
Installation
7.0 Administration Console

To open the administration console, where you perform all configuration tasks, perform one of the following steps:

- Click the product icon created when McAfee® OTP Server is installed.
- Start the McAfee® OTP Server process, and then click **Configuration**.

The administration console consists of the following features:

- **Menu Bar** — From the Menu Bar, you can create configuration objects, update functions, and access help.
- **Select Pane (left)** — On the Select Pane, you can select the type of object that you want to create, configure, delete, or view.
- **Configuration Pane (right)** — When you select an object type on the Select Pane, you can view the object’s configuration options on the Configuration Pane.
- **Save Config** — When you click **Save Config**, the configuration is saved to the otp.properties file in the installation directory.
- **Close** — When you click **Close**, the administration console closes.
7.1 Select Pane

In the Select Pane, you select the type of object that you want to create, configure, delete, or view. The object types are:

- **Server** — Select this object type to configure the McAfee® OTP Server. Configuration options include IP address, port number, OTP length, and the OTP clients that are allowed to connect to the server.
- **RADIUS** — Select this object type to configure McAfee® OTP Server as a RADIUS server for RADIUS clients.
- **Logs** — Select this object type to configure logging and the log files.
- **Alerts** — Select this object type to configure error messages and alerts that can be sent to a list of administrators using SMS or email.
- **Licenses** — Select this object type to configure license information and options.
- **Databases** — Select this object type to configure connections to user stores.
- **Clients** — Select this object type to provide configuration information that a client can use to connect to McAfee® OTP Server and to access a database.
- **Delivery Methods** — Select this object type to configure and enable one or more OTP delivery methods for the McAfee® OTP Server. Available methods include:
  - CIMD2
  - Concurrent Sender
  - Extended HTTP
  - HTTP
  - Instant Messaging
  - NetSize*
  - McAfee® SMS
  - SMPP
  - SMTP
  - UCP File
- **Miscellaneous** — Select this object type to configure the following functions:
  - Expired Password Notification
  - OATH Configuration
  - Prefetch Proxy Config
  - Unlock User Accounts
  - AES Encryption
  - Embedded HTTP Server
  - Pledge Enrollment
  - Web Manager
  - Yubico
7.2 Other Features

The administration console supports the following mouse functions:

- **Tool tips** — Provide context-sensitive help.
- **Mouse left-click** — 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.
- **Mouse right-click** — Opens a context menu for the selected object type in the Select Pane.
8.0 Configuration Overview

To configure McAfee® OTP Server, you configure the following object types in the administration console:

1. Server — Configure the port number, IP address, OTP length, and the allowed clients.
2. RADIUS — To configure McAfee® OTP Server as a RADIUS server, select the “Enable RADIUS” check box, and then configure the Radius Server Settings.
3. Logs and Alerts — Configure options for the Logs and Alerts object types.
4. Databases — Configure connections to one or more user stores. The information in user stores is used to authenticate users.
5. Clients — Create an OTP client, configure a connection to the client, and specify the database used by the client to authenticate users.
6. Delivery Methods — Select, enable, and configure the delivery method that McAfee® OTP Server uses to deliver the one-time password.
7. Misc — Optionally configure the functions of this object type.

Note: For more information, see the McAfee® OTP Server step-by-step implementation guides.
To configure McAfee® OTP Server, select the Server object type in the Select Pane. Server configuration options open in the Configuration Pane, as shown in the following screenshot. Configure the port number, IP address, OTP length, and the allowed clients. For complete information about the settings on the Configuration Pane, see the sections in this chapter. Each section corresponds to a different heading on the Configuration Pane.
9.1 Server Settings

The following settings are located in the Server Settings area on the Server Configuration Pane:

**Port number**
- Specifies the port number that native OTP clients use when connecting to the McAfee® OTP Server.
- **Default:** 3100

**Bind to IP Address**
- Specifies the IP address of the hardware server on which the McAfee® OTP Server software is installed.

- **All**
  - Selecting this check box specifies that the McAfee® OTP Server accepts connections from native OTP clients on all IP addresses assigned to the host server’s system.

**Session Timeout**
- Specifies the number of milliseconds that the connection between the OTP client and the McAfee® OTP Server can be idle before the session times out.
- **Note:** A zero value specifies that there is no timeout.

9.2 Mobile Numbers

The following settings are located in the Mobile Numbers area on the Server Configuration Pane:

**Check Mobile Number**
- Selecting this check box specifies checking the mobile number for non-numeric characters and removing them, including spaces. This setting does not remove the “+” character from mobile numbers.

**Default Country Prefix**
- Specifies removing any leading zeros and then adding the default country prefix that you provide. This setting is only available when the Check Mobile Number check box is selected.

9.3 One-time Password Options

The following settings are located in the One-time Password Options area on the Server Configuration Pane:

**OTP Length**
- Specifies the length of the one-time password in number of characters.

**OTP Valid Time**
- Specifies how long in minutes the one-time password is valid. A zero value specifies that one-time password is valid indefinitely.

**OTP Retries**
- Specifies the number of times that the end user can automatically receive a new one-time password after entering the previous password incorrectly. A zero value disables this function.
- **Note:** This setting is only available for RADIUS OTP clients.
Configuring the Server Object Type

Retry Message
Specifies the message that the end user receives after entering an incorrect one-time password. This setting is only available when the retry function is enabled.

Regenerate Timeout
Specifies the time in seconds required between OTP requests. This setting is designed to prevent end users from requesting multiple one-time passwords in quick succession. To disable this requirement, set the timeout value to zero.

Composition
Select one of the following options to specify the set of characters allowed in a one-time password:
- Digits (0-9)
- Letters & Digits (A-Z,a-z,0-9)
- Custom Characters — This option allows you to specify a custom set of letters and digits. Letters are case-sensitive.

9.4 Client Settings

The following settings are located in the Client Settings area on the Server Configuration Pane:

All Clients Are Allowed
Selecting this check box specifies that all OTP clients are allowed to use the McAfee® OTP Server.

Allowed Clients
Specifies a comma-separated list of IP addresses corresponding to the OTP clients that are allowed to use the McAfee® OTP Server. This setting is only available when not all clients are allowed.

Allow remote configuration
Selecting this check box allows remote configuration of the McAfee® OTP Server through the OTP client API.

Remote Password
Specifies the password that is required for remote configuration of the McAfee® OTP Server through the OTP client API. This setting is only available when remote configuration is allowed.
9.5 Encryption

The following settings are located in the Encryption area on the Server Configuration Pane:

No encryption
Specifies that messages between the OTP client and McAfee® OTP Server are not encrypted.

Encryption if client does encryption
Specifies that messages between the OTP client and McAfee® OTP Server are encrypted if the OTP client supports encryption.

Always encryption
Specifies that messages between the OTP client and McAfee® OTP Server are always encrypted. McAfee® OTP Server rejects messages from the OTP client that are not encrypted.

9.6 Options

The following settings are located in the Options area on the Server Configuration Pane:

Enable Monitor
Select this check box to start the Statistics Monitor when the McAfee® OTP Server starts.

Debug
Select this check box to display the output of the Debug function on the console.

Use Secure Random
Select this check box to use the more complex java.security.SecureRandom algorithm when generating the one-time password for the end user. This algorithm requires more CPU capacity.

9.7 Global Options

The following settings are located in the Global Options area on the Server Configuration Pane:

Prevent SQL Injection Attacks
Selecting this check box 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, then user authentication is denied.

Use whitelist
Specifies that McAfee® OTP Server 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.

Is RegEx
Selecting this check box allows you to define the whitelist for SQL databases using a regular expression. This option is only available when the "Use whitelist" check box is selected.
Configuring the Server Object Type

Test
Using this field, you can verify characters against the whitelist configured for SQL databases. This field is only available when the “Use whitelist” check box is selected.

Prevent LDAP Injection Attacks
Selecting this check box specifies that all user names are checked for the following characters: *, (, ), &. If any of these characters are found, then user authentication is denied.

LDAP follow referrals
Selecting this check box specifies that McAfee® OTP Server automatically follows a referral to another LDAP directory, which is provided when a directory tree is distributed over multiple LDAP servers.

LDAP idle reconnect
Selecting this check box specifies that McAfee® OTP Server automatically follows a referral to another LDAP directory, which is provided when a directory tree is distributed over multiple LDAP servers.

Set System Charset
Selecting this check box allows you to specify a system character set other than UTF-8, the default.

Note: All OTP clients must be configured for the character set that you specify.
Configuring the Server Object Type
10.0 Configuring the RADIUS Object Type

To configure McAfee® OTP Server as a RADIUS server, select the RADIUS object type in the Select Pane. RADIUS configuration options open in the Configuration Pane, as shown in the following screenshot. Select the “Enable RADIUS” check box. For complete information about the settings on the Configuration Pane, see the sections in this chapter. Each section corresponds to a different heading on the Configuration Pane.
10.1 RADIUS Server Settings

The following settings are located in the RADIUS Server Settings area on the RADIUS Configuration Pane. All settings apply to McAfee® OTP Server when configured as a RADIUS server.

Enable RADIUS
Selecting this check box enables McAfee® OTP Server as a RADIUS server.

Port number
Specifies the port number that native OTP clients use when connecting to the McAfee® OTP Server configured as a RADIUS server.

Default: 1645
Note: When communicating over the Internet, RADIUS servers use UDP, the User Datagram Protocol, not TCP, the Transmission Control Protocol.

Bind to IP Address
Specifies the IP address of the hardware server on which McAfee® OTP Server software is installed and configured as a RADIUS server.

All
Selecting this check box specifies that the McAfee® OTP Server configured as a RADIUS server accepts connections from native OTP clients on all IP addresses assigned to the host server’s system.

Timeout
Specifies the number of milliseconds that the connection between the OTP client and the McAfee® OTP Server can be idle before the RADIUS session times out.

Note: A zero value specifies that there is no timeout.

Debug Packets
Select this check box to display the output of the Debug function in the console or write the output of the Debug function to a log file.

Restart RADIUS Server after reconfiguration
Selecting this check box restarts McAfee® OTP Server each time that you update and save the RADIUS server configuration.

10.2 Additional Ports

The following settings are located in the Additional Ports area on the RADIUS Configuration Pane. All settings apply to McAfee® OTP Server when configured as a RADIUS server.

Enable
Selecting this check box configures McAfee® OTP Server to listen on more than one port.

Port number
Specifies an additional port number on which McAfee® OTP Server can listen.

Used by Client
Specifies the OTP client that corresponds to the additional port number.
To configure logging for the McAfee® OTP Server, select the Logs object type in the Select Pane, and configure the options that open on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
11.1 Log Files

The following settings are located in the Log Files area on the Logs Configuration Pane:

**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.

**Accounting file**
Specifies the name of the log file that stores all successful OTP messages. 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.

**Log level**
Specifies one of the following log levels: Trace, Debug, Info, Warn, Error, or Fatal.
**Default:** Debug

**Max log file size**
Specifies the maximum size that a log file can reach before it is rolled, and a new log file is opened. When a log file is rolled, it is saved as a back-up file.
**Default:** 5000
**Units:** Kilobytes (KB)

**Max backup index**
Specifies the maximum number of back-up log files that can be saved before McAfee® OTP Server removes the oldest file.
**Default:** 100

**Example:** Saving 100 logging files, each file 5000 KB in size, requires 500 megabytes (MB) of disk space.

**Append session number**
Selecting this check box adds session numbers to the log file.
**Default:** Selected

**External Log Handler**
(Optional) Specifies a Java class name that implements the following interface:
se.nordicedge.interface.OTPlogging
**Note:** 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 Server.

11.2 Other Settings

The following settings are located in the Other Settings area on the Logs Configuration Pane:

**Check for config changes every**
Specifies a time interval in seconds for checking the McAfee® OTP Server configuration file for changes. To disable this function, set the time interval to zero.

**Check classpath during startup**
Selecting this check box specifies that McAfee® OTP Server reads changes in the lib directory during startup.
12.0 Alerts

To configure alerts for the McAfee® OTP Server, select the Alerts object type in the Select Pane, and configure the options that open on the Configuration Pane.

1. Select the Enable Alerts check box.
2. Configure the remaining settings on the Configuration Pane. For more information about the settings, see section 12.1 Alert Configuration.
12.1 Alert Configuration

The following settings are located in the Alert Configuration area on the Logs Configuration Pane:

**Use Method**
Selecting a configured delivery method from the drop-down menu specifies which method triggers the first alert.

**Default:** All

**Alert events**
Selecting one or more of the following check boxes specifies which errors trigger alert events:
- 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 (entered one per line) of each alert recipient.

**Test**
Outputs a test alert.
13.0 Licenses

The License configuration object type includes configuration options and license information. Because the license system for McAfee® OTP Server V3 is new and not compatible with V2, you need to obtain new license files from McAfee® to upgrade. For more information, contact McAfee® Technical Support:


The new license system compares the number of users to the number of registered licenses. When the number of users exceeds the number of registered licenses, new users can no longer authenticate using the McAfee® OTP Server. You can, however, configure an alert that notifies one or more administrators when the number of users is close to the number of registered licenses.

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.

To register a new license, follow these steps:

1. Copy the new license file to the license directory.
   
   Note: The license filename must end with the filename extension ".dat".

2. Select the Licenses object type in the Select Pane.

3. On the Configuration Pane, click Detect New.

4. Verify that the value in the Registered Licenses field is updated to include the number of licenses in the new license file.
13.1 **License Information**

In the License information area on the Licenses Configuration Pane, you can view the following information.

**Registered Licenses**
Displays the number of licenses specified in the license files.

**Detect new**
Clicking this button checks for new licenses in the license files in the license directory and updates the value in the **Registered Licenses** field.

**Used Licenses**
Displays the number of registered licenses used by current users.

**Reset**
Clicking this button resets the value in the **Used Licenses** field to zero.

**Unused Licenses**
Displays the number of registered licenses available to new users.

**Counter started**
Displays the date and time that the license counter was started.

**Refresh**
Clicking this button refreshes the information displayed in the License Information area on the Licenses Configuration Pane.
14.0 Configuring the Databases Object Type

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

- LDAP
- JDBC (ODBC via JDBC)
- RADIUS Forward Database
- Database Group (LDAP, JDBC, or both databases configured as a group)

McAfee® OTP Server supports the following database actions:

- New Database — To create a database, right-click the Databases object type, and then select the type of database from the context menu that opens. Alternately, you can select the Databases object type in the Select Pane, and then select the type of database in the Configuration pane. Specify a unique, meaningful name for the new database, and configure the database options.

- Delete Database — To delete a database, navigate to the database in the Select Pane, right-click the database, and select **Delete** from the context menu that opens.

- Duplicate Database — To duplicate a database, navigate to the database in the Select Pane, right-click the database, and select **Duplicate Database** from the context menu that opens. Specify a unique, meaningful name for the duplicate database, and configure the database options.

**Note:** You can also access the database actions through the File menu on the Menu Bar.

14.1 The OATH Database Option

You can configure any LDAP, ODBC, or JDBC database as an OATH database by selecting the "Uses HOTP or TOTP (OATH)" check box on the Databases Configuration Pane. Select this check box to integrate any OATH-compliant OTP client, such as the Pledge and YubiKey OTP clients, with McAfee® OTP Server. Enabling OATH authentication disables OTP delivery by SMS.

**Note:** To use both OATH authentication and OTP delivery by SMS for the same user store, configure two databases and select a differ user attribute for each one. For example, you can select the "Mobile" attribute for one database and the "carLicense" attribute for the other database.
14.2 Creating an LDAP Database

Creating an LDAP database involves the following steps.

1. Select the LDAP database type by one of the following methods:
   — Right-click the Databases object type in the Select Pane, and then select the new LDAP database option from the context menu that opens.
   — Select the Databases object type in the Select Pane, and then select the LDAP database type in the Configuration pane.

2. Specify a unique, meaningful name for the LDAP database in the Database Display Name field.

3. 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) check box. For example, select this check box when configuring the new LDAP database for use with Pledge, the McAfee® OTP client installed on mobile devices.
   **Note:** Selecting this check box modifies the available settings in the Account Settings, One-time Password Prefetch, and PIN code areas on the Configuration Pane.

4. Configure the remaining settings on the Configuration Pane. For complete information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
## Configuring the Databases Object Type

### 14.2.1 Host Settings

The following settings are located in the Host Settings area on the LDAP Database Configuration Pane:

**Host Address**

Specifies 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**

Specifies the port number of the LDAP server.

*Default:* 389 (LDAP) or 636 (LDAPS)

**SSL**

Selecting this check box specifies that the SSL protocol is used when communicating over the Internet.

*Note:* SSL is an acronym for Secure Sockets Layer.

**TLS**

Selecting this check box specifies that the TLS protocol is used when communicating over the Internet.

*Note:* TLS is an acronym for Transport Layer Security.

**Admin DN**

Specifies the Distinguished Name (DN) of an administrative user that has read and write access to the Account Disable attribute for all user accounts.

*Note:* An Active Directory (AD) search using LDAP requires the DN and password of a privileged user. If the DN is not specified, McAfee® OTP Server connects to the LDAP server using an anonymous bind.

**Password**

Specifies the password of an administrative user that has read and write access to the Account Disable attribute for all user accounts.

**Test Connection**

Tests the connection to the LDAP server.

### 14.2.2 Search Settings

The following settings are located in the Search Settings area on the LDAP Database Configuration Pane:

**Base DN**

Specifies the location in the directory tree from which McAfee® OTP Server searches for users.

*Note:* You can use the browse button to locate and select the base DN.

**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 Server can have to the LDAP server.
Filter Start
Specifies the beginning of the search filter.

Filter End
Specifies the end of the search filter.

Search Filter Example:
Filter Start = “(&(cn=
Filter End = “)(objectclass=inetorgperson))”
user name = “user1”
Filter = “(&{cn=user1}(objectclass=inetorgperson))”

Samples
Clicking this button allows you to select a sample search that populates the Filter Start and Filter End fields with values.

Test LDAP Authentication
Tests LDAP authentication.

14.2.3 Account Settings (HOTP/TOTP Disabled)
The following settings are located in the Account Settings area on the LDAP Database Configuration Pane when the “Uses HOTP or TOTP (OATH)” check box is not selected:

OTP Attribute
Specifies the attribute in the LDAP database that defines the OTP delivery method.
Note: You can use the browse button to search the LDAP schema and select the attribute.

Login Retries
Specifies the maximum number of incorrect passwords that users can provide before the user’s account is disabled.
Note: If you do not specify a value for this field, then there is no limit on the number of incorrect passwords that users can provide.

Accept Pwd change
Selecting this check box allows users to change their passwords.
Note: You must select this check box, which is required by Microsoft Active Directory.

Locked Attribute
Specifies the LDAP attribute that is read to determine whether the user account is locked.

Locked Value
Specifies the value of the Locked Attribute when the user account is locked.
Note: When the user’s account is disabled by too many login retries, the Locked Attribute is set to the Locked Value.

Disable OTP Attribute
Specifies the LDAP attribute that is read to determine whether OTP authentication is required.
Configuring the Databases Object Type

**Disable OTP Value**
Specifies the value of the Disable OTP Attribute when OTP authentication is not required.

**Not**
Selecting this check box specifies that OTP authentication is not required when the Disable OTP Attribute is not set to the Disable OTP Value. For clarification, see the following table.

<table>
<thead>
<tr>
<th>“Not” Check Box</th>
<th>OTP Authentication is not required when...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleared</td>
<td>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>Selected</td>
<td>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>

14.2.4 **Account Settings (HOTP/TOTP Enabled)**
The following settings are located in the Account Settings area on the LDAP Database Configuration Pane when the Uses HOTP or TOTP (OATH) check box is selected:

**OATH Key**
Specifies the attribute that stores the user’s OATH key.  
*Note:* You can use the browse button to search the LDAP schema and select the attribute.

**Login Retries**
Specifies the maximum number of incorrect passwords that users can provide before the user’s account is disabled.  
*Note:* If you do not specify a value for this field, then there is no limit on the number of incorrect passwords that users can provide.

**Accept Pwd change**
Selecting this check box allows users to change their passwords.  
*Note:* You must select this check box, which is required by Microsoft Active Directory.

**Locked Attribute**
Specifies the LDAP attribute that determines whether the user account is locked.

**Locked Value**
Specifies the value of the Locked Attribute when the user account is locked.  
*Note:* When the user’s account is disabled by too many login retries, the Locked Attribute is set to the Locked Value.

**Time drift attribute (TOTP)**
Specifies the LDAP attribute which stores a time drift value for TOTP tokens.  
*Data Type:* String
14.2.5 One-time Password Prefetch

The OTP prefetch feature allows users to obtain a configurable number of one-time passwords in advance. This feature is useful when mobile phone coverage is an issue.

When using this feature, users prefetch one-time passwords through a web server that is configured with the McAfee® OTP Server Prefetch Web Application developed using JavaServer Pages (JSP) technology. Users log in to the web application and request prefetch one-time passwords which are sent to a mobile phone number or email address. You can also configure McAfee® OTP Server to send a new set of prefetch one-time passwords to the user each time all of the passwords are used.

In the One-time Password Prefetch area on the LDAP Database Configuration Pane, select the **Enable OTP Prefetch** check box, and click **Configure Prefetch OTP**. The OTP Prefetch configuration options open, as follows:

**Prefetch OTP Attribute**
- Selects the attribute that contains the prefetch OTP string.

**Enable LDAP Filter**
- (Optional) Specifies an LDAP filter that allows users to use prefetch one-time passwords.

**Maximum No of Prefetch OTPs**
- Specifies the maximum number of prefetch one-time passwords that can be sent to a user at one time.

**Must be used in order**
- Selecting this check box specifies that the prefetch one-time passwords must be used in order.
  - **Note:** This option is global and applies to all user databases.

**OTP Length**
- Specifies the length of each prefetch one-time password in characters.

**Automatically send new Prefetch OTPs when last OTP is used**
- Selecting this check box specifies that a new set of prefetch one-time passwords is automatically sent to users when the last password from the previous set is used.

**Message to user**
- Specifies a message to send to users that includes the prefetched one-time password. McAfee® OTP Server replaces the tag $$OTP$$ with the one-time password. If you omit the tag from the message, McAfee® OTP Server appends the one-time password to the end of the message.
  - **Note:** This option is global and applies to all user databases.

**Message Delivery**
- Specifies whether to send a set of prefetch one-time passwords in one message or more than one message.
Configuring the Databases Object Type

Allow administration creation of Prefetch OTP
Selecting this check box allows administrators to create prefetch one-time passwords for any user. Clearing this check box limits requests for prefetch one-time passwords to users themselves.

Administrator Database
Specifies the database to use when authenticating the administrator or group of administrators that can create prefetch one-time passwords for other users.

Allowed IP Addresses
Specifies a comma-separated list of client IP addresses from which an administrator can create prefetch one-time passwords.

14.2.6 PIN Code
The PIN Code feature adds another layer of security. When this feature is enabled, users are required to specify a PIN code value which is stored in a PIN code attribute. When prompted for a one-time password, users must provide a string which is the concatenation of the PIN code and the one-time password. For example, if the PIN code is “1234” and the one-time password is “OTPOTP”, then the resulting string is “1234OTPOTP”.

In the PIN Code area on the LDAP Database Configuration Pane, select the Enable PIN Code check box, and click Configure PIN Code. The PIN Code configuration options open and include hashed Pin codes. McAfee® OTP Server supports the following hash algorithms:

- SHA1
- Secure SHA256 (SSHA256)

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

Select LDAP attribute for the PIN code
Specifies the attribute that stores the PIN code.
Note: You can use the browse button to search the LDAP schema and select the attribute.

Show advanced hashed PIN code options (Global)
Selecting this check box enables hashed PIN codes.
Note: All hashed PIN code options are global and apply to all user databases.
Digest Charset
  Specifies the character set used by the user store where the hashed PIN codes are saved.
  **Default:** ISO-8859-1
  **Note:** This setting is only available when configuring hashed PIN codes.

Hashed value format
  Specifies one of the following formats to use when reading hashed PIN codes: Base64 or Hexadecimal.
  **Note:** This setting is only available when configuring hashed PIN codes.

### 14.2.7 Advanced Options

The following setting is located in the Advanced options area on the LDAP Database Configuration Pane:

**External Databasehandler**
  Selecting this check box allows you to extend the database handler with your own Java class. Specify a Java class name that extends se.nordicedge.radius.DBHandler in the field that opens.
14.3 Creating a SQL Database

Creating a SQL database involves the following steps:

1. Select the SQL database type by one of the following methods:
   — Right-click the Databases object type in the Select Pane, and then select the new SQL database option from the context menu that opens.
   — Select the Databases object type in the Select Pane, and then select the SQL database type in the Configuration pane.

2. Specify a unique, meaningful name for the SQL database in the Database Display Name field.

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) check box. For example, select this check box when configuring the new SQL database for use with Pledge, the McAfee® OTP client installed on mobile devices.
   Note: Selecting this check box modifies the available settings in the SQL Queries area on the Configuration Pane.

4. Configure the remaining settings on the Configuration Pane. For complete information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
14.3.1 JDBC/ODBC Settings

The following settings are located in the JDBC/ODBC Settings area on the SQL Database Configuration Pane:

**Driver Manager**
- Specifies the Driver Manager using JDBC syntax.
  - ODBC example: sun.jdbc.odbc.JdbcOdbcDriver
  - MySQL example: com.mysql.jdbc.Driver

**Database URL**
- Specifies the URL of the JDBC/ODBC database.
  - ODBC example: jdbc:odbc:Databasename
  - MySQL example: jdbc:mysql://Ipaddress:portnr:/dbname

**Samples**
- Provides sample settings for the Driver Manager and Database URL fields.

**Username**
- Specifies the user name for the JDBC/ODBC database.

**Password**
- Specifies the password for the JDBC/ODBC database.

**No of conns**
- Specifies the number of concurrent database connections in the connection pool available to McAfee® OTP Server.

**Test Connection**
- Tests the database connection using the JDBC/ODBC settings.

14.3.2 SQL Queries (HOTP/TOTP Disabled)

The following settings are located in the SQL Queries area on the JDBC/ODBC Database Configuration Pane when the “Uses HOTP or TOTP (OATH)” check box is not selected:

**Authenticate**
- Specifies the SQL Query used for authentication, which must return the user name.
  - Example: SELECT NAME FROM UserDB WHERE NAME='$$NAME$$' AND PASSWORD='$$PASSWORD$$'

**OTP Field**
- Specifies the SQL Query that retrieves the mobile phone number or email address from the user’s account.
  - Note: In the query, use the $$NAME$$ tag for the user name.

**Login Retries**
- Specifies the maximum number of incorrect passwords that users can provide before the user’s account is disabled.
  - Note: If you do not specify a value for this field, then there is no limit on the number of incorrect passwords that users can provide.

**Get Locked (Get Disabled)**
- Specifies the SQL field that determines whether the user account is locked.
  - Note: Read this field during authentication, using the $$NAME$$ tag for the user name.
Configuring the Databases Object Type

Set Locked (Set Disabled)
Specifies the SQL Query to execute when the maximum number of Login Retries is exceeded.

**Note:** In the query, use the $$NAME$$ tag for the user name.

Get Disable OTP
Specifies the SQL Query that determines whether the user is required to provide a one-time password.

**Example:**
SELECT skipotpflag UserTable WHERE name='$$NAME$$'

**Note:** If you do not specify a value for this field, then the one-time password is always required.

Test Authentication
Tests authentication using the SQL Queries settings.

### 14.3.3 SQL Queries (HOTP/TOTP Enabled)

The following settings are located in the SQL Queries area on the JDBC/ODBC Database Configuration Pane when the “Uses HOTP or TOTP (OATH)” check box is selected:

**Authenticate**
Specifies the SQL Query used for authentication, which must return the user name.

**Example:**
SELECT NAME FROM UserDB WHERE NAME='$$NAME$$' AND PASSWORD='$$PASSWORD$$'

**Get OATHKey**
Specifies the SQL Query that retrieves the OATH key from the user’s account.

**Example:**
SELECT OATHKey FROM UserDB WHERE NAME='$$NAME$$'

**Set OATHKey**
Specifies the SQL Query that sets the OATH key in the user’s account.

**Example:**
UPDATE users SET OATHKey ='$$KEY$$' WHERE name='$$NAME$$'

**Get Disabled**
Specifies the SQL field that determines whether the user account is locked.

**Note:** Read this field during authentication, using the $$NAME$$ tag for the user name.

**Set Disabled**
Specifies the SQL Query to execute when the maximum number of Login Retries is exceeded.

**Note:** In the query, use the $$NAME$$ tag for the user name.

Test Authentication
Tests authentication using the SQL Queries settings.

### 14.3.4 One-time Password Prefetch

The One-time Password Prefetch settings are the same for LDAP and SQL databases. For more information, see section 14.2.5 One-time Password Prefetch in the LDAP section.

### 14.3.5 PIN Code

The PIN Code settings are the same for LDAP and SQL databases. For more information, see section 14.2.6 PIN Code in the LDAP section.
14.3.6 Advanced Options

The Advanced Options settings are the same for LDAP and SQL databases. For more information, see section 14.2.7 Advanced Options in the LDAP section.

14.4 Creating a RADIUS Forward Database

Using a RADIUS Forward database, McAfee® OTP Server can pass through and forward RADIUS requests to another RADIUS Server, thus supporting RSA SecurID and SafeWord tokens.

Creating a RADIUS Forward database involves the following steps.

1. Select the RADIUS Forward database type by one of the following methods:
   — Right-click the Databases object type in the Select Pane, and then select the new RADIUS Forward database option from the context menu that opens.
   — Select the Databases object type in the Select Pane, and then select the RADIUS Forward database type in the Configuration pane.

2. Specify a unique, meaningful name for the RADIUS Forward database in the Database Display Name field.

3. Click Add RADIUS Server, and specify the IP address and port number of the RADIUS Server. McAfee® OTP Server uses this information when forwarding requests to the server.

4. (Optional) To remove a RADIUS Server, select it, and click Remove RADIUS Server.

5. Configure the remaining settings on the Configuration Pane:
   - **Shared Secret**
     Specifies the secret shared by the McAfee® OTP Server and the RADIUS Server.
   - **Forward additional RADIUS attributes**
     Specifies whether the McAfee® OTP Server forwards additional RADIUS attributes to the other RADIUS Server.
   - **Test RADIUS request**
     Tests authentication to the selected RADIUS Server.
Configuring the Databases Object Type

14.5 Creating a Database Group

A Database Group consists of multiple databases configured as a group. The group can include LDAP databases, JDBC databases, or a combination. LDAP and JDBC databases must be configured before they can be added to a Database Group on the Configuration Pane.

When databases are configured as a group, McAfee® OTP Server 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 Server uses that database for that user.

Creating a Database Group involves the following steps.

1. Select the Database Group type by one of the following methods:
   — Right-click the Databases object type in the Select Pane, and then select the new Database Group option from the context menu that opens.
   — Select the Databases object type in the Select Pane, and then select the Database Group type in the Configuration pane.

2. Specify a unique, meaningful name for the Database Group in the Database Display Name field.

3. Click Add Database in the Database Group Settings area, and select one or more databases from the available options.

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

5. (Optional) Click Remove Database to remove a database from the Database Group.
Configuring the Databases Object Type
15.0 Configuring the Clients Object Type

McAfee® OTP Server uses OTP client objects to manage connections to OTP clients. Client objects hold information, such as client name, IP address, and database used for OTP authentication.

There are three types of OTP clients:

- **Native** — Native OTP clients communicate with McAfee® OTP Server using the API that it provides.
  
  **Examples:** CA SiteMinder, Microsoft Outlook Web Access, Microsoft SharePoint, and Novell GroupWise Web Access

- **RADIUS** — RADIUS OTP clients use the RADIUS challenge-response protocol to communicate with McAfee® OTP Server.
  
  **Examples:** Firewall and VPN (BlueCoat, Cisco, Citrix, F5, and Juniper)

- **Web services** — Web services OTP clients use SOAP-based web services implemented through an API to communicate with McAfee® OTP Server.
  
  **Note:** For more information about the web services client, see the McAfee® OTP Server guide to Web Service Client API (SOAP).

McAfee® OTP Server supports the following client actions:

- **New Client** — Right-click the Clients object type in the Select Pane, and then select the new client type option from the context menu that opens, or select the Clients object type in the Select Pane, and then select the new client type option in the Configuration pane.

- **Delete Client** — Select the Clients object type, select the client type, right-click the client to delete, and then select **Delete**.

- **Duplicate Client** — Select the Clients object type, select the client type, right-click the client to duplicate, and then select **Duplicate Client**.
15.1 Creating a RADIUS Client

Creating a RADIUS OTP client involves the following steps.

1. Select the RADIUS client type by one of the following methods:
   — Right-click the Clients object type in the Select Pane, and then select the new RADIUS client type option from the context menu that opens.
   — Select the Clients object type in the Select Pane, and then select the new RADIUS client type option in the Configuration pane.

2. Specify a unique, meaningful name for the RADIUS client in the Client Display Name field.

3. Specify the IP address of the RADIUS client in the Client IP Address field. Do not specify a DNS name. **Note:** you can specify multiple IP addresses by using a wildcard character, such as "*.*".

4. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
Configuring the Clients Object Type

15.1.1 Advanced Options

Clicking Advanced opens the following RADIUS configuration areas:

- **RADIUS Client Attribute Detection** — For more information, see section 15.1.1.1 RADIUS Client Attribute Detection.
- **Listen on RADIUS Ports** — For more information, see section 15.1.1.2 Listen on RADIUS Ports.
- **Encoding** — For more information, see section 15.1.1.3 Encoding.
- **RADIUS Reject Error Messages** — For more information, see section 15.1.1.4 RADIUS Reject Error Messages.

15.1.1.1 RADIUS Client Attribute Detection

Using the RADIUS Client Attribute Detection feature, you can specify a different client configuration and database for each user group at the same IP address. Using this feature, you can differentiate between user groups, such as employees, partners, and customers.

**Enable Attribute Detection**

Specifies whether the RADIUS attribute detection feature is enabled.

**RADIUS attribute number**

Specifies a RADIUS attribute by number.

**RADIUS attribute value**

Specifies a value for the selected RADIUS attribute.

**Match type**

Specifies whether the match must be exact.

**Match case**

Specifies whether the match is case-sensitive.

15.1.1.2 Listen on RADIUS Ports

The Listen on RADIUS Ports settings specify the RADIUS port numbers on which McAfee® OTP Server listens.

**Listen on ALL available port numbers**

Specifies whether McAfee® OTP Server listens on all RADIUS port numbers.

**Selected ports**

Specifies one or more RADIUS port numbers on which McAfee® OTP Server listens. **Note:** This option is only available when the previous option is disabled.

15.1.1.3 Encoding

The following setting is located in the Encoding Settings area on the RADIUS Client Configuration Pane:

**Charset encoding**

Specifies a system character set. **Note:** The RADIUS standard uses UTF-8 encoding to transform packet data to strings.
15.1.1.4 RADIUS Reject Error Messages

You can configure error messages for the end user which are sent when authentication fails.

**Failed Auth/Error**
- Specifies a message that is sent when the user fails to authenticate or a system error occurs. This message is sent by RADIUS attribute 18.
  - **Note:** 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.
  - **Note:** To disable this message, leave this field blank.

15.1.2 RADIUS Options

The following settings are located in the RADIUS Options area on the RADIUS Client Configuration Pane:

**Shared Secret**
- Specifies the RADIUS client’s shared secret.
  - **Note:** The RADIUS client and the RADIUS client application must have the same shared secret.

**Supports RADIUS Access-Challenge**
- Specifies whether the RADIUS client supports the RADIUS challenge-response protocol.

**Response Message**
- Specifies a message that is sent to the RADIUS client for prompting the user to enter a one-time password.
  - **Note:** If the RADIUS client does not support the RADIUS challenge-response protocol, type the IP address of the authentication server in this field instead of the message. The authentication server is the server that initiates the process of logging in with a user name and password.

15.1.3 User Database

From the drop-down menu, select one of the configured databases for the RADIUS client to use. For more information about creating and configuring databases, see section 14.0 Configuring the Databases Object Type.
15.1.4 Other Options

The following settings are located in the Other Options area on the RADIUS Client Configuration Pane:

Uses external OTP API
Selecting this check box specifies that the external code using the API generates and verifies the one-time password instead of the McAfee® OTP Server. Type the Java class name that implements the interface in the field that opens: `se.nordicedge.interfaces.OTPVerificationHandler`

RADIUS Attributes
Clicking Radius Attributes allows you 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 can be Static Value, UserDN, User Attribute, Login Name, or external code.

Force OTP Delivery Method
Selecting an OTP delivery method from the drop-down menu places the method at the top of the list of configured delivery methods.

15.1.5 Prefetch OTP Options

The prefetch OTP options are only available when the RADIUS client is configured to use prefetch one-time passwords only. This feature is useful for RADIUS clients that do not support the challenge-response protocol.

Require Password AND Prefetch OTP
Specifies that the user must enter a string which is the concatenation of the database password and the one-time password.
Example: `dbpassword012345`

Generate Prefetch OTP if none exists
Specifies that users can generate prefetch one-time passwords if none exist when they log in with user name and password.
15.2 Creating a Native Client

Creating a Native OTP client involves the following steps:

1. Select the Native client type by one of the following methods:
   - Right-click the Clients object type in the Select Pane, and then select the new Native client type option from the context menu that opens.
   - Select the Clients object type in the Select Pane, and then select the new Native client type option in the Configuration pane.

2. Specify a unique, meaningful name for the Native client in the **Client Display Name** field.  
   **Example:** CA SiteMinder

3. Specify the IP address of the Native client in the **Client IP Address** field. Do not specify a DNS name. 
   **Note:** you can specify multiple IP addresses by using a wildcard character, such as "*".

4. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
15.2.1 Advanced — Native Client Name Detection

Using the Advanced settings described in this section, you can enable the “Native Client Name Detection” feature and specify the name of the integration module that communicates with the McAfee® OTP Server through the OTP client API. The McAfee® OTP Server can then use the name of the integration module to differentiate between user groups at the same IP address, applying a different client configuration and database to each one. Examples of user groups include employees, partners, and customers.

Enable Name Detection
   Selecting this check box enables the “Native Client Name Detection” feature.

Client Name
   Specifies the client name used by the integration module.

15.2.2 Options

The following settings are located in the Options area on the Native Client Configuration Pane:

Accept User Lookup only
   Selecting this check box allows McAfee® OTP Server to look up users based on user name only and issue one-time passwords. The password field can be empty. Use this feature to enable OTP authentication without user name and password.

Client Name
   Specifies the client name used by the integration module.
   Note: This field is available when Accept User Lookup only is selected.

15.2.3 User Database

From the drop-down menu, select one of the configured databases for the Native client to use. For more information about creating and configuring databases, see section 14.0 Configuring the Databases Object Type.

15.2.4 Other Options

The following settings are located in the Other Options area on the Native Client Configuration Pane:

Uses external OTP API
   Selecting this check box specifies that the external code using the API generates and verifies the one-time password instead of the McAfee® OTP Server. Type the Java class name that implements the interface in the field that opens:
   se.nordicedge.interfaces.OTPVerificationHandler

Force OTP Delivery Method
   Selecting an OTP delivery method from the drop-down menu places the method at the top of the list of specified delivery methods.
15.3 Creating a Web Services Client

Creating a Web Services client involves the following steps.

1. Select the Native client type by one of the following methods:
   - Right-click the Clients object type in the Select Pane, and then select the new Web Services client type option from the context menu that opens.
   - Select the Clients object type in the Select Pane, and then select the new Web Services client type option in the Configuration pane.

2. Type a name for the Web Services client in the **WS Client Name** field.  
   **Note:** The name must correspond to the client name in the client’s Web Services requests.

3. Type a password for the Web Services client in the **WS Client Password** field.

4. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
15.3.1 Options

The following setting is located in the Options area on the Web Services Client Configuration Pane:

**Accept User Lookup only**

Selecting this check box allows McAfee® OTP Server to look up users based on user name only and issue one-time passwords. The password field can be empty. Use this feature to enable OTP authentication without user name and password.

15.3.2 User Database

From the drop-down menu, select one of the configured databases for the Web Services client to use. For more information about creating and configuring databases, see section 14.0 Configuring the Databases Object Type.

15.3.3 Other Options

The following settings are located in the Other Options area on the Web Services Client Configuration Pane:

**Uses external OTP API**

Selecting this check box specifies that the external code using the API generates and verifies the one-time password instead of the McAfee® OTP Server. Type the Java class name that implements the interface in the field that opens:

```
se.nordicedge.interfaces.OTPVerificationHandler
```

**Force OTP Delivery Method**

Selecting an OTP delivery method from the drop-down menu places the method at the top of the list of specified delivery methods.
16.0 Configuring the Delivery Methods Object Type

Using the Delivery Methods object type, you can configure one or more methods that McAfee® OTP Server uses to deliver one-time passwords. Selecting and right-clicking the Delivery Methods object type in the Select Pane opens the following options:

- Show all — Displays all delivery method types.
- Show enabled — Displays enabled delivery method types only.
- Show disabled — Displays disabled delivery method types only.

To enable a delivery method type, follow these steps:
1. Expand the Delivery Methods object type in the Select Pane.
2. Select the delivery method type that you want to enable.
3. In the Configuration Pane, enable the delivery method type.
4. Configure the remaining options for the selected delivery method type.

To change the order in which the delivery method types are used, move the type up or down in the Select Pane, as follows:
1. Select the delivery method type in the Select Pane. The delivery method type must be enabled.
2. Right-click the type, and select the "Move up" and "Move down" options as needed to reorder the delivery methods.
16.1 McAfee® SMS Gateway

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

Configuring the SMS Gateway delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select McAfee SMS.
2. Select the Enable McAfee SMS Gateway check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
16.1.1 General Settings and Proxy Areas

The following settings are located in the General Settings and Proxy areas on the McAfee® SMS Gateway Delivery Method Configuration Pane:

**Username**
Specifies the user name for the McAfee® SMS service.

**Password**
Specifies the password for the McAfee® SMS service.

**Flash SMS**
Selecting this check box allows the McAfee® SMS service to send Flash SMS messages to a mobile phone.

**Message**
Specifies the message to send to the mobile phone that includes the one-time password. McAfee® OTP Server replaces the $$OTP$$ tag in the message with the one-time password. If the tag is omitted from the message, McAfee® OTP Server appends the one-time password to the end of the message.

**Enable HTTP proxy server**
Selecting this check box enables the HTTP proxy server.

**Server**
Specifies the DNS name or IP address of the HTTP proxy server.

**Port**
Specifies the port number of the HTTP proxy server.

**Disable PF SMS Status**
Selecting this check box sends 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.

**Username in accounting file**
Selecting this check box includes the user name in the accounting file. If you are not using the accounting file, you can ignore this setting.

**Validate SSL Certificates**
Selecting this check box enables SSL certificate validation.

16.1.2 Location

Select the geographic area that corresponds to your location.
16.1.3 **Configuration and Status**

Click **Request a demo account** to configure the settings in the Configuration and Status area. The following settings are available:

**Test**
- Allows you to send a test SMS message to a mobile phone through McAfee® SMS Gateway.

**Update Config**
- Allows you to manually update the configuration for the McAfee® SMS Gateway service.

**Debug**
- Selecting this check box writes SMS debug information to the log files.

16.1.4 **Advanced**

Clicking **Advanced** opens the following settings:

**Enable max Limit**
- Selecting this check box enables the Max SMS limits that you set.

**Max SMS per user per day**
- Specifies the maximum number of SMS messages that each user can send in one day.

**Max SMS total per day**
- Specifies the total number of SMS messages that all users can send in one day.
16.2 HTTP

Configuring the HTTP delivery method allows the McAfee® OTP Server to send one-time passwords using the HTTP or HTTPS protocol to an SMS provider. Configuring the HTTP delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select HTTP.
2. Select the **Enable HTTP** check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
16.2.1 Headers or Template File

The following settings are located in the Headers or Templatefile area on the HTTP Delivery Method Configuration Pane:

User Header
Specifies the name of the HTTP header corresponding to the user’s mobile phone number or email address.

OTP Header
Specifies the name of the HTTP Header corresponding to the one-time password.

Headers in Query String
Selecting this check box specifies that HTTP headers are included in the query string as GET parameters.

Example: ?USER=070112233&CHALLENGE=123456

Template file
Specifies 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.

Auto-Accept SSL Certificates
Selecting this check box allows McAfee® OTP Server to automatically trust SSL certificates received over HTTPS.

Debug
Selecting this check box enables logging of HTTP messages.

16.2.2 Authentication

The following settings are located in the Authentication area on the HTTP Delivery Method Configuration Pane:

Enable HTTP Authentication
Selecting this check box enables HTTP authentication.

Username
Specifies the user name required for HTTP authentication.

Password
Specifies the password required for HTTP authentication.

16.2.3 Proxy

The following settings are located in the Proxy area on the HTTP Delivery Method Configuration Pane:

Enable Proxy Server
Selecting this check box enables HTTP requests and responses through a proxy server.

Proxy Server
Specifies the DNS name of the proxy server.

Proxy Port
Specifies the port number of the proxy server.
16.2.4 Other Settings

The following settings are located in the Other Settings area on the HTTP Delivery Method Configuration Pane:

**Content Type**
- Specifies the content type of HTTP email messages using the MIME standard.
- **Default:** application/x-www-form-urlencoded

**HTTP(S) URL**
- Specifies the URL where the one-time password is posted.

**Success String**
- Specifies the string that the HTTP server sends McAfee® OTP Server when the one-time password is posted successfully. Without this string, McAfee® OTP Server continues processing as though the post failed.
16.3 Extended HTTP

The Extended HTTP delivery method is like the HTTP delivery method except that it offers more configuration options. Configuring the Extended HTTP delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select Extended HTTP.
2. Select the Enable Extended HTTP Sender check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
16.3.1 Headers or Template File

The following settings are located in the Headers or Template File area on the Extended HTTP Delivery Method Configuration Pane:

**User Header**
- Specifies the name of the HTTP header corresponding to the user's mobile phone number or email address.

**OTP Header**
- Specifies the name of the HTTP Header corresponding to the one-time password.

**Remove leading +**
- Selecting this check box removes the leading “+” character from mobile phone numbers.

**Replace + with 00**
- Selecting this check box removes the leading “+” character from mobile phone numbers, and replaces it with two zeros.

**Template File**
- Specifies 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**
- Selecting this check box allows McAfee® OTP Server to automatically trust SSL certificates received over HTTPS.

**Debug**
- Selecting this check box enables logging of HTTP messages.

**Use GET**
- Selecting this check box specifies GET as the HTTP method in place of POST.
16.3.2 **Authentication and Proxy**

The following settings are located in the Authentication and Proxy area on the Extended HTTP Delivery Method Configuration Pane:

**Proxy Server**
- Selecting this check box enables HTTP requests and responses through a proxy server.
  - **Proxy Server**: Specifies the DNS name of the proxy server.
    - **Note**: This field opens when the proxy server is enabled.
  - **Proxy Port**: Specifies the port number of the proxy server.
    - **Note**: This field opens when the proxy server is enabled.

**HTTP Auth**
- Selecting this check box enables HTTP authentication.
  - **Username**: Specifies the user name required for authentication.
    - **Note**: This field opens when HTTP authentication is enabled.
  - **Password**: Specifies the password required for authentication.
    - **Note**: This field opens when HTTP authentication is enabled.

**Client Cert**
- Selecting this check box enables certificate authentication.
  - **Note**: Certificate authentication requires HTTPS.
  - **PKCS12 file**: Specifies the full path name to the certificate file.
    - **Note**: This field opens when certificate authentication is enabled.
  - **Password**: Specifies the password which is required to decrypt the certificate file.
    - **Note**: This field opens when certificate authentication is enabled.
16.3.3 Other Settings

The following settings are located in the Other Settings area on the Extended HTTP Delivery Method Configuration Pane:

**Content Type**
- Specifies the content type of HTTP email messages using the MIME standard.
- **Default:** application/x-www-form-urlencoded

**HTTP(S) URL 1**
- Specifies the first of three URLs where McAfee® OTP Server can post the one-time password.
- **Note:** McAfee® OTP Server uses the URLs in the order that you specify them. If one URL fails, then McAfee® OTP Server fails over to the last working URL.

**HTTP(S) URL 2**
- Specifies the second of three URLs where McAfee® OTP Server can post the one-time password.
- **Note:** McAfee® OTP Server uses the URLs in the order that you specify them. If one URL fails, then McAfee® OTP Server fails over to the last working URL.

**HTTP(S) URL 3**
- Specifies the third of three URLs where McAfee® OTP Server can post the one-time password.
- **Note:** McAfee® OTP Server uses the URLs in the order that you specify them. If one URL fails, then McAfee® OTP Server fails over to the last working URL.

**Success String**
- Specifies the string that the HTTP server sends McAfee® OTP Server when the one-time password is posted successfully. Without this string, McAfee® OTP Server continues processing as though the post failed.

**Set SOAP Action request header**
- Selecting this check box adds a SOAPAction header field to the HTTP request.
16.4 SMTP

Configuring the SMTP delivery method allows the McAfee® OTP Server to send one-time passwords using the SMTP protocol. SMTP is an acronym for Simple Message Transfer Protocol. When the SMTP delivery method is configured and the HTTP, Netsize, or both delivery methods are enabled, McAfee® OTP Server sends all messages containing the “@” character to users by SMTP.

Configuring the SMTP delivery method involves the following steps.
1. Expand the Delivery Methods object type in the Select Pane, and then select SMTP.
2. Select the Enable SMTP check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.

![Configure SMTP Settings](image-url)
16.4.1 SMTP Host

The following settings are located in the SMTP Host area on the SMTP Delivery Method Configuration Pane:

SMTP Host
   Specifies the IP address or DNS name of the SMTP host.

Mime Encoding
   Specifies the MIME encoding for messages delivered by the SMTP method.
   Default: ISO-8859-1

Port
   Specifies the port number of the SMTP host.
   Default: 25

SSL/TLS
   Selecting this check box specifies using the SSL or TLS protocol.

Force TLS
   Specifies using TLS, not SSL.
   Note: This check box is only available when SSL/TLS is enabled.

16.4.2 Authentication

The following settings are located in the Authentication area on the SMTP Delivery Method Configuration Pane:

Enable SMTP Authentication
   Selecting this check box enables SMTP authentication.

Username
   Specifies the user name required for SMTP authentication.

Password
   Specifies the password required for SMTP authentication.
16.4.3  SMTP Options

The following settings are located in the SMTP Options area on the SMTP Delivery Method Configuration Pane:

**Mail sender address**
Sspecifies the address of the email sender.

**Mail To Address**
Specifies the address of the email recipient.

*Note:* This setting is only available when the **Mail address** check box is not selected.

**Mail address**
Selecting this check box specifies using the user’s email address as the recipient’s address and disables the **Mail To Address** field.

**Subject**
Specifies the subject line of the email message.

*Note:* This setting is only available when the **User ID** check box is not selected.

**User ID**
Selecting this check box specifies using the user’s mobile phone number or email address as the subject of the email and disables the **Subject** field.

**Body Text**
Specifies the body of the SMTP message, including the $$OTP$$ tag which is replaced by the one-time password. If the $$OTP$$ tag is omitted, the one-time password is appended to the end of the text. Clicking the browse button opens the body text editor.

**Is filename**
Selecting this check box specifies that the body text is saved in a template file. In this case, type the full path name to the template file in the **Body Text** field.

*Note:* The template file can contain the $$IDENTITY$$ and $$OTP$$ tags.

**Debug**
Selecting this check box writes SMTP debug information to the log files.

**Look up mail address in database**
Selecting this check box allows you to specify an attribute that stores a complete email address. McAfee® OTP Server can look up the specified attribute when it encounters an email address that does not contain the “@” character.

*Note:* This function is helpful when using email as a back-up delivery method.

**Test**
Sends a test email message.
### Configuring the Delivery Methods Object Type

#### 16.5 Netsize

Configuring the Netsize delivery method allows the McAfee® OTP Server to send one-time passwords using the Netsize SMS Gateway. A Netsize account is required.

Configuring the Netsize delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select **Netsize**.
2. Select the **Enable Netsize** check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.

#### 16.5.1 Communication

The following settings are located in the Communication area on the Netsize Delivery Method Configuration Pane:

**SMS Gateway**

Specifies the IP address or DNS name of the Netsize SMS Gateway.

**Port nr**

Specifies the port number of the Netsize SMS Gateway.
16.5.2 Authentication

The following settings are located in the Authentication area on the Netsize Delivery Method Configuration Pane:

**Login**
Specify the user name required for authentication.

**Password**
Specify the password required for authentication.

16.5.3 Message

The following setting is located in the Message area on the Netsize Delivery Method Configuration Pane:

**Message**
Specify the message to send to the mobile phone that includes the one-time password. McAfee® OTP Server replaces the $$OTP$$ tag in the message with the one-time password. If the tag is omitted from the message, McAfee® OTP Server appends the one-time password to the end of the message.

*Note:* Clicking the browse button opens the editor.

16.5.4 Endpoint Settings

The following settings, located in the Endpoint Settings area on the Netsize Delivery Method Configuration Pane, are Netsize settings. Please consult your Netsize customer service representative for more information.

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

16.5.5 Options

The following settings are located in the Options area on the Netsize Delivery Method Configuration Pane:

**Debug**
Selecting this check box enables debugging of Netsize packets in the console or log files.

**Encryption**
Selecting this check box enables encryption. This function requires coordination between McAfee® OTP Server and the Netsize SMS Gateway. Consult your Netsize customer service representative for more information.

**Message Type**
Specify 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
Configuring the Delivery Methods Object Type

16.6 Concurrent Sender

Configuring the Concurrent Sender delivery method allows the McAfee® OTP Server to simultaneously send one-time passwords using two or more delivery methods. The delivery methods must be configured and selected on the Concurrent Sender Delivery Method Configuration Pane.

Configuring the Concurrent Sender delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select Concurrent Sender.
2. Select the Enable Concurrent Sender check box on the Configuration Pane.
3. Select a configured delivery method from the Add method drop-down menu, and click Add. The method is added to the list of Sending methods.
4. (Optional) To remove a delivery method from the list of Sending methods, select it, and click Delete.
5. Repeat steps 3 and 4 as needed to configure the Concurrent Sender delivery method.
6. Click Save Config to save the configuration.
16.7 Instant Messaging

Configuring the Instant Messaging delivery method allows the McAfee® OTP Server to send one-time passwords using three different Instant Messaging methods: Skype, Microsoft Live (MSN), and Jabber (Google Talk). Configuring the Instant Messaging delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select Instant Messaging.
2. Select the Enable Instant Messaging check box on the Configuration Pane.
3. In the OTP Message field, type the message to be sent to the user’s mobile phone using the $$OTP$$ tag as a placeholder for the one-time password.
4. Select the tab corresponding to the Instant Messaging delivery method that you want to configure:
   — Skype
   — MSN
   — Jabber
5. Configure the settings on the selected tab. For more information about the settings on each tab, see the following sections. Each section corresponds to a different tab.

16.7.1 The User Prefix Feature

All three Instant Messaging methods support the “User Prefix” feature, in which the user ID has a prefix that specifies the Instant Messaging service in use. Using the prefix, McAfee® OTP Server can route the incoming instant message to the specified service. You configure the prefix by typing a value in the User Prefix field on the tab corresponding to each Instant Messaging service on the Configuration pane.

Google example:

User Prefix: GOOGLETALK
User ID: GOOGLETALK;firstlast@mcafee.com
16.7.2 Skype

Before you test the Skype Instant Messaging delivery method with McAfee® OTP Server, verify that the following requirements are met:

- The Skype client is installed and running on the McAfee® OTP Server and logged in to the Skype network.
- The McAfee® OTP Server is running Java 1.5.
- The Skype client prompts you, and you select “Yes”, allowing McAfee® OTP Server to pass messages to the Skype client.

**Note:** When you test the Skype Instant Messaging delivery method, do not provide a user prefix.
16.7.3 **Microsoft Live (MSN)**

Before you test the MSN Instant Messaging delivery method with McAfee® OTP Server, verify that you have a valid MSN account and configure the **MSN login id** and **MSN Password** fields. Selecting the **Debug** check box writes MSN debug information to the log files.

**Note:** When you test the Skype Instant Messaging delivery method, do not provide a user prefix.
Configuring the Delivery Methods Object Type

16.7.4 Jabber (Google Talk)

Before you test the Jabber Instant Messaging delivery method with McAfee® OTP Server, verify that you have a valid Jabber account and configure the following fields:

**Server**
Specifies the host name or IP address of the Jabber server.

**Port nr**
Specifies the port number of the Jabber server.

**Use SSL**
Selecting this check box specifies using the SSL protocol.

**Jabber ID**
Specifies your Jabber user name.

**Password**
Specifies your Jabber password.

**Note:** When you test the Jabber Instant Messaging delivery method, do not provide a user prefix.
16.8 SMPP

Configuring the SMPP delivery method allows the McAfee® OTP Server to send one-time passwords using the SMPP protocol. SMPP is an acronym for Short Message Peer-to-Peer. Configuring the SMPP delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select SMPP.
2. Select the Enable SMPP check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, contact McAfee® Technical Support:

   https://mysupport.mcafee.com
Configuring the Delivery Methods Object Type

16.9 CIMD2

Configuring the CIMD2 delivery method allows the McAfee® OTP Server to send one-time passwords using the proprietary Nokia CIMD2 protocol. Configuring the CIMD2 delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select **CIMD2**.
2. Select the **Enable CIMD2** check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, contact McAfee® Technical Support:
   
   [https://mysupport.mcafee.com](https://mysupport.mcafee.com)
16.10 UCP File

Configuring the UCP File delivery method allows the McAfee® OTP Server to create UCP files, one file for each one-time password. UCP is an acronym for Uniformity Correction Parameters. Configuring the UCP File delivery method involves the following steps.

1. Expand the Delivery Methods object type in the Select Pane, and then select UCP File.
2. Select the Enable UCP File check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see section 16.10.1 UCP File Options.
16.10.1 UCP File Options

The following settings are located in the UCP File Options area on the UCP File Delivery Method Configuration Pane:

**File Directory to drop file**
- Specifies the directory where one-time passwords are stored, each password in a separate UCP file.

**Filename starts with**
- Specifies a string that occurs at the beginning of each filename.
  **Example:** ucp

**Filename ends with**
- Specifies a string that occurs at the end of each filename.
  **Example:** .txt

**Template File**
- 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.

**Control+New Line (0D 0A)**
- Selecting this check box adds line breaks to the UCP file.

**File character set**
- Specifies the character encoding for the UCP file.
  **Example:** ISO-8859-1
Configuring the Delivery Methods Object Type
17.0 Misc

The Misc object type includes the following miscellaneous configuration types. For more information about each type, see the corresponding section:

- Expired Password Notification — See section 17.1 Expired Password Notification.
- OATH Configuration — See section 17.2 OATH Configuration.
- Prefetch Proxy Config — See section 17.3 Prefetch Proxy Config.
- Unlock User Accounts
- AES Encryption — See section 17.4 AES Encryption.
- Embedded HTTP Server — See section 17.5 Embedded HTTP Server.
- Pledge Enrollment — See section 17.6 Pledge Enrollment.
- Web Manager — See section 17.7 Web Manager.
- Yubico — See section 17.8 Yubico.
17.1 Expired Password Notification

Configuring the Expired Password Notification feature involves these steps.

1. Expand the Misc object type in the Select Pane, and then select **Expired Password Notification**.
2. Select the **Enable Expired Password Notification** check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see section 17.1.1 Expired Password Notification.

17.1.1 Expired Password Notification

The following settings are located in the Expired Password Notification area on the Expired Password Notification Configuration Pane:

**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 end 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 end users.
17.2 OATH Configuration

McAfee® OTP Server supports OATH HOTP and TOTP hardware tokens used by the Pledge OTP client. Configuring OATH authentication involves the following steps.

1. Expand the Misc object type in the Select Pane, and then select **OATH Configuration**.

2. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.
17.2.1 HOTP

The following settings can be configured for HOTP tokens:

**Encrypt Key and counter**
Specifies whether the HOTP key and counter are encrypted in the database.

**Validation LookAhead Value**
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.

**OTP Length**
Selects the length of the one-time password.

**Truncation value**
Specifies an offset value for OATH devices. A value of -1 specifies variable truncation. Do not modify this value.

17.2.2 TOTP

The following settings can be configured for TOTP tokens:

**Accept time drift**
Selecting this check box allows McAfee® OTP Server to accept the preceding, current, or succeeding one-time password instead of only the current one-time password to compensate for time drift.

**Anti-replay check**
Selecting this check box specifies that each one-time password is only valid once in a specified time frame set by the token device, usually 30 or 60 seconds.

**Encrypt Key value**
Selecting this check box specifies that the TOTP key is encrypted in the database.

**Max Out of Synch Time Steps**
Specifies the maximum number of time steps that an OATH device can be out-of-sync with McAfee® OTP Server. The time step is set by the OATH device, for example, 30 seconds.

17.2.3 General OATH Settings

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

**Pincode placement**
Selects whether the end user enters the PIN code before or after the HOTP/TOTP token when a PIN code is used.

**Accept OATH Token Identifier**
Selecting this check box adds support for token devices that send a token identifier in addition to a one-time password.

**Enable Automatic Enrollment (Class A - OATH Token Identifier)**
Selecting this check box 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.

**Note:** For more information about storing OATH keys in user databases, see the McAfee® OTP Server guide to OATH integration.
17.2.4 Automatic OATH Enrollment

The settings in the Automatic Oath Enrollment area on the OATH Configuration Pane are only available when the Accept OATH Token Identifier and Enable Automatic Enrollment check boxes are selected in the General section:

Key storage database
Selects the database containing the keys and token identifier.

Check SQL Database
Tests whether the TOKENDB database and Tokens table exist in the selected SQL database. If they do not exist, click Yes to create them.

Note: The Check SQL Database button is only visible when the selected database is a SQL database.

Object DN
Selects an LDAP object in which to store the keys.

Note: This field is only visible when the selected database is an LDAP database.

Attribute
Selects an LDAP attribute in which to store the keys.

Note: This field is only visible when the selected database is an LDAP database.

Upload keyfile to database
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. PSKC is an acronym for Portable Symmetric Key Container.

Allow multiple token assignments
Selecting this check box accepts a user that has one OATH token and wants to enroll for a second token.

Encrypt keys in keystorage database
Selecting this check box specifies that the keys in the key database are encrypted.

Note: If AES is configured, then the keys are encrypted using AES encryption.
17.2.5 **Advanced Automatic OATH Enrollment**

Some LDAP databases limit the number of keys per object to 1000. To overcome this limitation, you can configure multiple LDAP objects and attributes for storing OATH keys on the Advanced Configuration dialog. To open the dialog, click **Advanced** in the Automatic OATH Enrollment area on the OATH Configuration Pane.
17.3 Prefetch Proxy Config

Using the Prefetch Proxy Config feature, you can specify one or more proxy OTP servers to manage the prefetch one-time passwords, and you can select the OTP delivery method used. Configuring the Prefetch Proxy Config feature involves the following steps.

1. Expand the Misc object type in the Select Pane, and then select Prefetch Proxy Config.
2. To send all prefetch one-time passwords to a proxy OTP server for management, select the Proxy Sending of Prefetch OTPs check box on the Configuration Pane.
3. Type the IP address and port number (separated by a colon) of the proxy OTP server in the field that opens when you enable proxy sending of prefetch one-time passwords.
   **Note:** To specify multiple proxy OTP servers, use a semi-colon to separate each IP address-port number pair.
4. Select the OTP delivery method to use when sending prefetch one-time passwords to the end user from the Force Sending Prefetch OTP with Method drop-down menu.
   **Note:** Only configured OTP delivery methods are available.
17.4 AES Encryption

McAfee® OTP Server V3.1 (and above) supports AES encryption and decryption. Using AES, McAfee® OTP Server can store OATH keys and other sensitive information in the databases. Configuring AES encryption involves the following steps.

1. Expand the Misc object type in the Select Pane, and then select AES Encryption.
2. Select the Enable AES Encryption check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the following sections. Each section corresponds to a different heading on the Configuration Pane.

17.4.1 General Settings

In the General Settings area, click Add to specify the attributes that you want McAfee® OTP Server to encrypt. To enable AES encryption for a specific database, follow these steps:

1. On the Configuration Pane corresponding to the database, select the External Databasehandler check box, and type “ext.aes” in the field that opens.
2. Click Save Config to save the configuration.
17.4.2 Advanced Settings

The following settings are located in the Advanced Settings area on the AES Encryption Configuration Pane:

AES Key
Specifies the key to use for AES encryption and decryption, as follows:
- To specify a 128-bit key, provide a string of 32 characters.
- To specify a 256-bit key, provide a string of 64 characters.

**Note:** Do not modify the AES key in a production environment. All data encrypted with the key that you erase can no longer be decrypted or recovered.

Key size
Selects a key size from the drop-down menu: 128, 192, or 256.
**Units:** bits

AES prefix
Specifies the encryption format of an encrypted value. The prefix is added to the front of the value.
**Default:** {AES}

Key type format
Selects a format for the AES key: hex (hexadecimal) or Base64.
**Default:** hex

Data format
Selects a format for the encrypted data: hex (hexadecimal) or Base64.
**Default:** hex

Use CBC
Selecting this check box enables cipher-block chaining (CBC).

IV (CBC)
Specifies the initialization vector required to implement CBC.
**Note:** The initialization vector must be specified in hexadecimal format and be 32 characters in length (16 bytes).

Lock
Clicking this button alternately locks and unlocks the AES settings. Locking the settings protects them from being changed unintentionally.

17.4.3 Test Encryption and Decryption

The following settings are located in the Test encryption and decryption area on the AES Encryption Configuration Pane:

Value
Specifies a value to encrypt or decrypt with the AES key that you configured.
**Note:** For the test, specify a value that is as long as or longer than the AES key.

Result
Displays the encryption or decryption result when you click Encrypt or Decrypt, respectively.
17.5 Embedded HTTP Server

McAfee® OTP Server includes an embedded HTTP server, which is used for Pledge Enrollment, Identity Management, and other web applications. Configuring the embedded HTTP server involves these steps.

1. Expand the Misc object type in the Select Pane, and then select Embedded HTTP Server.
2. Select the Enable Embedded HTTP Server check box on the Configuration Pane.
3. Configure the following settings on the Configuration Pane:
   - **Port nr**: Specifies the port number of the embedded HTTP server.
     - **Default**: 8080
   - **Enable SSL**: Selecting this check box enables SSL for the HTTP server.
     - **Default**: Selected
   - **SSL Options - PKCS12 file**: Selects the P12 certificate file used by the SSL protocol.
   - **SSL Options - PKCS Password**: Specifies the password that protects the P12 certificate file.
   - **Enable AJP**: Selecting this check box enables the AJP option for the Apache front end. AJP is an acronym for Apache JServ Protocol.

**Note:** The embedded HTTP server reads the configuration settings each time it starts. Therefore, McAfee® OTP Server must be restarted for the new settings to take effect. If McAfee® OTP Server 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.
17.6 Pledge Enrollment

Using a web application installed on the Tomcat server, end users can follow an easy, step-by-step Pledge Enrollment process that downloads a Pledge Profile which includes an HOTP key. Using a web services interface that is integrated with the Profile Factory, administrators can customize the Pledge Profile.

Configuring the Pledge Enrollment web application involves the following steps:

1. Expand the Misc object type in the Select Pane, and then select **Pledge Enrollment**.
2. Select the **Enable Pledge Enrollment** check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the McAfee® OTP Server step-by-step guide to implementing Pledge Enrollment.
17.7 Web Manager

McAfee® OTP Server includes a preconfigured version of the Web Manager Portal installed on the Tomcat server. Administrators and help desk personnel can use the Portal to manage user information in user stores (databases). End users can also use the Portal to update information in their accounts.

Configuring the Web Manager web application involves the following steps:

1. Expand the Misc object type in the Select Pane, and then select **Web Manager**.
2. Select the **Enable Web Manager** check box on the Configuration Pane.
17.8 Yubico

McAfee® OTP Server supports the integration of Yubico YubiKey Validation Server, which provides OTP validation and management services through web services APIs. To configure Yubico integration, follow these steps.

1. Expand the Misc object type in the Select Pane, and then select **Yubico**.
2. Select the **Enable Yubico** check box on the Configuration Pane.
3. Configure the remaining settings on the Configuration Pane. For more information about the settings, see the McAfee® OTP Server guide to Yubico integration.
18.0 Starting and Stopping McAfee® OTP Server

McAfee® OTP Server supports the following operating systems. For information about starting and stopping McAfee® OTP Server on each operating system platform, see the corresponding sections:

- UNIX, Linux, Mac OS X — See section 18.2 Starting and Stopping on UNIX.

Note: We recommend that you stop McAfee® OTP Server by clicking Shutdown on the McAfee® OTP Server Monitor. For this option, the Monitor must be enabled. For information about enabling the Monitor, see section 19.0 The McAfee® OTP Server Monitor.

18.1 Starting and Stopping on Windows

To start and stop McAfee® OTP Server on Microsoft Windows, you have the following options:

- You can start and stop McAfee® OTP Server using Microsoft Windows Services.
- You can start McAfee® OTP Server by running the following program file which is located in the installation directory: OTPServer.exe.
- You can stop McAfee® OTP Server by clicking Shutdown on the Monitor.

18.2 Starting and Stopping on UNIX

To start and stop McAfee® OTP Server on UNIX, Linux, or Mac OS X, you have the following options:

- You can start McAfee® OTP Server by running the "OTPServer" program file in the background using the following UNIX command: OTPServer &.
- You can stop McAfee® OTP Server by using the UNIX kill command.
- You can stop McAfee® OTP Server by clicking Shutdown on the Monitor.
19.0 The McAfee® OTP Server Monitor

To enable the McAfee® OTP Server Monitor, select the Server object type in the Select Pane. Then in the Options area on the Configuration Pane, select the Enable Monitor check box. If this check box is selected, the Monitor opens when the McAfee® OTP Server starts. The Monitor requires GUI support.

When the monitor opens, it displays three options:

- Configuration — Clicking this option opens the OTP Configuration window, where you can select and configure the following object types. For more information, see section 8.0 Configuration Overview.
  - Server
  - RADIUS
  - Logs
  - Alerts
  - Licenses
  - Databases
  - Clients
  - Delivery Methods
  - Misc

- Show Details — Clicking this option displays statistics. For more information, see section 19.1 McAfee® OTP Server Statistics.

- Shutdown — Clicking this option shuts down the McAfee® OTP Server. For more information, see section 18.0 Starting and Stopping McAfee® OTP Server.
19.1 McAfee® OTP Server Statistics

Clicking Show Details on the McAfee® OTP Server Monitor opens the following page.

![McAfee OTP Server Monitor](image)

The statistics on this page can be grouped as follows. For more information about each group, see the corresponding section:

- Sending one-time passwords — See section 19.1.1 Sending One-time Passwords.
- One-time passwords — See section 19.1.2 One-time Passwords.
- RADIUS — See section 19.1.3 RADIUS.
- Licenses — See section 19.1.4 Licenses.
- Connections — See section 19.1.5 Connections.
- Encryption — See section 19.1.6 Encryption.
- User Database Authentication — See section 19.1.7 User Database Authentication.
19.1.1 Sending One-time Passwords

The following statistic shows how many one-time passwords were created and sent.

**Total OTPs**
Displays the total number of one-time passwords created and sent.

19.1.2 One-time Passwords

The following statistics provide more information about the one-time passwords that were created and sent.

**Successful OTPs**
Displays the number of one-time passwords that the OTP clients successfully returned.

**Failed OTPs**
Displays the number of one-time passwords that the OTP clients failed to return.

**Unfetched OTPs**
Displays the number of one-time passwords that the OTP clients did not retrieve.

**Expired OTPs**
Displays the number of one-time passwords that expired.

19.1.3 RADIUS

The following statistics provide more information about the McAfee® OTP Server when configured as a RADIUS server.

**RADIUS Packets Sent**
Displays the number of RADIUS packets sent.

**RADIUS Packets Received**
Displays the number of RADIUS packets received.

19.1.4 Licenses

The following statistics provide more information about registered licenses.

**Nr of Licenses**
Displays the total number of registered licenses.

**Used Licenses**
Displays how many registered licenses out of the total are currently in use.
19.1.5 Connections

The following statistics provide more information about the connections between McAfee® OTP Server and the native OTP clients.

Active Connections
Displays the number of connections to native OTP clients that are currently active.

Successful Connections
Displays the number of successful connections to native OTP clients.

Failed Connections
Displays the number of failed connections to native OTP clients.

19.1.6 Encryption

The following statistics provide information about whether requests from native OTP clients to McAfee® OTP Server are encrypted.

Encrypted Requests
Displays the number of encrypted requests from native OTP clients to the McAfee® OTP Server.

Unencrypted Requests
Displays the number of unencrypted requests from native OTP clients to the McAfee® OTP Server.

Rejected Unencrypted Req
Displays the number of unencrypted requests from native OTP clients to the McAfee® OTP Server that were rejected because they were not encrypted.

Note: To enable this feature, select the “Always encryption” option in the Encryption area on the Server Configuration Pane.

19.1.7 User Database Authentication

The following statistics provide more information about user authentication and locked user accounts.

Successful Logins
Displays the number of times that end users successfully authenticated to LDAP and JDBC/ODBC databases.

Failed Logins
Displays the number of times that end users failed to authenticate to LDAP and JDBC/ODBC databases.

Locked Accounts
Displays the number of times that McAfee® OTP Server locked end user accounts, because the number of login attempts to LDAP or JDBC/ODBC databases exceeded the maximum allowed.
20.0 On-demand Services

On-demand services are hosted by McAfee® on its own servers, so there is no need to install the product in your environment. The following on-demand services are offered:

- **OTP as a Service** — You access the McAfee® OTP service through web services.
- **SMS as a Service** — You access the McAfee® SMS service through web services.
- **SMS Gateway** — You access McAfee® SMS Gateway through a plug-in. McAfee® SMS Gateway is a hosted service that delivers one-time passwords using SMS.