Product Guide

Revision A

McAfee Enterprise Authentication 1.0.0

COPYRIGHT

TRADEMARK ATTRIBUTIONS

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

LICENSE INFORMATION

License Agreement

Contents

Deployment

Setup

Configuration and use

Preface

This guide provides the information you need to work with your McAfee product.

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
ℹ	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
❗	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1. Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.

2. Enter a product name, select a version, then click **Search** to display a list of documents.

1 Introduction

Protect your enterprise network data and resources against unauthorized access by integrating McAfee® Enterprise Authentication (Enterprise Authentication) directly with your on-premise or cloud-based environment.

Contents

About Enterprise Authentication

Enterprise Authentication supports many strong authentication methods to ensure your network is protected.

Today, simple passwords are no longer a secure solution for protecting your enterprise data and resources such as networks, applications, and services. Enterprise Authentication combines multiple authentication methods to securely authenticate users in your on-premise or cloud-based environments.

Adding Enterprise Authentication helps you to avoid these potential high-risk issues:

- Unauthorized network access
- Maintaining lists of long and complex passwords
- Security attacks
- Uncontrolled access to sensitive data
- Online identity theft

How authentication works

Users initiate the authentication process when they request access to protected resources.

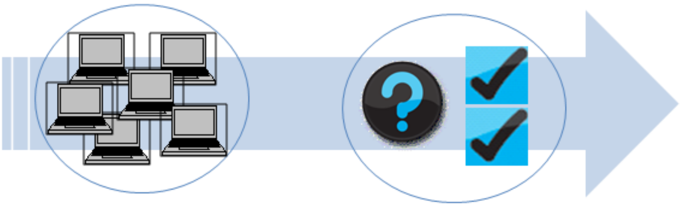

Figure 1-1 Authentication process

Enterprise Authentication receives authentication requests through these protocols:

- Remote Authentication Dial-In User Service (RADIUS)
- Security Assertion Markup Language (SAML)
    - Hyper Text Transfer Protocol/Secure Sockets Layer (HTTP/HTTPS)
    - Representational State Transfer (REST)

Depending on your configuration, various authentication methods are used to authenticate user identities. Once authenticated, the validated information is passed to the protected resources and users are permitted access.

Deployment

Before you deploy Enterprise Authentication on your network, consider your options and create your deployment plan.

2

Deployment options

Enterprise Authentication offers several options to meet your deployment needs.

Contents

Types of installations

Enterprise Authentication offers two installation options.

Required installation

Install Enterprise Authentication on your dedicated standalone server to use as a secure central point for managing the software, storing data, and hosting the web-based interfaces.

Use the Enterprise Authentication server to perform these tasks:

- Install the Enterprise Authentication software
- Facilitate deployment
- Manage the database
- Manage configuration and user data

Cluster installation

When you install Enterprise Authentication on several servers, you can cluster and configure the servers to share configuration and user session data.

Clusters contain these server types:

- **Master server** — The first Enterprise Authentication installation you install and configure in the cluster.
- **Seed server** — All subsequent server installations configured in the cluster.

Each server within a cluster shares the following Enterprise Authentication data:

- **Configuration** — Settings configured on the administration interface that is persistently stored in a configuration database.
- **Session** — Sequences of client browser requests that are tracked when users are successfully authenticated until they log off.

By default, Enterprise Authentication stores session data locally for 30 minutes.

Configuring the servers to share data enables:

- **Failover** — If one server fails, the other servers within the cluster automatically absorb the workload.
- **High Availability** — The ability for each server to absorb the workload.

Example: An Enterprise Authentication server receives an authentication request but is disconnected from the network for routine maintenance. Another Enterprise Authentication server within the same cluster immediately absorbs the request and seamlessly continues to authenticate the user.

Cluster installations are helpful to:

- Ensure that the authentication process is uninterrupted during routine server maintenance
- Monitor and maintain separate databases for multiple resources
- Recover system data after a failure

Web-based interface

Enterprise Authentication is comprised of two web-based interface portals designed specifically for administrator and user needs.

Table 2-1 Interface definitions

Interface	Definition
Administration	Provides administrators with a single, central point for configuring and managing Enterprise Authentication.
Web Manager	User administrators and service desk personnel use their network user name and password to log on and access these settings: • General user information • Reset user lockout • Token management • PIN management Users log on with their network user name and password to access these settings: • General information • Token enrollment • Security questions • PIN management

Tenancy and administrator roles

Enterprise Authentication supports multi-tenant architectures, where one Enterprise Authentication server hosts multiple client-organizations, also called tenants. To manage each tenant, Enterprise Authentication uses role-based access to assign different sets of administrator permissions.

Contents

Multi-tenancy

Tenants represent businesses within an enterprise or companies that subscribe to cloud-based services through a Service Provider.

In a multi-tenant architecture, all tenants share the Enterprise Authentication software, but each tenant manages their own data, which is isolated from all other tenants. Enterprise Authentication securely isolates tenant data using metadata that links each tenant to their own database.

Multi-tenancy is helpful for:

- Enterprise data centers — Avoid security and management issues by virtualizing data server systems behind fewer resources.
- Cloud-based Service Providers — When managing many subscribers, simplify tasks and performance maintenance.

Administrator roles and permissions

Enterprise Authentication supports three administrator roles.

Contents

System administrators

Enterprise Authentication is installed with a default tenant account, which has a built-in administrator account used to log on to the web-based administration interface.

The administrator using the built-in account logs on to the administration interface to access and manage all configurable Enterprise Authentication settings, including:

- Administrator roles and permissions
- Tenant configuration
- Certificate and token management
- User data storage
- Authentication requests

Tenant administrators

In a multi-tenant environment, you can assign one administrator role to each tenant.

Each tenant administrator manages their own tenant settings. Although multiple tenants can be hosted on the same server, each tenant is unable to access other tenant data.

Tenant administrators log on to the administration interface to access and manage these tenant domain functions:

- Manage identity stores
- Manage actions
- Export authentication flows

User administrators

User administrators assist users with common administrative tasks.

User administrators log on to the Web Manager interface to access and manage these user settings:

- Maintain user contact information
- Reset user lockout

- Manage tokens
- Manage PINs

3 Deployment scenarios

When creating your deployment plan, consider each Enterprise Authentication deployment scenarios.

You can implement Enterprise Authentication for various environment infrastructures, and these deployment scenarios vary depending on your network needs.

Contents

RADIUS deployment scenario

RADIUS is a client and server protocol that enables remote access servers to communicate with the Enterprise Authentication server to authenticate users.

Example use case

Use Enterprise Authentication to authenticate off-premise users that request access to your protected network through the Virtual Private Network (VPN).

How it works

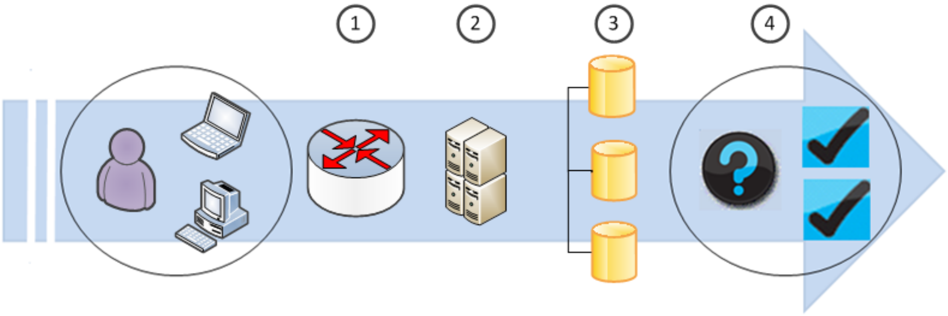

Figure 3-1 RADIUS authentication process

Number	Description
1	Off-premise users request access to protected networks through VPN.
2	Network VPN servers process the request, gathers user identity information, then passes the requests to Enterprise Authentication.
3	Enterprise Authentication matches user identity information against the identity store.
4	Users are successfully authenticated and access to the protected networks is granted.

Considerations

- UPD ports configured on the Enterprise Authentication server and RADIUS client are identical.
- The shared secrets configured on the Enterprise Authentication server and RADIUS client are identical.
- All multi-factor authentication tokens have been uploaded using the administration interface.
- If using one-time password authentication, the RADIUS client must support RADIUS challenge-response.

High-level steps for configuration

1. On the administration interface, set up the RADIUS listener.
2. Connect Enterprise Authentication to the user data source.
3. Configure the RADIUS authentication flow.
4. Verify the configuration.

See also

Configure RADIUS listeners on page 39
Connect Enterprise Authentication to data sources on page 41
Configure RADIUS flows using the guided configuration tool on page 36

Enterprise Authentication as the Identity Provider

When deployed as the Identity Provider, Enterprise Authentication uses SAML to separate Identity Provider and Service Provider roles.

Example use cases

- Enterprise Authentication receives authentication requests from Service Providers and responds by validating user identities against a configured identity store. If the identity information is validated, Enterprise Authentication passes the authentication response to the protected resource, and users are granted access.
- Network users log on to the company intranet to access third-party Service Providers, such as their health insurance and 401k providers. When users log on to the company intranet, Enterprise Authentication validates their identity against a configured identity store and creates the user session. As long as the user session is active, users can access the third-party Service Providers without providing their user authentication credentials.

How it works

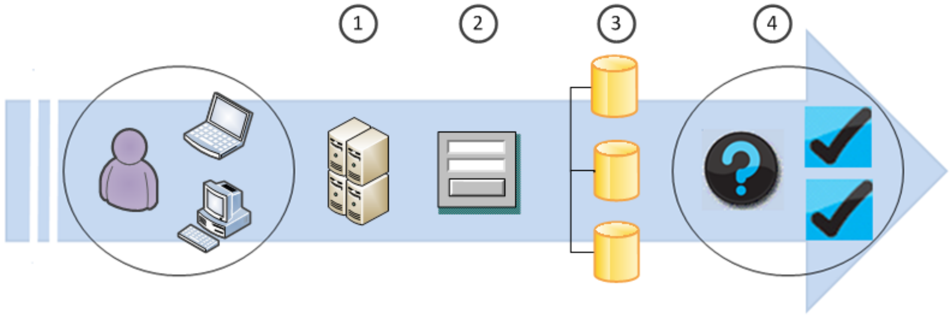

Figure 3-2 Enterprise Authentication as the Identity Provider

Number	Description
1	Users request access protected applications and are redirected to Enterprise Authentication (Identity Provider) for authentication.
2	At the logon screen, users are prompted to provide their identity credentials, such as a user name and password.
3	Enterprise Authentication validates user identity information against the identity store and issues secure access tokens.
4	Users and tokens are redirected to the protected application Service Providers and access is granted. For future requests, users are automatically granted access since a session is already established between users and Identity Providers.

Considerations

All certificates and tokens are available on the Enterprise Authentication administration interface.

High-level steps for implementation

1. Using the administration interface, set up the HTTP listener.
2. Connect Enterprise Authentication to the data source.
3. Configure the SAML authentication flow.
4. Establish the Enterprise Authentication and Service Provider relationship with these metadata settings:
   - Entity ID — URL type, such as idp.mcafee.com
   - SSOURL — URL where the Identity Provider is hosted and where the Service Provider redirects the client
5. Verify the configuration.

See also

Configure HTTP listeners on page 40
Connect Enterprise Authentication to data sources on page 41
Configure SAML Identity Provider flows using the guided configuration tool on page 37

4 Plan your deployment

Before you install Enterprise Authentication, plan and prepare your network environment.

Contents

Requirements

To ensure that your deployment is successful, your environment must meet the minimum requirements.

Table 4-1 Requirements

Component	Requirement
Dedicated server	You must have administrator rights to the dedicated network server.
Server-class operating system	Install Enterprise Authentication on any of these 32- and 64-bit server-class operating systems that support Java Runtime Environment version 1.7 or later: • Linux • Microsoft Windows 2008 R2 • Microsoft Windows 2012
Hardware memory	2 GB available RAM
Software	Java 7
Virtual infrastructure software	These virtual infrastructure software types are supported: • VMware • Microsoft Hyper-V
Internet browsers	Web-based components require one of these supported browsers: • Google Chrome, version 31 and later • Microsoft Internet Explorer, version 9 and later • Mozilla Firefox, version 26 and later

Table 4-1 Requirements *(continued)*

Component	Requirement
User data stores	These user data stores are supported: • Active Directory (AD) • Lightweight Directory Access Protocol (LDAP) • Structured Query Language (SQL) • Oracle • MySQL • Microsoft SQL Server • PostgreSQL
Certifications support	Enterprise Authentication includes a certified RSA BSAFE CryptoJ 6.1.0.0.2 module and always starts in FIPS mode.

Authentication methods

For strong authentication, Enterprise Authentication provides several authentication methods to securely validate user identities.

Contents

Multi-factor authentication

Enterprise Authentication supports multi-factor authentication (MFA), which uses a combination of authentication factors to determine user identities.

The more factors used to determine user identities, the greater the trust of authenticity.

Strong MFA uses combinations of these factors:

- Something you know, such as a password or PIN
- Something you have, such as a token or smart card

Example: When using MFA to gain access to protected resources, users are authenticated using their password and one-time password. Enterprise Authentication grants access when the user successfully returns the generated one-time password.

Table 4-2 One-time password support

Factor	Options
McAfee Message Gateway cloud service	Sends one-time passwords to user devices with these delivery methods: • Short Message Service (SMS) • Voice
McAfee® Software Token Pledge (Pledge)	Mobile and desktop application that generates one-time passwords using these algorithms: • Open Authentication (OATH) • Time-based One-time Password (TOTP) • HMAC-based One-time Password (HOTP) • OATH Challenge-Response Algorithm (OCRA) For additional security, you can require users to enter PINs for access to their Pledge application. For more information, see the *McAfee Pledge Software Token User Guide*.
Simple Mail Transfer Protocol (SMTP)	Sends one-time passwords to user email addresses.
Hardware token	Generate one-time passwords based on these OATH algorithms: • TOTP • HOTP
Temporary token	If users forget or lose their tokens, you can issue them temporary tokens that generate one-time passwords.

Certificate-based authentication

Enterprise Authentication supports public and private certificates, which replace user names and passwords in the authentication process with electronic documents.

Certificates process and validate authentication requests between you and protected resources.

Each certificate includes public and private keys, also known as key pairs, issued by trusted third-party certificate authorities (CAs). Key pairs include the following information:

- Unique serial number
- User identity information, such as name, telephone number, and email address
- Certificate expiration date
- Digital signature of the CA that issued the certificate

Successful certificate-based authentication between you and protected resources only occurs when the associated key pair data is verified as current and authentic.

Certificate-based authentication is helpful to avoid:

- Identity theft — Since passwords are more prone to theft, certificates ensure that identity information is valid and secure.
- Unauthorized access — When certificates become compromised, they also become unusable.
- Password maintenance — Avoid requiring users to maintain long lists of complex passwords that are difficult to remember and easy to lose.

Integrated Windows authentication

Enterprise Authentication supports Integrated Windows authentication (IWA), which uses the Windows client user information for authentication.

When users log on to the corporate network from their Windows client, Enterprise Authentication uses IWA to grant access to protected resources with the Windows user authentication credentials.

IWA is helpful to:

- Bypass initial logon prompts
- Avoid transferring user credentials over the network

Context-aware authentication

Enterprise Authentication combines context-aware information with other authentication factors to authenticate user identities.

To enable context-aware authentication, Enterprise Authentication uses this information:

- Geographical location
- Browser type
- Operating system type

Example: To access online bank accounts, users enter a user name and password. When users access their account outside their home location, the bank websites recognizes the new location using context-based information. To securely validate the user identity, the bank website prompts users to identify themselves using a user name, password, and several additional authentication methods.

Deployment checklist

To make sure that your network is ready to install Enterprise Authentication, review the deployment checklist.

Table 4-3 Environment structure

Determine...	Verified
The location of the network server where you plan to install the Enterprise Authentication software	
If you plan to install the Enterprise Authentication software in cluster. If so, gather the following information for each cluster: • Choose a name for the cluster • Get the IP address for each server • Determine the seed servers • If you have firewalls running on the servers in your cluster, you must open the ports used for communication	

Table 4-3 Environment structure *(continued)*

Determine...	Verified
That you have administrator rights on all servers you intend to use	
If these minimum requirements are met: • Server-class operating system • Hardware memory • Software • Virtual infrastructure software • Internet browser	
The location of your Enterprise Authentication license file	

Table 4-4 Users

Determine...	Verified
How many users in your network require authentication and whether they are located on-premise or remote	
Where your user data is stored and confirm that you have an Enterprise Authentication supported directory server	
Which users to assign these administrator roles: • System • Tenant • User	

Table 4-5 Resources

Determine...	Verified
The network resources that require secure protection	
Which of these supported protocols to use for authentication: • RADIUS • Kerberos • HTTP • SAML 2.0 • REST	
That the ports between network resources and Enterprise Authentication are configured for communication	
The appropriate authentication methods to use for securing your protected network resources	
That Enterprise Authentication supports your software and hardware tokens, including these OATH standards: • HOTP (RFC 4226) • TOTP (RFC 6238) • Pledge ❗ If you use Pledge, also determine that you have a valid Pledge Profile Service account	

Table 4-5 Resources *(continued)*

Determine...	Verified
If you plan to send one-time passwords using the McAfee Message Gateway. If so, you must have a: • Valid McAfee Message Gateway account • License file that supports sending SMS	
If you plan to send one-time passwords with an email address. If so, verify that you have an SMTP server that accepts and relays email messages from Enterprise Authentication.	
That Enterprise Authentication supports your certificate file formats, including: • Java Key Store (JKS) • PEM encoded public certificates • PKCS 12 (based on the PKCS #12 standard) ! If you currently have PKCS 12 files with weak encryption, you must rebuild the PKCS 12 container with FIPS compatible encryption.	
If you plan to use IWA, verify that Enterprise Authentication is installed on the same domain as the Windows client.	

Setup

Install Enterprise Authentication on your computer and complete the post-installation tasks.

5 Installation

To complete the installation, download and install the Enterprise Authentication product files on your supported server-class operating system.

Contents

Download the product files

Download the Enterprise Authentication product files from the McAfee Downloads page.

Task

1. Log on to your operating system as the administrator.
2. Go to the McAfee Downloads page.
3. Enter your grant number, then click **Go**.
4. Go to Enterprise Authentication, and select the version.
5. Download the installation file appropriate for your computer.

Install the product files

Install the Enterprise Authentication product files on your computer.

Task

1. Locate and unzip the downloaded Enterprise Authentication product files.
2. Double-click the Enterprise Authentication installation program.
3. Follow the on-screen command prompts.

6 Post-installation tasks

To ensure your network is prepared for authentication, complete the post-installation tasks.

Contents

Set up clusters

Install the Enterprise Authentication software on each additional server and configure the servers to share data.

Task

1. Install and start the Enterprise Authentication software on the seed servers.
2. Locate the C:/Program Files/McAfee/EA/config directory.
3. For each seed server, follow these steps:

Table 6-1 Data store configuration

Task	Steps
Enable the configuration data store.	1 Use your text editor to open cassandra.yaml. 2 Edit these values: • **initial_token** — Specifies the number of tokens assigned to the server. • **listen_address** — Replaces the default value with the IP address accessible by the other servers in the cluster. • **seeds** — Specifies the internal IP address of each seed server in the cluster. 3 Save and close the file.
Enable the user session data store.	1 Use your text editor to open vas.properties. 2 Locate SessionStore and remove: com.mcafee.vas.session.impl.HazelcastSessionStore 3 Save and close the file.

4. Restart the server.

5. Verify the cluster setup.
   a. On the administration interface, click the **Cluster** tab.
   b. Move your cursor over the server and verify that the correct information appears.

Access the administration interface

Log on to the administration interface where you perform all configuration and management tasks.

Contents

Change the default HTTP port

Change the default 8443 HTTP port you use to access the web-based interfaces.

Task

1. Locate the C:/Program Files/McAfee/EA/config directory.
2. Use your text editor to open vas.properties and type: `vas.service.http.ssl.listenPort=<port number>`
3. Save and close the file.

Log on to the administration interface

Use the built-in administrator account to log on to the administration interface.

Task

1. On your browser, type: `https://<Enterprise Authentication server host name or IP address>:<port number>`
2. On the Enterprise Authentication logon page, enter the initial built-in administrator user name and password.
   a. In the **user ID** field, enter `admin`.
   b. In the **password** field, enter `password`.
3. From the **Language** drop-down list, select your preferred language, then click **Login**.

Change the built-in administrator account credentials

When you log on to the administration interface for the first time, you are prompted to change the built-in administrator account password.

Task

1. On the **Change password** window, enter `password` in the **Current password** field.
2. In the **New password** field, enter your password.
3. In the **Repeat new password** field, re-enter your password, then click **Change password**.

Add tenants

To add tenants that are hosted on the same Enterprise Authentication server, use the administration interface.

Task

1. In the administration interface, click the **Tenants** tab.
2. Click **Add Tenant**.
3. On the **Create tenant** window, enter the tenant user name in the **Name** field.
4. Click **Create**.

Configuration and use

Use the Enterprise Authentication web-based components to configure your authentication options.

7 Processing authentication requests with flows

When users request access to protected resources, Enterprise Authentication uses authentication flows to securely authenticate user identities.

Contents

Authentication flow configuration options

Configure authentication flows that contain various sequences of authentication paths, which control how Enterprise Authentication responds to different authentication scenarios.

These configuration options are available:

Guided — To help you become familiar with the administration interface, walks you through each required configurable setting to create flows for common RADIUS and SAML scenarios.

Manual — Allows you to create custom flows by configuring each authentication flow setting.

To configure authentication flows, you must use conditions and actions to ensure only permitted users have access protected resources. Each authentication flow contains a sequence of events that contain:

- **Conditions** — Rules that determine which flow is used for incoming authentication requests
- **Actions** — Tasks that are executed during the authentication process

  Each time an action is processed, it responds in one of these ways:

  - **Success** — Action processed successfully and the next action process begins.
  - **Incomplete** — Action required more information and the authentication process restarts.
  - **Failure** — Action received incorrect information and the authentication process stops until the correct information is provided.

Example: When users request access to protected resources, Enterprise Authentication receives the authentication request and uses conditions to determine the appropriate flow to use. Enterprise Authentication processes the sequence of actions configured in the authentication flow, which prompt to:

- Provide their user name and password
- Generate and return the one-time password using their token
- Provide their PIN

The response of each processed action determines whether the user is granted access to the protected resource.

Both configuration options include these basic steps:

1. Designate an authentication method.
2. Configure the listener that handles incoming traffic for specific protocols.
3. Define where user information is stored, and how Enterprise Authentication can access it.
4. Configure actions and conditions.

Configure flows using the guided configuration tool

To configuration RADIUS and SAML authentication flows, McAfee recommends using the guided configuration tool until you become familiar with the administration interface.

Contents

Configure RADIUS flows using the guided configuration tool

Use the guided configuration tool to create RADIUS authentication flows for your VPN or firewall solution.

Task

1. On the administration interface, click the **Main** tab, then click **Start | Create New Authentication Flow.**
2. Select **Setup VPN or Firewall (RADIUS)**, then follow the on-screen prompts.
3. On the **Finish Configuration** window, enter a unique name in the **Display name** field.
4. In the **Description** field, enter any additional information.
5. Verify that the **Enable now** checkbox is selected.
6. Add conditions.
   a. Click **Add.**
   b. In the **Attribute** field, enter the attribute on which you want to build the condition.
   c. Select one of these operators:
      - **must**
      - **can not**
   d. Choose from one of these options:
      - Select **exist.**
      - In the **contain** field, enter the value.
      - In the **match** field, enter the value.

e Click **Add**.

f Check and resolve any possible condition conflicts.

7 Click **Next**.

Configure SAML Identity Provider flows using the guided configuration tool

Use the guided configuration tool to configure Enterprise Authentication as the Identity Provider.

Task

1 On the administration interface, click the **Main** tab, then click **Start** | **Create New Authentication Flow**.

2 Select **Setup SAML IdP**, then follow the on-screen prompts.

3 On the **Finish Configuration** window, enter a unique name in the **Display name** field.

4 In the **Description** field, enter any additional information.

5 Verify that the **Enable now** checkbox is selected.

6 Add conditions.

a Click **Add**.

b In the **Attribute** field, enter the attribute on which you want to build the condition.

c Select one of these operators:

- **must**
- **can not**

d Choose from one of these options:

- Select **exist**.
- In the **contain** field, enter the value.
- In the **match** field, enter the value.

e Click **Add**.

f Check and resolve any possible condition conflicts.

7 Click **Next**.

Create custom authentication flows

To create custom authentication flows that meet your specific network needs, manually combine Enterprise Authentication actions and conditions.

Tasks

- *Upload certificates* on page 38
  To enable certificate-based authentication, upload certificate files to Enterprise Authentication.
- *Import tokens* on page 39
  To enable user token authentication, import tokens to Enterprise Authentication.
- *Configure listeners* on page 39
  Configure the options that control how Enterprise Authentication handles incoming authentication requests.
- *Connect Enterprise Authentication to data sources* on page 41
  Connect Enterprise Authentication to the data sources where your user data is stored.
- *Configure the custom flow settings* on page 42
  Configure a custom authentication flow that meets the specific needs of your network.
- *Import authentication flows* on page 43
  To create custom authentication flows, import existing flows and edit the actions and conditions.

Upload certificates

To enable certificate-based authentication, upload certificate files to Enterprise Authentication.

Task

1 On the administration interface, click the **Certificates** tab.

2 One of these options:

Table 7-1 Certificate configuration options

Option	Task steps
Upload private key store	1 In the **Display name** field, enter the unique private key store name. 2 In the **Password** field, enter the private key store password. 3 In the **Certificate** field, browse and select the private key store file, then click **Open**.
Upload Trusted Certificate	1 In the **Display name** field, enter the unique trusted certificate name. 2 In the **Certificate** field, browse and select the private key store file, then click **Open**.
Paste Trusted Certificate Text	1 In the **Display name** field, enter the unique trusted certificate name. 2 In the **Certificate data** field, paste the certificate text.

3 Click **Create**.

Import tokens

To enable user token authentication, import tokens to Enterprise Authentication.

Task

1. On the administration interface, click the **Main** tab, then select **Import tokens**.
2. Next to the **File** field, click **Browse**, navigate to the token file, then click **Open**.
3. Upload optional protected key files.
   a. Next to the **Key file** field, click **Browse**.
   b. Navigate to the key file, then click **Open**.
4. Click **Upload**.

Configure listeners

Configure the options that control how Enterprise Authentication handles incoming authentication requests.

Tasks

- *Configure RADIUS listeners* on page 39
  To enable Enterprise Authentication to accept RADIUS authentication requests, configure RADIUS listeners.
- *Configure HTTP listeners* on page 40
  To enable Enterprise Authentication to accept HTTP authentication requests, configure HTTP listeners.

Configure RADIUS listeners

To enable Enterprise Authentication to accept RADIUS authentication requests, configure RADIUS listeners.

Task

1. On the administration interface, click the **Listeners** tab.
2. Create the RADIUS listener.
   a. Click **Add listener**.
   b. From the **Implementation** drop-down list, select **RadiusListener**.
   c. In the **Name** field, enter a unique name, then click **Continue**.
3. In the **Listen port** field, use the arrows to select the UDP port.
4. In the **Shared secret** field, enter the shared secret used by the RADIUS device and Enterprise Authentication.
5. Verify that the **Enabled** checkbox is selected.
6. Click **Configure Tenant Mapping**, then select and configure one of these options:

Table 7-2 Tenant mapping configuration options

Option	Task steps
Bind listener to tenant	1 From the **Tenant** drop-down list, select the tenant. 2 Click **OK**.
Bind IP to tenant	1 In the **IP** field, enter the IP address. 2 From the **Tenant** drop-down list, select the tenant. 3 Click **Add**. 4 Click **OK**.

7 To bind the port, select and configure one of these options:

Table 7-3 Port binding configuration options

Option	Task steps
Bind all server IP addresses.	Select the **Bind to all IP addresses** checkbox.
Apply one server and IP address to bind the port.	1 From the **Bind node** drop-down list, select the server. 2 From the **to IP address** drop-down list, select the IP address.

8 In the **Timeout** field, use the arrows to select the allowed listener timeout in seconds, then click **Save and close**.

Configure HTTP listeners

To enable Enterprise Authentication to accept HTTP authentication requests, configure HTTP listeners.

Task

1 On the administration interface, click the **Listeners** tab.

2 Create the HTTP listener.

a Click **Add listener**.

b From the **Implementation** drop-down list, select **HTTPListenerImpl**.

c In the **Name** field, enter a unique name, then click **Continue**.

3 Configure the HTTP listener options.

a In the **URI** field, enter the web resource name.

b In the **Port** field, use the arrows to select the listener port.

c Verify that the **Enabled** checkbox is selected.

d From the **SSL server certificate** drop-down list, select the certificate key pair.

e To enable the client certificate and SSL encryption protocol on the port, select the **SSL client auth** checkbox.

f To upload certificates, select and configure one of these options:

- **Upload trusted certificate**
- **Add from store**

4 Click **Save and close**.

Connect Enterprise Authentication to data sources

Connect Enterprise Authentication to the data sources where your user data is stored.

Tasks

- *Add a connection to the SQL Server database* on page 41
  To add a connection to your SQL Server database, set up the JDBC driver.
- *Add a connection to the LDAP directory* on page 41
  If users and groups are stored in your corporate directory, connect Enterprise Authentication to the LDAP directory server.
- *Add a connection to the Active Directory* on page 42
  When users and groups are stored in the corporate Active Directory, connect Enterprise Authentication to the Active Directory server.

Add a connection to the SQL Server database

To add a connection to your SQL Server database, set up the JDBC driver.

Task

1. On the administration interface, click the **Datasources** tab.
2. Click **Add SQL Connection**.
3. On the **JDBC Settings** window, configure the JDBC driver options.
   a. In the **Display name** field, enter the unique connection name.
   b. From the **Driver** drop-down list, select one of these options:
      - **Microsoft SQL**
      - **MySQL**
      - **PostgreSQL**
   c. In the **Server IP** field, enter the SQL Server database server IP address.
   d. In the **Port** field, enter the SQL Server database port.
   e. In the **Username** field, enter the SQL Server database user name.
   f. In the **Password** field, enter the SQL Server password.
4. Click **Verify connection**.
5. If verification is successful, click **Create**.

Add a connection to the LDAP directory

If users and groups are stored in your corporate directory, connect Enterprise Authentication to the LDAP directory server.

Task

1. On the administration interface, click the **Datasources** tab.
2. Click **Add LDAP Connection**.
3. On the **LDAP Settings** window, configure the LDAP directory server options.
   a. In the **Display name** field, enter the unique connection name.
   b. In the **LDAP Server IP** field, enter the LDAP directory server IP address.

   c. If the LDAP directory server uses an SSL connection, select the **SSL enabled** checkbox.
   d. In the **Port** field, enter the LDAP directory server port.
   e. In the **Administrator DN** field, enter the administrator distinguished name.
   f. In the **Administrator password** field, enter the administrator password.
4. Click **Verify connection**.
5. If verification is successful, click **Create**.

Add a connection to the Active Directory

When users and groups are stored in the corporate Active Directory, connect Enterprise Authentication to the Active Directory server.

Task

1. On the administration interface, click the **Datasources** tab.
2. Click **Add Active Directory Connection**.
3. On the **Active Directory Settings** window, configure the Active Directory server options.
   a. In the **Display name** field, enter the unique connection name.
   b. In the **LDAP Server IP** field, enter the directory server IP address.
   c. If the directory server uses an SSL connection, select the **SSL enabled** checkbox.
   d. In the **Port** field, enter the directory server port.
   e. In the **Administrator DN** field, enter the administrator distinguished name.
   f. In the **Administrator password** field, enter the administrator password.
4. Click **Verify connection**.
5. If verification is successful, click **Create**.

Configure the custom flow settings

Configure a custom authentication flow that meets the specific needs of your network.

Task

1. On the administration interface, click the **Authentication Flows** tab, then select **New Flow**.
2. On the **New flow** window, enter a unique name in the **Display name** field.
3. From the **Listener** drop-down list, select the authentication flow listener.
4. Use the arrows to select the number of allowed failed actions.
5. To add child entities, select and follow the on-screen prompts for these options:
   - **Add a federation meta data handler**
   - **Add a SAML entity**

6 Add conditions.

   a Click **Add**.

   b In the **Attribute** field, enter the attribute on which you want to build the condition.

   c Select one of these operators:

   - **must**
   - **can not**

   d Choose from one of these options:

   - Select **exist**.
   - In the **contain** field, enter the value.
   - In the **match** field, enter the value.

   e Click **Add**.

   f Check and resolve any possible condition conflicts.

7 Click **Create**.

Import authentication flows

To create custom authentication flows, import existing flows and edit the actions and conditions.

Task

1 Click the **Flows** tab, then select **New flow** | **Import**.

2 Click **Select file**, select the authentication flow file, then click **Open** | **Upload**.

3 To configure the conditions, select the imported flow, and click **Edit**.

Table 7-4 Configurable conditions options

Task	Steps
Add conditions to the flow.	1 In the **Attribute** field, enter the attribute name. 2 Configure the remaining settings. 3 Click **Add**.
Remove conditions from the flow.	Next to the condition, click **Delete**.

4 Click **Save and close**.

5 To configure the actions, select the imported flow.

Table 7-5 Configurable action options

Task	Steps
Add actions to the flow.	1 Click **Action catalog**. 2 Click and drag individual actions to the flow **Action** list. 3 In the **Order** column, use the arrows to reorder the actions.
Temporarily disable actions.	1 Next to the action, click **+**. 2 Click **Disable**.

Table 7-5 Configurable action options *(continued)*

Task	Steps
Add listeners to the action.	1 Next to the action, click **+**. 2 Click **Add listener response handler**. 3 Configure the available options, then click **Add**.
Remove actions from the flow.	1 Next to the action, click **+**. 2 Click **Remove**.

8 Assigning administrator permissions

Assign administrator permission sets to network users.

Contents

Assign system administrator permissions

Assign additional system administrator role permissions to network users.

Task

1. On the administration interface, click the **Tenants** tab.
2. Next to the default_tenant account, click **Edit**.
3. On the **default_tenant** window, click **Administrators**, then click **Add User**.
4. On the **Create** window, configure the system administrator settings.
   - a. In the **User ID** field, enter the system administrator user name.
   - b. In the **Password** field, enter the system administrator password.
   - c. Click **Create**.

Configure default tenant account settings

Configure the settings for the Enterprise Authentication default tenant account.

Tasks

- *Configure Pledge Profile Service settings* on page 46

  To enable users to use their Pledge software token, configure the Pledge Profile Service settings.
- *Configure Message Gateway settings* on page 46

  To enable users to send one-time passwords by SMS, configure the McAfee Message Gateway settings.
- *Configure user management settings* on page 46

  Configure the network data source where user information is stored.
- *Configure SMTP settings* on page 47

  To enable users to send one-time passwords by email, configure the SMTP settings.

Configure Pledge Profile Service settings

To enable users to use their Pledge software token, configure the Pledge Profile Service settings.

Task

1. Click the **Tenants** tab, then click **Edit** next to the default tenant account.
2. Select **Pledge Profile Service**.
3. Configure the available settings, then click **Test Pledge Profile Service settings**.
4. If the settings are correct, click **Save**.

Configure Message Gateway settings

To enable users to send one-time passwords by SMS, configure the McAfee Message Gateway settings.

Task

1. Click the **Tenants** tab, then click **Edit** next to the default tenant account.
2. Select **McAfee Message Gateway**.
3. Choose from these configuration options:

Table 8-1 McAfee Message Gateway configuration options

Option	Task steps
Configure an existing McAfee Message Gateway account.	1 In the **Username** field, enter the McAfee Message Gateway account user name. 2 In the **Password** field, enter the McAfee Message Gateway account password.
Create a McAfee Message Gateway account.	1 Click **Request Message Gateway account**. 2 On the **Account created** dialog box, click **OK**.

4. Click **Test Message Gateway settings**.
5. If the settings are correct, click **Save**.

Configure user management settings

Configure the network data source where user information is stored.

Task

1. Click the **Tenants** tab, then click **Edit** next to the default tenant account.
2. Select **User Management**.
3. Select one of these options and configure the available settings:
   - **New LDAP Connection**
   - **New AD Connection**

   Enterprise Authentication uses these connections to connect with your network data stores. The user credentials stored in these data stores are also used as the authentication credentials to log on to the Web Manager interface.
4. Click **Save**.

See also

Add a connection to the LDAP directory on page 41
Add a connection to the Active Directory on page 42

Configure SMTP settings

To enable users to send one-time passwords by email, configure the SMTP settings.

Task

1 Click the **Tenants** tab, then click **Edit** next to the default tenant account.

2 Select **SMTP**.

3 Configure these settings:

Table 8-2 SMTP configuration settings

Setting	Definition
From Address	Specifies the email address from where email messages are sent.
SMTP host	Specifies the host name or IP address of the SMTP server that sends the email messages.
SMTP port	Specifies the port number of the SMTP server that sends the email messages.
SMTP auth	Enables SMTP authentication.
SMTP TLS	Enables the TLS protocol.

4 Click **Save**.

Assign tenant administrator permissions

Assign tenant administrator permissions to the default tenant account.

Task

1 Click the **Tenants** tab, then click **Edit** next to the default tenant account.

2 Select **Administrators**, then click **Add User**.

3 In the **User ID** field, enter the tenant administrator user name.

4 In the **Password** field, enter the tenant administrator password.

5 Click **Create | Save and Close**.

9 Assisting users with Web Manager

To assist users with their authentication settings, user administrators use the Web Manager interface.

Contents

Log on to the Web Manager

To access the Enterprise Authentication user settings, log on to the Web Manager.

Task

1. On your browser, go to https://<Enterprise Authentication_server_name>:<port number>/webmanager
2. Enter your log on credentials.
   a. In the **User ID** field, enter your user name stored in the network identity store.
   b. In the **Password** field, enter your password stored in the network identity store.
3. From the **Language** drop-down list, select your preferred language, then click **Login**.

Search for users and tokens

Search for users and tokens stored in the configured network data source.

Task

1. Click the **Search** tab.
2. Configure these options: then click **Search**.
   - To search for users, enter the user information in the **Search user** fields.
   - To search for tokens, enter the token information in the **Find tokens** fields.
3. Click **Search**.

Update user telephone numbers

To ensure that one-time passwords are delivered to the correct devices, keep the user telephone number current.

Task

1. Double-click the user name.
2. Click the **General** tab.
3. In the **Mobile** field, delete the old telephone number, then enter the new.
4. Click **Save**.

Reset user lockout

If users attempt to log on multiple times using an incorrect password, Web Manager locks out the user.

Task

1. Double-click the user name.
2. Click the **General** tab.
3. Click **Reset user lockout**.

Assign and manage tokens

For multi-factor authentication with one-time passwords, assign and manage user tokens.

Contents

Assign hardware tokens

To enable users to authentication with one-time passwords, assign hardware tokens.

Task

1. Double-click the user account.
2. Click the **Manage tokens** tab, then select **Hardware OTP**.
3. From the **Token ID** list, select the token, then click **Close**.
4. Click **Save**.

Enable the Pledge Profile Service

To enable users to use Pledge, configure the Pledge Profile Service settings.

Task

1. Double-click the user account.
2. Click the **Manage tokens** tab, then select **Enroll pledge profile**.
3. Configure the available settings.
4. Click **Save**.

Assign temporary one-time passwords

Assign users temporary one-time passwords if they forget or lost their hardware token device.

Task

1. Double-click the user account.
2. Click the **Manage tokens** tab, then select **Temporary OTP**.
3. Use the arrows to select the allowed number of generated one-time passwords.
4. Use the calendar to select the one-time password expiration date.
5. Select one of these one-time password delivery options:
   - **Mobile**
   - **Mail**
   - **Manual**
6. Click **Save**.

Manage tokens

To assist users with tokens, use the Web Manager interface.

Task

1. Double-click the user account.
2. Click the **Manage tokens** tab, then select the token.
3. Select from these options:

   Table 9-1 Token management options

Option	Definition
Delete	Removes the assigned token from the user.
Edit description	Specifies the token information.
Disable/Enable	Temporarily disables or enables the assigned token.
Synchronize	To troubleshoot unsynchronized tokens, enter the following information. • **First OTP** — Specifies the first user generated one-time password. • **Second OTP** — Specifies the second user generated one-time password.
Verify OTP	Verifies enabled OATH-tokens or PIN settings.

4. Click **Save**.

Generate user PINs

When enabled, generate PINs that are used for authentication.

Task

1. Double-click the user account.
2. Click the **PIN Code** tab.
3. Click **Generate**.

10 Maintenance

Maintain the Enterprise Authentication software.

Contents

Uninstall the software

To remove the Enterprise Authentication features, uninstall the software from your computer.

Task

1. From the **Start** menu, select **Control Panel** | **Programs and Features**.
2. Select **McAfee Enterprise Authentication**, then click **Uninstall/Change**.

   The **Uninstall McAfee Enterprise Authentication** window appears.
3. Select a method to uninstall the software features, then click **Next**.
4. Click **Uninstall**.

   The Enterprise Authentication software is uninstalled from your computer.
5. Click **Done**.

Uninstall cluster installations

Uninstall the Enterprise Authentication software from your Windows-based cluster environment.

Task

1. Stop all Enterprise Authentication services and open the **Windows Cluster Administrator/Management** tool.
2. From the **Start** menu, select **Programs** | **Administrative Tools** | **Failover Cluster Management**.
3. In the Enterprise Authentication application group, right-click each of the Enterprise Authentication configurations and select **Delete**.
4. On each server, select **Programs and Features** | **McAfee Enterprise Authentication** | **Uninstall/Change**.

Index