2FA

configuration guide

ManageEngine
ADAudit Plus

Table of contents

1. Overview

Two-factor authentication (2FA) adds an extra layer of security to your account along with your username and password. When 2FA is enabled, ADAudit Plus will request that you authenticate twice during login.

ADAudit Plus supports the following six authentication modes for 2FA:

- Email Verification
- SMS Verification
- Google Authenticator
- RSA SecurID
- Duo Security
- RADIUS Authentication

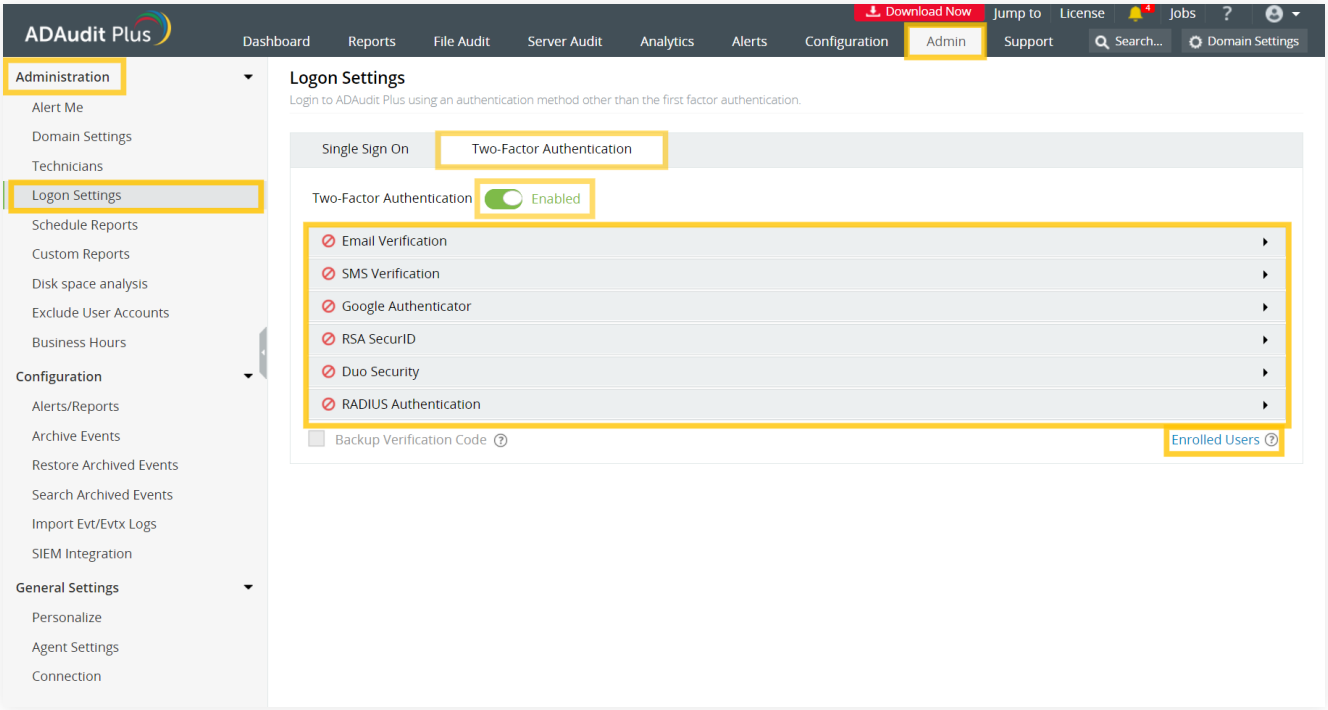
This guide will take you through the steps involved in enabling 2FA and setting up the authentication modes in ADAudit Plus.

2. Enable 2FA in ADAudit Plus

2.1 Steps to enable 2FA in ADAudit Plus

1. Open the **ADAudit Plus web console.**
2. Navigate to **Admin > Administration > Logon Settings.**
3. Select **Two-Factor Authentication**, and toggle to enable 2FA.
4. Configure one or more of the following six authentication modes for 2FA.

- Email Verification
- SMS Verification
- Google Authenticator
- RSA SecurID
- Duo Security
- RADIUS Authentication



Note:

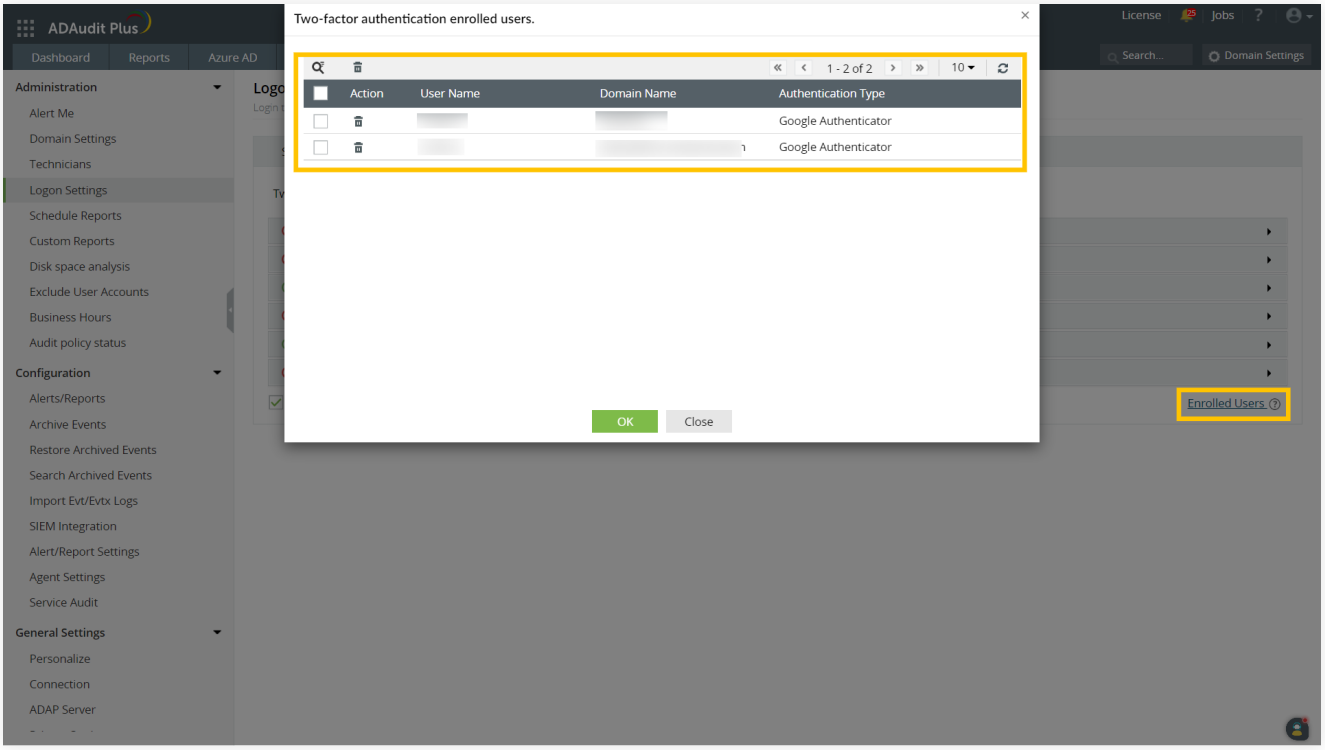
- When 2FA is enabled, technicians will have to authenticate twice before accessing ADAudit Plus. Only the default admin user has the option to **skip** the 2FA process during login. 2FA cannot be mandated for the default admin account.

- When multiple authentication modes are configured for 2FA, ADAudit Plus will request you to select a preferred authentication method.

2.2 Manage 2FA for users

As an admin, you can view and manage the authentication modes selected by users.

1. Under the **Two-Factor Authentication** tab, click **Enrolled Users.**
2. In the pop-up that appears, you can view the list of users enrolled in 2FA as well as the authentication mode each has chosen.
3. To remove a user, select them and click the **delete icon.**



2.3 Backup verification codes

Backup verification codes allow users to bypass the second factor of authentication when they don't have access to their phone or face issues with any of the authentication modes. When enabled, a total of five codes will be generated for the users to store safely. Once a code is used, it will become obsolete and cannot be used again. The users also have the option to generate new codes.

Enable backup verification codes

As an admin, you can enable backup verification codes to allow users to access and manage their backup verification codes in ADAudit Plus.

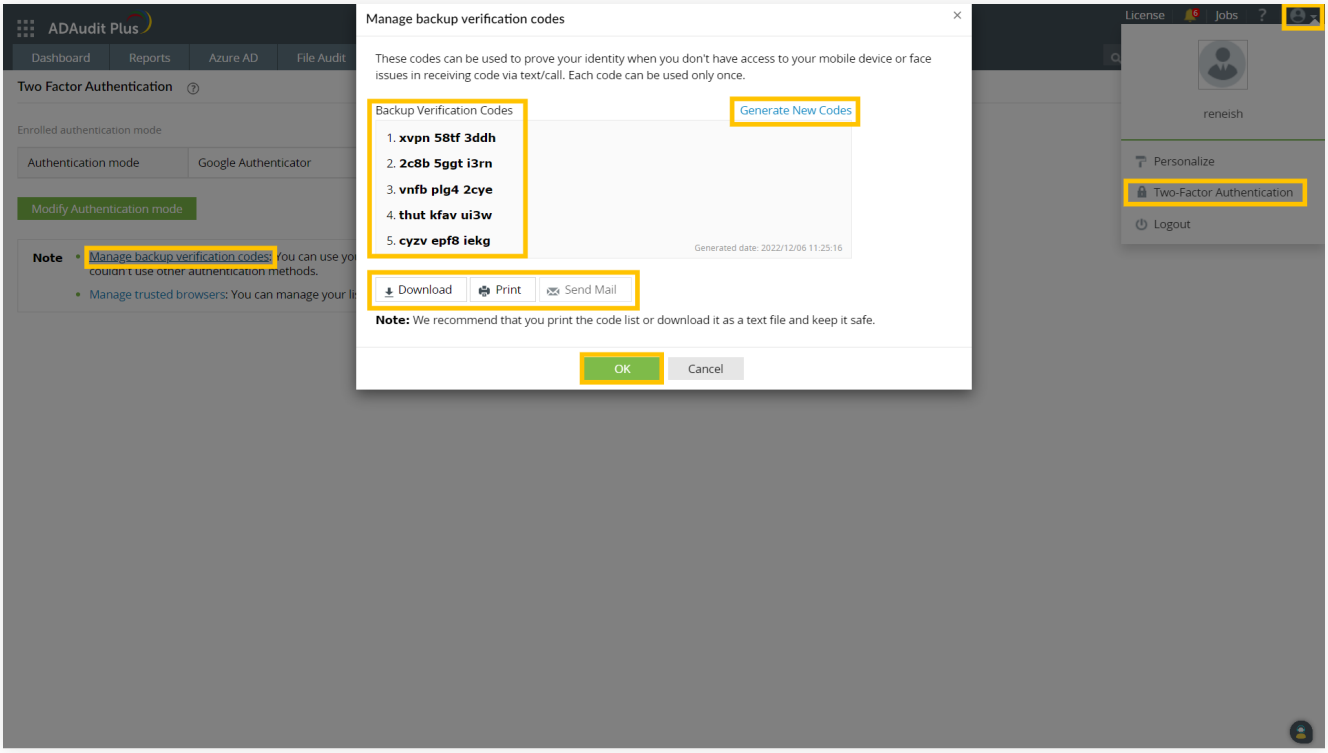
1. Log in to the **ADAudit Plus web** console using admin credentials.
2. Navigate to **Admin > Administration > Logon Settings.**
3. Under the **Two-Factor Authentication** tab, select the **Backup Verification Code** check box.

Manage backup verification codes

When backup verification codes are enabled, users can access and manage their backup verification codes by following the steps below.

Prerequisite: To generate backup verification codes, at least one of the authentication modes must have been successfully configured when logging in to ADAudit Plus.

1. Click the drop-down next to your profile picture in the top-right corner and select **Two-Factor Authentication.**
2. Click **Manage backup verification codes.** This will open the *Manage backup verification codes* pop-up, which will list the backup verification codes.
3. To generate new codes, click **Generate New Codes.**
4. Users can download, print, or email the codes and store them in a secure location.
5. Click **OK.**



Using backup verification codes during login

When users do not have access to their phone or face issues with any of the authentication modes, they can use a backup verification code to log in to ADAudit Plus.

1. To use a backup verification code during login, select one of the authentication modes and click **Next.**
2. Click the **Use backup verification codes** link. This will open the *Backup Verification Code* page.
3. Enter one of your backup verification codes and click **Verify Code** to log in to ADAudit Plus.

2.4 Manage trusted browsers

Users can manage their trusted browsers for 2FA by following the steps below:

1. Click the drop-down next to your profile picture in the top-right corner and select **Two-Factor Authentication.**
2. Click **Manage trusted browsers.**

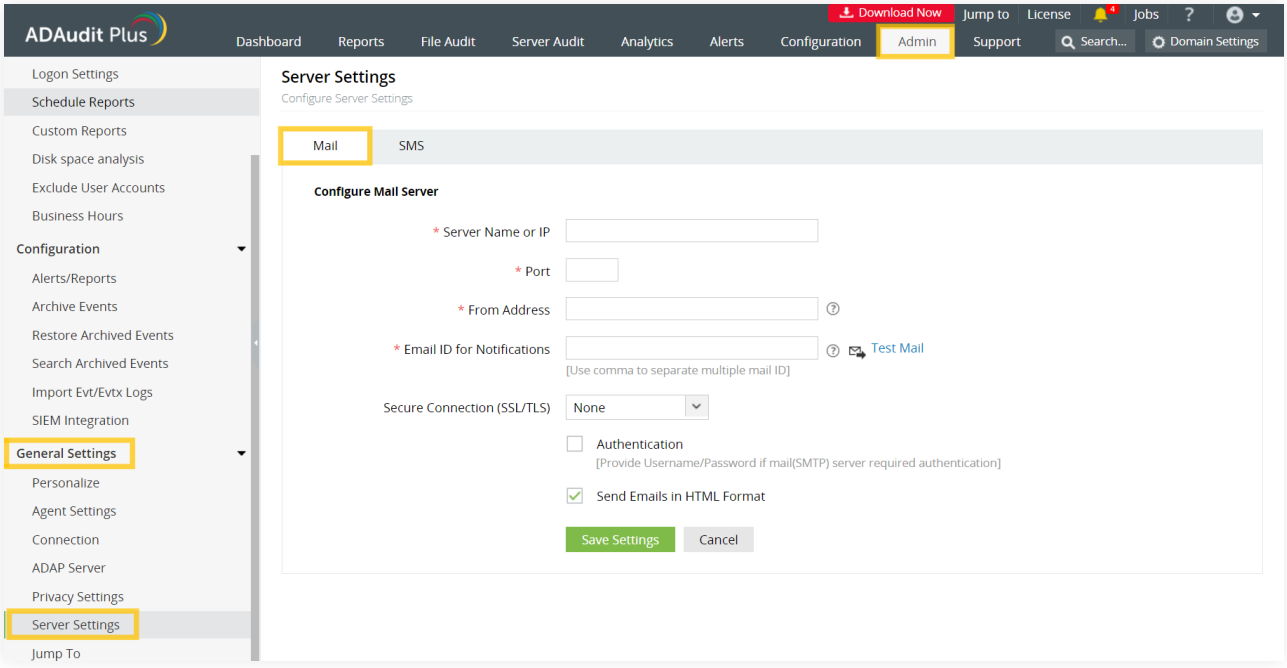
3. Authentication modes

3.1 Email Verification

If you're enabling Email Verification as a 2FA method, you have to configure the email server settings first, and follow up with the steps to enable Email Verification in ADAudit Plus.

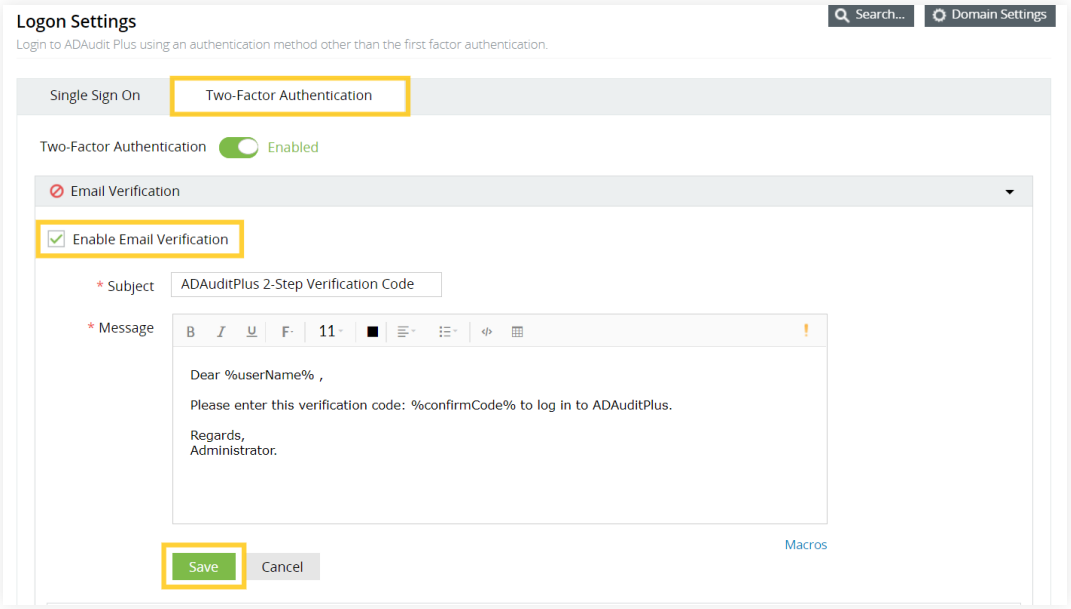
3.1.1 Steps to configure email server settings in ADAudit Plus

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > General Settings > Server Settings.**
3. Under **Mail**, specify the **Server name, Port, From Address**, and the **Email ID for Notifications.**
4. Check Authentication, and enter the Username and Password for mail server access.
5. Verify the email server settings by clicking the **Test Mail** link to ensure that the test email is received by the recipient email address specified in **Email ID for Notifications.**
6. Click **Save Settings.**



3.1.2 Steps to enable Email Verification in ADAudit Plus

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > Administration > Logon Settings**, and select **Two-Factor Authentication.**
3. Under **Email Verification**, check **Enable Email Verification.**
4. Enter the **Subject** of the email (e.g. ADAuditPlus 2-Step Verification Code).
5. Enter the content of the email in the **Message** box using macros.
6. Click **Save.**



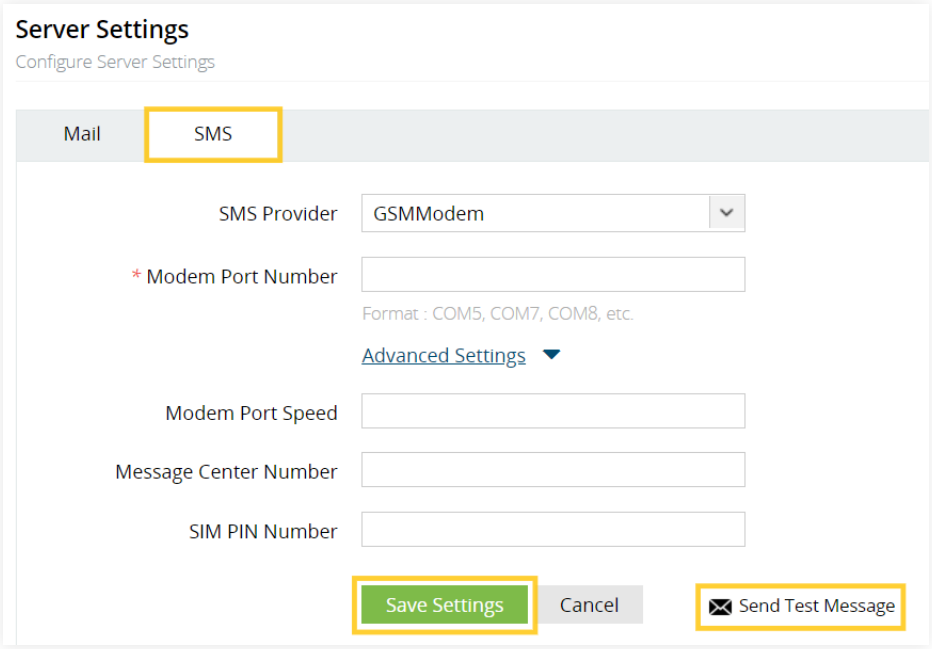
3.2 SMS Verification

If you're enabling SMS Verification as a 2FA method, you can configure ADAudit Plus to use a GSM Modem for sending SMS notifications, or you can configure your own custom SMS gateway.

3.2.1 Steps to configure ADAudit Plus to use a GSM Modem as an SMS provider

1. Connect the **GSM modem to the serial communication port** with a serial cable.
2. Open the **ADAaudit Plus web console.**
3. Navigate to **Admin > General Settings > Server Settings.**
4. UUnder **SMS**, select **GSMModem** from the **SMS Provider** drop-down.
5. Enter the port number the modem is connected to in **Modem Port Number.**
6. Click **Advanced Settings.**
7. Specify the **Modem Port Speed, Message Center Number,** and **SIM PIN Number.**

8. Click **Send Test Message**, and enter the recipient's **Mobile Number** and the **Message** to be sent.
9. Verify the SMS server settings by clicking **Send SMS**, and ensure that the test message is received by the recipient.
10. Click **Save Settings.**



Note:

- If the message exceeds 160 characters, then the notification will be split into two or more text messages.

- To find the modem port number, go to **My Computer > Manage > Device Manager > Modems > (select your modem) > Properties > Modem.**

3.2.2 Steps to configure ADAudit Plus to use a custom SMS gateway

a. To use an HTTP-based custom SMS gateway:

Follow these steps to use an HTTP-based custom SMS gateway in ADAudit Plus:

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > General Settings > Server Settings.**
3. Under **SMS**, select **Custom** from the **SMS Provider** drop-down.
4. Select **HTTP** from the **Send SMS** via drop-down.
5. Select either of the available HTTP Methods, **Post** or **Get.**
6. Enter the HTTP URL of your SMS gateway provider.

7. Specify the **HTTP Parameters** specific to your SMS provider, the user's **mobile number**, and the **message** to be sent.
8. Select the **Success** or **Failure** response from the **Select Response Type** drop-down.
9. Specify the **Success and Failure Response** from the provider.
10. Click **Advanced Settings.**
11. Enter the **HTTP Request Headers** specific to your SMS provider.
12. If the SMS provider expects unicoded messages, check **Convert Message into Unicode.**
13. Click **Send Test Message**, and enter the recipient's **Mobile Number** and the **Message** to be sent.
14. Verify the SMS server settings by clicking **Send SMS**, and ensure that the test message is received by the recipient.
15. Click **Save Settings.**

Note:

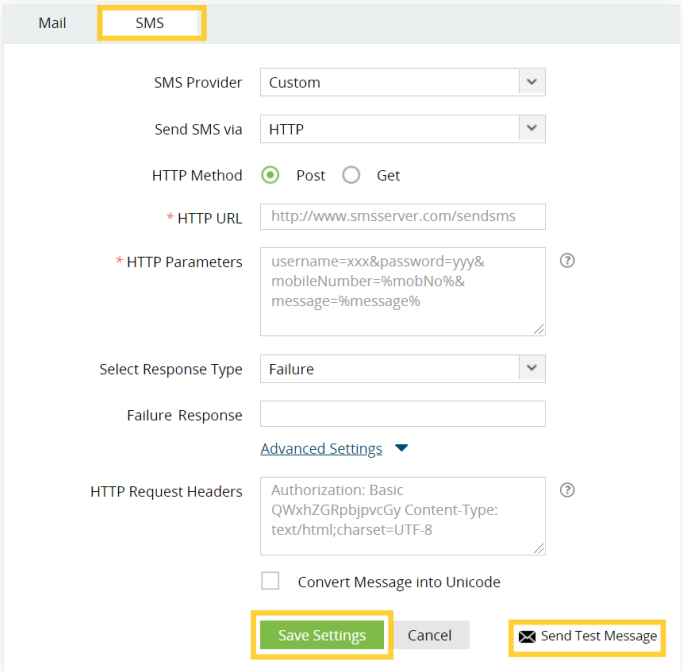
- Separate the HTTP parameters with an ampersand (&) sign.

  Example:

  userName=xxx&password=yyy&mobileNumber=%mobNo%&message=%message%.

  1. xxx: API authentication username.
  2. yyy: API authentication password.
  3. %mobNo%: This macro denotes the user's mobile number.
  4. %message%: This macro denotes the SMS message content.

- More HTTP parameters: If your SMS provider requires more parameters like unicode and apiID, include them as well using the "&" sign.

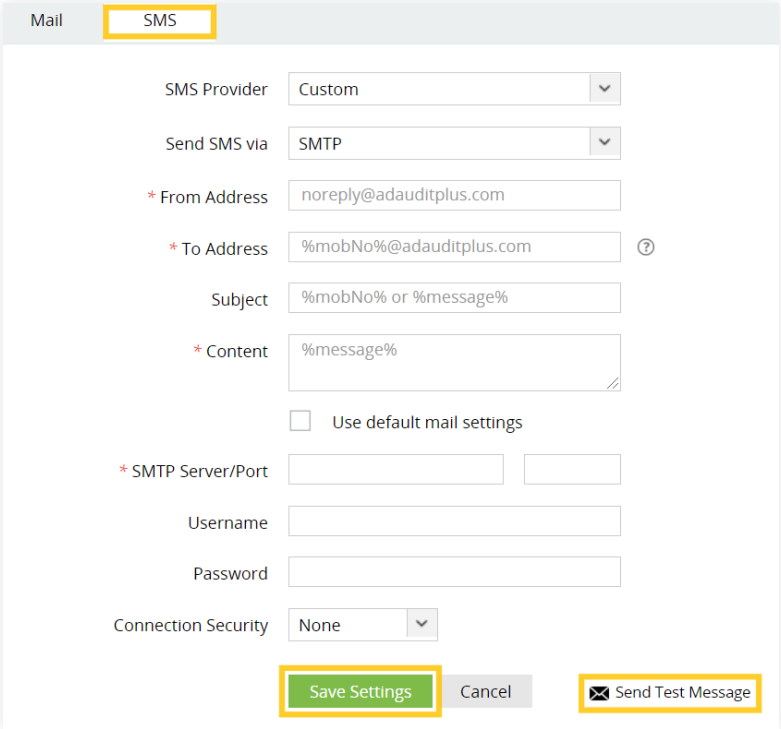


b. To use an SMTP-based custom SMS gateway:

Follow these steps to use an SMTP-based custom SMS gateway in ADAudit Plus:

1. Open the **ADAudit Plus web console.**
2. Navigate to **Admin > General Settings > Server Settings.**
3. Under **SMS**, select **Custom** from the **SMS Provider** drop-down.
4. Select **SMTP** from the **Send SMS** via drop-down.
5. Enter the email address the SMS will be sent from in the **From Address field.**
6. Specify the mobile number macro (%mobNo%), followed by the email address of the SMS provider in the **To Address field.**

   Example: %mobNo%@adauditplus.com.
7. Enter the required **Subject** using macros. Generally, it's either the mobile number (%mobNo%) or the message (%message%), depending on your SMS provider.
8. Specify the **Content** to be sent using macros (%message%).
9. Enter the name or the IP address of the **SMTP Server**, and the **SMTP Server port.**
10. Provide the **Username** and **Password** with required permissions on the SMTP server.
11. Select your connection security preference from the **Connection Security** drop-down.
12. Click **Save Settings.**



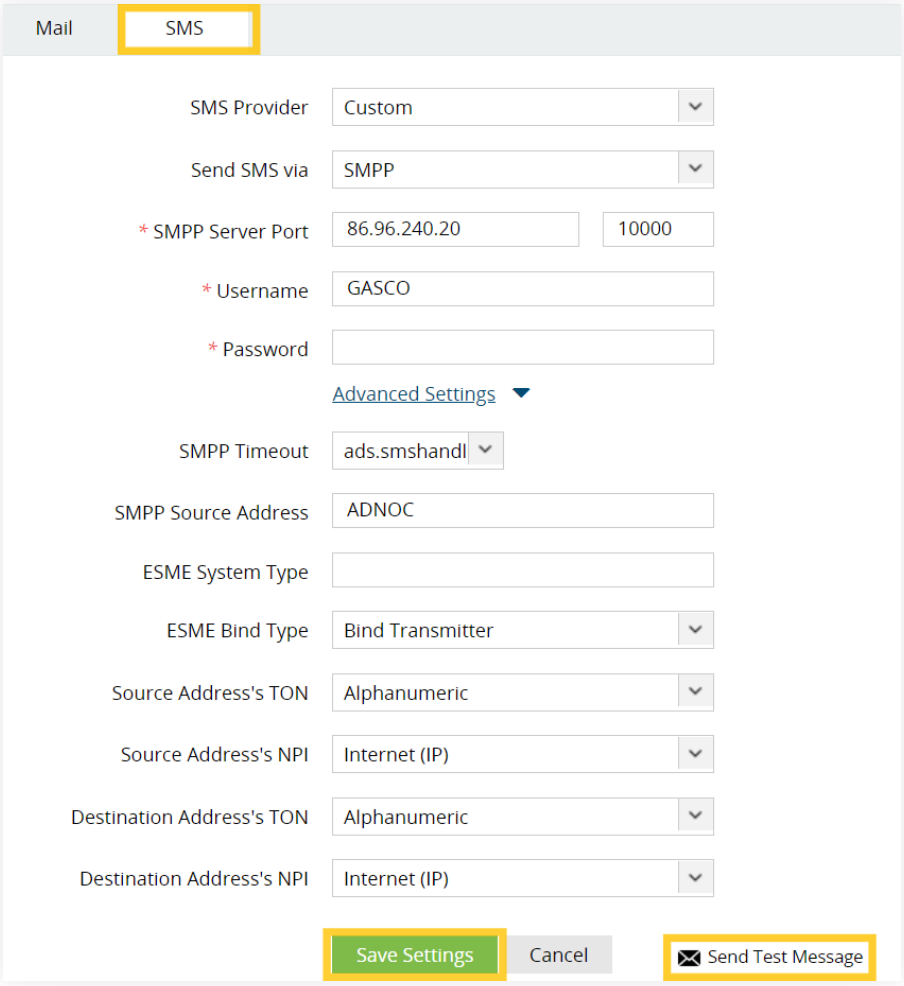
Note:

If the SMTP server is not configured, check **Use default mail settings** for the mail server configured under the **Mail** tab to be used.

c. To use an SMPP-based custom SMS gateway:

Follow these steps to use an SMPP-based custom SMS gateway in ADAudit Plus:

1. Open the **ADAudit Plus web console.**
2. Navigate to **Admin > General Settings > Server Settings.**
3. Under **SMS,** select **Custom** from the **SMS Provider** drop-down.
4. Select **SMPP** from the **Send SMS via** drop-down.
5. Enter the SMPP Server Port number.
6. Specify the **Username** and **Password** with required permissions on the SMPP server.
7. Click **Advanced Settings.**
8. Specify the **SMPP Time-Out** and **SMPP Source Address.**
9. Enter the **ESME System Type** and from the **ESME Bind Type** drop-down, and select **Bind Transmitter** or **Bind Transceiver.**
10. Select the **Source Address' TON, Source Address' NPI, Destination Address' TON,** and **Destination Address' NPI** from their respective drop-downs.
11. Click **Save Settings.**

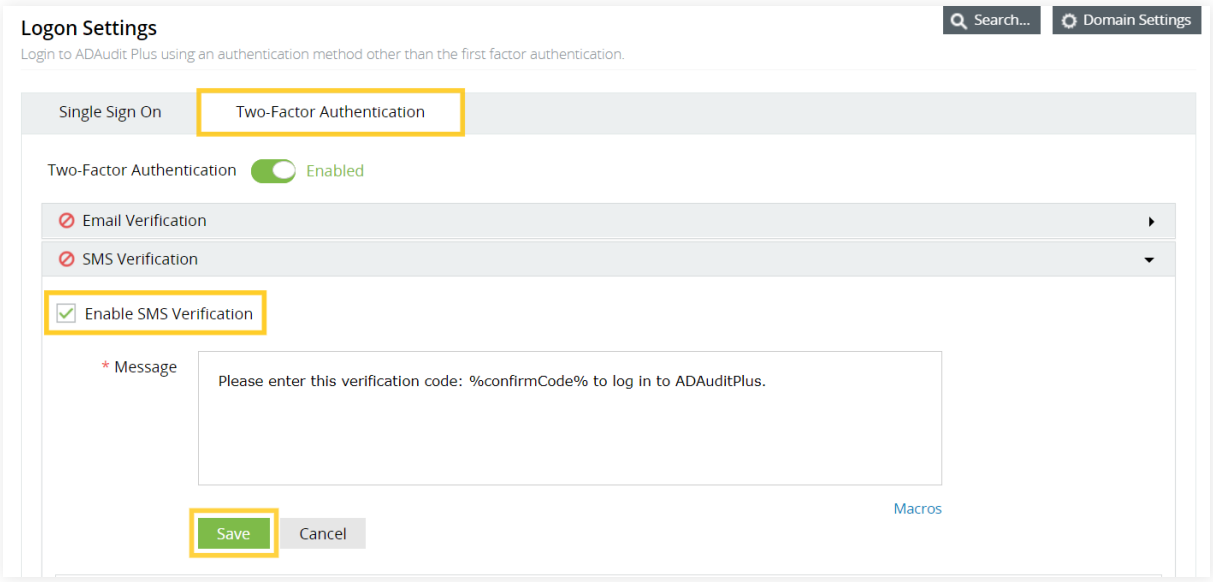


Note:

- TON: Type of number
- NPI: Numeric plan indicator

3.2.3 Steps to enable SMS Verification in ADAudit Plus

1. Log in to your **ADAaudit Plus' web console.**
2. Navigate to **Admin > Administration > Logon Settings, and select Two-Factor Authentication.**
3. Under **SMS Verification,** check **Enable SMS Verification.**
4. Enter your content in the **Message box** using macros.
5. Click **Save.**



3.3 Google Authenticator:

When Google Authenticator is enabled, users will be required to enter a code generated by the Google Authenticator app during the login process.

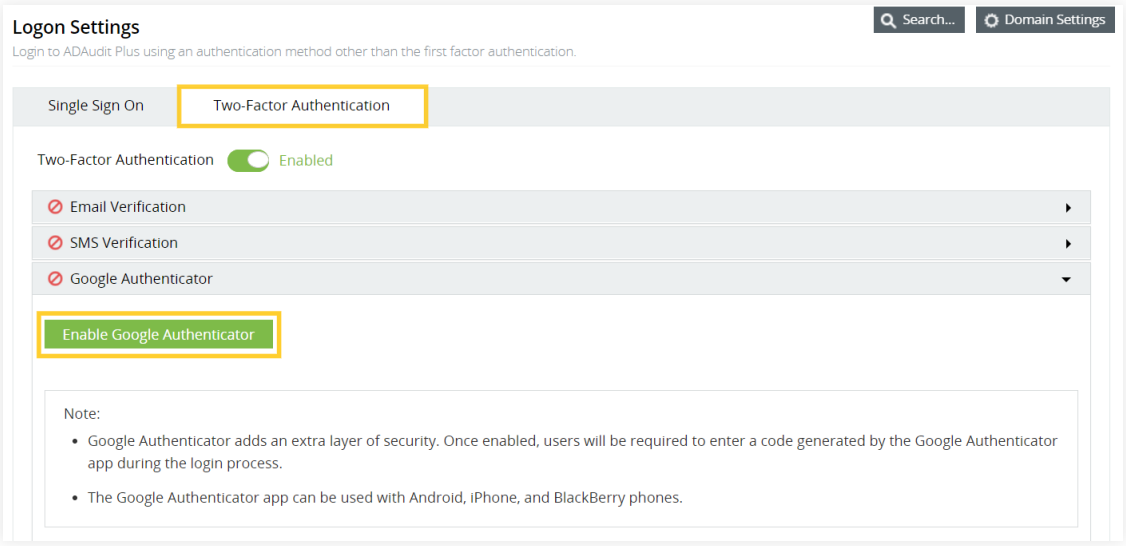
3.3.1 Steps to enable Google Authenticator in ADAudit Plus

Prerequisite:

Download and install Google Authenticator on your mobile device from Google's website.

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > Administration > Logon Settings,** and select **Two-Factor Authentication.**
3. Under **Google Authenticator**, click **Enable Google Authenticator.**

4. When logging in to the **ADAudit Plus web console** for the first time, a **QR code** will be displayed. Open the **Google Authenticator app** on your mobile device, and scan the QR code to create an account for ADAudit Plus.
5. When ADAudit Plus is added to the Google Authenticator app, a **secret code** will be generated automatically.
6. Enter the **secret code** generated by the Google Authenticator app, and click **Verify** to access ADAudit Plus.



Note:

› The Google Authenticator app can be used with Android, iPhone, and BlackBerry phones.

3.4 RSA SecurID

When RSA SecurID is enabled, users can use the RSA security console's security codes for identity verification while logging in to ADAudit Plus.

Note: When enabling RSA SecurID two-factor authentication in ADAudit Plus, contact RSA support or use your RSA login to get the RSA dependent libraries named authapi.jar and its compatible log4j jars, and paste them into the ADAudit Plus lib folder (<product_installation_path>/lib/).

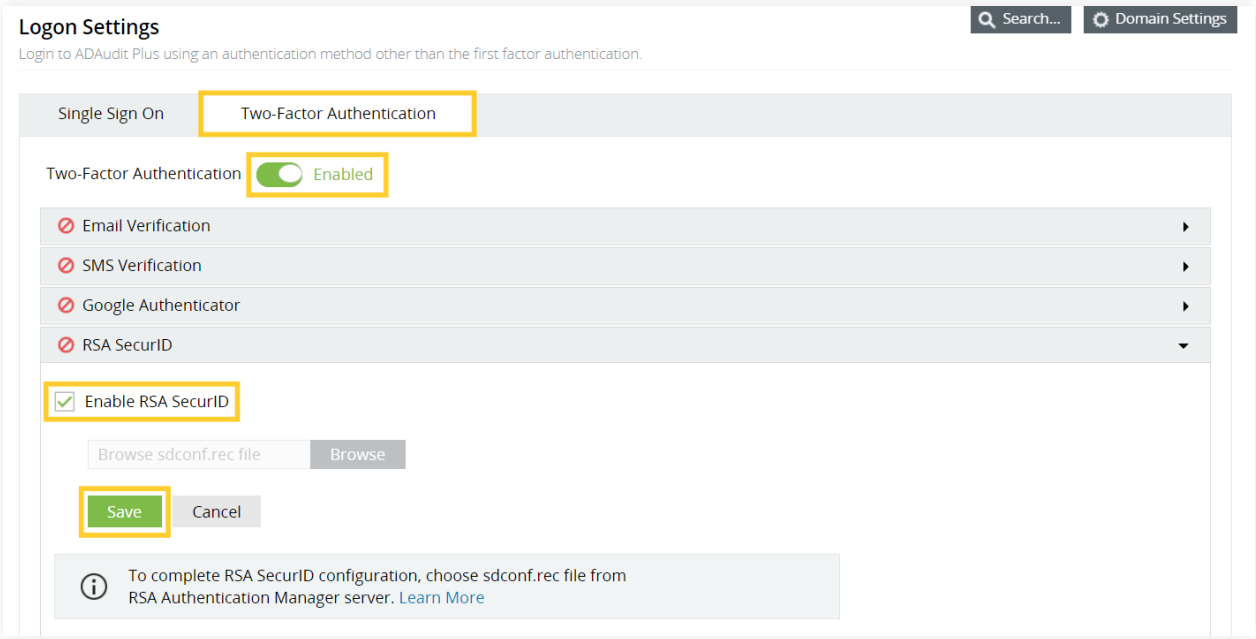
3.4.1 Steps to add the ADAudit Plus server in the RSA admin console

1. Log in to your **RSA admin console** (e.g., https://RSA machinename.domain DNS name/sc).
2. Go to the **Access** tab, select **Authentication agent** from the drop-down, and click **Add new.**
3. Create a **Client**, and set its type as **Standard Agent.**

4. Go to the **Home** tab, select **Manage Users**, and click **Add new.**
5. Create a user with a **last name** and a **user ID** similar to the SAM Account name in the domain.
6. After adding the user, click the **username**, and in the menu, select **Secure ID Token.**
7. Click **Assign Token**, select any one token, click **Assign**, and click **Save.**
8. Go to the **Authentication tab**, click **On Demand Authentication,** and select Enable Users.
9. Select the **User** from the list, and click **Enable for ODA.**
10. Select the associated pin and expiration date, and click **Save.**
11. Go to the **Access** tab, and select **Authentication agent** from the drop-down.
12. Click **Generate Configuration File,** select **Generate Config File**, and click **Download now.**
13. Extract the **AM_Config.zip** file to get the **sdconf.rec file.**

3.4.2 Steps to enable RSA SecurID in ADAudit Plus

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > Administration > Logon Settings,** and select **Two-Factor Authentication.**
3. Under **RSA SecurID**, check **Enable RSA SecurID.**
4. Browse and select the **sdconf.rec file** downloaded from the RSA Authentication Manager Server.
5. Click **Save.**

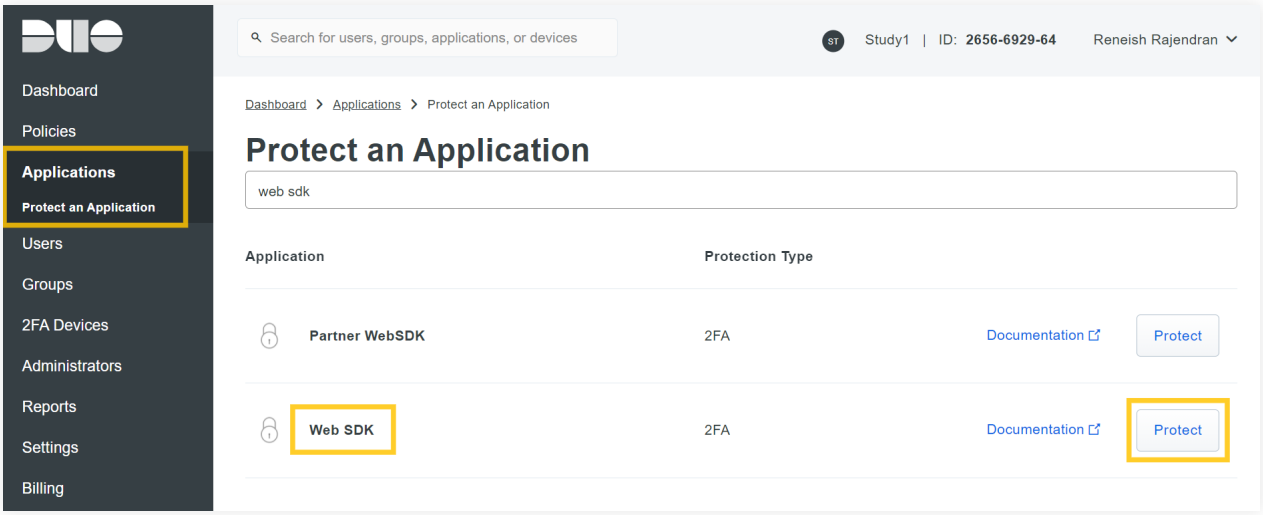


3.5 Duo Security

When Duo Security verification is enabled, users can use the six-digit security codes generated by the Duo Mobile app to prove their identity.

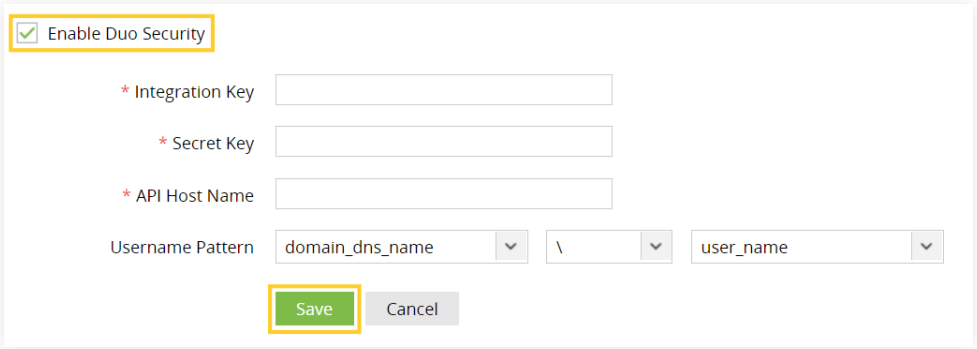
3.5.1 Steps to retrieve security details from Duo Security

1. Log in to your **Duo Security account.**
2. Navigate to the **Applications** section in the left pane, and click **Protect an Application.**
3. Search for **Web SDK**, and click **Protect.**
4. Copy the Integration Key, Secret Key, and **API Host Name.**



3.5.2 Steps to enable Duo Security in ADAudit Plus

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > Administration > Logon Settings, and select Two-Factor Authentication.**
3. Under **Duo Security**, check **Enable Duo Security.**
4. Enter the **Integration Key, Secret Key,** and **API Host Name** copied from Duo Security.
5. Choose the **Username Pattern**, and click **Save.**



Note:

If an enrolled user is deleted in Duo, it is essential to remove the user's enrollment in ADAudit Plus as well. Otherwise, the user will not be able to access ADAudit Plus without entering the Duo security code during login.

3.6 RADIUS Authentication

When RADIUS Authentication is enabled, end users can use their username and password from the RADIUS server to log in to ADAudit Plus.

3.6.1 Steps to integrate the ADAudit Plus server with RADIUS

1. Access your **RADIUS server** and find the **/etc/raddb/** folder.
2. Select the clients.conf file, and enter the ADAudit Plus server details.

   For example, if the name of the ADAudit Plus server is "ADAP" and its IP address is 172.21.193.194, add the following entry in the **clients.conf file:**

   client ADAP{

   ipaddr = 172.21.193.194

   secret = Radius@123

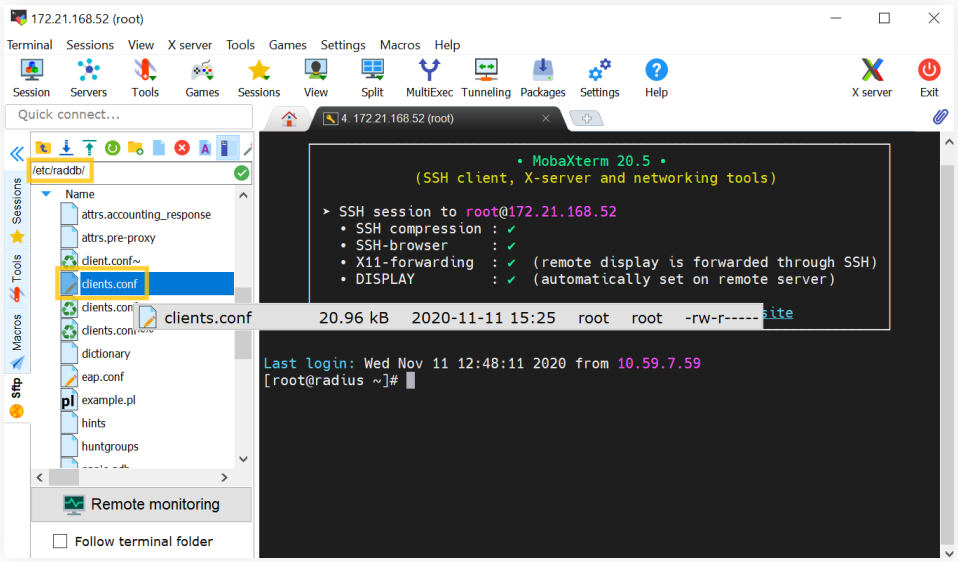
   require_message_authenticator = no

   nastype = other

   }

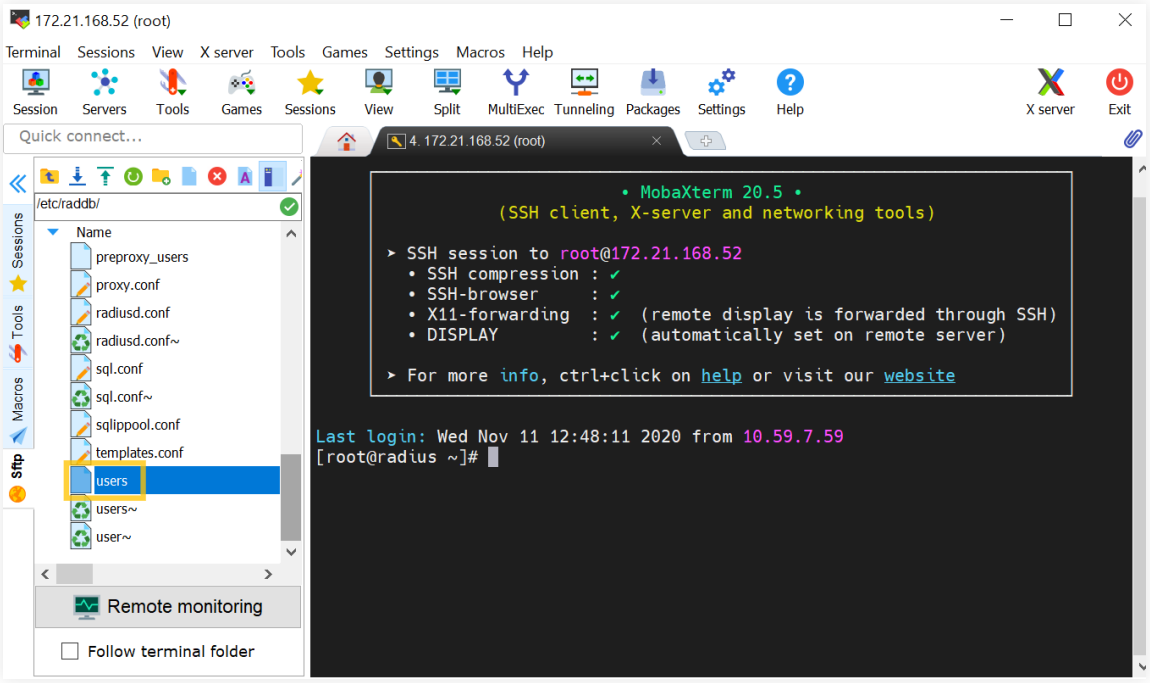
   Note:

   Here, "Radius@123" is the **Secret Key** that must be entered in the **ADAudit Plus web console** while configuring RADIUS.



3. Select **users**, and enter the user details.

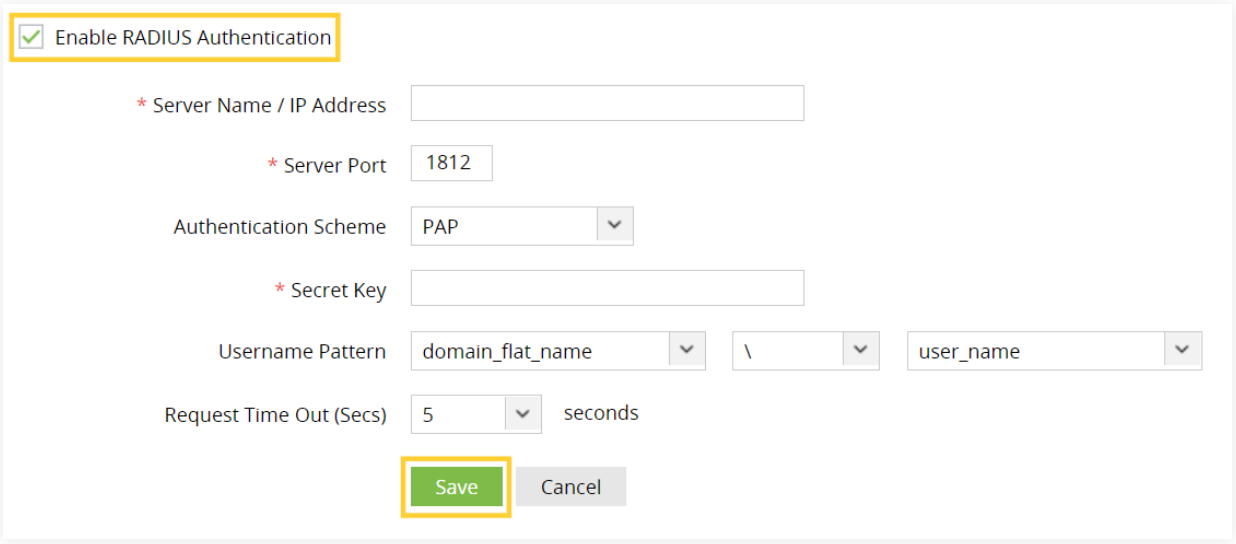
   Example format: **"domain_name\\user_name" Cleartext-Password := "Test@123"**



4. Restart the **Radiusd service** using shell script.

3.6.2 Steps to enable RADIUS Authentication in ADAudit Plus

1. Open the **ADAaudit Plus web console.**
2. Navigate to **Admin > Administration > Logon Settings,** and select **Two-Factor Authentication.**
3. Under **RADIUS Authentication**, check **Enable RADIUS Authentication.**
4. Enter the hostname or IP address of the host where the RADIUS server is running in the **Server Name / IP Address** field.
5. Enter the port used for RADIUS server authentication in the **Server Port** field (by default, RADIUS is assigned the UDP port 1812).
6. Select the **Authentication Scheme** used to authenticate users. Choose from four protocols: Password Authentication Protocol (PAP), Challenge-Handshake Protocol (CHAP), Microsoft Challenge-Handshake Protocol (MSCHAP), or Microsoft Challenge-Handshake Protocol Version 2 (MSCHAP2).
7. Enter the **Secret Key** that you specified while adding ADAudit Plus server as a client in your RADIUS server.
8. Choose the **Username Pattern,** and set the **Request Time Out** limit.
9. Click **Save.**

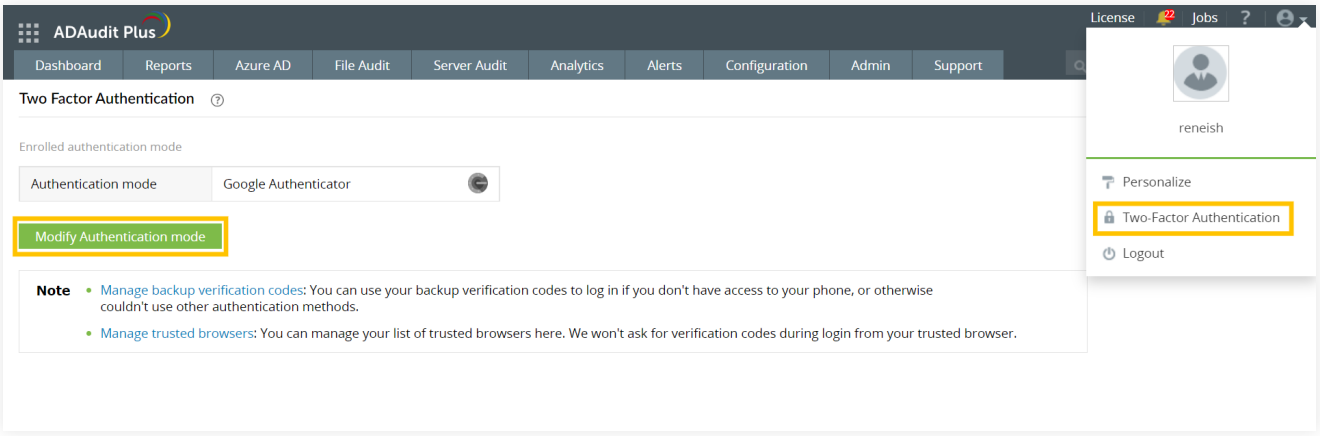


4. Set a preferred authentication mode

When multiple authentication modes are enabled, you will be asked to choose which authentication mode you want to use to prove your identity during login. You can also set a preferred authentication service that will serve as your default authentication mode for 2FA.

Steps to select a preferred authentication mode:

1. Click the drop-down next to your profile picture in the top-right corner.
2. Select **Two-Factor Authentication,** and click **Modify Authentication mode.**
3. Choose your preferred authentication mode, and click **Next.**
4. Complete the verification process for the authentication service you choose to set as your preferred authentication mode for 2FA.



Note:

- If you choose Google Authenticator as your preferred method, the next step will prompt you to scan a QR code and enter the code generated by the app in your smartphone, then click **Verify Code.**

5. Reset the second authentication factor for the default admin

If you have lost your authentication device or are unable to retrieve the verification code required to complete the authentication, you can reset the second authentication factor to access ADAudit Plus.

Note:

- The authentication factor can only be reset for the default administrator account.

To reset the authentication factor:

1. Navigate to the <product_installation_path>\bin folder.
2. Find and run the resetAdminTFAEnrollment.bat file.
3. You can now log in to ADAudit Plus and reenroll for the second authentication factor by repeating the steps to configure the authentication mode(s).