Data Security

MODULE 3

ZOHO CRM

Course for Administrators

Table of Contents

Overview

Managing the complexities of security administration is one of the growing concerns in any enterprise, even more so when it comes to organizations which deal with e-commerce and have large networks. In such demanding times, the availability of ecurity management is extremely crucial, as it can affect all sectors of an enterprise. Organizations which have a large customer base need to have complex security systems in place to keep their data from reaching the hands of unauthorized users.

To fulfill this requirement, Zoho CRM offers many important security measures to make sure that the accounts of customers stay safe and secure from possible hackers and intruders.

These measures are:

- Two-factor authentication
- SMS Text Message/Voice Call
- OneAuth
- Verification Codes
- Trusted Browsers
- Backup Phone Number
- Account Settings
- Allowed IP addresses
- Data Encryption

Lesson A:

Authentication (TFA and MFA)

Lesson Objectives

In this lesson, you will:

- Learn about Two-Factor Authentication.
- Know the benefits of Two-Factor Authentication.
- Find out the different modes of authentication.
- Learn how to enable and disable TFA.

Two-Factor Authentication

Two-factor authentication (TFA) is an additional identity-verification step that can keep your account and data secure from potential intruders. In addition to entering their login credentials, users will have to verify their identity by providing a biometric Face ID (on the iPhone X) or Touch ID, confirm their login via a notification on their personal mobile device, or submit a verification code received on the mobile device.

The ***Multi-Factor Authentication (MFA)*** app created by Zoho provides additional security. ***Zoho OneAuth***, an industry-standard verification application, gives you four different modes of verification to choose from. You can choose to authenticate your account either through:

- Face ID/ Touch ID
- Push Notification
- Scanning QR Code
- Time-based OTP

Benefits

- By offering you an extra layer of security, TFA rules out the probability of an attacker impersonating a user and gaining access to computers, accounts or other sensitive resources. Even if a hacker gets access to the password, he won't have the second element needed to authenticate the account.
- Mobile TFA lets you securely access corporate applications, data and documents from virtually any device or location, without putting the corporate network and sensitive information at risk.
- When it comes to online transactions, TFA gives another layer of security for the website, the transaction and the customer.

How it works

Whenever you try to sign in to your account, you enter your email address and password. Once two-factor authentication is configured, sign-in will require an additional verification step via Zoho OneAuth, Google Authenticator, or an SMS/phone call. Once verified, you will be granted access to your Zoho account. We recommend using OneAuth, as it both covers offline scenarios and helps you configure secondary devices in case your primary device is lost

To enable TFA for your account

1. Go to accounts.zoho.com and log in with your registerd email address and password.
2. Choose Two -Factor Authentication.
3. Select the **Authentication Mode** through which you would like to verify (SMS, Google Authenticator, or any other).
4. Follow the steps mentioned to set up, verify and confirm the addition of TFA for your account.

To disable TFA

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication from the menu.
3. Click **Disable**.

SMS Text Message/Voice Call

In this mode, you will receive a seven digit verification code or a voice call with the verification code for authentication.

To enable SMS Text Message/Voice Call

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. Select SMS text message/Voice call as your mode.

4. Enter the mobile number which you want to the verification code to be sent.
5. Choose whether you want to receive the code through SMS or voice call and click **Text Me**.
6. Enter the verification code that you received.
7. Seelct the **Trusted Browser** checkbox and click **Verify.**
8. Enter your account password for security confirmation and click **Turn On**.
9. Click Continue.
10. Store the backup verification codes using one of these options **(Save as text, Print codes or Send email)**
11. Add a backup phone number to which the verification code will be sent in case your primary device is inaccessible.
12. Click **Send code**.

Google Authenticator

Before you choose this mode, install the Google Authenticator mobile app on your phone.

To enable Google Authenticator

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. Select **Google Authenticator** as your mode.
   Before you choose this mode, install the "Google Authenticator" mobile app on your phone.
4. Scan the barcode image displayed on the Setup page to configure your account in Google Authenticator.
   If you have any issues with image loading, then you can use the 16-character "secret key" displayed on clicking the **Have a problem in loading the image?** message to configure your account in Google Authenticator.
5. Enter the verification code that is generated by Google Authenticator.
6. Select the **Trusted Browser** checkbox and click **Verify**.

7. Enter your account password for security confirmation and click **Turn on.** Google Authenticator will now be successfully configured for your account.

OneAuth

OneAuth is the Multi-Factor authentication app created by Zoho to add an extra layer of security to your Zoho account and protect it from password breaches. Accounts secured only by login credentials are at risk of being compromised. Anyone who knows or obtains your password can open up your account and take whatever information they want.

Multi-Factor Authentication (MFA) can help protect you from such vulnerabilities by requiring two identity checks. This means that in addition to login credentials, the user must provide further authentication such as a biometric Face ID (on an iPhone X) or a One-Time Password (OTP) shown on a mobile device.

OneAuth provides multiple authentication modes to protect your account so that you can choose the authentication mode that works best for you. With OneAuth, users can implement a robust multi-factor authentication process that’s simple to use and requires no additional hardware.

Key benefits

- **Stronger security:** Your Zoho account will be protected with an industry-standard authentication mechanism that makes it harder to hack.
- **Facilitates Single Sign on:** You can access 14+ Zoho apps on your mobile device through a single sign-on.

How it works

Once you've installed the OneAuth application on your phone, you can use your login credentials for access. Set up an MFA mode that you are comfortable with. From there, you'll be able to use the OneAuth app on your mobile device to securely log in to your Zoho account. OneAuth is available in both the iOS App Store and Google Play Store. You can choose form these MFA modes:

- Touch ID

- Push Notification
- Scan QR
- Time-Based OTP

Touch ID

To enable Touch ID

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. Choose the **Authentication Mode** as **Touch ID.**
   Before you choose this mode install "Zoho OneAuth - Multi Factor Authenticator" on your iOS/Android device.
   If you haven't installed it, you will get a prompt asking you to install it on your mobile device.
   (If you are using the app for the first time follow step 4 and 5, else skip to step 6)
4. Open the app on your device and Sign in with your Zoho account.
5. Tap **Switch to MFA** *(Multi Factor Authentication)* on the home page.
   This will take you to the Setup MFA window.
6. In the *Setup MFA* window, tap the **Touch ID** mode or click and drag it into the circle.
7. **Verify** with your fingerprint.
8. Tap **confirm.**
   A window pops up asking your Zoho Account password.
9. Enter the password.
   You will be logged out from your active sessions on the web once you enter the password.

To log in using Touch ID

1. Log-in to your Zoho CRM account.
   Zoho OneAuth app on your mobile asks for your fingerprint.

2. Place you finger for fingerprint verification.
   Access is granted once the fingerprint is verified.

Notes:

Uninstalling the OneAuth app will lock you out of your account. Disable MFA for your Zoho Account before you uninstall.

Push Notification

To enable push notification

1. In the Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. Choose the **Authentication Mode** as **Push Notification.**
   Before you choose this mode install "Zoho OneAuth - Multi Factor Authenticator" on your iOS/Android device.
   If you haven't installed it, you will get a prompt asking you to install it on your mobile device.
   (If you are using the app for the first time follow step 4 and 5, else skip to step 6)
4. Open the app on your device and Sign in with your Zoho account.
5. Tap **Switch to MFA** on the home page.
   This will take you to the Setup MFA window.
6. In the *Setup MFA* window, tap the **Push Notification** mode or click and drag it into the circle.
7. Tap **confirm.**
   A window pops up asking your Zoho Account password.
8. Enter the password.
   You will be logged out from your active sessions on the web once you enter the password.

To log in using push notification

1. Log in to your Zoho CRM account.
   Zoho OneAuth app on your mobile asks for your approval.
2. Tap **Approve** to grant access.

Notes:

Uninstalling the OneAuth app will lock you out of your account. Disable MFA for your Zoho Account before you uninstall.

Scan QR

To enable QR code

1. In the Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. Choose the **Authentication Mode** as **Scan QR.**
   Before you choose this mode install "Zoho OneAuth - Multi Factor Authenticator" on your iOS/Android device.
   If you haven't installed it, you will get a prompt asking you to install it on your mobile device.
   (If you are using the app for the first time follow step 4 and 5, else skip to step 6)
4. Open the app on your device and Sign in with your Zoho account.
5. Tap **Switch to MFA** on the home page.
   This will take you to the Setup MFA window.
6. In the *Setup MFA* window, tap the **Scan QR Code** mode or click and drag it into the circle.
7. Tap **confirm.**
   A window pops up asking your Zoho Account password.
8. Enter the password.
   You will be logged out from your active sessions on the web once you enter the password.

To log in using QR code

1. Log in to your Zoho CRM account.
   Zoho OneAuth app on your mobile asks for your approval.
2. Scan the QR code from your device to sign-in to your Zoho Account.

Notes:

Uninstalling the OneAuth app will lock you out of your account. Disable MFA for your Zoho Account before you uninstall.

Time-Based OTP

To enable Time-Based OTP

1. In the Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. Choose the **Authentication Mode** as **Time-Based OTP**.
   Before you choose this mode install "Zoho OneAuth - Multi Factor Authenticator" on your iOS/Android device.
   If you haven't installed it, you will get a prompt asking you to install it on your mobile device.
   (If you are using the app for the first time follow step 4 and 5, else skip to step 6)
4. Open the app on your device and Sign in with your Zoho account.
5. Tap **Switch to MFA** on the home page.
   This will take you to the Setup MFA window.
6. In the *Setup MFA* window, tap the **Time-Based OTP** mode or click and drag it into the circle.
7. Tap **confirm.**
   A window pops up asking your Zoho Account password.
8. Enter the password.
   You will be logged out from your active sessions on the web once you enter the password.

To log in using Timer-Based OTP

1. Log in to your Zoho CRM account.
   Zoho OneAuth app on your mobile asks for your approval.
2. Tap **View Code** to get your One Time Password.

Verification Codes

A verification code is a unique code that is generated when you sign in to your Zoho account.

How can I get a verification code?

You can choose to receive the verification codes either through:

- Your ***Zoho OneAuth*** app.
- Your mobile device via an SMS **text message**.
- Through a call to your mobile device.
- In your Google Authenticator app.

If you requested but not did not receive a verification code, then try to use the **Resend** option to send the verification code. Depending on the mobile service provider, SMS text messages may take some time to reach your device.

What are backup verification codes?

Backup verification codes can be used when you have set up Two-factor authentication on your account and do not have access to your phone. You can either print backup codes, download them as text, or send them to your personal email address. You must keep these codes safe. This will help you access your Zoho account when you don't have your mobile device with you or you have no internet on your mobile device.

To get backup verification codes

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. In the *Two Factor Authentication* page, click **Manage Backup Verification Codes**.
   A set of backup codes will be listed.
4. Click **Save as text** to save the backup codes locally.
   If required, you can print the backup codes and file them in a safe place. These codes can be used only once, in place of a verification code when you sign in to your account.
5. Click **Generate new codes**, in case you want to regenerate the backup codes.
   This will delete the existing codes and generate a new set of backup codes.

How can I use backup verification codes?

After entering your login credentials to sign-in to your account, click **Can't access your phone?** in the sign in verification code page and enter any one of the backup codes from the list, to sign in to your account.

Note: If your phone is unavailable, these codes will be the only way to sign in to your account. Make sure to keep them in a secure and accessible place. If you have lost the backup codes, please contact Zoho Accounts support.

Trusted Browsers

The browsers that you have marked as "trusted browsers" on a computer won't ask for a verification code when you sign in to your Zoho account for the next 180 days. This saves you the effort of having to repeatedly enter the code each time you sign in to your account.

To do this, select the **Trust this browser** option while entering your verification code during sign in.

To view/delete trusted browsers in your account

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. In the *Two Factor Authentication* page, click **Manage Trusted Browsers**. This will list the details of the browsers you've trusted on any computer IP address. You can delete a trusted browser at any time from this list using the **Remove** link.

Note:

Once you revoke the trusted status of a browser in a computer, you will be required to enter a verification code the next time you sign in using this browser on this same computer.

Backup Phone Number

Backup phone numbers are used to send you verification codes during sign in if your primary phone is unavailable, lost, out of network range or drained of power.

To add or delete backup phone numbers

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. Choose Two-Factor Authentication.
3. In the *Two Factor Authentication* page, click the **Add Phone** icon corresponding to the *Phone Number* field.
4. In the popup, enter your phone number and click **Text me**.
   A verification code will be sent to your number.
5. Enter this verification code and click **Verify**.
   Your backup phone number will be added automatically.
6. Click the **X** option corresponding to the phone number you wish to delete.
7. Enter the password and click **Verify** to delete a phone number.

Zoho Account Settings

In Zoho Accounts, the mandatory fields under the Personal Information section are set to default as soon as you register with any Zoho service. After logging in, you can change the information according to your preference. When you change certain fields under the Personal Information section, the corresponding fields in Zoho CRM will be updated automatically.

Change Name

The First Name and Last Name in Zoho CRM are combined to form the Full Name in Zoho Accounts. When you modify the Full Name field in Zoho Accounts, the First Name and Last Name fields in Zoho CRM get updated and vice versa.

When you enter the First Name and Last Name without a space (e.g., ZohoCRM) in the Zoho Accounts Full Name field, the Zoho CRM Last Name field will be replaced with the Full Name provided in Zoho Accounts.

To change the name

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. In the *Zoho Accounts* page, click **My Profile Info** > **Personal Information**.
3. In the *Personal Information* page, update your **Full Name** and click **Save**. The First Name and Last Name field will be updated in Zoho CRM.

Change Password

You can change your password for all Zoho services in Zoho Accounts..

To change the password

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. In the *Zoho Accounts* page, click **Security.**
3. In the *Password* page, specify your **Current Password** and **New Password** in the corresponding fields.

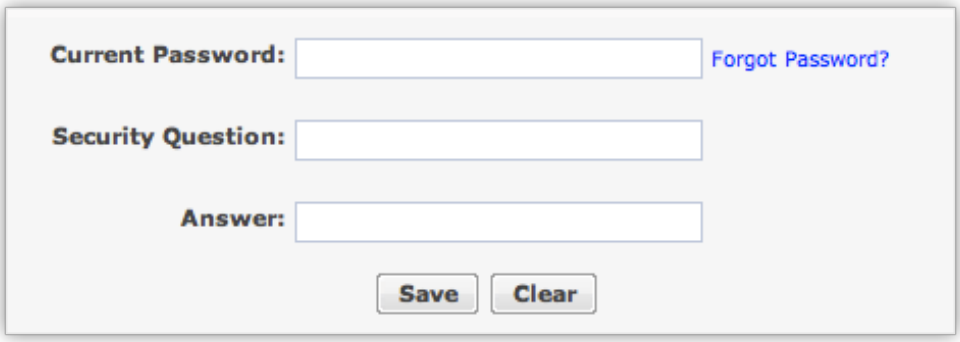
4. Click **Save**.
   The New Password will be updated and should be used to sign in to all Zoho services.

Change Security Question

Zoho Accounts allows you to create your own personal security question when you log in for the first time. This question can be modified whenever required and can be used to retrieve your password.

To create a security question

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. In the *Zoho Accounts* page, click **Security** > **Security Question.**
3. In the *Security Question* page, specify the **Current Password**, **Security Question** and the corresponding **Answer**.



4. Click **Save**.
   The security question will be updated and applicable for all Zoho services.

Change Preferences

You can specify the date format, newsletter subscriptions and browser connection according to your preference in the Zoho Account Preferences page.

To change your preferences

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. In the *Zoho Accounts* page, click **Preferences**.

3. In the *Preferences* page, follow these steps:
    - **Photo View Permission** – Specify who can view your photo.
    - **Date Format**: Specify the date format, either as dd /mm/yy or mm/dd /yy from the drop-down box, or you can customize a new date format by selecting **Custom** from the list.
    - **Password Expiry Notification** – Select the checkbox to get reminder email.
    - **Newsletter Subscription**: Select the type of newsletter subscription you want such as General Announcements, Product Announcements or Updates to Product, by clicking on the checkbox.
4. Click **Update Preferences**.
   Your preferences will be saved in Zoho Accounts.

Note:

Changing any of the fields under Zoho Accounts, including the date format, will not make any changes in Zoho CRM.

Authorized Websites

You can grant access to all Zoho services (including Zoho CRM) from trusted third party websites. For example, there may be a case of Zoho resellers & partners requesting for embedding a Zoho account "Sign Up" page in their website. If you grant this request, the third-party site becomes an 'authorized website' and users can access their Zoho account from within the reseller's website. The granted websites will be displayed in the Authorized Website section in Zoho Accounts and from where you can view, or delete the authorized Websites.

To manage authorized websites

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. In the *Zoho Accounts* page, click **Preferences** > **Authorized Websites**.
   In the *Authorized Websites* page, you can view the websites that have been authorized.

User Sessions

This feature keeps track of all the user sessions for a particular Zoho account. Active sessions for the past 7 days (including the current session) are listed in the sessions screen with additional information like start time, IP address, etc. Users have the option to end individual sessions or end all sessions (excluding the current one).

For example, you have logged in to a Zoho service from your home and have forgotten to sign out. Your session remains active and when you reach the office, you realize that the previous session was not closed. In such instances, the Zoho Accounts user sessions feature allows you to check all active sessions and close the sessions that should have ended. It also helps you to identify any unauthorized access to your accounts by checking session details such as start time, the IP address that conducted the session, and actions taken.

To view user sessions

1. In Zoho CRM, click on your profile and then click the **My Account** link.
2. In the *Zoho Accounts* page, click **Active Sessions**.
   In the *User Sessions* page, you can view the list of sessions and their details.
3. In the *Authorized Websites* page, you can view the websites that have been authorized.
4. Click **Close** to close a specific session, or **Close All Other Sessions** to close all the sessions (other than the current session).

Lesson B:

Allowed IP Addresses

Lesson Objectives

In this lesson, you will:

- Add Allowed IPs.
- Remove Allowed IPs.

Allowed IP Addresses

When you are dealing with customers' data, security is a major concern. You need to make sure that your data in Zoho CRM is not accessed from an insecure network. You may even prefer that your employees access CRM only from the office. You can also restrict logging in to and using Zoho CRM to specific IP Addresses only.

With the Allowed IPs feature, an administrator can add IPs for individual users or for users in a specified role or group. Users can log in to Zoho CRM only from these allowed IPs added by the CRM administrator. This also applies to all the other Zoho products. So if you are not able to access Zoho CRM from a specific IP, say your home office, then you will also not be able to access the other Zoho applications like Zoho Mail or Zoho Docs.

Profile Permission Required:

Users with the Administrator profile can access this feature

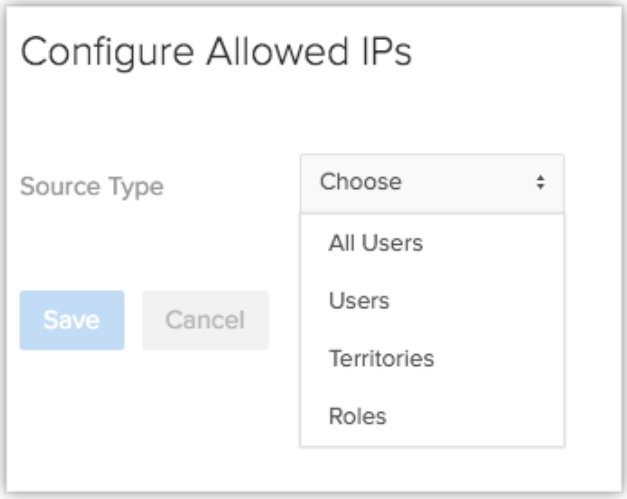
Add Allowed IPs

As an administrator, you can add the IPs which users of your CRM account can use to log in. You can allow only those trusted IPs from which the Zoho account can be accessed. Logging in through any other IP would give the user an "Access denied from this IP address" alert message. This restriction will also apply to login attempts from mobile devices and tablets. Additionally, APIs using the user's Authtoken will not work from the IPs that are not allowed.

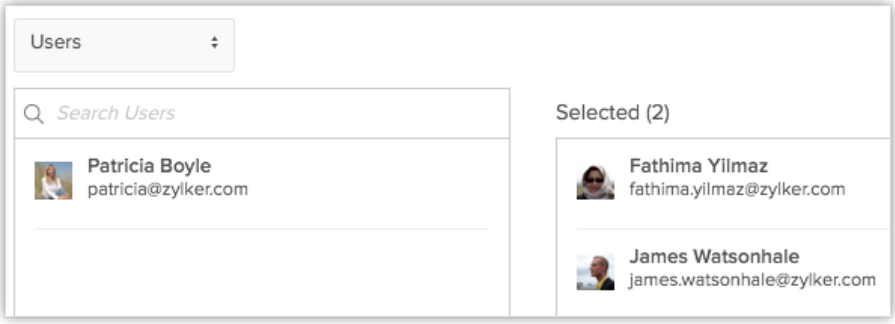
To add allowed IPs

1. Go to Setup > Users & Control > Security Control > Allowed IPs.
2. In the *Allowed IPs* page, click **Add Allowed IPs**.
3. In the *Configure Allowed IPs* page, select the **SourceType**.
    - **All Users:** Select this to give all users the access to Zoho CRM from only the specified IPs.
      A common IP for all users might be your office IP that all the users

access.



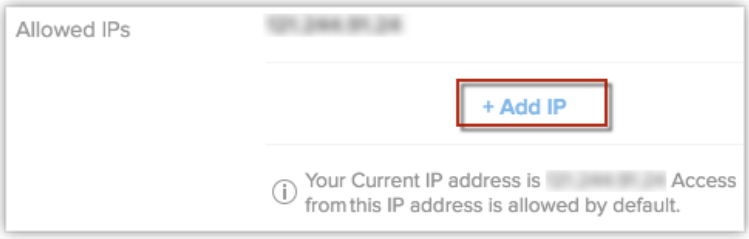
- **Users:** From the list, click on the users to move them to the Selected group.
  Select users for whom you want to allow CRM access only through certain specified IPs.



- **Groups**: From the list, click on the groups to move them to the **Selected** group.
  All the users in the selected group will have access to CRM only through the specified IPs.
- **Roles**: From the list, click on the roles to move them to the **Selected** group.
  All the users in the selected roles will have access to CRM only through the specified IPs.

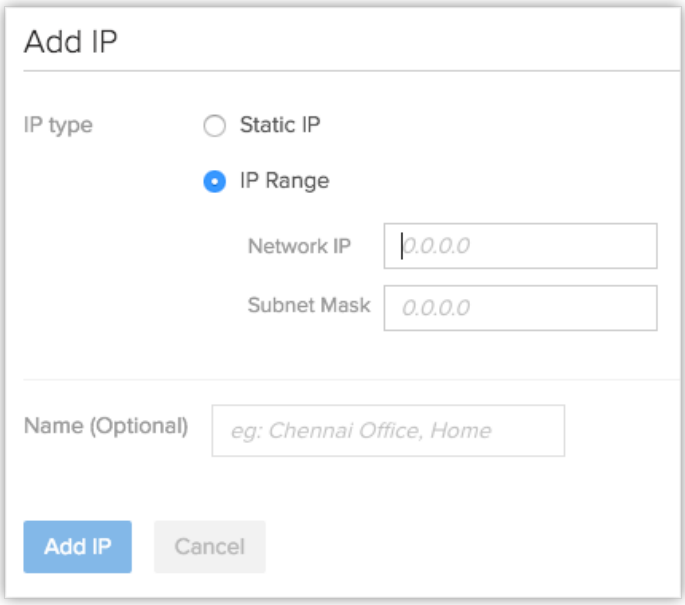
4. Click the **Add IPs** link.

   Your current IP address will be added by default.



5. In the Add IP popup, select the **IP Type** and enter the IP address.
   a. **Static IP:** Enter a valid IP.
   b. **IP Range:** Enter the NetworkIP and SubnetMask.

      You can contact your internet service provider for the Network IP and Subnet Mask.
   c. **Already Added IPs:** Select already added IPs from the drop-down list.



6. Enter a **Name** for the IP configuration, if required.
7. Click **AddIP**.
8. Click **Save**.

Remove Allowed IPs

You can remove the added IPs whenever you need. If a user is not part of any IP restriction, then the user will be allowed to access CRM from any IP. Make sure that you do not delete your own IP from the Allowed IPs list.

To remove allowed IPs

1. Go to Setup > Users & Control > Security Control > Allowed IPs.
2. In the *Allowed IPs* page, hover the cursor on an entry and click the **Delete** link.

To remove a single IP from the list of allowed IPs

1. Go to Setup > Users & Control > Security Control > Allowed IPs.
2. In the *Allowed IPs* page, hover the cursor on an entry and click the **Edit** link.
3. In the *Configure Allowed IPs* page, hover the cursor on an allowed IP and click the **Remove** link.
4. Click **Save**.

FAQs

1. How do I find my IP address?

It is best to contact your internet service provider for your IP address.

Zoho CRM will automatically list your current IP address under Allowed IPs by default, but if you have a dynamic IP address this is bound to change. So we strongly recommend that you enter the IP address provided by your internet service provider.

2. How do I enter the IP range? What are Network IP and Subnet Mask?

Unlike a static IP address which never changes, you have something called a dynamic IP address which keeps changing. This is the IP range. In the case of a

dynamic IP address, the IP address which you use to access the internet today may not be the same tomorrow.

To enter the IP range you need the network IP and subnet mask. You need to contact your internet service provider (ISP) to get the network IP and subnet mask.

3. I receive an error that says I have entered a private IP address. What does this mean?

There are two kinds of IP addresses: public and private. Zoho CRM lets you list only public addresses under Allowed IPs. If you have entered a private IP address, you will receive this error. Contact your ISP for your public IP address and enter it..

4. I configured the same IP address in more than one Zoho service. Will this overlapping cause issues?

No. Even if you have configured the same IP address in multiple services—for example, in Zoho Docs and Zoho CRM—this will still be considered one IP address for the whole of Zoho's services. There will be no issues. Even if you have configured this IP address in only one application—for example, only in Zoho Docs—this would apply to all Zoho products including Zoho CRM. You will not be able to access your Zoho account from IP addresses that are not listed under Allowed IPs.

5. I entered an incorrect IP address. I am not able to access my account. How can I overcome this?

If you have entered an IP address for a location other than the one you intended, first try to access your account from the location you entered. For example, if you have entered only your office IP address and you are trying to access Zoho CRM from your house, you will not be able to log in to your account. In this case, try to reach your office and access your account from there. Once you have gained access, you can include your home IP address on the list of Allowed IPs.

If you have made a mistake while entering your IP address and entered another valid IP address to which you have no access, we can help you. Please send an email to support@zohocrm.com.

Lesson C:

Audit Log

Lesson Objectives

In this lesson, you will:

- View Audit Log.
- Export Audit Log.

Audit Log

The Audit Log is a chronological sequence of entries, each resulting from the actions performed by users in Zoho CRM. Audit logs are helpful to determine what has happened before and after an event, and also to identify records associated with certain events.

Profile Permission Required:

Users with the Administrator profile can access this feature.

The Audit Log feature captures the following actions performed in the modules:

Modules	**Actions Performed**
• Leads • Accounts • Contacts • Potentials • Activities (Tasks, Events, Calls)	• Add, update, and delete records • Mass update and mass delete • Import and export records • Lead conversion • Delete from recycle bin • Rollback • Restore deleted records • Restore records in bulk • Find and merge duplicates • Deduplicate Records • Map fields for lead conversion
• Campaigns • Solutions • Vendors	• Delete records

• Quotes • Sales Orders • Purchase Orders • Invoices	
• Cases • Price Books	• Delete records • Import and export records

The Audit Log feature captures the following actions performed in the Setup:

Features	Actions Performed
• Users	• Add • Edit Details
• Auto Response Rule's Status • Case Escalation Rule's Status • Web Form's Status	• Activate • Deactivate
• Field Dependency Mapping	• Create • Edit
• Super Administrator	• Edit

• Email Templates & Folders • Inventory Templates & Folders • Mail Merge Templates & Folders • Auto Response Rules • Rule Entry for Auto Response Rule • Workflow Rules • Workflow Alerts • Workflow Tasks • Workflow Field Updates • Workflow Follow-ups • Webhooks • Case Escalation Rules • Rule Entry for Case Escalation Rules • Web Forms (Leads, Contacts, Cases) • Business Hours • Roles, Profiles, Groups • Reports & Report Folders • Assignment Rules • Rule Entry for Assignment Rules • Web Tabs	• Create • Delete • Edit
• Users	• Add • Edit details •
• Auto Response Rule's status • Case Escalation Rule's status	• Activate

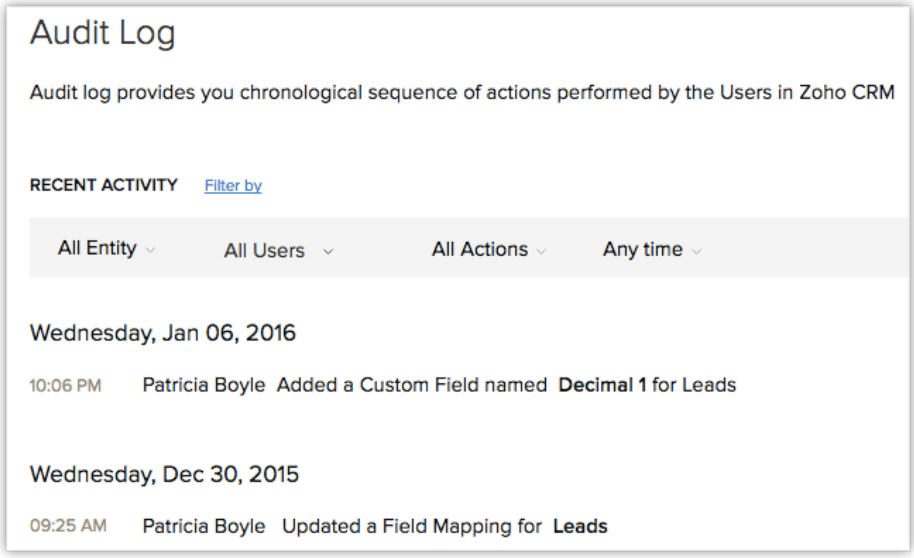
• Web Form's status	• Deactivate
• Field Dependency Mapping	• Create • Edit
• Super Administrator	• Edit

View Audit Log

The audit log displays the activities performed by users in your organization with the CRM account. Users with the Administrator profile or CEO role can access the audit logs. However, other users can only view their own and their subordinates' audit logs.

To view audit logs

1. Log into your Zoho CRM account.
2. Go to **Setup** > **Data Administration** > **Audit Log**.
   The *Audit Log* page displays all the actions performed by all users for the last 60 days.



Since the audit log is exhaustive, it could be tiresome to sift through the entries if you are looking for a few specific details. For example, if you wish to see only the records added by a particular user or a list of actions performed in the last 7 days, it could be difficult to find those specific entries among a huge list. In such a case, you can use the Filter options offered to you and narrow down the entry orentries you are looking for.

To filter the entries in the *Audit Log* page

1. Select an **Entity** in order to view the log of actions performed on that entity. You can choose from one of the following.
    - Choose a specific module to view the log of actions performed on that module only. For example, you can view the audit log for the Leads module.
    - Choose **Setup** to view the log of all Setup-related actions only.
    - Choose **All Entities** to view the log of actions performed on all the modules as well as Setup-related actions.
2. Select a **User** in order to view the log of actions performed by a particular user. You can do one of the following:
    - Choose a specific user to view the log of actions performed by that user only.
    - Choose **All users** to view the log of all actions performed by users in your organization.
3. Select an **Action** in order to filter the entries based on the actions that have been performed.
    - Choose an among **Added**, **Updated**, and **Deleted** actions depending on your requirements.
    - Choose **All Actions** to view the log of all three actions.
4. Select a **Time** in order to view the log of actions performed in the chosen timeframe. Choose among the following options:
    - Anytime
    - Today

- Last 7 Days
- Last 30 Days
- A Specific Date (which falls within the last 60 days)
- A Date Range (which falls within the last 60 days)

For example, if you want to view all the records added by a specific user in the Leads module in the last 7 days,

- Choose *Entity* as **Leads**.
- Choose the desired *User*.
- Choose *Action* as **Added**.
- Choose the *Time* as **Last 7 Days**.

The audit log will be displayed according to the above filters.

Notes:

- Users can only view their own and their subordinates' Audit Logs.
- Administrators can view the logs of subordinates, and the CEO has the privilege to view the logs of all users.

Export Audit Log

You can export all the audit log entries in CSV format.

To export audit log entries

1. Log in to Zoho CRM with Administrator privileges.
2. Go to Setup > Data Administration > Audit Log.
3. In the **Audit Log** page, click **Export Audit Log.**
   The entries will be exported in a .csv format.

Lesson D:

Data Encryption

Lesson Objectives

In this lesson, you will:

- Set up data encryption.
- Understand the encryption process in Zoho.

Data Encryption

Zoho CRM gives you further means to protect sensitive and confidential user data through encryption. Encryption is the process of encoding information and making that information accessible only to the authorized parties. The encryption process converts plain (or readable) text into cipher (or non-readable) text, which can only be read when decrypted by an authorized user.

At Zoho CRM, we use an encryption method called AES (Advanced Encryption Standard), which uses keys to encrypt and decrypt the data.

Data can be encrypted automatically with AES in Zoho CRM by enabling encryption in a custom field. Encrypting the data does not come in the way of the effective and quick use of Zoho CRM, by authorized users. It simply prevents unauthorized parties—such as blocked users and potential hackers—from gaining access to sensitive or valuable data.

Permission Required:

Users with the Administrator profile can access this feature.

Set up data encryption

Data encryption is a way to safeguard the information you store in your CRM. Only the data from custom fields can be encrypted. Say, for instance, you need to store confidential information like credit card details, backup phone numbers, etc.: you can include those fields in the user layout as a custom fields. Data encryption is done when a custom field is created or edited.

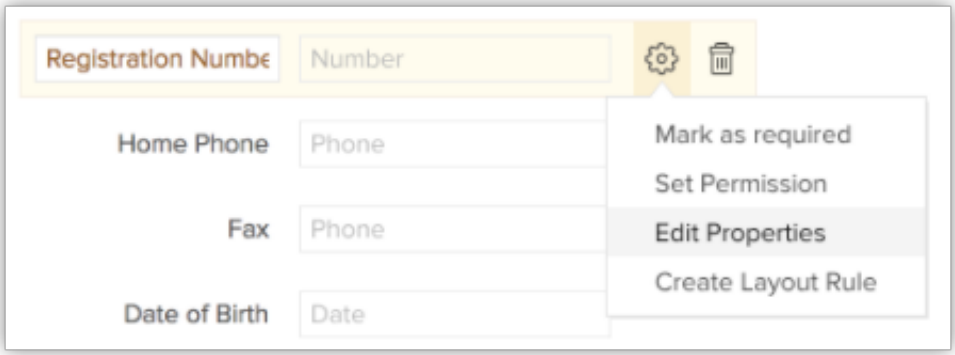
Notes:

Only the Leads, Accounts, Contacts, Deals, Linking modules, Users, and any Custom modules support encryption.

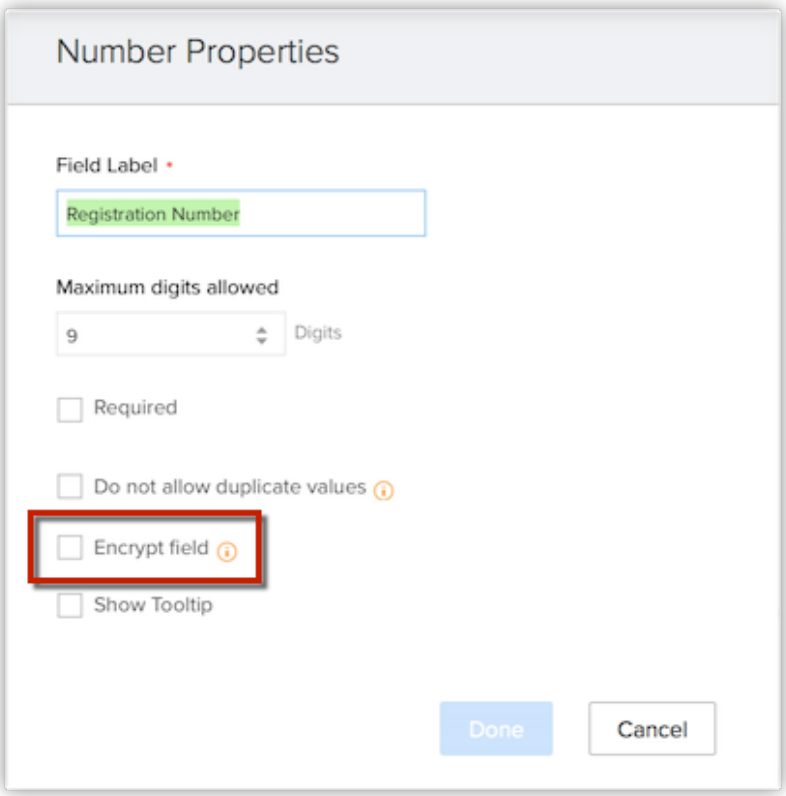
To encrypt or decrypt custom fields

1. Go to Setup > Customization > Modules and Fields > [Select the module].

2. In the module layout editor, go to the field you wish to encrypt, click the **Settings** *icon* and select **Edit Properties**.



3. In the *Field Properties* popup, select the **Encrypt Field** checkbox.



4. Click **Done**.
5. **Save** the layout.

Feature Specifications

Field and Module-based specifications:

- Only custom fields (new and existing) can be encrypted. Unique fields can also be encrypted, as long as they are custom/user-generated.

- The field types which support encryption are Single Line, Email, Phone, and Number.
- Only the Leads, Accounts, Contacts, Deals, Linking Modules, Users and any Custom Modules support encryption.
- Encryption can be disabled for a field at any time.
- In lead conversion mapping, data can be converted and stored only between two encrypted fields.
- Encrypted fields can be used as inputs in Formula fields.

Handling Encrypted Data

- Find & Merge and Deduplication are supported for encrypted fields.
- Any data imported to encrypted fields will be encrypted by default and exported data are decrypted.
- Encrypted fields can be included in web forms.
- An encrypted field can be displayed in Reports as a column, but cannot be used in Criteria and Columns to Total.
- Encrypted fields can be used as inputs in custom functions, and as merge fields in templates.
- APIs are supported for encrypted data.
- Encrypted fields can be used in integrations. Using the information in integrations is entirely at the user's risk.

Limitations and Trade-offs

- Only full-text search is supported in global search. For instance, if the encrypted data is "Joseph Wells," the encrypted field record does not show in the results of a search for "Joseph."
- Encrypted fields cannot be used in Advanced Filters
- Encrypted fields cannot be found using Search by Criteria
- Encrypted fields are not visible in the Sort option.
- Encrypted information is only stored in the *crm.zoho.com* domain. Use the encrypted information in other domains or third-party services at your own discretion.
- In the Forecasts module, encrypted fields cannot be used as Target Fields.

The Encryption Process in Zoho

Encryption is a method of adding a layer of security to data, preventing the data from being stolen or lost. It is the process of encoding information to make itaccessible only by authorized parties.

Even if a potential hacker gets ahold of the data, the information stored in the cipher text is non-readable.

Encryption can be used in two situations:

- Encryption in Transit
- Encryption at Rest (EAR)

Encryption in Transit

Data is usually encrypted when it is in transit (transferred from one place to another). This is to prevent others from accessing the data en route. This provides a considerable level of security for the information.

Encryption at Rest (EAR)

The encryption of data during transit provides good security. However, the encryption of this data when it is stored in servers provides an even higher level of security. Encryption At Rest (EAR) prevents any possible security leaks or losses when the data is in storage.

This method of encryption is done using the AES-256 protocol. A symmetric encryption algorithm, which uses 128-bit blocks and 256-bit keys, is used for encrypting/decrypting the data. It is one of the more advanced methods of encryption.

There are many modes of operation of AES. Some of them are:

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

- Counter (CTR)

Zoho encrypts data using the *Counter* mode.

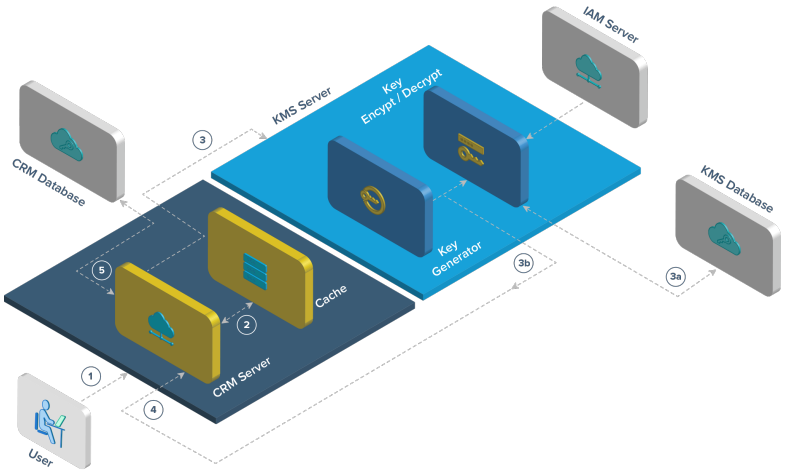
You can retrieve the encrypted data using keys. The key used to convert the data from plain text to cipher text is called a Data Encryption Key (DEK). This DEK is further encrypted using the KEK (Key Encryption Key), providing yet another layer of security.

So the data in your CRM is well equipped and has three layers of security.

- Encrypted data (ciphertext) is stored in the Zoho Services database.
- Encrypted DEKs are stored in the KMS (key management system).
- Encrypted KEKs are stored in IAM (identity and access management) servers.

The retrieval of data goes through three levels. Hence, the level of security is increased considerably.

Encryption Process



1. The encryption agent determines, from the metadata, whether to encrypt the field before storing it in the database.
2. The encryption agent checksthe cached memory for matching DEKs. If no matching DEKs are found, the encryption agent requests a DEK from the KMS.
3. The KMS checks its database for a matching encrypted DEK.

4. If the matching encrypted DEK is found, the KMS decrypts the encrypted DEK and returns it to the encryption agent.
5. If no matching DEK is found, the KMS generates a DEK. This new DEK is encrypted with KEKs and stored in the KMS servers.
6. The agent receives the Data Encryption Key (DEK), then encrypts/decrypts the data using 256-bit AES encryption.
7. The cipher text (the encrypted data) is then stored in CRM (in the Zoho Services Database/File System).