POWER OF SIMPLICITY

Knowledge Map

Tally.ERP 9

Preface

What is a Knowledge Map?

A Knowledge Map is a representation of a concept using levels of information. Each level provides deeper understanding than the previous one. The emphasis is on gaining the maximum understanding in the shortest possible time.

Why Knowledge Map for Tally.ERP 9?

Tally.ERP 9 is one of the most widely used financial software that has extended capabilities and great potential to transform a business. Many areas of Tally, when implemented, actually translate to increased efficiency, reduced costs, and organised business operations.

This Knowledge Map has been created to help readers gain an immediate understanding of the key areas of expertise; such an understanding can bring about positive impact on your business.

This Knowledge Map on Tally.ERP 9 aims to

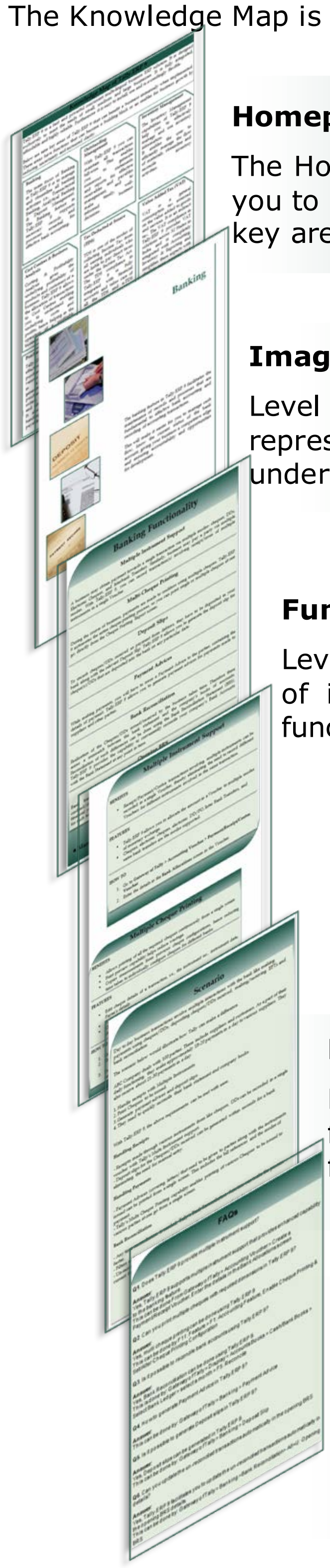
1. Get you closer to understanding the key areas in a short time.
2. Illustrate how these key areas can benefit a business.
3. Encourage the efficient use of the most appropriate solutions.
4. Have the most beneficial information handy, enhancing usability of Tally.ERP 9.
5. Helps users find critical information quickly.
6. Enhance decision-making and problem-solving by providing access to applicable information.

Benefits of using the Knowledge Map for Tally.ERP 9

- Grasp the necessary know-how quickly without having to refer to any secondary material.
- Arrive at information faster! This is a non-continuous, easily understandable guide on how to obtain a positive impact with Tally.ERP 9.
- Information on any page is complete and relevant to the functionality of the key area; you don’t have to refer to another page to understand it.
- Immediate awareness of where you are in the Knowledge Map. All pages have been marked for easy navigation.

Structure of the Knowledge Map for Tally.ERP 9

The Knowledge Map is layered as shown below, with each layer zooming in on each key area.



Homepage (Level 1)

The Homepage consists of the key areas. Clicking on any of these topics will take you to the page containing pictorial representation of the key functionalities of that key area.

Image Trigger (Level 2)

Level 2 provides a pictorial overview of the key areas. The purpose of pictorial representation is to act as triggers, to help you remember the basics of the topic under discussion. The images will lead you to Level 3 when clicked.

Functionality (Level 3)

Level 3 contains a brief explanation of the main functionality of the key area of interest. For example, Banking is one of the key areas, and the main functionalities are:

● *Multiple Instrument Support* ● *Multi Cheque Printing* ● *Deposit Slips* ●*Payment Advices* ● *Bank Reconciliation* ● *Opening BRS*

A brief introduction on banking functionalities in Tally.ERP 9 will be given here. Zoom in to Level 4 for more details by clicking the name of the functionality.

Functional Details (Level 4)

Navigating to Level 4, will lead you to further information on the functionality of the key area i.e., the benefits and features of the functionality, and how to use it.

Scenario and FAQs

A typical business situation that can be simplified with Tally.ERP 9 is presented as a Scenario.

The FAQs section, as the name suggests, contains a set of Frequently Asked Questions pertaining to each of the key areas discussed.

Table of Contents

Password Policy

Keeping financial data safe is of utmost importance to preserve its purity, avoid unauthorized changes and to keep customers' financial information safe.

A good password policy will enhance data security and allow only authorized users to view financial data. In Tally.ERP 9, the Administrator can set a password policy in place; which users will have to adhere to, while creating and managing passwords for their company.

Password Policy Functionality

Password Strength

Password Strength is the level of complexity which is attributed to your password, which will keep it safe from unauthorized attempts to retrieve or guess it. The components that decide the strength of a password are its length, complexity and unpredictability.

Password Expiry

Password Expiry is a mechanism which requires users to change their passwords regularly. This is done because, over time users tend to give out their passwords, write it down, or otherwise compromise the secrecy of their passwords. Passwords leaked over time pose a security risk, which is mitigated by Password Expiry.

Password History

It's possible to maintain a user's password history and prevent the user from re-using their old passwords. The Administrator can specify how many previous passwords that should be stored in the Password History.

Password Overriding

Some users can be excluded from following the Password Policy as they might be higher up in grade than the Administrator, like Supervisor, Manager, etc. For these users the, Administrator can remove the Password Policy.

Allow User to change Password

In Tally.ERP 9, usually the Password is assigned to users, such as Data Entry Users, by the Administrator. The Administrator can also allow a user to change his/her own password at any point in time as per the Password Policy described.

User Status

When a user is no longer active that is, user will not be accessing the company data, the Administrator can make his account Inactive. When the user resumes to use the company data, the status can be made active again.

Segments Benefitted

• Manufacturing • Trading • Retail • Service • Professionals

Password Strength

BENEFITS

- The administrator can set the strength of a password; hence make set standards for data security.

FEATURES

- Minimum password length can be defined.
- Complexity of the password in terms of the number of characters, digits and special characters.

HOW TO

1. Go to **Gateway of Tally** > **Company Info** > **Security Control** > **Password Policy**
2. Set the **Minimum Password Length**.
3. To set the complexity of the password, set **Yes** to **Specify ADVANCED Password Strength**.

Password Expiry

BENEFITS

- Reduces security risks due to password leaks.

FEATURES

- Administrator can define after how many days a password expires.
- The users can be notified before the password expires and hence they can change it on time.

HOW TO

1. Go to **Gateway of Tally** > **Company Info** > **Security Control** > **Password Policy**
2. **Password Expires after** can be defined in days.

Password History

BENEFITS

- Restricting users to use old passwords is another was of setting a good password policy in place to secure company data.

FEATURES

- Disallows users to use old passwords that are stored in the password history.
- The number of passwords to be stored in the password history can be defined.

HOW TO

1. Go to **Gateway of Tally** > **Company Info** > **Security Control** > **Password Policy**
2. Set **Yes** to **Restrict the use of old passwords**.

Password Overriding

BENEFITS

- Allows the Administrator to choose the users for whom the Password Policy is applicable.

FEATURES

- Administrator can remove the applicability of Password Policy to some users as they may be higher up in the company than the Administrator.

HOW TO

1. Go to **Gateway of Tally** > **Company Info** > **Security Control** > **User and Passwords**
2. In **F12: Configuration**, set **Yes** to **Show Apply Password Policy**.

Allow User to change Password

BENEFITS

- As users can set their own passwords, lesser people will know the password. This will help keep the company data more secure.

FEATURES

- Users can change their password when they log-in to the company.

HOW TO

1. Go to **Gateway of Tally** > **Company Info** > **Security Control** > **Password Policy**
2. Set **Yes** to **Allow Users to change password**

User Status

BENEFITS

- Instead deleting a user, Administrator can simply make them inactive.

FEATURES

- Can make users active or inactive. In other words, the users can be restricted from accessing the company data by using this option.

HOW TO

1. Go to **Gateway of Tally** > **Company Info** > **Security Control** > **User and Passwords** > **F12: Configure**
2. Enable **Show User Status**.

Scenario

Data security is one of the major concerns for a business, as many people will have access to it.

Some of the problems faced are:

- Some people may keep very weak passwords that can be hacked easily by unauthorized users
- Passwords may be leaked over a time period for various reasons
- Some use may use their old passwords over and over again, and this may also lead to leaking of passwords.

To prevent all this, a strong Password policy should be in place.

With Release 3.6, Tally.ERP 9 allows Administrators to define a strong Password Policy for their company, to ensure their company data.

Password Strength

The Administrator can set the length and complexity for a password, hence making it difficult for unauthorized users to access the company data.

Password Expiry and Password History

Making users change their password on a regular time interval is a good way of ensuring data security. Tally.ERP 9 also notifies the users before the current password expires. Both the time period for expiry and notification period can be defined by the Administrator.

One more aspect of Password Policy in Tally.ERP 9 is, that the Administrator can disallow users to use previously used passwords. The number of passwords stored in the Password History determines the previous passwords that the user cannot keep when the password is changed.

Password Overriding

Tally.ERP 9 allows the Administrator to override the password policy for some users. These users will usually be the users who are higher up in the company than the administrator.

FAQs

1. **How to disable Password Expiry?**

   By setting zero to Password Expiry, we can disable the **Password Expiry**.

   To do so, Administrator has to:

   - Go to **Company Info.** > **Security Control** > **Password Policy**
   - Set **Password Expires after** to **0** days

2. **How to disable Password Strength?**

   By setting zero to Password Strength, we can disable the **Password Strength**.

   To do so, Administrator has to:

   - Go to **Company Info.** > **Security Control** > **Password Policy**
   - Set **Minimum Password Length** to **0**

3. **Will User be notified to change the Password on first login, if the option Change Password on first login is disabled?**

   If Password set by the Administrator is not as per the Policy, then it will notify the user to change password as per the policy.

4. **Are Users who aren't under Password Policy allowed to change Password on their own?**

   No. They are not allowed to change their Password, since they are not under Password policy.

5. **Can Password policy be disabled on the currently working company, which is Security Enabled?**

   Yes. By disabling the **Activate Password Policy** option, Administrator can disable the Password policy.

   To do so,

   - Go to **Company Info.** > **Security Control** > **Password Policy**
   - Set **Activate Password Policy?** to **No**

FAQs

6. **When Company Data is opened for the first time in Release 3.6, will Password Policy be Applicable automatically?**

   No. Until Administrator enables the Password Policy in Security Control, it will not be applicable to the Company Users.

   To activate Password Policy,

   - Go to **Company Info.** > **Security Control** > **Password Policy**
   - Set **Activate Password Policy?** to **Yes**