Virtual Code Authentication
User Guide for Administrators
# Table of Contents

**Overview of New Security** ........................................................................................................................................................................... 4

**Passwords** ........................................................................................................................................................................................................ 5
  - Password Preferences .......................................................................................................................................................................................... 5
  - Additional Password Changes: ........................................................................................................................................................................ 6

**Multi-Factor Authentication - Virtual Code** ................................................................................................................................. 7
  - MFA Overview ........................................................................................................................................................................................................ 7
  - MFA Approval List ................................................................................................................................................................................................ 8
  - Importing Employees with Existing Passwords ........................................................................................................................................... 8
  - MFA - The User’s Experience ............................................................................................................................................................................ 9

**Additional MFA Options** ........................................................................................................................................................................ 13
  - Updating Employee MFA Information .......................................................................................................................................................... 13
  - Approving or Rejecting Updated MFA Virtual Code Credentials ............................................................................................................... 14
    - Selecting Approvers ................................................................................................................................................................................................ 15
  - Clearing MFA Configuration ........................................................................................................................................................................ 16

**Kiosk Mode – Non Virtual Code** ......................................................................................................................................................... 17
  - Overview ........................................................................................................................................................................................................... 17
  - IP Addresses .................................................................................................................................................................................................. 17
  - Browsers and Cookies ..................................................................................................................................................................................... 17
  - Certifying and Configuring a Computer .................................................................................................................................................. 18
  - De-Certifying a Computer ............................................................................................................................................................................. 18
Overview of New Security

Modern technologies call for higher security standards as practiced among many other online systems. Configurable password settings have been in place which allows for sub-standard password practices among users.

As such, we will now require a two-step log in process.

1. **Enhanced Passwords**
   - Going forward, your password must contain a minimum of 8 characters and include at least one of the following:
     - Uppercase Letter
     - Lowercase Letter
     - Number
     - Symbol
     - Example: Password1$

2. **Multi-Factor Authorization (MFA) or Virtual Code Authentication**
   - After you enter your username/password and click login, if the system does not recognize this computer as one you have used in the past 30 days, the system will require a second form of authentication before you can continue. A code will be emailed, texted, or sent to you via an automated voice call, which you will then enter, in order to access the system. The security combination factors are as follows:
     - Password = something you know
     - Code = something you have
Passwords

Password Preferences

Under Company Settings > Global Setup > Company Setup, on the Login Config tab within the Password Preferences widget, there are new minimum standards for all passwords in the system.

They are as follows:

- **New Account Default Password**: Will deploy in order. If not using Option #1 (unchecked and not set), the system will move to Option #2, where you can designate the default password. If none of the above are used, the system will assign the default password shown in Option #3.
  Note: Option #3 will not display if a password has been set in Option #2.

- **Password History**: 10 day history (hard-coded)

- **Maximum Password Age**: Open field to set limit (can be set up to 99999)

- **Minimum Password Length**: 8 characters

- **Password Complexity Level**: 4 complexities (hard-coded). There are 4 different character classes that are required in a password. This means each password must contain at least one of the following: An upper case letter, lower case letter, number, and a symbol.
  - Example password: Password1!

- **Lock Account After**: Minimum 1, Maximum 5 invalid attempts within 5 minutes (minutes is hard-coded)

- **Lock Account**: If set to “Temporary,” the minimum time allowed is 30 minutes. If set to “Permanently,” an Administrator must login and unlock the account.
Additional Password Changes:

New Accounts

- New accounts will be forced to login and change their password within 5 days of account creation or they will be locked.
  
  - To unlock, the administrator will login to unlock the new account. The user will then have another 5 days to login before being locked again. Cycle repeats.
Multi-Factor Authentication - Virtual Code

MFA Overview

The Multi-Factor Authentication, or MFA, is required functionality for all Workforce Ready account users including Partner Admins, Company Admins, Managers and Employees. This functionality generates a Numeric code for the user to enter which provides a second factor of their personal identity.

Certain logins will not require a second factor of identity. They are:

- Mobile Application
- Middleware
- Clocks
- Web Clocks*
- Single Sign On
- Applicant Logins

Individual accounts which are already configured with a form of Multi-Factor Authentication such as an RSA code will not be required to use this particular form of MFA.

For the rest of the accounts moving forward, a code will be used and sent to the user either by Text, Voice Call or E-mail which will be required, along with the username or password, in order to enter into the system.

* Multi-Factor Authentication will **NOT** be required when using a Web Clock unless the Login feature is used.
MFA Approval List

After enabling MFA, and then saving the page under Company Settings > Global Setup > Company Setup containing the “Password Preferences” widget, it will be mandatory, upon clicking the Save button, to create an approvers “Admin List” and “Approval Period” within the “Multi-Factor Authentication” section. This will ensure that the necessary approvers are in place when employees begin configuring their information to receive their virtual codes. See the “Approving or Rejecting Updated MFA Virtual Code Credentials” section below for details about how this works.

![Password Preferences screenshot](image)

Importing Employees with Existing Passwords

When importing employees, existing passwords will not be imported. This includes new hires as well as existing employees.
MFA - The User’s Experience

A first time login, as well as all new accounts, will require a Password Change and configuration of the MFA settings for future logins.

Step 1: Enter Username and Password as usual on the login page.

The Change Password screen will display where the password must be changed to one with the new requirements. The screen will explain the new password standards. Mobile users will also receive this screen.
Step 2: Once the password has been changed, users will be taken to a form to configure their MFA Settings.

- Up to three methods can be configured for receiving a code. The user has the option to configure their Text Message #, Voice Phone # and/or Email address. One or more methods may be selected. Any information that is already listed in the account will be pre-populated. If multiple phone or email numbers are stored in the system, those will be made available to the user via the drop-down lists shown in each field. Users may also enter new information not stored in the system. When this happens, an administrator must approve the new credentials. See the “Approving or Rejecting Updated MFA Virtual Code Credentials” section below for details about how this works.

- Once this step is completed, the user will be logged directly into the system.

- For any logins thereafter, the code will be delivered via the selected method and is unique to the user and will expire in 15 minutes.

- Once the user enters the code, they can choose to make the computer trusted by checking “Remember This Device” where an encrypted cookie will be placed on the machine for that browser. A trusted computer will not require the 2nd factor again unless the cookie expires or is deleted via the web browser options. It can expire if a user does not log in for 30 days and the 30 day counter is reset on every successful login.
Step 3: Anytime thereafter, when logging in from a device that has not been remembered, the user will be asked which method they would like to use to receive their code for that specific login. Select a method and click the button to send either Text Message, Voice, or Email.*

NOTE: It is recommended that users select “Text Message #” as their primary option. The other methods are valid, but due to inconsistencies in email policies and practices (such as Spam/Junk folders, server down-time, etc.), a text message will deliver the code immediately to the user.

Screen to request code:

![Screen to request code](image)

Screen after sending the code:

![Screen after sending the code](image)

After the code is received, enter the code, check the box** and click “Continue.” The user will now be logged in to the system. This option will not show for users who still have approval items pending for the MFA administrator.

* If Email is selected as the method to send the code, the email will be sent from the Company Email Address displayed under **Company Settings > Global Setup > Company Setup**, on the **Company Info** tab, in the **Company Address** section. If there is no Company Email Address listed, the email will be sent from NoReply@Kronos.com.

** If the box is checked, the next time this specific user is logged in from this device, a second factor of authentication (code) will not be required for login. As a best practice, this option should only be checked on individual personal computers and should never be checked on a public or shared computer.

Coming Soon: For any accounts with outstanding approvals, this box will be disabled.
Additional MFA Options

Updating Employee MFA Information

- Employees may change their SMS, Voice and Email settings at any time by navigating to My Account > My Settings > Change Multi-Factor Authentication. If a user enters information that is not already stored in the system, an approval will be needed by an administrator. See the “Approving or Rejecting Updated MFA Virtual Code Credentials” section below for details about how this works.

This feature is enabled for users within Company Settings > Profiles/Policies > Security within the ESS tab.
Approving or Rejecting Updated MFA Virtual Code Credentials

When employees configure their MFA code and enter credentials that are not already on file in the system, approval will be required. This will apply to all employees who log in to the system. The purpose of this feature is to protect users’ data by ensuring that the virtual codes are sent to their legitimate phone numbers and email addresses.

There are two ways that changed or updated employee credentials will trigger the approval process:

- Employee enters information under My Account > My Settings > Change Multi-Factor Authentication that is not on file within their account in Employee Information.

- Employee enters information in the MFA Configuration screen that is not on file within their account in Employee Information.
Selecting Approvers

To designate administrators who can approve new employee information, and if not already set up, go to **Company Settings > Global Setup > Company Setup**, within the “Password Preferences” widget in the “Multi-Factor Authentication” section and create an “Admin List” where one or more administrators are designated as approvers. A maximum of 72 hours (the default setting) may be set for the “Approval Period” which is the recommended setting. Less time may be selected. If set to Zero (0) hours, employees will be locked out immediately when entering new credential information until the approval is completed.

It is recommended to select more than one approver in cases where staff may out of the office. One or more approvers may be selected using the filters as shown below.

To approve, an email will be sent to all the approvers in the “Admin List,” as well as sending a “My To Do” action to each approver. One approval will clear the “My To Do” action for the other approvers on a first come, first served basis. Approval will be needed by an administrator within the window set in the “Approval Period” field, which is usually 72 hours. If the approval is not done within the 72 hour window, the employee will be locked out until approved by an administrator.

In the example shown below, an administrator has been sent an approval request for an employee. If the approver has access to the employee, the name will be shown as a hyperlink. When clicked, the hyperlink will take the approver to the employee’s account under Employee Information, where information can be viewed and confirmed. A Utilities icon is also available to navigate to various areas of the system.

Based on the example shown above, the employee is not locked and still can log in using the new information for up to the 72 hour limit (or whatever is set in the “Approval Period” field.)

- **When Approved** – Employee can log in now, and in the future, using the new credentials.
- **When Rejected** – Employee’s account will be locked.
Clearing MFA Configuration

For any users who require a complete reset to their MFA Configuration, there is an option available to managers or administrators within the Employee Information profile within the Account Information widget to “Clear MFA Configuration”. By doing this, the employee will be brought back to Step 1 as described above.

The access to this feature is granted within the HR tab of the Security Profile under Company Settings > Profiles/Policies > Security.
Kiosk Mode – Non Virtual Code

Overview
Kiosk Mode allows certain computers to be configured and certified as terminals so that users logging in to those computers can bypass the Multi-Factor Authorization, or MFA process for logging in. Since MFA requires the use of personal phones and email addresses, this feature is useful for companies who have policies in place that prevent employees from using their personal phones, or accessing email from work. Employees can instead use a computer in "Kiosk Mode" to perform their normal duties or access Employee Self Service features.

Computers will go through a configuration process called “certifying” in which settings will be applied that will save, or certify the computer to an exclusion list that will allow it to bypass the MFA process. Computers may also be “de-certified” as needed.

IP Addresses
In order for this feature to work correctly, a static IP address must be used. If DHCP addresses are used, the computer will not be able to be certified for kiosk mode.

Once the configuration is complete and the computer is certified for kiosk mode, the IP will be saved to an exclusion List. This list will be used to allow certified computers to bypass the MFA process when users log in to that device.

Browsers and Cookies
Browsers must be configured to accept Cookies. Each terminal configured for kiosk mode will store a Cookie on the computer being used for each entry.

NOTE: If it is a normal practice for your company to periodically clean and remove Cookies from your computers, whether done daily when the Browser is closed, or on a schedule, will de-certify a previously certified machine since Cookies are required for Kiosk Mode. It is recommended that for all browsers on all computers that are certified for Kiosk Mode that you do not remove Cookies. If Cookies are removed, the terminal will need to be configured again.
Certifying and Configuring a Computer

The configuration of this feature must occur on the computer being certified for kiosk mode. Administrators will log in using the MFA process. Navigate to: Company Settings > Global Setup > Company Setup and add the "Kiosk Mode – Non Virtual Code" widget by clicking the "Edit Tabs" icon and selecting it from the "Available Windows" list.

- Multiple entries can be created on each terminal and each IP Address.
- No maximum on the number of terminals that can be added.
- If using more than one computer to set up Kiosk Mode, the same Static IP Address may be used for each computer.

Step 1: Click the "Certify This Kiosk" to register the terminal.

![Certify This Kiosk](image1)

Step 2: Enter a Name in the "Kiosk Name" field. The IP Address of the kiosk will automatically be filled.

![Kiosk Name Entry](image2)

Example:

![Example Kiosk Configuration](image3)

De-Certifying a Computer

You may de-certify a computer from Kiosk Mode by deleting Cookies in the web browser or by clicking the red X in the widget and deleting the terminal from the list.