Multi-Factor Authentication (MFA) in ServiceNow: Implementation Guide

Contents

1. Introduction

Multi-Factor Authentication (MFA) enhances the security of user logins by requiring multiple forms of verification. Implementing MFA in ServiceNow ensures that only authorized users can access the system, thereby safeguarding sensitive data and applications from unauthorized access.

2. Benefits of MFA

- **Enhanced Security**: Reduces the risk of compromised credentials.
- **Compliance**: Helps meet regulatory requirements.
- **User Confidence**: Boosts trust by protecting user data.
- **Risk Mitigation**: Decreases the likelihood of security breaches.

3. Prerequisites

Before implementing MFA in ServiceNow, ensure the following:

- An active ServiceNow instance with admin access.
- A compatible identity provider (IdP) that supports MFA.
- Users' devices configured for receiving MFA tokens (e.g., mobile phones for SMS, authentication apps).

4. MFA Methods Supported in ServiceNow

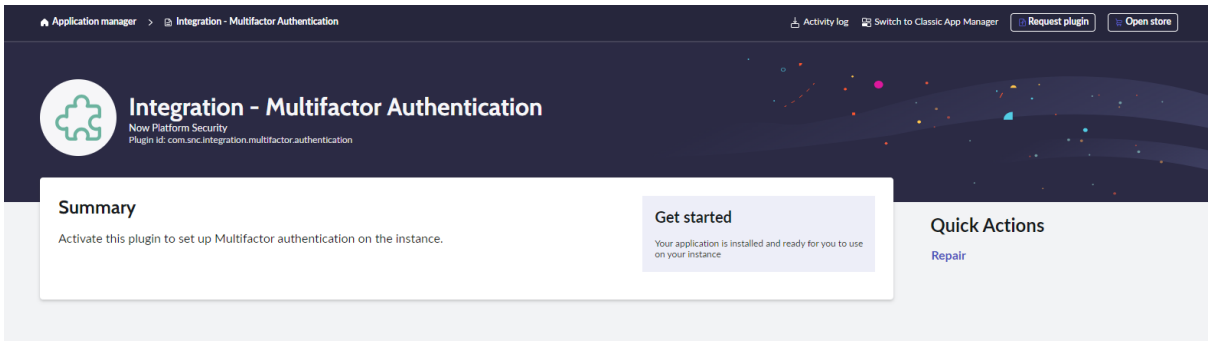
ServiceNow supports various MFA methods, including:

- **SMS-Based OTP**: One-time password sent via SMS.
- **Email-Based OTP**: One-time password sent via email.
- **TOTP Apps**: Time-based One-Time Password applications like Google Authenticator or Authy.
- **Push Notifications**: Using apps like Duo Mobile for approval requests.

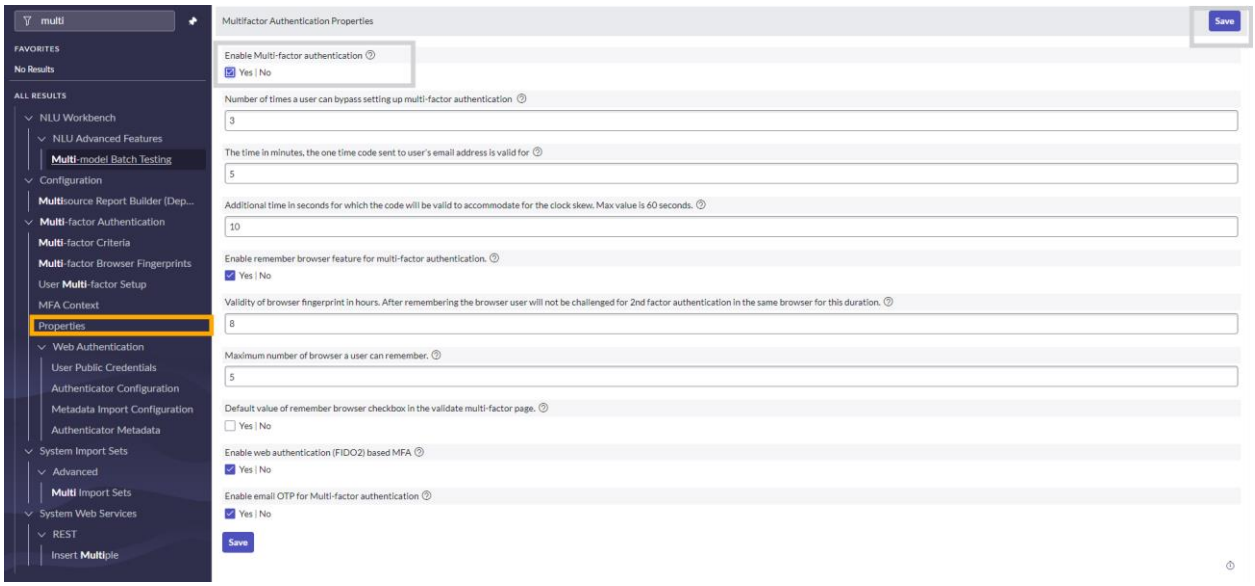
5. Implementation Steps

A. Enabling MFA in ServiceNow

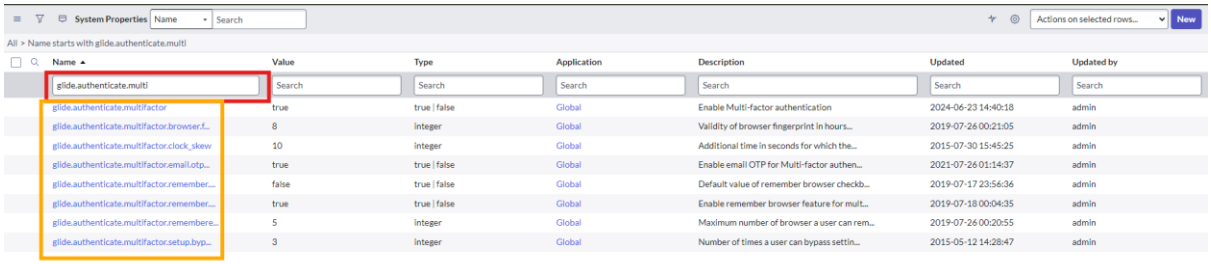
1. **Enable required plugin:**
    - Enable " Integration Multifactor Authentication" Plugin from Application manager



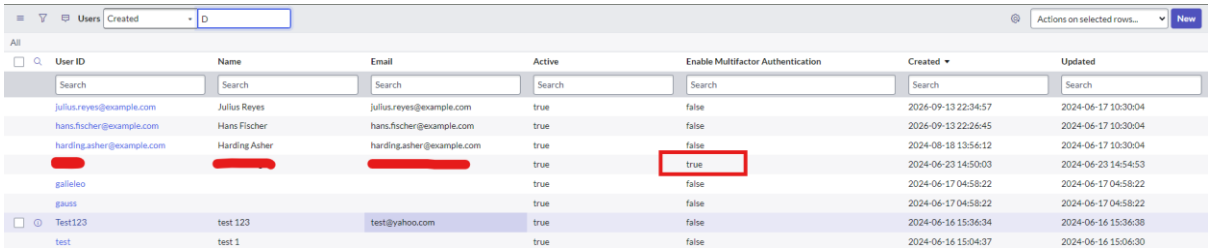
2. **Navigate to the Multi-Factor Authentication Settings**:
    - Go to `Multi-Factor Authentication > Settings` in the ServiceNow instance.
    - Toggle the MFA option to enable it for your instance.
    - Choose the desired MFA methods (SMS, Email, TOTP, Push Notifications).



3. **Activate all multifactor Authentication Properties:**
    - Go to sys_properties table and search for "glide.authenticate.multi"

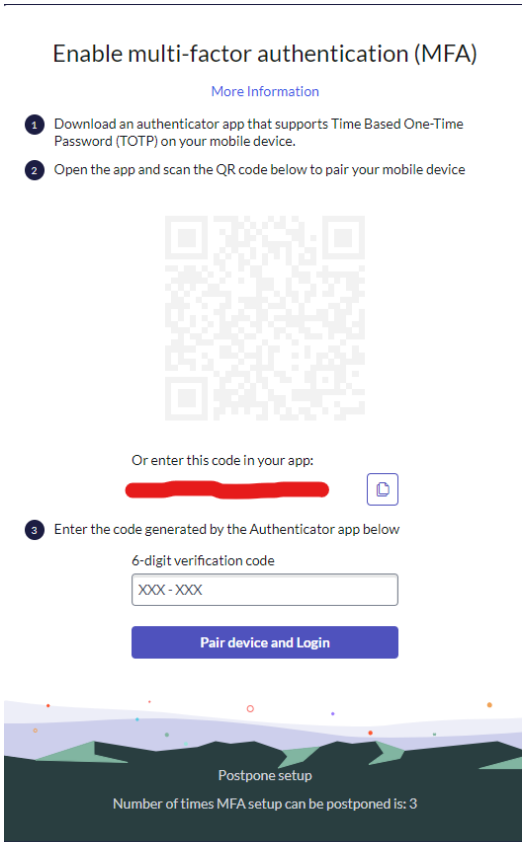


- Make sure to Enable multifactor authentication to user in user table

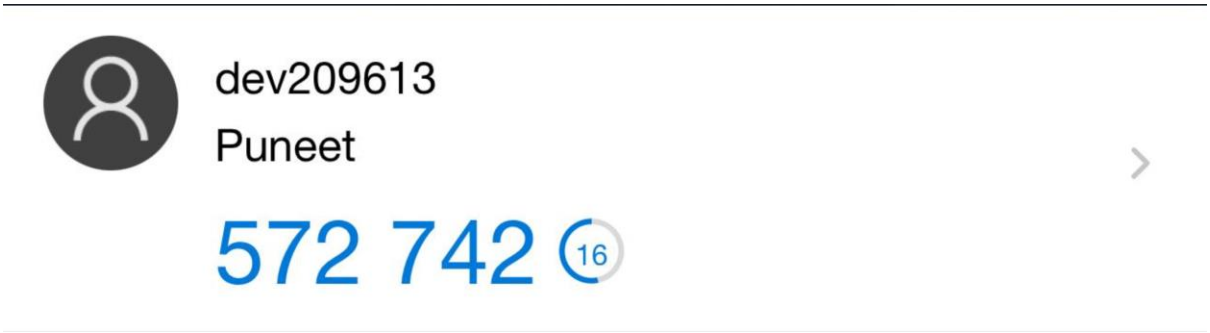


4. Configuring Multifactor authentication:

- Once user log back to another session it will pop up to create a multifactor Authentication to user.

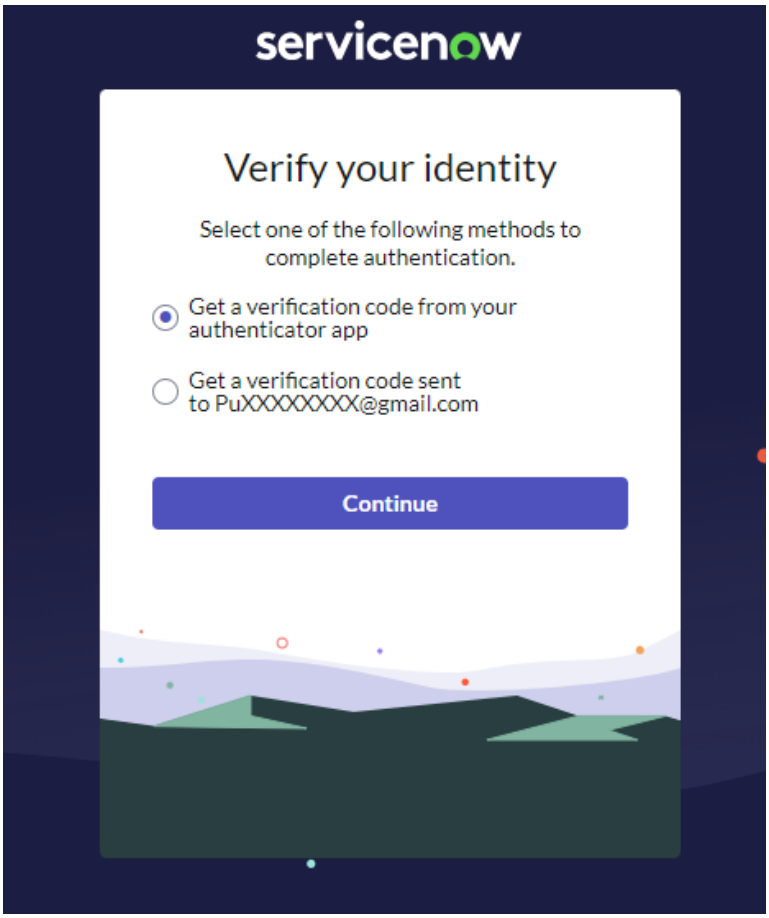


- Using above example user can use multifactor authentication application or OTP.

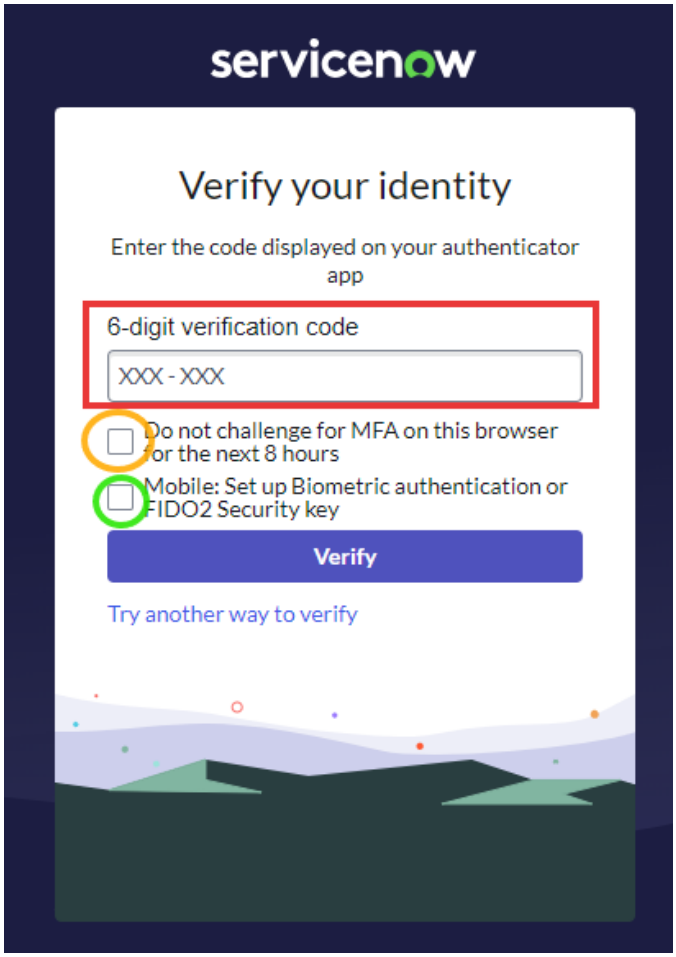


- As shown above You will receive TOPT from the authenticator application which will secure your instance more

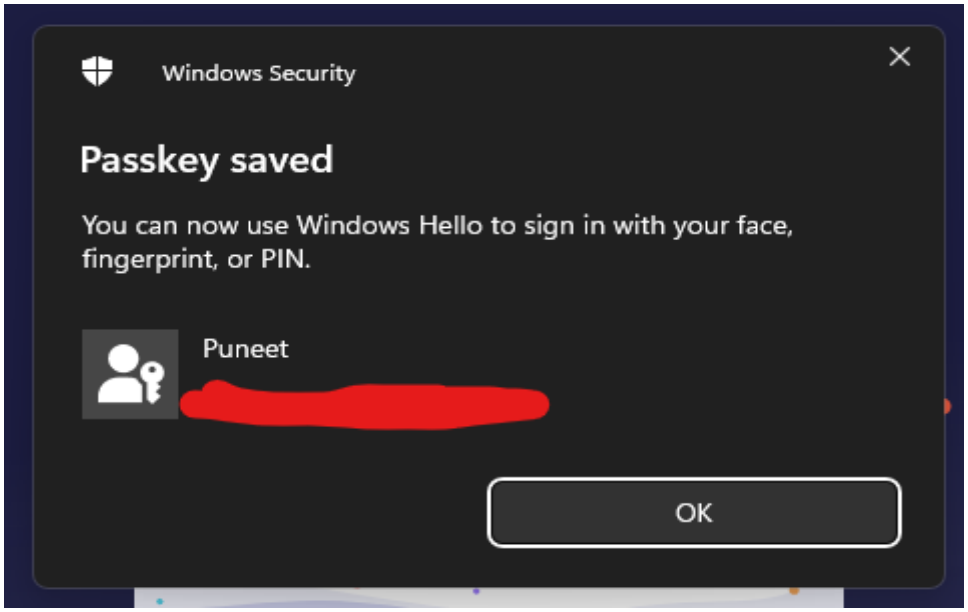
5. **Logging in with Multifactor Authentication:**
   - Once user login It will provide opportunity to choose the authentication method if more then 1 type of authentication option are there



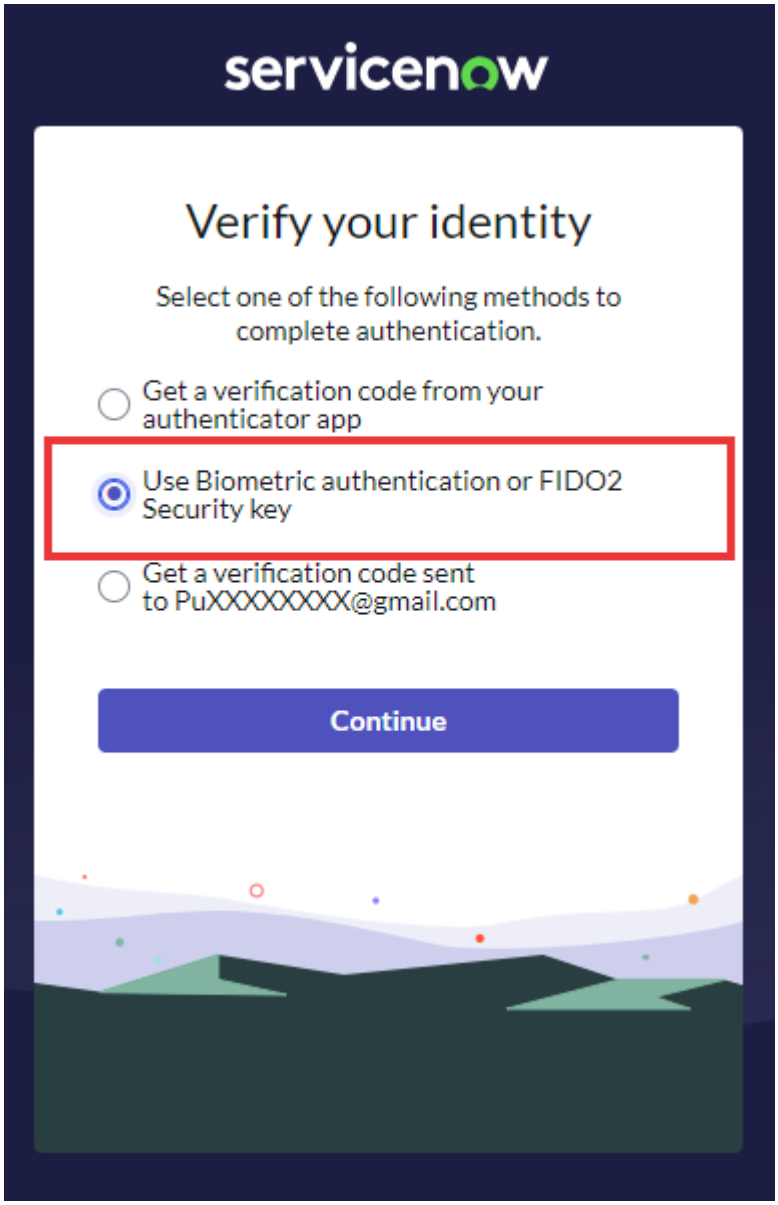
   - Once you have selected type of authentication it will move to seps to insert generated 6-digit code



- As shown in above screenshot it will ask you to skip the MFA for next 8hr and user can enable biometric or face unlock on their device based on the requirement.



- In case of enrolling device for Biometric MFA on that case new option will be visible to authenticate user



B. Testing the Implementation

1. **Test User Logins**:
   - Log in with a test user account to verify MFA prompts.
   - Ensure that the selected MFA methods are functioning as expected.
2. **Review Logs**:
   - Check `Multi-Factor Authentication > Logs` for any issues or errors during login attempts.

6. Best Practices

- **Backup Codes**: Provide backup codes for users in case they lose access to their MFA device.
- **User Training**: Educate users on the importance of MFA and how to use it effectively.

- **Regular Audits**: Conduct regular security audits to ensure compliance and effectiveness of MFA.
- **Policy Updates**: Keep MFA policies updated based on evolving security needs.

Multi-Factor Authentication (MFA) in ServiceNow: Implementation Guide

Table of Contents

1. Introduction

Multi-Factor Authentication (MFA) enhances the security of user logins by requiring multiple forms of verification. Implementing MFA in ServiceNow ensures that only authorized users can access the system, thereby safeguarding sensitive data and applications from unauthorized access.

2. Benefits of MFA

- **Enhanced Security**: Reduces the risk of compromised credentials.
- **Compliance**: Helps meet regulatory requirements.
- **User Confidence**: Boosts trust by protecting user data.
- **Risk Mitigation**: Decreases the likelihood of security breaches.

3. Prerequisites

Before implementing MFA in ServiceNow, ensure the following:

- An active ServiceNow instance with admin access.
- A compatible identity provider (IdP) that supports MFA.
- Users' devices configured for receiving MFA tokens (e.g., mobile phones for SMS, authentication apps).

4. MFA Methods Supported in ServiceNow

ServiceNow supports various MFA methods, including:

- **SMS-Based OTP**: One-time password sent via SMS.
- **Email-Based OTP**: One-time password sent via email.
- **TOTP Apps**: Time-based One-Time Password applications like Google Authenticator or Authy.
- **Push Notifications**: Using apps like Duo Mobile for approval requests.

5. Implementation Steps

A. Enabling MFA in ServiceNow

1. **Navigate to the Multi-Factor Authentication Settings**:
   - Go to `Multi-Factor Authentication > Settings` in the ServiceNow instance.
2. **Enable MFA**:
   - Toggle the MFA option to enable it for your instance.
3. **Select MFA Methods**:
   - Choose the desired MFA methods (SMS, Email, TOTP, Push Notifications).

B. Configuring Identity Providers

1. **Integrate Identity Provider**:
   - Go to `Multi-Provider SSO > Identity Providers`.
   - Click `New` to add an identity provider.
   - Fill in the required fields such as Name, URL, and Client ID.
   - Configure the identity provider to support MFA.
2. **Configure SAML 2.0 Settings**:
   - Set up SAML 2.0 settings for authentication.
   - Ensure that the `AuthnContextClassRef` is set to require MFA.

C. Setting Up MFA for Users

1. **User Enrollment**:
   - Users need to enroll their devices for MFA.
   - Navigate to `Self-Service > Multi-Factor Authentication Enrollment`.
   - Follow the prompts to register the device (e.g., scan QR code for TOTP).
2. **Assign MFA Policies**:
   - Go to `Multi-Factor Authentication > Policies`.
   - Create and assign policies to users or groups to enforce MFA.

D. Testing the Implementation

1. **Test User Logins**:
   - Log in with a test user account to verify MFA prompts.
   - Ensure that the selected MFA methods are functioning as expected.
2. **Review Logs**:
   - Check `Multi-Factor Authentication > Logs` for any issues or errors during login attempts.

6. Best Practices

- **Backup Codes**: Provide backup codes for users in case they lose access to their MFA device.
- **User Training**: Educate users on the importance of MFA and how to use it effectively.
- **Regular Audits**: Conduct regular security audits to ensure compliance and effectiveness of MFA.
- **Policy Updates**: Keep MFA policies updated based on evolving security needs.

7. Troubleshooting

- **Device Sync Issues**: Ensure the user's device clock is synchronized for TOTP.
- **Connectivity Problems**: Verify that there are no network issues affecting SMS or push notifications.
- **User Enrollment**: Assist users in enrolling their devices correctly and troubleshooting common issues.

8. Conclusion

Implementing MFA in ServiceNow is a crucial step towards securing your organization's sensitive information. By following the outlined steps and best practices, you can ensure a smooth and effective deployment of MFA, enhancing the overall security posture of your ServiceNow instance.