ivanti | Identity Director

Password Reset Guide

Version 2019.0

Disclaimer

While care has been taken by Ivanti to ensure that the information contained in this document is correct and complete, it is possible that this is not the case. Ivanti provides the information "as is", without any warranty of any kind. To the maximum extent permitted by applicable law, Ivanti is not liable for any damage which has occurred or may occur as a result of or in any respect related to the use of this information. Ivanti may change or remove this document at any time without notice and shall not be responsible for any consequence(s) arising therefrom. Ivanti is not responsible for any contributions by third parties to this information.

Contents

Chapter 1: Introduction

Passwords are one of the most common forms of authentication in the world. Passwords are easy, require little training and present few technical challenges. However, passwords are also very prone to user error and can present one of the most expensive support burdens in an IT environment. With Ivanti Identity Director, you can enable users to reset their Active Directory password from the sign in page of the Ivanti Identity Director Web Portal and the log on page of Microsoft Windows. This reduces the number of help desk password tickets and enhances productivity of the user.

This document describes how to enable password resets in Ivanti Identity Director, based on three scenarios:

- By using a private e-mail address of the user.
- By using security questions.
- Optionally, you can add verification code validation in scenario 1 and 2. This adds an extra check to authenticate the user who requests a password reset.

More information

You can find more documentation at https://www.ivanti.com/support/product-documentation

- **Ivanti Identity Director Administration Guide**: This document provides detailed information about the installation and configuration of Ivanti Identity Director features and components. http://help.res.com/IdentityDirectorAdminGuide10.

- **Getting Started with Ivanti Identity Director**: This document describes how to configure a basic Ivanti Identity Director environment. https://help.ivanti.com/iv/help/en_US/iid/2019/GetStarted/Content/LandingPageGS.htm

Ivanti Support: If you experience difficulties with any of our products, you may find the solution in our Knowledge Base or you can contact Ivanti Support directly.

Chapter 2: Prerequisites

- An Ivanti Identity Director 2018.3 or newer environment.
- An Ivanti Password Director 2018.3 or newer environment.
- An Ivanti Automation 2018.3 or newer environment.

For more information about Ivanti Identity Director and Ivanti Automation see:

- The **Ivanti Identity Director Administration Guide**, available at https://help.ivanti.com/iv/help/en_US/iid/2019/Administration/Content/LandingPage.htm
- The Ivanti Identity Director Password Reset help available at https://help.ivanti.com/iv/help/en_US/iid/2019/PWDReset/Content/LandingPage.htm
- The **Ivanti Automation Administration Guide**, available at https://help.ivanti.com/res/help/en_US/IA/2019/Admin/Content/25602.htm

Other prerequisites

- Install PowerShell 1.0 or higher on the device that runs the Ivanti Automation Agent that executes the Run Book to reset Active Directory passwords.
- Install the Identity Director Windows Client on all devices on which you want to enable users to reset their password from the Windows logon screen.
- Configure **Ivanti Automation Integration** in Ivanti Identity Director to enable services to invoke Run Books (in the Management Portal at **Setup > Ivanti Automation**).
- This document comes with preconfigured Building Blocks that make it easier to apply the password reset functionality: the Building Blocks **Password reset for Ivanti Identity Director** and **Password reset for Ivanti Automation**.
- Sending verification codes via SMS services requires SMS integration. In addition, the mobile phone numbers of your users to which the verification is sent must be registered in the Ivanti Identity Director environment (e.g. as a people attribute). SMS integration is not covered in this document.

Chapter 3: Import the Building Blocks

Before you implement any of the password reset scenarios, you need to import the Building Blocks that accompany this document in Ivanti Identity Director and Ivanti Automation. This makes it easier to implement the scenarios.

Ivanti Identity Director

1. In the Management Portal, import the Building Block **Password reset for Ivanti Identity Director**.
2. Select all items and click **Import**.
3. In the **Import Building Block** page, select the following options and continue with the wizard:
   - **Overwrite existing items**
   - **Include images**
4. This will import 5 new services, including the relevant people identifiers and people attributes:
   - *E-mail registration for password reset*
   - *Security Questions for password reset*
   - *Reset password and mail a new one*
   - *Reset password based on user input*
   - *Generate and send verification code*

Ivanti Automation

1. In the Ivanti Automation Console, import the Building Block **Password reset for Ivanti Automation**.
2. Select all items and click **Import**.
3. When prompted, provide input for two Run Books, *Password Reset* (used in scenario 1) and *Set New Password* (used in scenario 2):
   - **RunBookWho**: Specify the name of the Agent that will execute the Run Book.
   - **Domain**: Specify the NETBIOS name of the domain in which the password reset will be performed.
   - **DomainController**: Specify the NETBIOS name of the domain controller that will perform the password reset.
   - **Username and Password**: Specify the credentials of an account with permissions to reset Active Directory passwords. Use the format “NETBIOS domain name\username”.

Chapter 4: Scenario 1: E-mail

In this scenario, users can reset their Active Directory password via their private e-mail address. In this scenario, a new password will be generated automatically.

Sign up for password resets

Before users can reset their password, they need to sign up for password resets by registering a private e-mail address. If the privacy policies of your organization prohibit this, please implement scenario 2. This enables password resets via security questions.

1. The user requests the service that signs up for password resets.
2. The user provides a private e-mail address.
3. The user receives a confirmation e-mail at this address.
4. After confirmation, the e-mail address is registered for password resets.

Perform password resets

After registration, users can reset their password.

1. The user clicks the **Password Reset** link.
2. The user identifies him/herself.
3. The user receives a confirmation e-mail at a private e-mail address.
4. A service automatically generates a new password.
5. The user receives this password at the private e-mail address, after which he or she can sign in again.

4.1 Configure the service that registers a private e-mail address

1. In the Management Portal at **Service Catalog**, open the service **E-mail registration for password reset**.
2. On the **Properties** tab, select **Enable transactions**.
3. On the **Attributes** tab, adjust the service attributes **E-mail server** and **Noreply** to your situation.
4. On the tab **Workflow > Delivery**, edit the **Confirm Transaction** action.
5. On the **E-mail settings** tab, adjust the **User name** and **Password** fields to your situation.
6. Save the changes to the service.

4.2 Configure the service that generates and e-mails a new password

1. In the Management Portal at **Service Catalog**, open the service **Reset password and mail a new one**.
2. On the **Properties** tab, select **Enable transactions**.
3. On the **Attributes** tab, adjust these service attributes to your situation:
   - **@NoReply**: Specify the address from which the password reset e-mails will be sent.
   - **E-mail Server**: Specify the SMTP server that will send these e-mails.
   - **Identity Director Web Portal**: Specify the URL of your Web Portal.
   - If your Active Directory Password Policy exceeds the default complexity requirements of the service, you may need to change the values of the service attributes that specify this behavior:
     - **ComplexityLevel**:
       - **H**: High (Alphabet Upper/Lower Case, Numbers and Diacritics). This is the initial value.
       - **L**: Low (Alphabet Upper/Lower Case)
       - **M**: Medium (Alphabet Upper/Lower Case and Numbers).
     - **Password Length**: The initial value is 7.
4. On the tab **Workflow > Delivery**, edit the **Confirm Transaction** action.
5. On the **Properties** tab, optionally specify a different expiration time. When the user requests the service, a confirmation request will be sent to the user's private e-mail address. By default, the user needs to confirm this request within 5 minutes.
6. On the **E-mail settings** tab, adjust the **User name** and **Password** fields again to your situation.
7. Save the changes to the service.

4.3 Configure the Password Reset settings

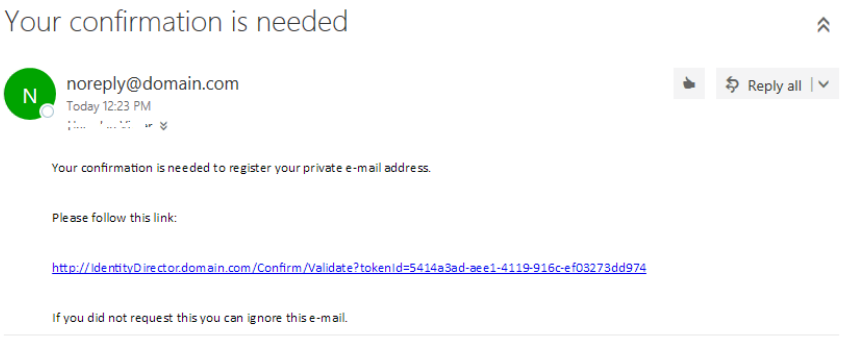
1. In the Management Portal, click **Setup > Password Reset**.
2. On the **General** tab, select **Windows logon screen**, **Web Portal logon screen** and **Include captcha validation**. Captcha validation provides additional security to validate users.
3. Optionally, in the **Reset link text** field, customize the text of the password reset link. The default text (*Password Reset*) is available in all supported languages on the Web Portal.
4. In the **People identifier** field, select **Windows user account**. If configured in your environment, you can select other people identifiers.
5. Click the browse button in the **Service** field.
6. In the **Select Service** pane, select the service **Reset password and mail a new one** and click **OK**.
7. Optionally, in the **User instructions** and **Status page message** fields, provide additional information for the user.
8. Optionally, in the **Redirection URL** field, specify a URL of choice after a password reset, rather than the default Identity Director sign-in page. In certain scenarios, for example when users access the Identity Director from a thin client, redirecting them to the default page may not be user-friendly. By specifying a URL of choice, you can prevent scenarios like these.
9. In the **Password input** field, select **Provided through service workflow**.
10. On the **Security Questions** tab, set the number of security questions to 0.
11. On the **Verification Code** tab, disable **Verification code validation**.
12. Save the changes.

You have now configured password resets via e-mail.

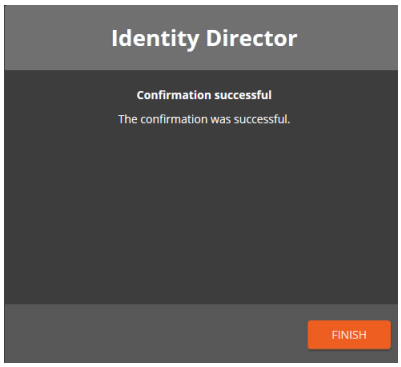
4.4 Testing

Web Portal

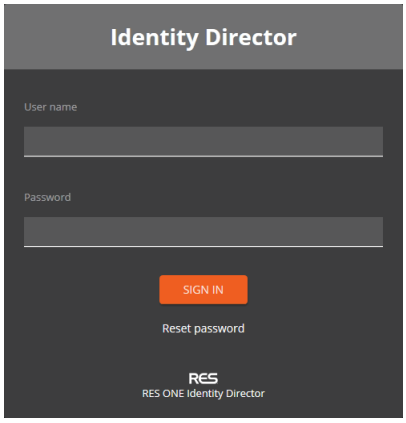
1. Sign in to the Web Portal.
2. In **My Store**, request the service **E-mail registration for password reset**.
3. When prompted, provide a private e-mail address and click **OK**.
4. Ivanti Identity Director will send a confirmation link to the private e-mail address.



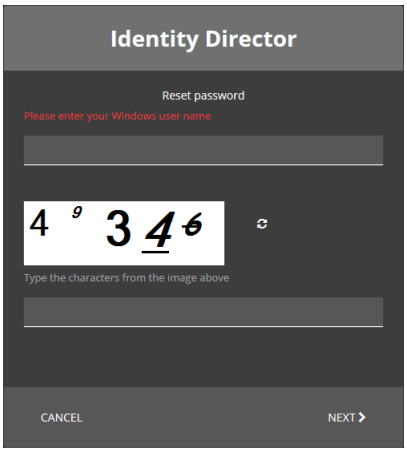
5. Click the confirmation link. Upon successful confirmation, the following page is shown in the Web Portal:



6. Click **Finish** and sign out from the Web Portal.
7. The sign in page of the Web Portal contains a **Reset Password** link:

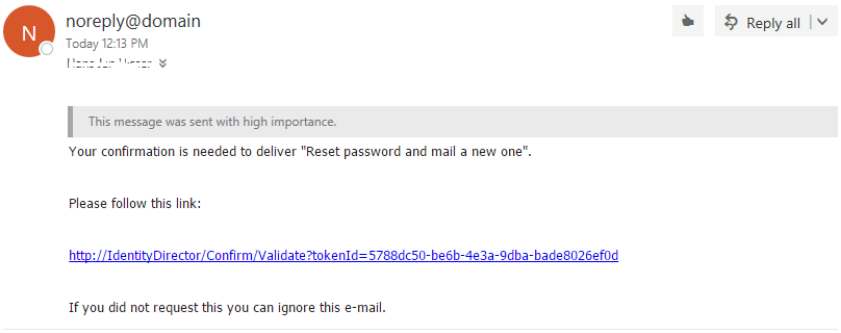


8. Click the link and provide identification for the test user:

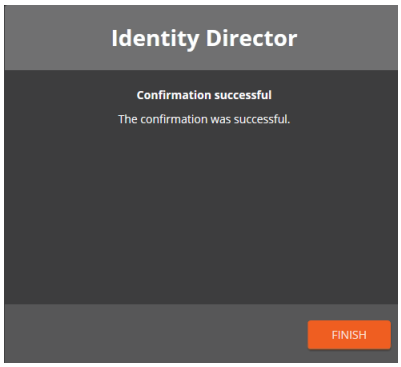


9. Specify the Windows (Active Directory) user account of the test user.
10. Type the captcha characters shown and click **Next**.

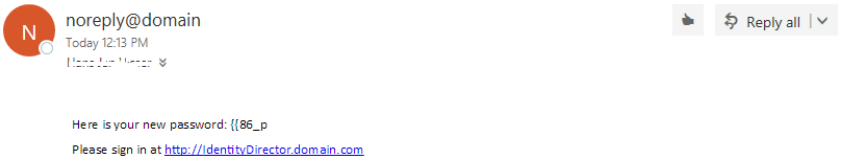
11. Upon successful identification, Ivanti Identity Director will send a confirmation link to the private e-mail address.



12. Click the confirmation link. Upon successful confirmation, the following page is shown in the Web Portal:



Ivanti Automation will perform the actual password reset. The new password will be e-mailed to the user's private e-mail address. You can use this password to sign in to the Web Portal.



Windows

In this scenario, users can reset their password from the Windows logon screen.

1. Click **Reset Password** in the upper right corner of the logon screen.
2. Specify the Windows (Active Directory) user account of the test user.
3. Upon successful authentication, a confirmation link will be sent to the private e-mail address.

Ivanti Automation will perform the actual password reset. The new password will be e-mailed to the user's private e-mail address. You can use this password to log on to Windows.

Chapter 5: Scenario 2: Security questions

In this scenario, users can reset their password via security questions. In this scenario, a new password is provided by the user.

You can choose to adapt the scenario slightly and have the password generated automatically, after which it is send to a private e-mail address. This requires that users also register their private e-mail address.

Sign up for password resets

Before users can reset their password, they need to sign up for password resets by registering security questions and their answers.

1. The user requests the service that signs up for password resets.
2. The user selects security questions and provides answers.
3. These questions and answers are registered for use with password resets.

Perform password resets

After registration, users can reset their password.

1. The user clicks the **Password Reset** link.
2. The user identifies him/herself.
3. The user provides answers to the security questions.
4. The user provides the new password.
5. A service resets the password to the new one, after which the user can sign again.

5.1 Configure the service that registers the security questions

1. In the Management Portal at **Service Catalog**, open the service **Security Questions for password reset**.
2. On the **Properties** tab, select **Enable transactions**.
3. Save the changes to the service.

5.2 Configure the service that resets the password based on user input

1. In the Management Portal at **Service Catalog**, open the service **Reset password based on user input**.
2. On the **Properties** tab, select **Enable transactions** and clear all other options.
3. Save the changes.

If you configure a custom service that resets the user password via service questions, after which users can choose their own password, its workflow needs to include a **Provide Information** action that asks for user input for the new password.

5.3 Configure the Password Reset settings

1. In the Management Portal, click **Setup > Password Reset**.
2. On the **Properties** tab, select **Windows logon screen**, **Web Portal logon screen** and **Include captcha validation**. Captcha validation provides additional security to validate users.
3. Optionally, in the field **Reset link text**, customize the text of the password reset link. The default text (Password Reset) is available in different languages on the Web Portal.
4. In the **People identifier** field, select **Windows user** account.
5. Click the browse button in the **Service** field.
6. In the **Select Service** pane, select the service **Reset password based on user input** and click **OK**.
7. In the **Password input** field, select **Wizard to include a page for end user to provide input**.
8. In the **Password attribute** field, specify the service attribute that can store the password that is provided by the user, in this case **Password**.
9. In the **Password complexity hints** area, configure a password complexity policy. This ensures that passwords provided by your users meet the complexity requirements of your organization. See also the example below.
    - Use the **Regular expression** field to configure the regular expression that determines the password complexity requirements. In the Web Portal, the provided password by the user will be validated according to this regular expression.
        - When you configure a regular expression, you can add flags to the pattern.
        - You can split complex rules in multiple rules, to make it easier to configure the desired policy.
        - Use the **Test** field to verify the regular expression. Green and red coloring indicate whether the text field is conform the configured regular expression.
    - Use the **Password complexity hints** field to provide users with information about the characteristics of the new password. In the Web Portal and Windows Client, if the provided password matches a regular expression, the related complexity hint will be marked.
10. In the **Security questions** field, select the number of questions that will be asked to the user. This is the maximum number of security questions the users will have to provide answers to. Normally, each user should define more questions and answers than the number specified here; if they do, each time they go through the password reset wizard, the questions they need to answer will be picked randomly. This increases security.

11. On the **Verification Code** tab, disable **Verification code validation**.
12. Save the changes.

You have now configured password resets via security questions.

Example

When you configure the password reset functionality, you can configure a password complexity policy, for example a password that matches the password complexity rules as determined by Microsoft Active Directory.

You can split complex rules in multiple rules, to make it easier to configure the desired policy. For example:

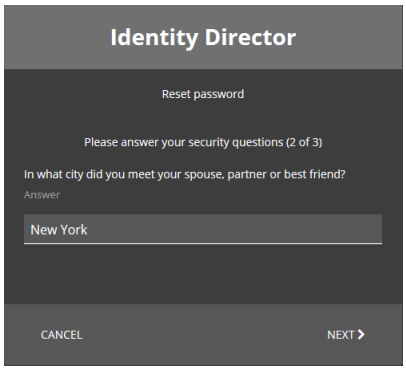
Regular expression	Password complexity hint
^(?=.*[`~!@#$%^&*()_+{}|\]["':;\'?><,./])	Specify one special character
^(?=.{8,12}$)	Specify 8 to 12 characters
^(?=.*\d)	Specify one numeric digit
^(?=.*[a-z])	Specify one lower case character
^(?=.*[A-Z])	Specify one upper case character

See also

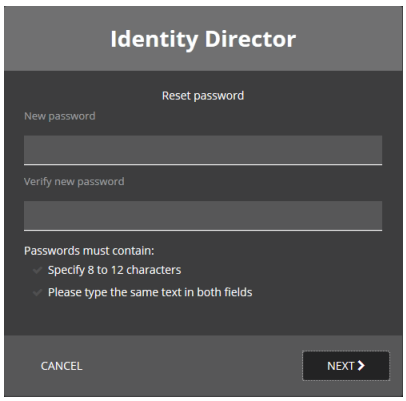
- https://msdn.microsoft.com/en-us/library/ff650303.aspx

5.4 Testing

1. Sign in to the Web Portal.
2. In **My Store**, request the service **Security Questions for password reset**.
3. When prompted, select the security questions, provide their answers and click **OK**.
4. Ivanti Identity Director will now register the security questions and answers, so they can be used for password resets. You can check this in the Management Portal, on the **Attributes** tab of the person page.
5. Sign out from the Web Portal.
6. On the sign in page, click **Reset Password**.
7. Specify the Windows (Active Directory) user account of the test user.
8. Type the captcha characters shown and click **Next**.
9. Provide the answers to the security questions that you configured earlier:



10. When prompted, provide the new password and click **Finish**.



Ivanti Automation will perform the actual password reset and change the Active Directory password to the one provided. You can use this password to sign in to the Web Portal.

You can also test this scenario from the Windows logon screen, in which the password reset works similarly as described above.

Chapter 6: Scenario 3: Verification code validation

Optionally, you can add verification code validation to password resets. This ensures that password resets can occur as secure as possible.

In this scenario, the verification code will be sent via SMS. This requires SMS integration (not covered in this document).

- Configure a Run Book that can send text messages via SMS to a user. The mobile phone number of your users must be known in your Ivanti Identity Director environment, for example stored in a people attribute **Mobile Phone**.
- Include parameters for:
  - The people attribute that holds the mobile phone number of the subscriber to the service.
  - The service attribute that generates the verification code.

Perform password resets with verification code validation

Verification code validation adds an extra check to authenticate the identity of the user who requests a password reset.

1. The user clicks the **Password Reset** link.
2. The user receives an e-mail or SMS with a verification code.
3. The user provides the verification code.
4. After confirmation, the password is reset according to the scenario you implemented.

6.1 Configure the service that sends a verification code

1. In the Management Portal at **Service Catalog**, open the service **Generate and Send Verification Code**.
2. On the **Properties** tab, select **Enable transactions**.
3. On the **Workflow** tab, add an **Invoke Run Book** action after the **Set Service Attribute** action. In this scenario, the specified Ivanti Automation Run Book in this action will be used to send an SMS with the validation code to the user. You need to configure this Run Book in Ivanti Automation first. Alternatively, you can use a regular **Send Message** action for this purpose, and have the verification code send by e-mail.
4. On the **Run Book Parameters** tab, link the relevant Run Book parameters to the people attribute `#Subscriber[Mobile Phone]` and the service attribute `#Service[Verification Code]`.
5. Click **OK** and save the service.

6.2 Configure the Password Reset settings

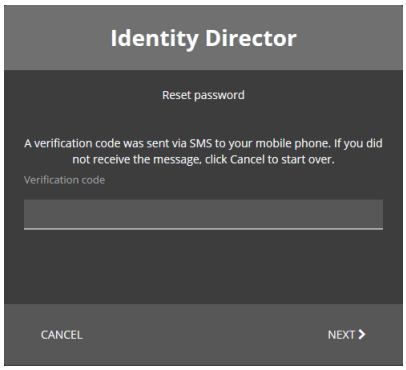
1. In the Management Portal, click **Setup > Password Reset**.
2. Configure the functionality as usual.
3. On the **Verification Code** tab, enable **Verification Code Validation**.
4. In the **Service** field, select the service **Generate and send verification code**.
5. Optionally, select **Limit the number of attempts** to limit the number of attempts a user can make to provide a verification code during a password reset.
   - In the **Maximum number of attempts** field, configure the maximum number.
     - You can configure a number from 1-999. If the user exceeds the limit, the workflow action in the service that validates the verification code will fail.
6. Optionally, adjust the texts in the other **Verification Code Validation** fields to your situation.
7. Save the changes.

You have now added verification code validation to your configuration.

6.3 Testing

Sign in to the Web Portal.

1. On the sign in page, click the **Reset password**.
2. Specify the Windows (Active Directory) user account of the test user.
3. Type the captcha characters shown and click **Next**.
4. Provide the verification code that was sent via SMS:



5. Click **Next**.

The verification code will be validated. If this is successful, the password reset will continue as configured in the scenario that you chose.

Chapter 7: Where to go from here?

- Many more scenarios are possible than the scenarios explained in this document. Consider:
  - Adding an approval step before users can reset their password
  - Delegating the permission to reset passwords for other users
  - Recovering a lost user account name
  - Just unlocking a user account (versus generating a new password)
- If you only support password resets from the Web Portal, we recommend that users should not be required to change their password at next logon: this disallows users to sign in.
- When you configure the Ivanti Automation Run Books, you may want to consider using variables instead of parameters. The advantage of this is that you only need to set the values once in the **Variables** node, after which they are automatically created.