Knowledge Base Article 00895

Verification Procedure

Updated Monday June 1, 2020

All customers must be verified before any changes are made to their account. This includes any changes to services like passwords, usernames and emails, two-factor authentication, security questions, voicemail passwords and access, or any service where the customer needs to verify themselves to use.

In this article:

Prerequisites

Customers must have an account in order to be verified.

Automatic Escalations

1. If the customer's account does appear in the public directory or information management directory, but they believe they have an account, escalate to Tier 2 Accounts. If the customer is unsure whether they have an account, escalate to Human Resources.
2. If the customer cannot be verified and cannot visit a walk-in location, escalate to Tier 2 Accounts.

Procedure

1. Identify the customer's person type according to Table 1.

Person Type	Verification Procedure
Manager, Supervisor, Executive, or any customer with access to HIPPA confidential information on their device	Verify using three methods, one of which must be either call back or video verification. Middle initials and employee ID numbers may not be used for verification of this person type.
Employee, Retired Employee, Intern, Part-time Employee	Verify using three types of verification. Middle initials and employee ID numbers may not be used for verification of this person type.
Incoming Employee or Intern	Verify using three types of verification.
External Client or Customer	Verify using two types of verification.

Table 1

2. Search for the customer's account in the information management directory and verify them using the following according to their person type:
    a. Employee ID number
    b. Call back at a phone number on file
    c. Date of birth
    d. Shared secret or security questions
    e. Suppressed information such as a phone number, alternate email address, or mailing address
        i. Note this can only be used if information is suppressed and not available in the public directory
    f. Last four digits of social security number
    g. Middle initial or name
    h. Direct the user to a walk-in location
    i. Video verification with government issued photo ID
3. After verifying the customer, refer to the appropriate KB article to complete their request.

Troubleshooting

1. The customer does not have enough information to verify or cannot be verified
    a. Direct the customer to a walk-in location
    b. If that is not possible, escalate to Tier 2 Accounts.
2. The customer gives multiple incorrect answers to verification questions or is suspicious

    a. Use discretion when verifying customers. If the customer appears suspicious, you may refuse to verify them or escalate to Tier 2 Cybersecurity.
3. Someone else is attempting to change information on behalf of another user or on an account that is not their own
    a. If the account is a collaborative account, confirm that the customer is the contact listed on the collaborative account. If they are, they may be verified and account information may be changed.
        i. If the customer is someone other than the listed contact, inform the customer that the listed contact will need to call in instead to be verified.
    b. If the customer wants to change another user's account on their behalf, the customer will need to provide four methods of verification before any account information may be changed.
4. The customer's account has been deactivated or their verification information is not available
    a. Escalate to Tier 2 Accounts.

Escalations

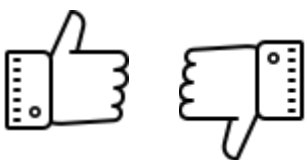
1. If the issue is related to the customer's account information, verification, or other account issues, escalate all incidents to Tier 2 Accounts.
2. If the issue is related to security concerns or suspicious customers escalate all incidents to Tier 2 Cybersecurity.
3. If the customer does not have an account and would like one, escalate to Human Resources.

Related KB Articles

Password Reset
Two Factor Authentication Updates

Give your feedback on this article

Was it helpful?



Knowledge Base Article 00896

Password Reset

Updated Monday May 21, 2020

Passwords for email accounts and employee logins can be changed by both customers and the service desk. All customers must be verified according to the Verification Procedure KB article.

In this article:

Prerequisites

Customers must have an active account to perform a password reset and they must have a device with a working internet connection.

Automatic Escalations

1. Customer wants to reset password due to a potential security concern
    a. Escalate to Tier 2 Cybersecurity
2. Customer cannot be verified, temporary password does not work, customer's account has been deactivated or suspended
    a. Escalate to Tier 2 Accounts

Procedure

1. Open a contact in ITSM and collect a callback number and email address or employee ID number.
2. Search for the customer's account in the information management directory.
3. Identify the customer's person type according to Table 1 in the Verification Procedure KB article and verify the customer.
4. In the admin tab of the information management directory, select the option for password reset.
5. Click the 'generate' button to generate a temporary password. Read this password out to the customer using the phonetic alphabet.

6. If possible, have the customer try to login with the temporary password over the phone to confirm they are able to login.
7. Inform the user that upon login, they will be asked to reset their password and that the temporary password will expire after 24 hours. New passwords must be at least 16 characters long and must contain one uppercase letter, one lowercase letter, one number, and one special character. Acceptable special characters include: !@#$%^&*()œ∑´®†¥¨ˆøπåß∂ƒ©˙∆˚¬Ω≈ç√∫˜µ

Troubleshooting

1. The customer is hearing impaired and the password cannot be read over the phone
    a. Start an encrypted video call and copy and paste the password into the chat. Never send a password over email.
2. The temporary password does not work for the customer
    a. Try to login to the customer's account in an incognito or private window. If it works, then the issue is likely user error. Confirm that the customer has the password correct or re-read the password. Other fixes could include: clearing the customer's cache and browsing history, connecting to a VPN, or attempting to login using an incognito or private window.
    b. If the password does not work in an incognito or private window, escalate to Tier 2 Accounts.

Escalations

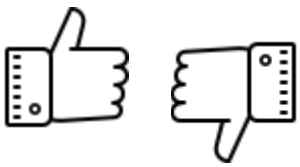
1. If the issue is account related, escalate all incidents to Tier 2 Accounts
2. If the issue is security related or if the customer appears suspicious, escalate to Tier 2 Cybersecurity

Related KB Articles

Verification Procedure
Two Factor Authentication Updates

Give your feedback on this article

Was it helpful?



Knowledge Base Article 00897

Connect to VPN Using Cisco AnyConnect Secure Mobility Client

Updated Monday May 26, 2020

Working remotely often requires the use of a Virtual Private Network (VPN). Cisco AnyConnect Secure Mobility Client is the VPN tool of choice for this organization.

In this article:

Prerequisites

Customers must have an active account to connect to the VPN and must be in front of a device with a strong internet connection.

Automatic Escalations

1. Customer cannot install Cisco AnyConnect Secure Mobility Client because the device is too old and does not support the latest version
    a. If using an organization issued device, collect the device number and callback information and then escalate to Tier 2 Zone and Device Support
    b. If using a personal device, follow the KB article for setting up a native VPN.
2. Customer's credentials do not work for Cisco AnyConnect Secure Mobility Client, even though the credentials are valid.
    a. Escalate to Tier 2 Network and Telecommunications

Procedure

1. Install Cisco AnyConnect Secure Mobility Client from the device's app store. (Macs will use the AppStore and PCs will use the software center or download from the organization's downloads page).
2. Once downloaded open the application and select the correct dropdown option from the following list:
    a. Split Tunnel General Access is typically the correct option unless the customer's department or supervisor has indicated otherwise.

   b. Full Tunnel is used for customers needing general access but that also have confidential and sensitive data stored on their device. Most customers will know if they need to use a full tunnel.
   c. Departmental Pools are used for customers working with information subject to HIPAA or other sensitive information. Most customers will know if they need to be using departmental pools.
      i. If this option is selected, the application will prompt the user to enter the correct address for their department. This should be available to them through their department or supervisor.
3. After selecting the correct drop down option, have the customer enter their credentials.
4. The application should take a few seconds to secure a VPN connection. Once set up, the connection will last until the device is put in sleep mode, turned off, or the VPN is logged out.

Troubleshooting

1. The VPN connection disconnects and reconnects frequently
   a. This is usually due to a poor internet connection.
      i. If the customer is not using the organization's internet, encourage them to do so or have them check their router, ethernet cable, or troubleshoot their WiFi.
      ii. If the customer is using the organization's internet, gather their building and room number and escalate to Tier 2 Zone Support.

Escalations

1. If the issue is account related, escalate all incidents to Tier 2 Accounts
2. If the issue is related to the Cisco AnyConnect Secure Mobility Client application or another issue specific to setting up and connecting to a VPN, escalate to Tier 2 Network and Telecommunications

Related KB Articles
Microsoft Remote Desktop

Give your feedback on this article

Was it helpful?