AccountTECH Security Manual

accounttech

Table of Contents

Threats

List of Security Threats at AccountTECH

Types of threats

The threats to AccountTECH as a company are primarily threats to our clients data and threats to their software provided by us, and the infrastructure that hosts our software. The company's security risks focus is on:

- Risks from actions taken by AccountTECH staff.
- Risks from AccountTECH Programming errors.
- Client data theft or damage.
- Security infrastructure damage from hardware failure.
- Damage from breach allowed by network or software vulnerability.

Data Security Managers

Data security has to be approached from a number of perspectives, so different people at AccountTECH are responsible for different aspects of data security.

Its the job of everybody on the AccountTECH team to assure that no security modification in our infrastructure, network or software is never made without 100% signoff from the following persons in the Security Team:

- AccountTECH Ownership
- AccountTECH Programming
- Network / Cisco Management
- Citrix Management
- Security Consultants

Director of Operations - responsible to make sure that AccountTECH staff does not:

- Print reports of client data.
- Discuss confidential client data with unauthorized persons.
- Allow unauthorized people into the datacenter.
- Use Company computers for any unauthorized purpose.
- Take any client data (printed or digital) offsite.

Director of Programming

- Responsible to keep LIVE client data away from programmers.
- Responsible to keep programmers out of the production environment.
- Make sure all code is subject to security review analysis by VeraCode (or similar).
- Make sure all code undergoes peer review by programming and management.
- Make sure only approved code is loaded into the production environment.

Citrix Vendor

- Responsible to make sure that the Citrix environment has no mechanism that anyone can use (staff, programmers or clients) to download anything from the Citrix network.
- Make sure that the citrix environment is patched for security as needed.
- Make sure redundant Netscalers (client login) are functioning with automatic fail-over for 100% uptime.
- Make sure 2FA is protecting all networks as expected

Firewall Security Vendor

- Make sure that no unauthorized access is allowed into the network .
- Guarantee that no network or firewall or perimeter modifications are ever made without 100% signoff from all the security team members.

- Notify and resolve new and emerging threats to the network.
- Make sure all firewalls are constantly updated with the latest security threat definitions.
- Make sure redundant firewalls are functioning with automatic fail-over for 100% uptime.
- Advise on enhancements to continue to reduce threat vectors.
- Responsible to make sure that no server in the environment allows a web browser to be used to access the internet for anything … especially uploading or downloading data.

Data Protection Rules

AccountTECH rules for protecting client data

Rules for Programming Staff

- Programmers are never allowed access to the production environment (with the exception of administrators who are installing approved software versions). - H need an update on this - is this still the case?
- Programmers are not allowed to work with copies of client databases for software testing unless they are working on a specific work order submitted by a client in writing for custom software development.
- Programmers are required to make sure that both onsite and offsite backups are fully functioning every day.

Rules for AccountTECH Staff (Operations, Training, and Support Departments)

- Staff may not print reports from client software in the office.
- Staff may not reset any users password without explicit instructions from either the Broker or designated Keeper of Passwords.
- Staff may never setup or change individual user access or permissions to different parts of AccountTECH software. Permissions can only be set by the Broker or their designated Keeper of Passwords.

Rules for the AccountTECH Environment to be enforced by the Citrix Security Team

- The network can never allow unauthorized access.
- The network can never allow file download or file upload.
- The network can never allow anyone on staff (except highest level administrators) to open a browser and connect to the internet from any server in the environment.
- The network can never allow any client to open a browser and connect to the internet from any server in the environment.
- Virtual servers or bare metal servers should neve be brought on to the enviorment without being fully patched, updated and with antivirus being installed.

Vendor Responsibility for Application Environment

AccountTECH vendors need to make sure that all AccountTECH software resides in an environment that is protected from attack or breach from unauthorized persons or criminals that could disrupt the use of the application or the privacy of the client data.

Explicitly, vendors will ensure the following:

- No network, configuration, port access, protocol, policy will ever be changed without 100% signoff and approval from every member of the Security Team.
- Firewall threat definitions are up to date.
- Antivirus definitions are up to date.
- Hardware drivers are up to date.
- Operating systems (Citrix, Windows, etc) are up to date.
- QUALSYS scans are showing an A rating for outside security risks.

Business Stability

Keys for Protecting Clients & the Company

Primary Objectives

To protect clients data and preserve both the company and the environment that the clients depend on to run their companies.

Key foundations

- Protect client data from:
  - Theft.
  - Database damage.
- Protect the environment that clients depend on to do their work.
  - Deliver uptime reliability.
  - Protect against external forces that could access and damage the environment.
  - Protect against external forces that could deny access to the environment.
- Protect against software issues the can keep the clients from doing their work or negatively affect their data.
- If we do all of the above, that will protect the company.

Policy Overview

Roles and Responsibilities for Information Security?

Environment security

CEO has role of developing and enforcing policy around environment security.

- Datacenter security performed by Coresite.
- Firewall and traffic security performed by Integris.
- Network security performed by Integris.
- Citrix security performed by Decisive IT Solutions.

The Director of Programming as role of developing and enforcing policy around application development and developers network environment security.

The Director of Operations is responsible for enforcing security policy for all staff working in the support and administrative offices.

Remote Access Overview

Remote access is controlled with the following measures

- Connection must originate from IP address in either USA, Canada or Peru.
- User must have Citrix Workspace installed locally.
- Username / password validation for connectivity to production environment enforced by Citrix via NetScaler.
- Password change policy enforced by Citrix Netscaler technology.
- Citrix license issuance controlled by AccountTECH management.
- 2nd username / password required to access any application within the production environment.
- 2 factor authentication is enforced for all citrix logins

Employee Access

- Programmers should generally never access the production environment.
- Support staff generally should never access the production enviorment, and work only in the application enviorment provided to customers.
- Only employees with the highest level security access can have direct access to the domain controllers.
- Only employees with the highest level security access can create new users.
- Lower security level employees have limited access to update Active Directory passwords using a secure but highly restricted application; ADManageEngine.

Client Database Management

Access to client data

As a general rule, no support staff, office staff or programmers at AccountTECH will have any access to or use of client data. There are a few exceptions:

- Administrators setting up client databases or modifying client databases for a specific maintenance request.
- Administrators researching a data modification that needs to access a historical backup at the written request of a client.
- Administrators modifying client data at their request (typically data imported from the MLS).
- Final production environment testing of software release candidates may only test with copies of client data after obtaining verbal permission to copy clients data for testing a new or enhanced feature requested by the client.

And there are a few general rules

- Client databases should not exist in the Developers network.

Retention of client data

Client data (including client data after termination) is stored on secure backup servers (both on and offsite) and is never deleted.

Change Policy

Software change

1. Client software change requests and internal software change requests and approvals are tracked in AccountTECH's ticketing system.

2. Software change requests get approval / rejected by the CEO with input from senior staff based primarily on these: value of the change to AccountTECH customer base overall, security / privacy of client data, technical difficulty, time/cost needed to execute the change.

3. Change requests are subject to our internal risk score matrix and have to score no greater than 1 to be approved.

4. If approved, the software development goes into the development pipeline.

Network or Environment change

Network or Environment changes are vetted with each of our vendors for threats (or enhancements) that a proposed change would bring to the environment. All 3 systems environment vendors need to be consulted before any change can be ordered:

- Perimeter security vendor
- Networking switch management vendor
- Citrix vendor

All need to approve a network request before it is approved. Final network change requests are only authorized by the CEO.

New Equipment in Production

When installing new servers in production (either virtual or bare metal):

- All patching must be done and antivirus installed before placing the new equipment on the production environment.

Adding Software Tools in Production Environment

Tool analysis only applies to tools deployed in either the production or development networks.

We evaluate the acquisition of any tool (or update of any existing 3rd party tools) we use, in an internal meeting between CEO, The Director of Programming and relevant senior staff. This meeting focuses on business needs and security impact:

1. Easy to install?
2. Easy to maintain?
3. Does it include support ?
4. Does it need admin permissions to run it or not?
5. Does it expose us to security risks or not?
6. Break our security policies?
7. Will the tool impact clients on application performance?
8. Can we get advice to industry experts or users of the tool for their feedback ?

If a software tool is determined to be valuable to the development or production environment, it must be reviewed and signed off on by each of AccountTECH's security advisors. This means that if any tool is deemed to pose a security risk by either our network security vendor (Integris) or our citrix security vendor (Decisive IT solutions), then the tool cannot be deployed in our production or developers environment.

CEO makes final decision whether the use of this tool is approved or not

Acceptable Use

For AccountTECH clients, Acceptable Use is entirely determined by the client. They entirely decide who in their environment has access to what data. Further, they entirely control what is done with their data.

AccountTECH as a company has does not use, aggregate, sell or in any way re-purpose client data.

Database Encryption

Database encryption is required on any password field in any table in any database that stores user passwords.

Database encryption is required on any Tax ID field in any table in any database that stores Company, Agent or Vendor tax ID information - either personal or corporate.

Because AccountTECH provides ACH services and Credit card services through partnerships with merchant services companies, it is not necessary to plan for encryption of this data. AccountTECH will never store ACH or CC data.

Data Access

Data Access by Clients

Client access to the AccountTECH network

Clients using AccountTECH software withing our Citrix environment have no access to directories, folders, drives, etc on the network.

Published application settings in XenCenter control which application a user is connected to at login. This published application connects them to:

1. A specific published application on a specific server in a specific folder
2. Application connectivity to only their own data in a discreet db that contains only their information

There is no application functionality that would allow users to get to the Windows explorer, etc from the published application. Once connected to their AccountTECH software, there is no mechanism thru which a user could access the internet from any AccountTECH server.

AccountTECH will never comingle client data into a single database. Each client has a distinct database that contains only their data.

Drive visibility

By Group policy on all application servers all drives are hidden. If a client was ever to gain access to windows explorer on an AccountTECH application server, it would appear to them that the server had no drives. "This PC" is empty.

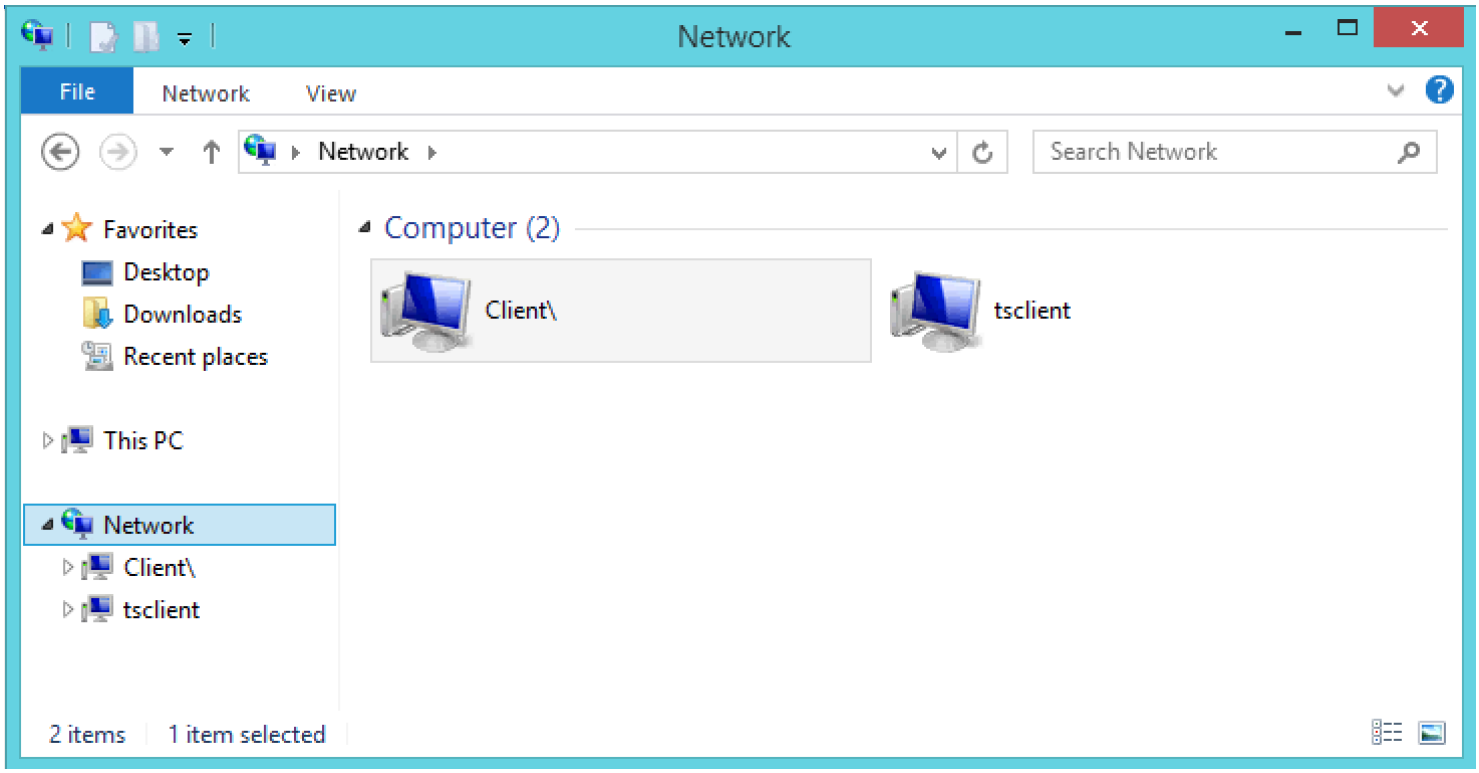
Citrix local drive mapping disabled

A common feature of Citrix is disabled in the AccountTECH environment. Local Drive mapping at login is disabled. Further there is no ability to map to a local drive after login. This prohibits clients (or AccountTECH staff) from being able to copy or download anything from the Citrix production environment to their local machine. This keeps any client datafiles from being download using a Citrix login session. This rule also applies to all AccountTECH Staff at all levels, including senior administrators and senior management.

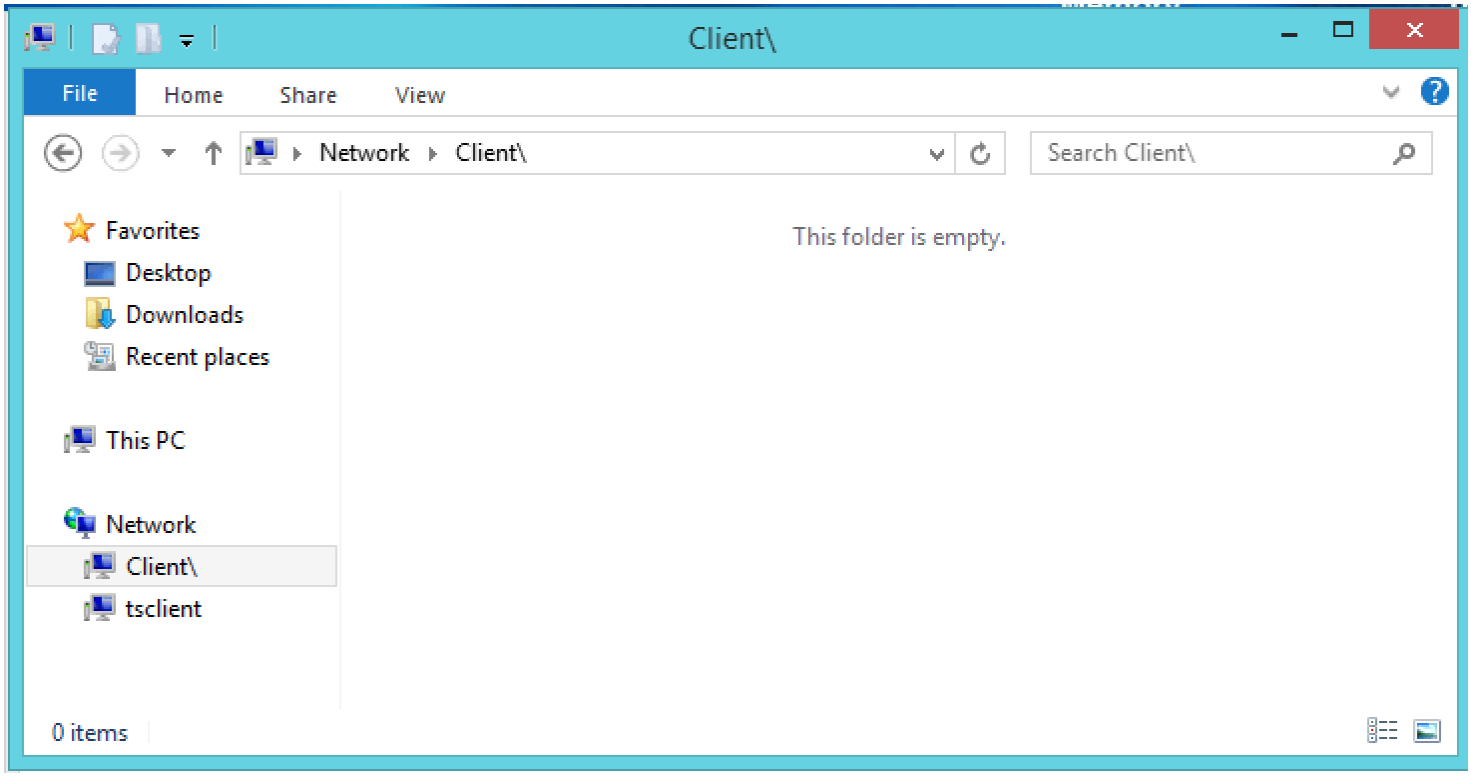
Network browsing is disabled

Again, though a client could never get to an application desktop or open the windows file explorer, if they did and clicked on network, they would only see two items:

- Client\
- tsClient\



then if a client wanted to browse one of these icons, they would find that there is no content



All these limitations are also enforced for all AccountTECH Staff at all levels

Exporting Report Data

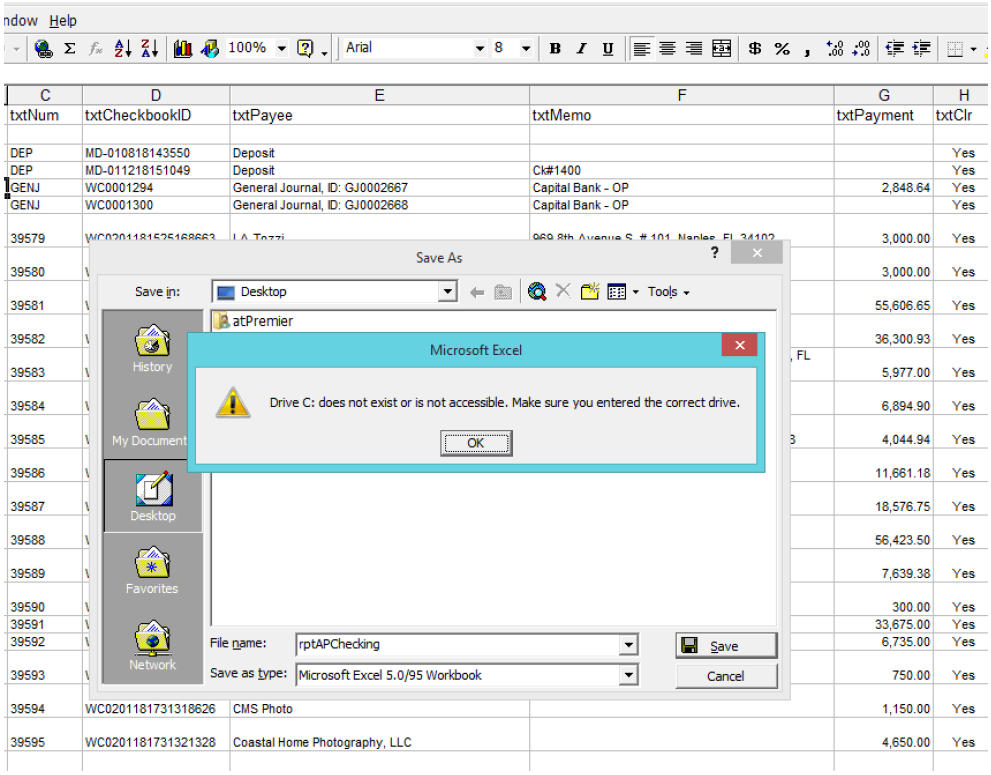
Export Report Protection

Using SSRS built into our application, it is possible that a user could export a report as a PDF, or TXT or Excel, etc.

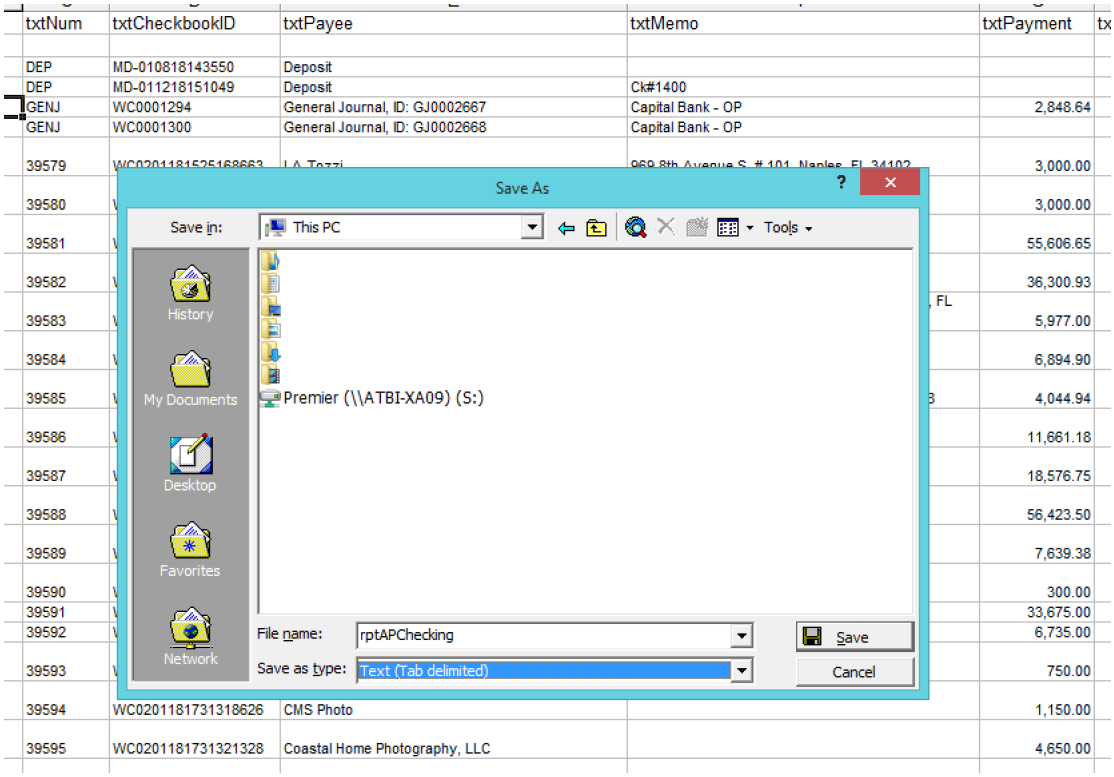
If a client exports a report to Excel, then MS Excel opens within the Citrix environment and displays the report to the user. The user can work with / analyze / modify the report content in Excel on our application server.

If the user tries to download or save the file in any way outside the Citrix environment:

The first thing the user encounters is a message that the C:\ drive on the application server does not exist.



If the client tries to browse to save in an alternate location, all they see are empty folders that they do not have access to and the drive letter S:\ which is the shared folder created specifically for storing their client data - and which they are supposed to be able to access.



There is no way to save a file off the network and onto local storage.

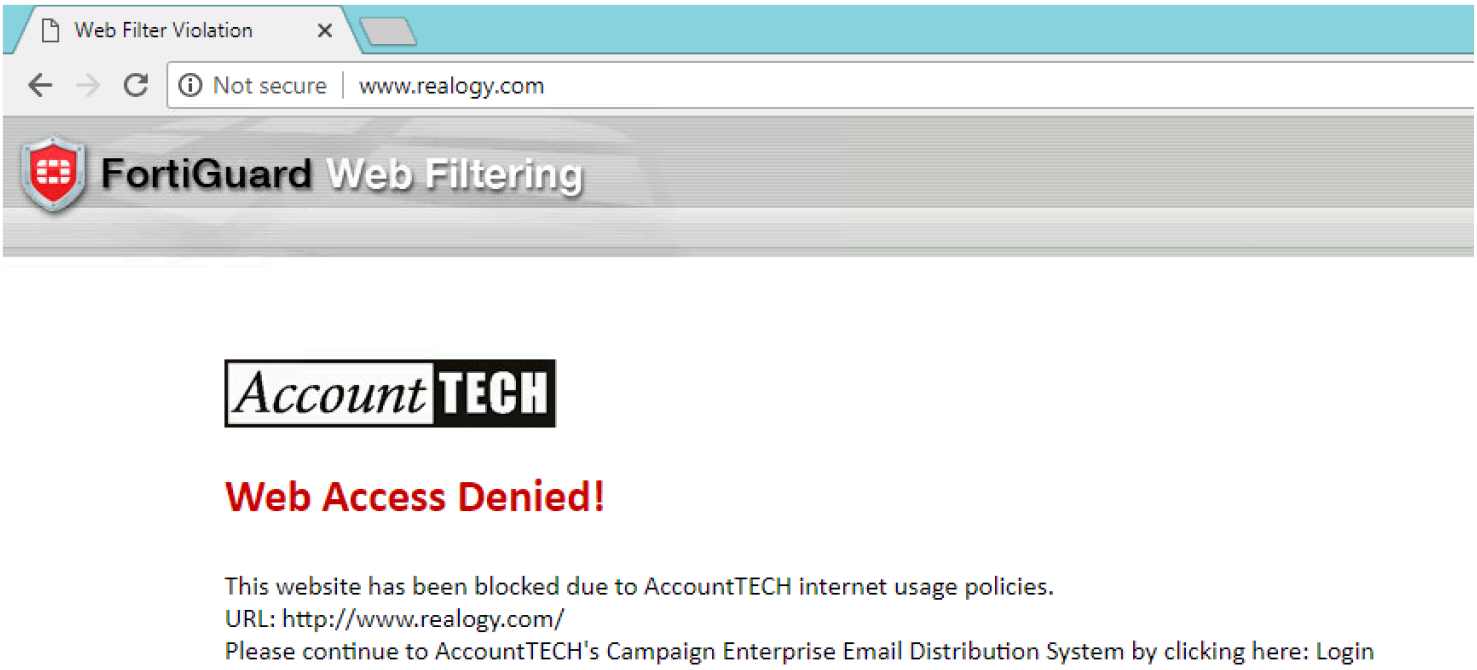
This rule also applies to AccountTECH Staff using the Citrix environment.

Use the Web to transfer data off Citrix network

If an AccountTECH client (or any one on AccountTECH Staff, or any infrastructure vendor) tries to transfer a file out the AccountTECH production environment, they will be blocked.

Company policy and Firewall security rules make it impossible for clients, staff or vendors to transfer files from the network to any other location using the web.

If anyone tries to use the web to transfer a file out of the environment, they receive this message:



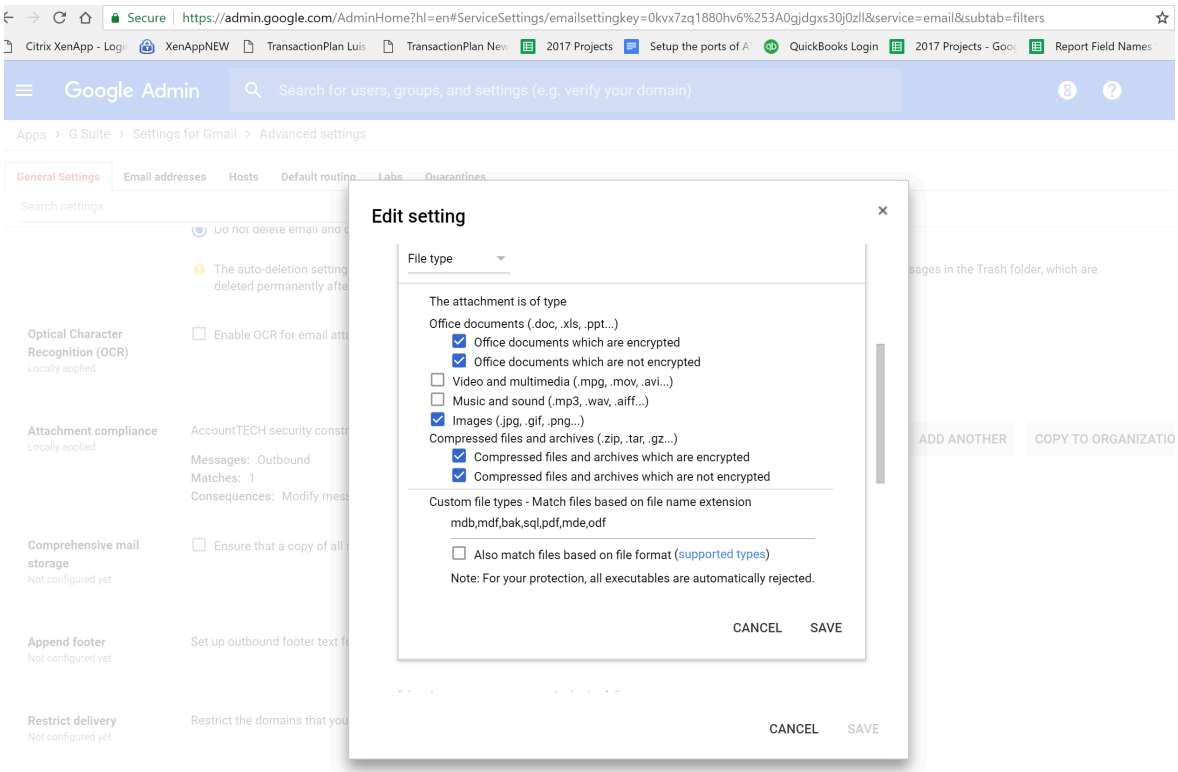
Email File Attachments

Attaching files to outgoing email

While working at AccountTECH, you will discover that you are not allowed to attach files to outbound emails. This is to keep information that belongs to clients from being transmitted outside our network. Please do not interpret this policy to be a mistrust of you as a new employee. This rule applies to all employees of AccountTECH at all levels. Only the CEO has the rights in Gmail to send attachments.

> Note. As part of the email security policy, all other web based email clients are blocked from being opened on your computer

If you have a file that for some reason needs to be emailed out as an attachment, please discuss it with the Director of Operations. They can have the CEO send the file if necessary.



It looks like you can send attachments ?

One of the quirks of Gmail is that when using your email at AccountTECH, it will appear that Gmail allows you to attach files. This can be confusing. What happens is that Gmail strips attachments out of your email when you send them.

Clients cannot receive file attachments from you thru your AccountTECH email account. If you need to send a screenshot to a client, that is only possible within Zendesk.

Understanding Time Clock Wizard monitoring

While working at AccountTECH, there are both rules and systems in place to keep client data in any format from being transferred off the premises. Please do not interpret these policies and controls to be an expression of distrust of you and in any way reflective of the company perception of any one individual.

The following controls affect all AccountTECH employees including management:

Time Clock Wizard monitoring

Time Clock Wizard is installed on everyone's work computer and is always running and always recording the work that each employee is performing (with screen shots of the monitor display).

The recording serves as documentation (if it was ever needed) about all activity of every employee. Time Clock Wizard records everything you do on your computer. It tracks every screen you open, all the tickets you work on in Zendesk. It tracks the websites you visit. Essentially, it creates a video of how you spend your time each day.

For security, this provides us as a company, one more tool for guaranteeing that all company policies are being adhered to.

For efficiency tracking, Time Clock Wizard does also provide managers with an approximate analysis of each individual employee's productive and unproductive time each day.

Time Clock Wizard site blocking

When first installed by AccountTECH in 2015, Time Clock Wizard came pre-loaded with obvious sites that should be blocked in an office environment. Over the years, AccountTECH has added to the list of blocked sites in an effort to further strengthen the company's stance regarding data security.

When using your office computer, you will see that many websites are not able to be loaded on your computer. Primarily, these are web-based email sites or file upload sites. Since company policy states that no client data in any format should leave the AccountTECH network, these controls provide one more mechanism to keep client data secure.

The Time Clock Wizard controls, if configured correctly, should keep us all limited to using only the company provided Gmail accounts for email. When using Gmail @accounttech.com, you will notice that you cannot attach many file types to an outbound email . (Please note there is no limitation on inbound email attachments other than virus scanning provided by Google).

You can help support AccountTECH's efforts to take care of clients but notifying any senior staff of sites you think should be added to the blocked list we maintain within Time Clock Wizard.

Zendesk and File Attachments

When working with client tickets in Zendesk, you may find that an outbound message from you will not attach a file you are trying to upload.

Zendesk at AccountTECH is configured to only support screenshots as attachments to tickets. Most any image file extension you use will work fine as a screenshot attachment.

If you need to attach some other file type for some reason, please contact the Director of Operations or the CEO to handle the file attachment for you.

Data center

Data center requirements

Data center physical security

Data center to provide and maintain the following physical plant controls (current provider: CoreSite 001, Sommerville, MA)

- Badge only fenced parking lot
- Badge only access to reception
- Security guard protection main entry to facility
- No visitor access with prior authorization and identity verification to security guard and temporary badge issuance
- Finger-print scanning access through multiple security doors in every section of data center on every floor
- Combination locked server cabinets

Network restrictions

Security 7 configuration for traffic through Fortinet firewall has the following restrictions:

- IP traffic limited to only US and Canada
- No cross-server traffic allowed within a network
- Internet access disabled on servers on the network

Citrix Netscaler restrictions limit:

- Data cannot be uploaded into the network from any connection
- Data cannot be downloaded from the network

AccountTECH application features for network security:

- Features in application that appear to load and store photos from MLS are never actually loaded or stored in production network. Instead, they are routed to remote online storage provided by an outside data warehouse company. Only a URL that points to the images is stored in AccountTECH databases
- Features in application that appear to load and store transaction documents are never actually loaded or stored in production network. Instead, they are routed to remote online storage provided by an outside data warehouse company. Only a URL that points to the documents is stored in AccountTECH databases

Username & Password Policy

Overview: Limit access to client data with username / password control

AccountTECH staff are required to follow the following rules regarding control of who gets access to client data

1. AccountTECH Administrators control usernames & password to access the client's Citrix login (1st username / password).

2. Only AccountTECH Administrators have rights to add/edit the Active Directory.

3. The number of remote access logins allowed per client is controlled by Citrix per user licensing policy.

4. Only clients determine which application login usernames and passwords (2nd username / password) are created. Clients will decide what each individual in their company is allowed to do and see for each application login. AccountTECH staff can train, but never participate in setting up application permissions.

5. AccountTECH staff may never change application permissions... even if requested during a phone call or in an email. Instead, AccountTECH staff can guide users on how to change the application access permissions themselves.

6. AccountTECH Staff may not issue or maintain application logins to client data.

7. In the event of a client perceived emergency, AccountTECH Staff may disable or delete an application login.

Overview: Application Login Security Rules

AccountTECH staff need to protect application login security in the following ways:

- Ensure that Active Directory / Citrix logins are not issued or enabled in excess of the number of licenses secured by the client for Citrix access.
- Make sure Active Directory password strength and password change rules are followed.
- Make sure there is no way to log into any AccountTECH application without valid credentials.

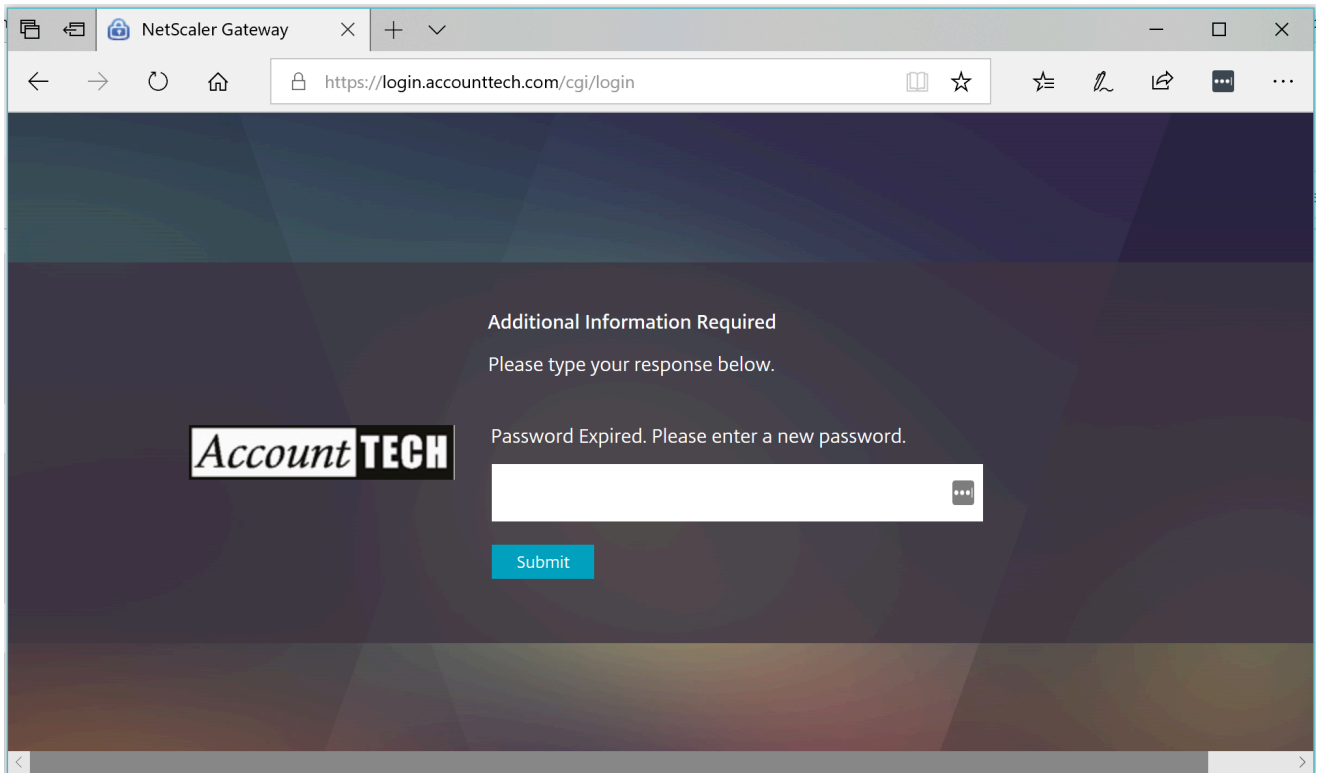
Step-by-Step: Issue Client Username / Password

Who can issue client usernames / passwords to AccountTECH

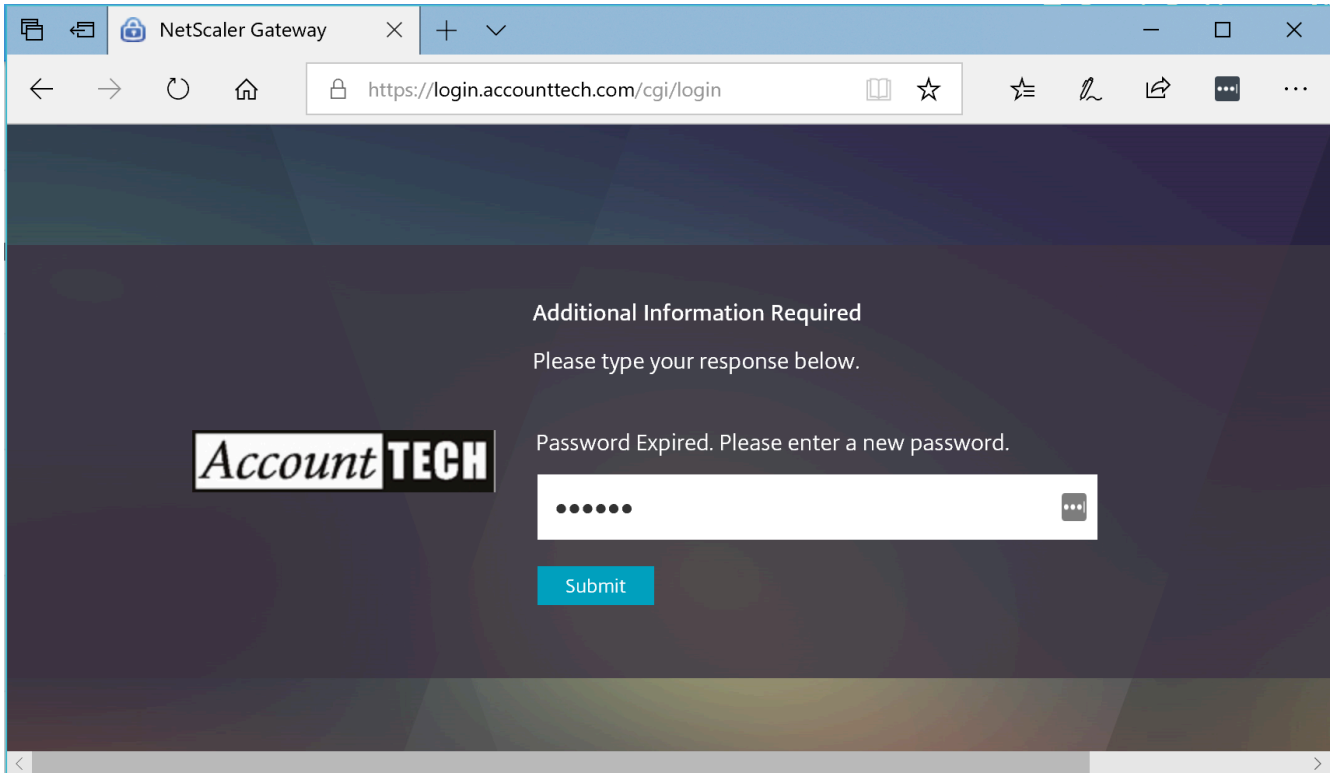
Only Administrators can setup (or modify) client usernames / temporary startup passwords. Before usernames and passwords are created, we need to check with accounting to confirm that the request for the Citrix license came from the Broker and that the Citrix license being issued has already been paid for. If these conditions are met, any of the administrators can create the username & password in the Active Directory with a temporary password.

Giving a user their username / password

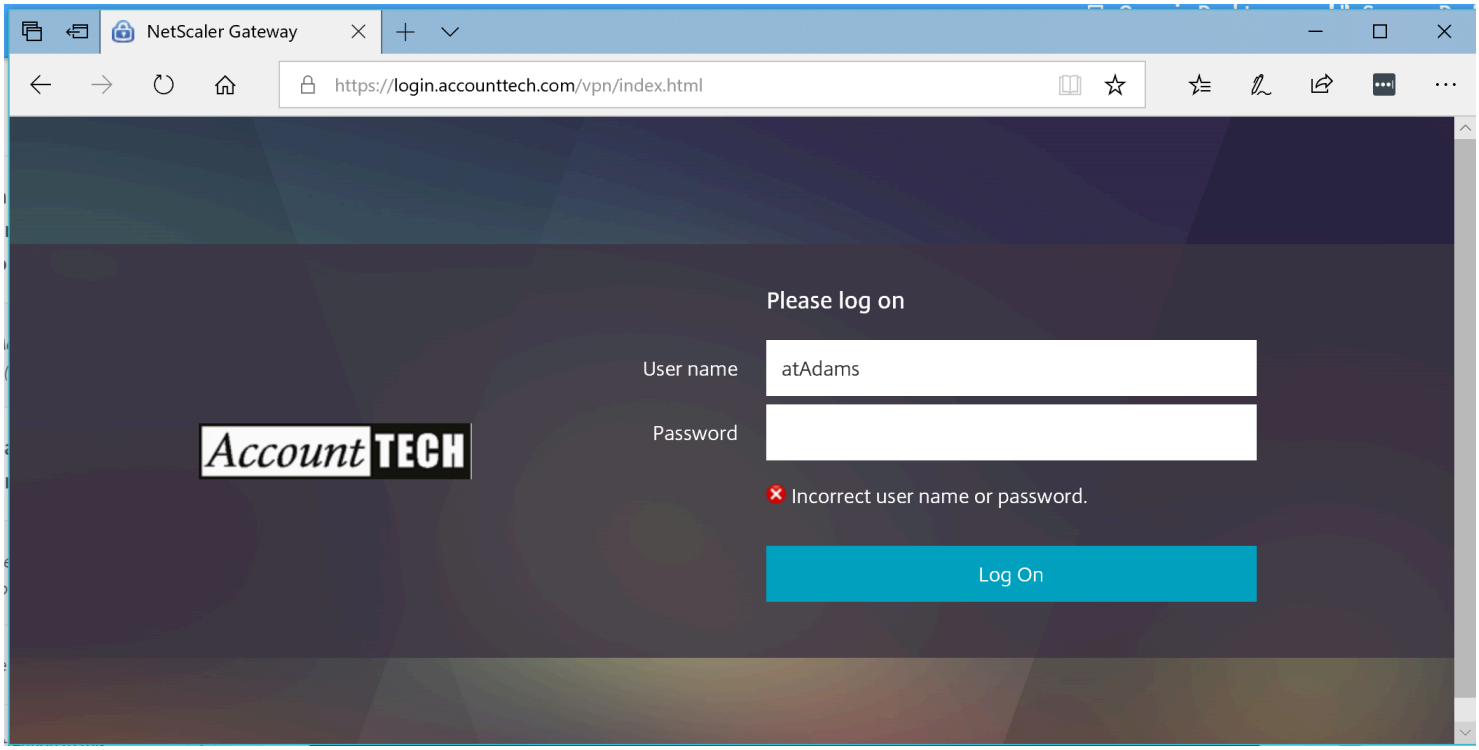
1. Get the username / temporary password from the administrator who created the client login either by walking to their office or calling them. Never retrieve a username / password by internal messaging systems, email or text.
2. For providing temporary passwords to designated Keeper of Passwords, and/or Broker Owner, the following methods are approved:
    1. Call the customer and provide the password directly to the designated Keeper of Passwords, and/or Broker Owner.
        1. Stay on the phone while they log in a change the temporary password to their password. Remind them not to repeat the password to you.
        2. If they are unavailable, leave a voicemail.
    2. Write the password down on a piece of paper. Using the RingCentral app and your work direct line, text a picture of the written password directly to the designated Keeper of Passwords, and/or Broker Owner. Employee then must shred the paper that the password was written on
    3. Employee may generate a privnote link to send to the designated keeper of passwords with the following parameters:
        1. Note Self Destructs after reading it
        2. Manual Password - provided to the customer by either methods 1 or 2, that protects the privnote link
3. Whenever a new/temporary password is provided to the designated Keeper of Passwords, and/or Broker Owner, you must do the following
    1. Explain password renewal and send the article with tips on how to remember to reset Citrix login passwords by day 42.
    2. Explain tips about password protection. send the article about password protection practices.



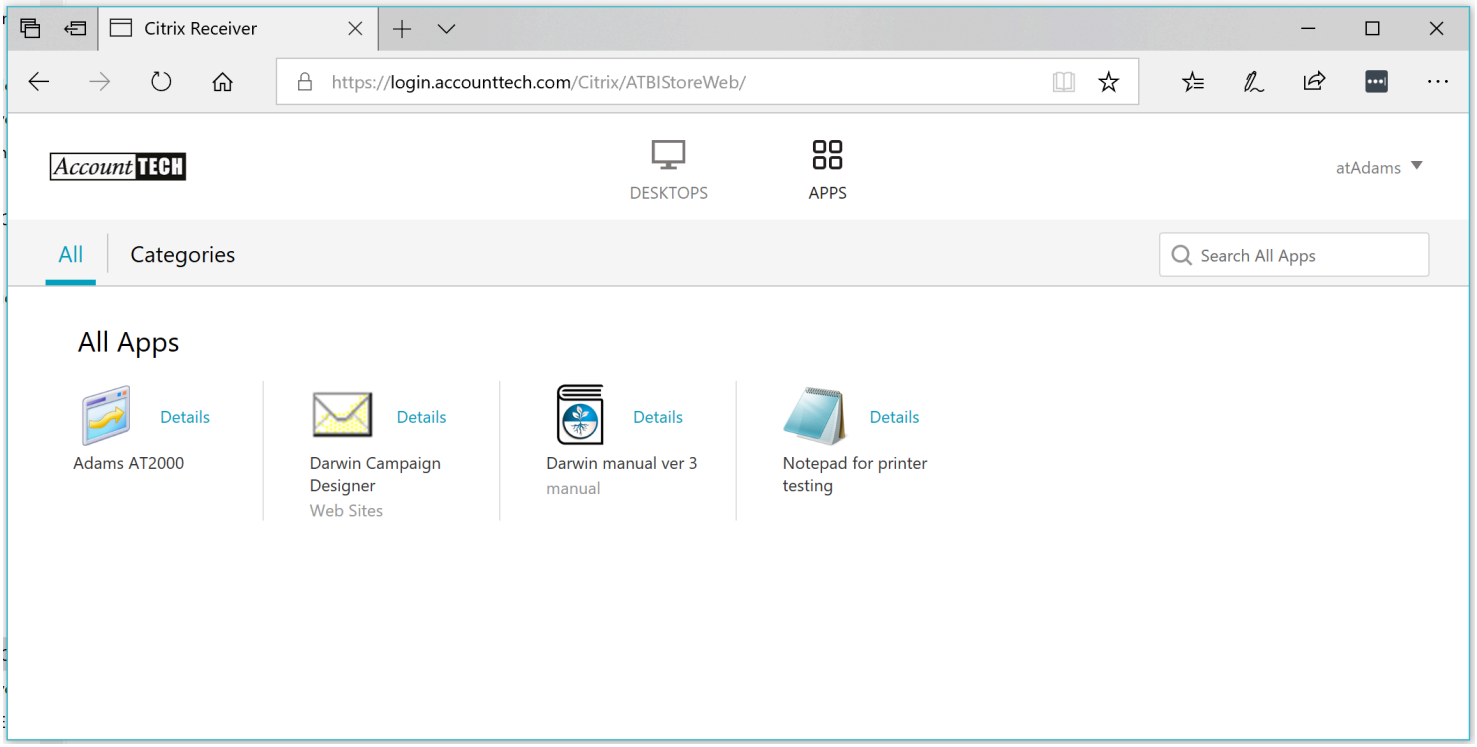
Pay attention to this important issue. If the user enters a new password that does not meet our password security rules, the Citrix login page is not "smart" enough to explain to users that their password is not acceptable... so it will go thru the process BUT NOT UPDATE the password. Say for instance the user enters a password that is only 6 digits:



When user tries to log in with the password reset they attempted, they will notice that the password was not changed and they will get an invalid password message:



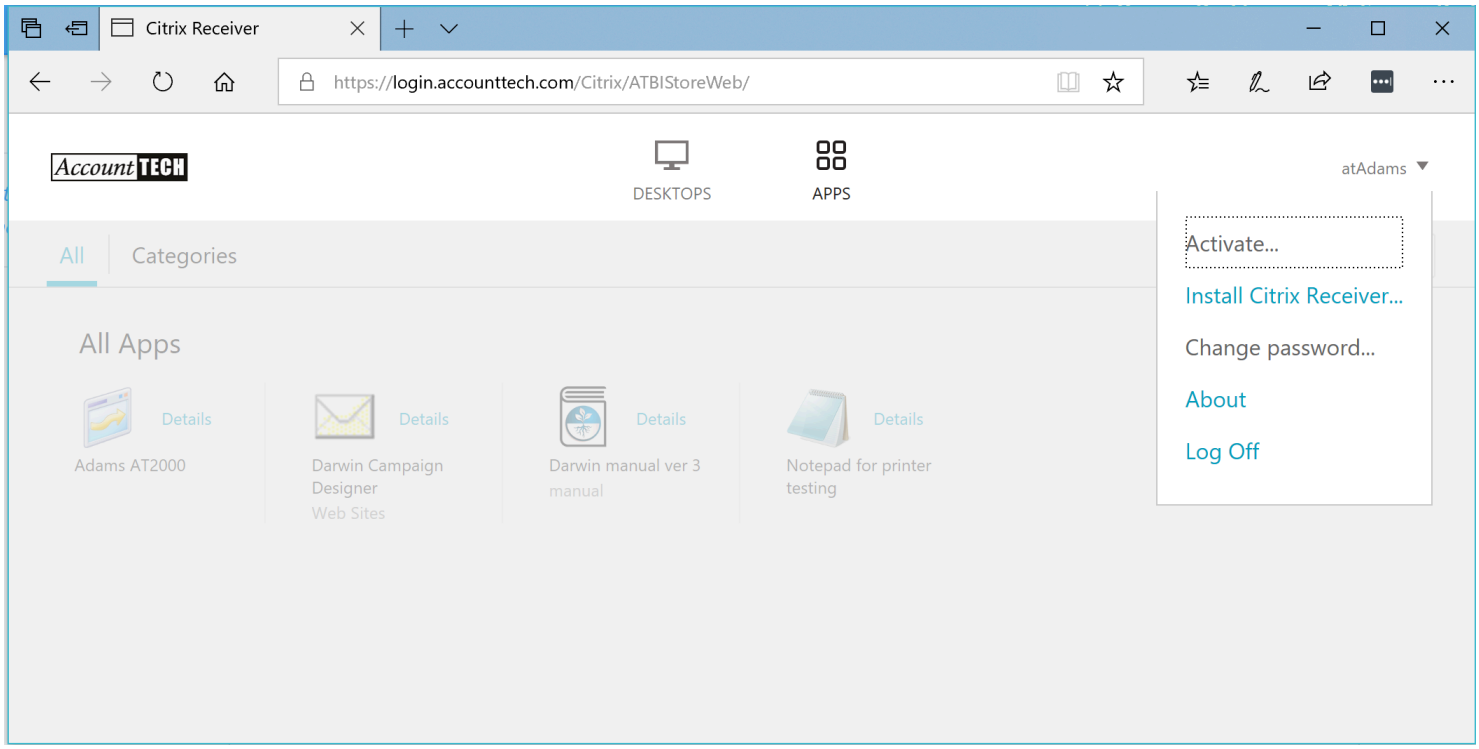
So users need to change the temporary password we give them to a strong password - and then their login will work. Please make sure to remind them that after 42 days, if they have not reset their password, the Citrix Netscaler will force them to do a password reset for access to their software.



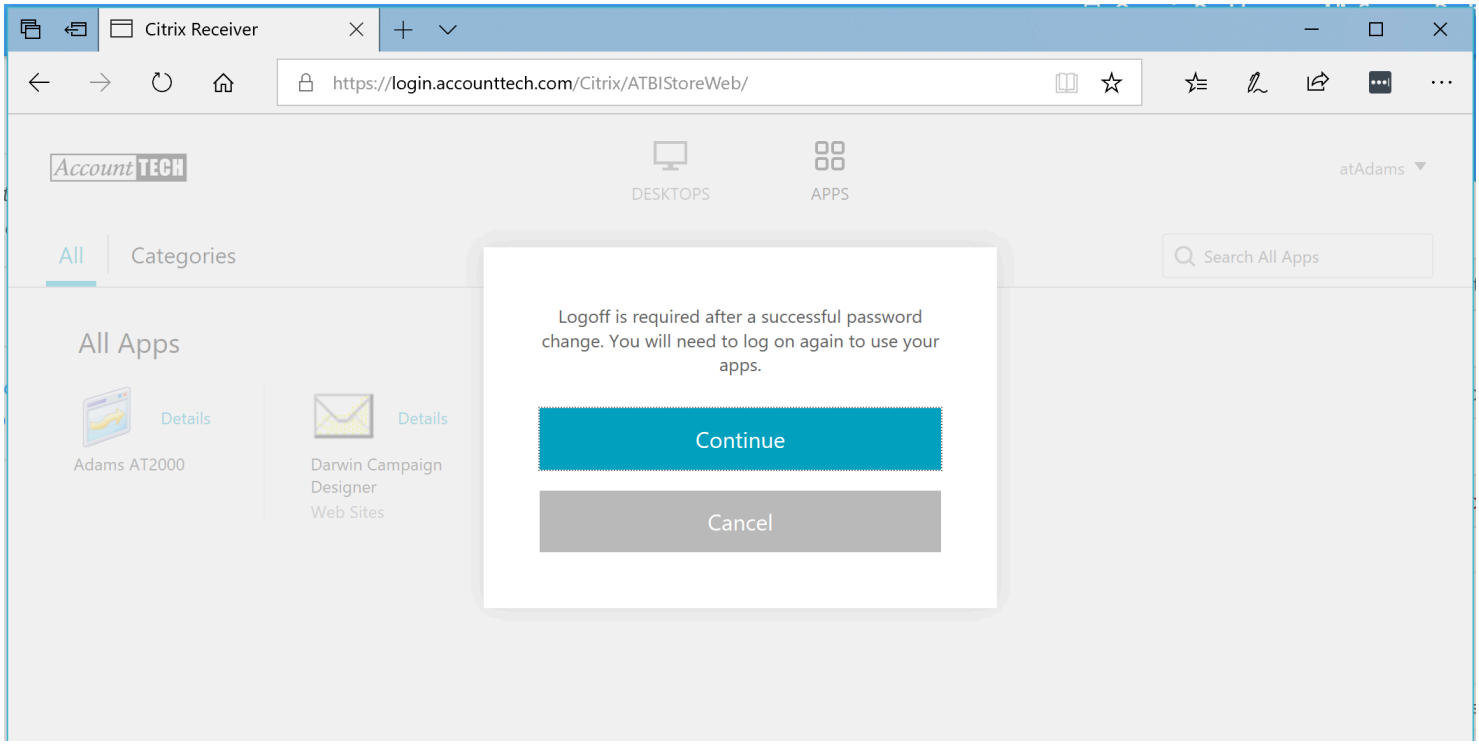
Client Reset of Their Login Password

AccountTECH clients can reset their Citrix login passwords at any time. If they go for 42 days without a password reset, they will be forced to reset to a new strong password to be given permissions to access their application.

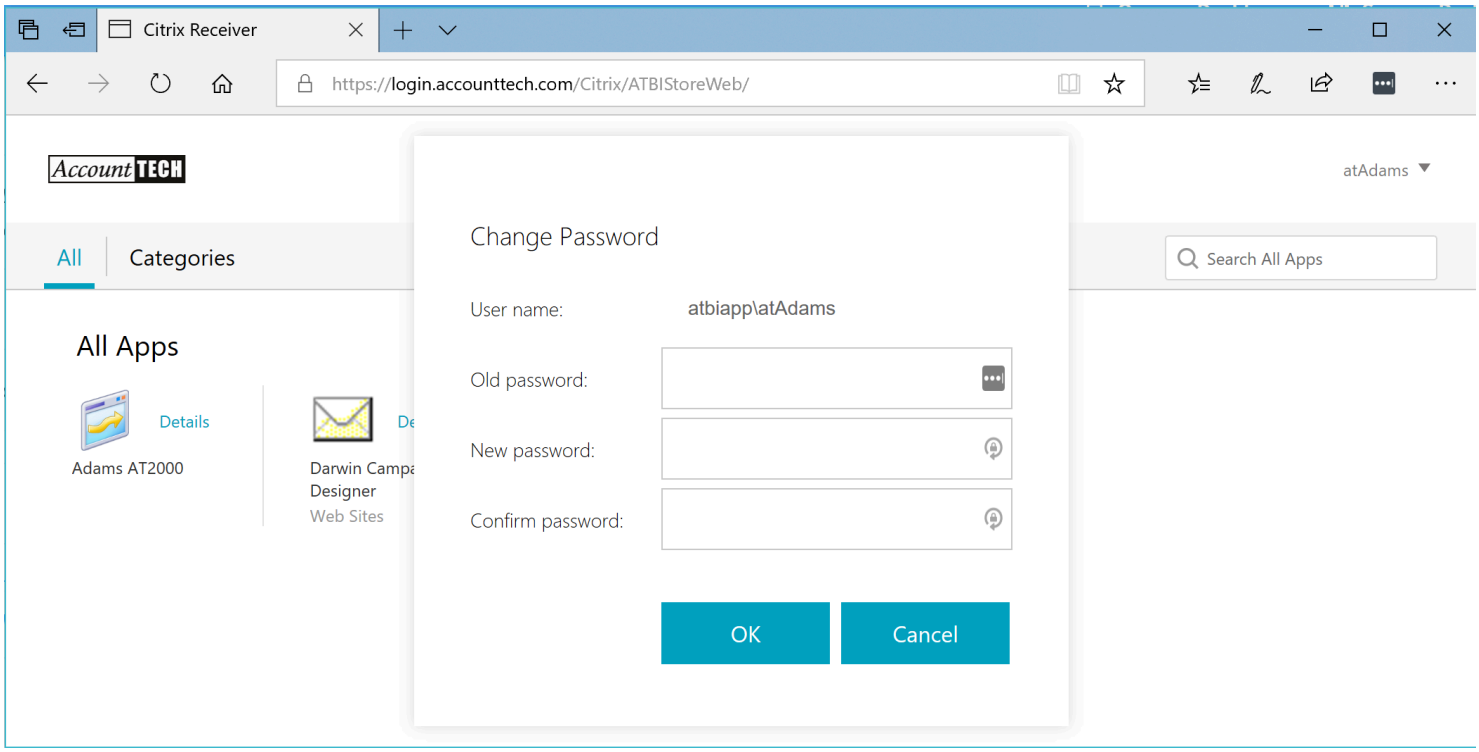
From the Citrix Netscaler page, the can choose: Change Password from the drop down menu in the upper right corner of the page.



After clicking: Change password, clients will see a screen designed to make sure that they understand that they need to log out / log back in after changing their password:



When they click: Continue. They see this screen and they can complete their password reset.



Citrix Username Control

Users have no access to create Citrix login usernames or modify Citrix usernames.

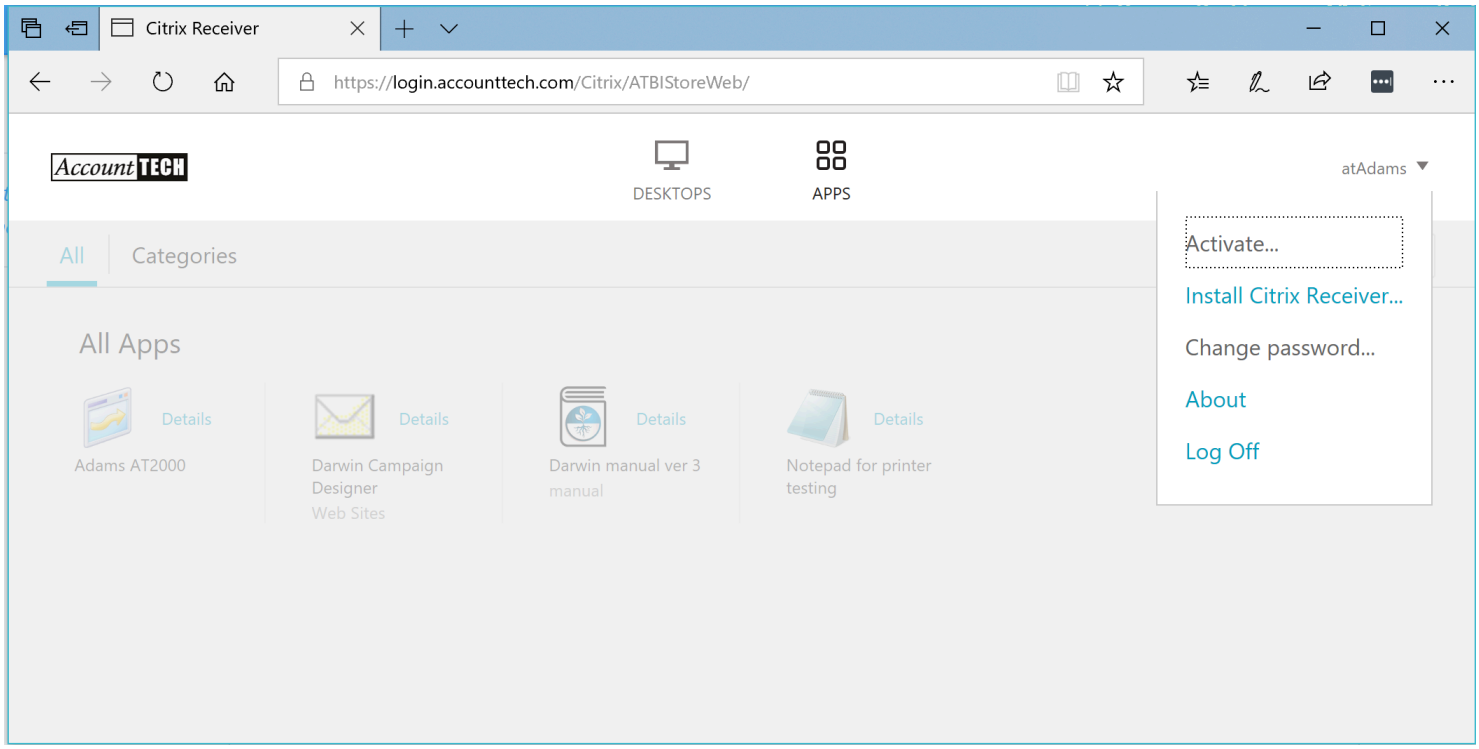
If you receive a request for a new username, Citrix license instance or a modification to an existing username, follow this protocol.

1. Confirm you are talking to the designated Keeper of Passwords and/or Broker Owner. If you do not know the designated contact well enough to confirm that the person on the phone is the designated contact, then send a confirmation code to the their email address while on the phone and have them confirm it for you.
2. If the Keeper of Passwords and/or Broker Owner is requesting a username modification. Follow these steps:
   - Find out why and record in Zendesk.
   - Confirm with Accounting that the account is not delinquent.
   - Find an available administrator to make the username modification.
   - Update the citrix username field in ZohoCRM
3. If the Broker is requesting an additional citrix license instance and/or username, follow these steps:
   - Transfer the call to Accounting for payment authorization.
   - After payment authorization is confirmed, Accounting will follow the steps above.

Emergency Change for Citrix Username or Password

There are occasions each year when some client will call in with a request for an immediate username change OR a Citrix login password change. Usually this occurs for some reason related to an employee termination.

Often, a password change is sufficient to meet the security concern. Designated Keeper of Passwords and/or Broker Owners can change their Citrix password at any time by using the NetScaler login screen. You should never reset a Citrix password for a designated Keeper of Passwords and/or Broker Owners if they are capable of re-setting the password themselves:



It can happen that a designated Keeper of Passwords and/or Broker Owner requests you to reset a password on their behalf for these reasons:

- The currently valid password is lost and the designated Keeper of Passwords and/or Broker Owner cannot login to effect the reset.
- The designated Keeper of Passwords and/or Broker Owner is travelling and has no internet access to reset the password. This is especially possible for international travel since there are so many countries where internet connectivity from that company to AccountTECH is blocked by policy.

If you need to help a Broker by creating a new temporary password:

- Follow the standard steps for validating the designated Keeper of Passwords and/or Broker Owner identity if they are unknown to you.
- Confirm with accounting that the customer account is not deliquinet.
- Contact an Administrator to have them create a temporary password.
- Communicate the temporary password to the designated Keeper of Passwords and/or Broker Owner via approved methods outlined in section "Giving a user their username / password "

Policy Staff

Simple Rules for Staff and Programming

Requirements for Support, Training & Operations Staff
Managed by: Director of Operations, Tori Mueck

As part of protecting client data, staff at AccountTECH are required to follow these simple rules:

- Never discuss client financials with anyone other than the Broker Owner or senior finance staff appointed by the owner.
- Never discuss a client's financial information or production information with any other client.
- Never save printed client financial data. Shred any reports printed locally for research while aiding a client.
- While technically not possible in the environment, never even attempt to download client databases and/or take copies offsite.
- Never execute data entry for a client into their database unless it is part of a specific work-order signed by the client.
- Practice Clean Desk End of Day Policy.

Requirements for programming staff
Managed by: Director of Programming, Helkyn Coello

- Use software evaluation tools.
- Follow policy around security and testing.
- Subject all code to peer review and management review before it goes to production.

Approved Uses for Office Computers

Office computer use limits

- Office computers are only to be used for AccountTECH work.
- Antivirus / AntiMalware installed should never have any changes made to the settings.
- Time Clock Wizard monitoring software is installed on each computer.
- Company computers are not allowed to be taken offsite unless for work purposes

Communicating with Clients

There are rules for communicating with clients so that a paper-trail exists for any / all work or support we do for each client

- Every task / question or answer / project needs to be logged in Zendesk.
- All client communication has to be done using your AccountTECH email account.

Email Management

Director of Operations will ensure that AccountTECH email system settings restrict all users from sending out emails that contain database file attachments.

Termination

Prior to a termination of an AccountTECH employee, all managers are notified via a meeting that a termination will take place. At that time, the termination process is reviewed, and a start date and time is established to start the pre-termination process. Director of Operations is responsible to ensure that any termination has an action plan for removal of all network access for the employee being terminated. The plan must include:

- Scheduling the termination to allow time for security changes necessary to protect the network.
- Confirmation process prior to termination that all network access has been denied to the person being terminated.

The following accounts need to be deleted or have a password change prior to termination:

- The employees Citrix License needs to be removed.
- The employees AccountTECH email account password changed.
- All editor Screensteps login account passwords changed.
- The employees Zendesk account needs to be suspended, and removed as an agent.
- The employees TransactionPlan account for AccountTECH needs to be deleted.
- The employees ZohoOne Phone login needs to be disabled.
- The employees ZohoOne Phone number to be reassigned to another member in the same department.
- The employees internal messaging account needs to be disabled (Glip).
- The employees Time Clock Wizard access needs to be revoked.
- The employees Apptoto account needs to be deleted.
- The employees ZohoOne account needs to be deleted.
- The employees email address needs to be removed as CC or BCC from any email campaigns.
- Retrieve office keys prior to re keying the offices.
- All darwin for AccountTECH Staff in all client databases needs to be updated.

Privacy Policy Violation

Privacy events are recorded and handled by our Director of Operations and resolved with offending employee.

A privacy event is any action taken by anyone on AccountTECH staff which exposes or risks exposure of client data to an unauthorized 3rd party.

All privacy events are logged in the employees permanent record and are part of the that employees evaluation.

Repeat violations of privacy policy require employee termination for cause.

Password Policy

We have a written password policy:

1. Passwords must be enforced on all our systems: Citrix network, Developers network, Backup network, DMZ, API, Active Directory.

2. Policy: minimum length of 8 characters, use of upper and lower case , use of at least 1 number and at least 1 special character, inability to repeat any of the prior 12 used password and blocking access if too many attempts in a time frame.

3. Password expiration in 42 days.

4. Test all systems to ensure that they enforce the password policy.

Policy Programming

Application Functional Security

AccountTECH programmers and the AccountTECH review process needs to ensure that the security built into the application environment is not "undone" by our software development.

Examples would be:

- Never violate the rule of one client, one database with any possibility of unauthorized data access.
- Never fail to enforce the data edit and data viewing rules setup for application users by the Brokers.
- Never allow a feature that somehow violates the network restrictions regarding no data download / no data upload.

Project Approval

Steps to get a project approved

1. *Selecting what software changes need to be deployed*

   Based on business needs. Director of Programming with CEO and other senior level staff have meet to determine to determine projects that should be "on the list". Projects come from the CEO, AccountTECH Staff and client input.

   If any project is selected to proceed, the project (new features, enhanced features or bug fixes) gets it's own change request document. This is essentially the work order.

2. *Do risk assessment for each change*

   For each change / fix request, a preliminary risk analysis is made by the Director of Programming with CEO and other senior staff. The risk score could range from 1 to 25 where the lower the number, the lower the risk. Only projects with a score of 1 are automatically selected for deployment. Projects with a score level of 5 or less are sent to the "Feedback review loop" - to see if programming can figure out some way to make them more secure.

3. *Do Feedback review loop*

   At AccountTECH, a "feedback review loop" is started whenever there is a project we would like to do - but its risk matrix score is too high.

   The project is re-evaluated with the input from the Director of Programming, CEO, programmers, etc. to see if it is technically possible to reduce the risk score by re-thinking or re-designing the change request.

   If there is a re-design plan that can be put in place to get the change approved, it gets resubmitted and starts the review process back at step 2. Generally a project needs to get a risk score of 1 to be approved. This process is repeated as many as 3 times before the CEO gives final approval as to whether to move forward on any project.

Project Development Process & Policy

Overview

All approved changes / fixes are programmed in the developers network. The developers network is a mirror of the production network. As a programmer, you will not have access to the production network. Only administrators can access the Production network.

Once you finish working on a change or fix, it will need to pass proper testing, in several layers, and then it will get scheduled for deployment in our QA environment first and then into production.

The following will describe in detail this whole process step by step, starting in how we get change requests until how we deploy changes into production.

Tools you will use:

1. *Corporate email*

   You will be assigned an AccountTECH corporate email where you will get notifications about the work you need to do.

2. *Zoho Bug Tracker credentials*

   You will get your own credentials to get into Zoho Bug Tracker tool where you will see the details of what changes / fixes you have been scheduled and assigned.

3. *Visual Studio 2017*

   You will find this installed in all computers in the Citrix development network as the IDE in which you will develop and test your code.

4. *Visual Studio Online credentials*

   You will get your own credentials to get into Visual Studio Team System Online services. You will use this as the source control and versioning tool for the code you build from within Visual Studio IDE.

5. *Veracode Greenlight tool*

   This is a plugin you will find incorporated into your Visual Studio IDE that will help you write better code - this tool highlights security concerns as you write your code.

6. *Detectify*

   If a project you are working on requires a Penetration Test of our web based software components, you will get credentials to use this tool. With this tool, you will be able to perform penetration testing of your code & our software and make sure we are Top 10 OWASP Compliance.

How do you get / received changes / fixes requests:

A request for a software change, fix or enhancement may come from your supervisor (VP fof Software Development) CEO, AccountTECH Staff or from client input. You will track all change requests you receive in our ticketing system: Zendesk.

Once tracked, the VP of Software Development will get notified about these change requests and get them in queue for approval.

Categorization of changes / fixes requests:

Before anyone in programming works on any project, the VP of Software Development has to analyze each change / fix request and categorize them into one of 2 levels:

1. *Minor or low-impact changes*:

   A change without any impact on the business rules, network rules or any change that does not change the business work flow at all AND does not constitute any security risk at all.

2. Major or high-impact changes

   Any change that will either take more than 1 week to develop or any change that modifies the business work flow at any level or any change that has security concerns.

Doing risk assessment of each change request:

Minor low-impact changes that are important for clients (risk score of 1) are automatically pre-approved for the VP of Software Development, but still need final approval from the CEO.

For all other change requests, but specially for the ones categorized as Major high-impact changes, the VP of software Development together with CEO and other senior level staff meet to determine which ones get approved to get worked on.

This is done by evaluating the project on these metrics: Benefit to clients, Cost to Produce, Benefit to Marketing & risk analysis. For Risk Analysis:

1. Each change request gets analyzed using our Risk Matrix that evaluates each change based on likelihood level and impact level and establishes a risk score for each change request.

2. The risk score could range from 1 to 25 where the lower the number, the lower the risk.

3. Only projects with a score of 1 are automatically approved for deployment. A low risk score does not mean the project will be approved. The client benefit, marketing benefit or cost to code may get a project request scrapped.

4. Projects with a score level of 5 or less are sent to the "Feedback review loop" - to see if programming can figure out some way to make them more secure.

Do Feedback review loop

In your role as a programmer at AccountTECH, you may be asked to participate in a Feedback review loop. A "feedback review loop" is started whenever there is a project we would like to do - but its risk matrix score is too high.

The project is re-evaluated with the input from the VP of Software Development, CEO, programmers, etc. to see if it is technically possible to reduce the risk score by re-thinking or re-designing the change request or by establishing a mitigation plan for any given change request and thus reduce its risk score. You may be asked to participate in this re-design process.

If there is a re-design plan that can be put in place to get the change approved, it gets resubmitted and starts the review process back at step 2. Generally a project needs to get a risk score of 1 to be approved. This process is repeated as many as 3 times before the CEO gives final approval as to whether to move forward on any project.

Selecting change / fix requests to be worked on

Once this evaluation and the change requests selection process is finished, the approved change requests are scheduled and assigned to programmers in our Zoho Bug Tracker tool. You will need to login to your Zoho Bug Tracker account and see what has been scheduled for you.

Automatic real time code security analysis

While you write code for your assigned projects, your Visual Studio IDE will analyze the code you write as you write it. This means that you might get warnings and your code will get highlighted in the IDE as an error if what you wrote violates the security guidelines and represent a security risk.

These warnings will prevent you from compiling your code until you take care of the security issues highlighted to you. The warnings will not only tell you there is a security concern. but also it will give you extra information on what could happen if the security concern is not resolved and it will even recommend how to fix each of them.

Security checklist usage

As part of our continuing effort of enhancing our security standards in the programming department and make the whole team security awareness, you will be provided with a document called "Security checklist". This document will give you some guidelines on what to do and not do when writing code in terms in security.

As part of our company policies, you must review this document BEFORE you start the implementation of any of your assigned project and AFTER finish the implementation of each of them as well. This is to ensure everything you wrote in code meets all the security criteria we need for your software.

The Security checklist includes the following items:

1. *Injection*
   - Do not build dynamic sql statements at the code level
   - Do not use dynamic SQL statements at the DB level.
     - If dynamic SQL statements are needed at DB level, validate all input parameters for range and domain restrictions.
2. *Broken Authentication and Session Management*
   - Do not transfer credentials back to the front end.
   - Do not store passwords or any other information that could reveal credentials or information about our infrastructure in any config file .
3. *Cross-Site Scripting (XSS)*
   - validate all relevant UI inputs for range and domain restrictions.
4. *Insecure Direct Object References*
   - Make sure neither code nor config files reference physical locations or names of any assets in our infrastructure.
5. *Security Misconfiguration*
   - Grant access to applications based on tokens that have an expiration time of 5 hours max.
   - Block users after 5 failed login attempts.
6. *Sensitive Data Exposure*
   - Encrypt all credentials and any sensitive information (like SSNs).
7. *Missing Function Level Access Control*
   - Make server side check for authorization to different parts of the applications data.
8. *Cross-Site Request Forgery (CSRF)*
   - Make all UI screens on web to be validated for CSRF Cross-site request (to avoid phishing).
9. *Using Components with Known Vulnerabilities*
   - Check the reliability and security compliance of any tool we use in development and production.
   - Check the reliability and security compliance of any component we use in development and production.

10. *Unvalidated Redirects and Forwards*
    - Avoid using redirects in code and if needed validate the page to be loaded to be a internal page we control.

Daily reviews by VP of Software development

While coding the projects you have been scheduled to work on, the VP of Software Development will meet with you to review the status of project you have in process. Together, you will analyze if the way the code is technically being implemented is in compliance with all security, business rule & company policies.

These meetings and all notes / suggestions / etc. are tracked in our Zoho Bug Tracker tool using a Kaban board to facilitate the visibility of the development process and how much progress is being made.

There will be times in which, depending on business needs, you will be unassigned a project and will get assigned another project. This is decided by the VP of Software Development as needed to speed up and maximize the usage of our development resources.

Summary: how do we deploy changes to production

Before any code changes moves into production, completed projects are selected as release candidates. Then a developer testing process and validation process begins in the developers network. The steps include:

1. Testing your code in the QA environment within the developers network. (you need to test both functionality & integration).
2. Code peer review.
3. Security analysis .
4. Filling in several documents needed for deployment.

There are four documents that we call "the packet". These all need to be completed before beginning developer testing:

1. *Deployment log*

   Think of this as a work order. It contains a list of all requested changes with its corresponding risk assessment.

2. *Deployment checklist*

   This includes:
   1. Tasks that need to be done prior to the start the testing.
   2. Approvals that are required from management before deployment.
   3. Final QA staff approvals needed before deployment.

3. *Security checklist*

   This is list of security validations needed for the project (PCI, OWASP - depending on the project)

4. *Test case scenarios*

   A list of all the tests needed to evaluate the project programming. (This is also where you will list test by code scanning tools for security flaws, etc.)

Selecting change requests for weekly deployment

Before starting the deployment process, the VP of Software Development with the CEO and senior staff will meet and determine which of the projects already completed will next be deployed. This is determined based on business needs.

Once decided, the VP of Software Development creates a folder for the current week's deployment in our online storage tool and will generate the "Deployment Log" document, where all change requests approved to be deployed will be listed with their corresponding risk score that was determined earlier in the development process.

Validate and curate the completed change requests to be deployed

The designated programmer will be instructed at this point to do a quick code review to look for missing changes, missing objects, change conflicts, etc. This designated programmer will analyze these conflicts and will resolve them with the input of all programmers before the deployment process can continue.

Performing final automatic code analysis (in the development environment)

Once all changes / fixes are approved to be in the deployment, the code to be deployed is scanned again, using Veracode greenlight tool to analyze security threats in the source code. If issues are found, then deployment is put on hold until the issue is resolved. This code analysis is done in the development environment, before the build is generated for QA and after all approved changes have been merged together and curated.

Perform first manual code peer-review (in the development environment)

For all final approved changes / fixes, the VP of Software Development will start a code Review in development environment to make sure everything in code looks ok and meets the security standards described in the security checklist document. This code analysis is done in the development environment, before the build is generated for QA and after all approved changes have been merged together.

This code peer-review must be done by reviewers who will complete the security checklist document that the VP of Software Development stores in the deployment folder. This is one of the documents part of the "deployment pack" described earlier in this document.

Perform second manual peer code review (in the development environment)

The final peer code review is done by senior staff not from the Programming department and needs to be passed successfully in order to continue with the deployment.

Before this step begins, the security checklist must be completely filled in 100% to be able to continue with the deployment process.

Installing and testing deployment on QA

If all prior steps are done successfully, the deployment is installed in the QA environment to start the formal functional testing. This formal functional testing will be initiated at this stage based on the Test Case scenarios document that the VP of Software Development will have ready for you at this point.

This document is part of the deployment "pack" and will also be stored in the deployment folder in our online share storage tool together with the Deployment log, deployment checklist and security checklist documents.

The test cases will be executed by the designated staff person (non-programmer) every Friday morning to confirm the changes are functionally correct and to re-confirm it meets all security standards.

Non-programmer testing must be completed by Friday noon and any observations will be written up in the Test cases document to be addressed by the programming team at their Friday afternoon meeting.

By Friday night, all observation must be resolved and approved by the VP of Software Development so that the next step can be performed (Penetration Testing). If all staff person testing concerns cannot be resolved by end-of-day Friday, the projects cannot be deployed on the regular schedule and they must be postponed to the next build.

Do a PenTest on the deployment installed on QA

Once the deployment is installed on the QA environment and once all test cases have been passed successfully, a penetration test to search for security vulnerabilities is done against the web components of the software (Darwin API & TransactionPlan web application) using our Detectity tool.

This is expected to be done between Friday night and Saturday morning by the designated person programmer. If vulnerabilities are found, the deployment is stopped until the vulnerabilities are

removed from the software and until the software is top-10 OWASP compliant.

Installing deployment on production

Only after all prior steps have been successfully completed - then the new deployment is approved to get installed in production. This is expected to happen every Monday before business hours: between 4 AM and 6 AM.

The VP of Software Development will activate a production account for the designated Administrator doing the production deployment - these permissions are available only for the time period in which the Administrator is doing the deployment. After the deployment is complete, the Administrators credentials for the production environment will get disabled again.

While doing the deployment the designated Administrator will login to the deployment server in the production network in which Visual Studio will be installed. The build for the deployment will need to be downloaded by using GET LAST VERSION command within the Visual Studio IDE.

Before starting the deployment, the Administrator does a backup of all components to be updated - in case there are problems

Once the new deployment build is fully downloaded (from the Microsoft Team System online) in the production environment, the designated Administrator will do the deployment as needed in the Application & Web servers.

Testing the deployment in production

Once the production deployment is ready, the designated Administrator will need to test it again against the Test Cases document and do a penetration test again using our Detectify tool. This is to check if any components were missed during the deployment.

If all test cases are performed with success and PenTest is done successfully, then deployment installation is confirmed. If the test cases are not successful after deployment, then the backups (that were made prior to do the deployment on production) will get restored until the issues are resolved.

General Deployment Rules

For Software development:

After developer network testing has been finished and the 4 deployment documents have been completed, the changes are installed on a test server in the production environment.

1. Tested changes are packed in binaries.

2. Binaries are obfuscated to avoid reverse-engineer hacking.

3. Binaries are transferred to development cloud (Microsoft Team System) and then downloaded by an Administrator from the Microsoft Team System and installed on the test server in the production environment.

4. A non-programmer AccountTECH staff support person is assigned to test the deploy using the test scenarios defined, and any other "real-world" tests they believe will replicate user behavior.

5. If software does not pass this QA testing or flaws in logic or security are uncovered, the deploy is either cancelled or returned to programming for further development.

6. If a software deploy passes final inspection, it is deployed to no more than 2 application servers per day until fully installed.

For network impact of software changes.

Our security vendor and internal traffic scans monitor our internal traffic 24/7 and alert us of any negative impact from the changes.

Access Control

Access control is based on the principle of "the least permissions possible". Access control policy:

1. Development team determines the minimum access that each system or application needs.
2. This gets reviewed by the Director of Programming and then presented to the CEO.
3. Security questions may require input from our security Vendors.
4. CEO gives final approval.
5. Unique system accounts are created for each distinct function or application with "least permissions" applied.
6. Active Directory service account creation or modification is reported in the monitoring tool AD Audit Plus.

Disaster Recovery

Disaster Recovery (DR) Plan Overview

Historically, the Disaster Recovery plan at AccountTECH has been focused on a these few risks - since 2001 the Disaster Recovery plan has been executed a few times due to network gear failure or hardware failure.

Throughout 2023, as the next generation of AccountTECH software moves off Citrix and into the browser, there will be major changes to the DR plan. Overall, the DR plan will be greatly simplified due to the real-time replication and application portability that is enabled by the architecture of darwin.Cloud.

With the current application, the primary areas of Disaster Recovery planning have always centered on:

1) Client data protection (backups onsite and offsite).

2) Citrix environment security.

3) Citrix environment capacity.

4) Citrix host failure and replacement planning.

5) Citrix VM failure and replacement planning.

6) Network equipment redundancy.

Now, Disaster Recovery planning is expanded to cover:

1) Hosting of entire hardware / network recovery at an secondary location using complete network & server imaging.

2) Alternatives to environment recovery by using locally installed desktop versions of AT software with API and alternate site hosted client data.

Recovery Action Plan Step-by-Step

Primary recovery goal when facing any disruption to client connectivity to AT applications is simple: get clients connected. While the reason for an outage will vary, the goal does not change. Listed below is a of instructions on "who to call" for each known potential situation.

If applications are offline for unknown reason

- Contact NOC for Security7 at (877) 664-9379
- Inquire if there is a security event that launched a shutdown of internet access in response to detected network activity.

Client login successful but client data not accessible:

- Check user access rights before proceeding (contact Broker if necessary).
- If privileges verified, contact any AccountTECH administrator and have them check user permissions on specific client folders.
- Escalate to programming.

Page unavailable: login.accounttech.com

- Contact NOC for Security7 at (877) 664-9379

Page available but Netscaler login not appearing: login.accounttech.com

- Contact Decisive Solutions: Larry Heier (617) 777-0477
- Contact Decisive Solutions: Mike Heier (617) 875-3600

Firewall failure:

- Contact NOC for Security7 at (877) 664-9379
- Get backup firewall installed at Coresite.
- Get backup firewall configuration loaded.

Switch failure:

- Contact NOC for Security7 at (877) 664-9379
- Get backup switch swapped out at CoreSite.
- Contact WatchDogIT: Adam Yen at (617) 504-6873
- Get switch configuration loaded.

Software file corruption on a single application server:

- Contact any AccountTECH administrator and have them:
  - Remove that specific application server from load balancer using XenCenter on Management desktop.
  - Restore current version of darwin application.
  - Test re-installed application.
  - Add specific application server back to load balancer using XenCenter on Management desktop.

Web application file corruption on a single web server:

- Contact Decisive Solutions, Larry Heier (617) 777-0477 or Mike Heier (617) 875-3600 and have them modify the Citrix NetScaler to remove the web server from load balancing.
- Contact any AccountTECH administrator and have them:
  - Re-install current version of TransactionPlan.
  - Test web server using developer specific TransactionPlan URL that overrides load balancer and takes programmer to a specific webserver.
  - When restored, contact Larry Heier (617) 777-0477 or Mike Heier (617) 875-3600 and have them restore web server to load balancing.

Application server VM failure (single application server):

- Contact any AccountTECH administrator and have them:
  - Remove that specific application server from load balancer using XenCenter on Management desktop.
  - Contact Decisive Solutions; Larry Heier (617) 777-0477 or Mike Heier (617) 875-3600 (or John O'Brien) and have them:
    - Disable remote logins attempts to failed VM in XenCenter.
    - Remove corrupted VM from XenHost.
    - Spin up replacement VM using same image name and same NAT IP address as VM being replaced.
    - Provision new VM and add back to XenCenter.
    - Enable logins.

Datafile failure:

- Contact Client with update on status.
- Disable logins to specific client published application.
- Contact any AccountTECH administrator and have them:
  - Recover lastest backup from onsite or offsite backup.

    - Restore client backup to database server.
    - Test darwin application against restored backup.

- Re-enable logins to specific client published application.
- Contact Client to login and review the date last modified for content in the recovered datafile.

XenHost failure

- Get VM inventory list from Google drive.
- Use email contact list to identify affected clients that need to be updated. Send email from ZohoCampaigns.
- Contact CoreSite technical support (866)777-CORE or submit a work order to have them:
    - Swap network cables from failed XenHost to replacement XenHost.
    - Power up replacement XenHost with a crash cart to confirm startup.

- Contact Decisive Solutions; Larry Heier (617) 777-0477 or Mike Heier (617) 875-3600 (or John O'Brien) and have them:
    - Use VM templates from storage to recreate all VM from failed XenHost on replacement XenHost.
    - Have them provision, and re-attach new VM to network and XenCenter.
    - Power up new VM.

- Schedule a virtual meeting and invite affected clients to be hosted by CEO or Director of Operations. Try to get an estimated time for restoration from Decisive Solutions to share with clients at the webinar.
- Contact any AccountTECH administrator and have them:
    - Restore current version of Darwin application.
    - Test re-installed application.
    - Add specific application back to published applications using XenCenter on Management desktop.

SQL Server failure

- Use email contact list in ZohoCRM to identify affected clients that need to be updated. Send email from ZohoCampaigns
- Schedule a Go-To-Webinar and invite affected clients to be hosted by CEO or Director of Operations. Try to get ETA for restoration from AccountTECH administrator to share with clients at the webinar.
- Contact any AccountTECH administrator and have them:
    - Disable client logins in XenCenter .
    - Restore client datafiles to backup SQL Server in Production.
    - Change client configuration in Admin database.
    - Test client login.
    - Re-enable client logins in XenCenter.

- Contact Client to login and review the date last modified for content in the recovered datafile.

Recovery Supplies & Recovery Team Members

Use these resources for recovery in each of the following situations

---

Client login successful but client data not accessible:

- Emergency contact list for Broker info
- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609

Page unavailable: login.accounttech.com

- Contact NOC for Security7 at (877) 664-9379
  - Escalate with
    - Ray Scholl (603) 570-9031 (ext 1737) / ray.scholl@security7.net

---

Page available but Netscaler login not appearing: login.accounttech.com

- Contact Decisive Solutions
  - Larry Heier (617) 777-0477
  - Mike Heier (617) 875-3600

Firewall failure:

- Contact NOC for Security7 at (877) 664-9379
  - Escalate with:
    - Ray Scholl (603) 570-9031 (ext 1737) / ray.scholl@security7.net
- get backup firewall from storage in Suite #8
- get backup to backup with Imperius in Google drive

Switch failure:

- Contact NOC for Security7 at (877) 664-9379
  - Escalate with Security7:
    - Ray Scholl
      - (603) 570-9031 (ext 1737)
      - ray.scholl@security7.net
- Get backup switch from storage in Suite #8
- Get backup to backup from Imperius in Google drive

Software file corruption on a single application server:

- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609
- Software backups
  - In Developers network
  - In onsite backup
  - In offsite backup with Code 42
  - In offsite backup with Imperius in Google drive

Web application file corruption on a single web server:

- Contact Decisive Solutions
  - Larry Heier (617) 777-0477
  - Mike Heier (617) 875-3600
- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609
- TransactionPlan source code backups
  - In Developers network
  - In onsite backup
  - In offsite backup with Code 42
  - In offsite backup with Imperius in Google drive

Application server VM failure (single application server):

- Contact Decisive Solutions
  - Larry Heier (617) 777-0477
  - Mike Heier (617) 875-3600
- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609
- Get VM templates from storage on
  - ATBI1 through ATBI 10

Datafile failure:

- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609
- Datafile backups
  - In onsite backup

- In offsite backup with Imperius in Google drive

XenHost failure

- VM inventory list from Google Drive
- Use email contact list from ZohoCRM
- Use ZohoCampaign with creds stored in ZohoVault
- User RingCentral Meetings with creds stored in ZohoVault
- Contact NOC for Security7 at (877) 664-9379
  - Escalate with:
    - Ray Scholl (603) 570-9031 (ext 1737) ray.scholl@security7.net
- Contact Decisive Solutions
  - Larry Heier (617) 777-0477
  - Mike Heier (617) 875-3600
- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609
- Get VM templates from storage on
  - ATBI1 thru ATBI 10

SQL Server failure

- VM inventory list from Google Drive
- Use Zoho Campaigns with creds stored in ZohoVault
- Use RingCentral Meetings with creds stored in ZohoVault
- Contact AccountTECH's Director of Programming
  - Helkyn Coello (978) 788-9609
- Datafile backups
  - In onsite backup
  - In offsite backup with Imperius in Google drive

Recovery Time Averages

Expected resolution time

Client login successful but client data not accessible:

- 20 min

Page unavailable: login.accounttech.com

- 30 min

Page available but Netscaler login not appearing: login.accounttech.com

- 4 min

Firewall failure:

- 4 - 8 hours

Switch failure:

- 4 - 8 hours

Software file corruption on a single application server:

- 30 min

Web application file corruption on a single web server:

- 20 min to change load balancer which should halt impact on clients.
- 2 hours to restore

Application server VM failure (single application server):

- 15 min for load balancer update which should halt impact on clients.
- 6 hours to restore.

Datafile failure:

- 30 min

XenHost failure

- Impact on clients can vary widely depending on the VMs hosted. For a VM loaded with redundant infrastructure servers (DC, Citrix DC, API) there will likely be in impact on clients.
- If VM represent many application servers, impact on performance (should not affect login) could last 48 hours.

SQL Server failure

- Impact on clients with data hosted on failed SQL server could be 6 - 10 hours to restore databases on alternate hardware in place.

Disaster Recovery Emergency Email Lists

The Operations Department shall maintain a list of all customers, users (excluding agents) and partners that may need to be notified in the event of an outage of any duration.

This list shall be updated every 6 months

So that notifications are sent only to clients affected by any outage, the list must include:

- The database storage location on the ATBI network the has the live client data.
- The application server that hosts the clients data (in the event that client's software is application server specific).

Recovery Point Objective

Conditional Recovery Point Objective

In the event of an event that interrupts service to a client, the RPO for client data depends on the nature of the interruption:

1. If the interruption is caused by Firewall or Network gear and not by any failure of the server hosting client software or application, the the RPO is "as of" the time of the outage, since all data will be saved an up-to-date as of that time.

2. If the interruption is caused by Application server failure and not by any failure of the server hosting client database, the the RPO is "as of" the time of the outage, since all data will be saved an up-to-date as of that time.

3. If the interruption is caused by a database server failure , then the the RPO is "end of day" for the prior day since both onsite and offsite backups are available every day.

4. If the interruption is caused by a datafile failure or corruption , then the the RPO is "end of day" for the prior day since both onsite and offsite backups are available every day.

5. If the interruption is caused by a complete failure or destruction of the entire network or infrastructure, then the the RPO is "end of day" for the prior day since both offsite backups are available every day.

In the event of an event that interrupts application availability, the RPO for any AT application is a restoration of the application to the version as of the time of the interruption. Application version restoration is possible from:

- Current version copies available in the developers networks.
- Current version available in Microsoft Team System online.
- Current version copies are available onsite backups.
- Current version copies are available in offsite backups.

Recovery Time Objective

In the event of an event that interrupts service to a client, the RTO depends on the nature of the interruption:

1. If the interruption is caused by firewall mis-configuration, then RTO should be 20 min.

2. If the interruption is caused by NetScaler performance or configuration, the the RTO should be not more than 4 min as the NetScaler self-corrects.

3. If the interruption is caused by Firewall or Network gear and not by any failure of the server hosting client data or the server hosting the client application or the Citrix infrastructure servers, then the RTO is 4-8 hours. This will allow for replacement equipment to be transported to the data center (if not already onsite) and installed and prior configuration loaded.

4. If the interruption is caused by a single application server failure and not by any failure of the server hosting client applications, the the RTO should be less than 30 min because application servers are redundant and only load balancer adjustments need to be made.

5. If the interruption is caused by an entire Xen Host failure, the RTO is two days to allow for server images to be restored to backup XenHost hardware on site. All Citrix traffic needs to be re-routed to the replacement hardware and security permissions set on all folders on the replacement hardware. Depending on the VM hosted on the failed hardware, clients may not be impacted by hardware replacement.

6. If the interruption is caused by a database server failure , the RTO is one day to allow for backup databases to be restored from either onsite or offsite storage restored on the replacement SQL Server hardware on site.

7. If the interruption is caused by a complete failure or destruction of the entire network and/or infrastructure, then the the RTO is currently unknown. We are currently developing the plan to restore the entire infrastructure based on utilizing daily veeam server images. The recovery plan we are developing involves a "plan a" recovery by reformatting existing hardware and reinstalling from offsite images (appropriate for a ransomware attack) and a "plan b" recovery by spinning up our entire environment offsite on servers contracted from Security7 (appropriate for a destruction of equipment or facility).

Step by Step Recovery Network / Darwin Desktop

Scenarios where we need to convert ALL clients to immediate Darwin desktop:

1. Citrix Storefront failure for both primary and backup. Then users would need to work with local Darwin desktop and the API servers in DMZ
2. Catastrophic network failure.

Step by Step for Citrix Storefront failure / SQL Servers and API Servers online

1. AccountTECH Staff will notify users about the failure

2. The Development team will make sure the Darwin Desktop download site is online, available and updated with the lastest version of the Darwin software
    - If not updated, the Development Team will update the software in the Darwin Desktop download site
    - Finally, the development Team will notify and send AccountTECH staff the download URL to distribute to clients

3. Using Darwin System internally at AccountTECH, from the SYSTEM --> App Clients option, the staff will get the following to give to clients
    - clientID
    - client Secret
    - API Keys

4. These are the three values required for the Darwin installation.
    - Note: Username and password is also required but there is not need to distribute this to clients since they will already know their credentials (the same always used when connecting to Darwin hosted).
    - From the App Clients screen in Darwin, AccountTECH staff will
        - select the clients to send these 3 keys to
        - Send a private note using the Privnote service and they all will get sent to each client, with a custom message that needs to include the Darwin Desktop download URL as well (and its corresponding instructions of how to install it).

5. Once clients have these keys, they will need to go to ADD/REMOVE PROGRAMS from their local computer to uninstall any previous version of Darwin Desktop they might have.

6. Then the users will need to go to the Darwin Desktop download site, download the lastest version of Darwin, follow the installation procedure

7. Once it is all installed, the client will need to launch the software in "administrator" mode by right-clicking in the software shortcut and selecting "Run as Administrator"

8. Once the software is opened, the user will be prompted to enter the clientID, clientSecret, API key, username and password.
    - Note: If not prompted to enter the clientID, clientSecret or API Key, it means they have been entered already in a prior installation so there is no need to do it again.

9. After entering all the information, the software will be ready to use for the client.

Step by Step for entire Network Catastrophic failure

1. Turn on emergency replacement hardware.
    - Power on the emergency Network
    - Make sure the following servers are running
        - Web server
        - API Servers in DMZ
        - SQL Database server in Production

2. Confirm all client databases are available on the SQL Database server emergency network

3. Depending on technology available at the moment (mirroring or backups), follow the following process in the Emergency network:

    1. If Mirroring is available: no further actions needed
    2. If Mirror backups are not available:
        1. Staff will login to the database server desktop on the emergency network
        2. Then staff will load every SQL Database backup for every client, making sure the latest one is downloaded from either the onsite or offsite backup storage
        3. Then run script to restore each of the databases on the database server on the SQL Database server emergency network

4. After this, follow the same protocol as for the "Step by Step for Citrix Storefront failure"

5. When users login to the Darwin Desktop software, the software will automatically check if the emergency network is online and if so, it will automatically connect to that network to serve the application.

Contingencies considerations

1. Darwin Desktop download with certificate embedded is also stored online in AT Emergency backup folder on Google drive
2. Double check the API URL for darwin desktop emergency network

Acknowledgement

Acknowledgement

The AccountTECH Security Manual

TO: The CEO & Senior Management

FROM: _____ (print name)

DATE: _____

This is to acknowledge that I received, read, and understand AccountTECH Security Manual. I agree to comply fully with the everything contained in the AccountTECH Security Manual and the related practices and procedures adopted by AccountTECH and understand that compliance with such standards, practices, and procedures is a condition of my continued employment with AccountTECH.

_____ _____

Employee Name (signed) Date

Violations of the AccountTECH Security Manual

Violations of the AccountTECH Security Manual

Violations of the Security Manual

The security of AccountTECH not only protects the company and our customers, but also the livelihood and mental health of all AccountTECH employees. Any violation of the AccountTECH Security Manual will lead to immediate termination.

Reporting Violations

For any employee that reports a violation of the security manual by another AccountTECH Employee will receive a $1,000.00 payment for reporting the violation. All violations must be reported directly to the designated Company Compliance Officer immediately.