GEOACL Location Based Security Solution Sample Configurations by Industry

---

Banking & Finance

Allow customers to secure access for:

- View Statement
- Search Transactions
- Stop Payment
- High-Risk Transactions like Fund Transfers, Bill Payments, Wire Transfers
- Withdrawals at ATM, Branch
- Account/Password Changes

eCommerce

Allow customers to decide from where they can do ecommerce and other **online** transactions using their credit/debit/ATM/Gift/Virtual Cards and set limits for transactions and spending limits for valid locations

Shopping & Payments

Allow customers to decide from where they can use their credit/debit/ATM/Gift/Virtual Cards for shopping at Mall, Coffee shop etc. and other retail (**offline)** payments at physical POS terminals and set limits for transactions and spending limits for valid locations.

Markets

Allow customers, traders to secure access to their trading accounts such as:

- Stocks, Bonds, Options Trading
- Commodities Trading
- Forex Trading

Investment, Asset Management Firms, Mutual Funds

Allow investors to secure their investment accounts such as:

- Retirement Accounts
- Mutual Fund Accounts
- Non-Traditional Assets like Gold, Realty

Communication & Collaboration

Allow users to secure access to their accounts such as:

- Instant Messenger,

- Chat,
- Email,
- Social Network

Corporate & Government
Take employees help to strengthen security by allowing them to secure access for:

- Account Logins to business applications they are provisioned for.
- Work related files, Documents, Data that they are working on and responsible for and saving on their allocated personal local and personal network drives or cloud storage.

Healthcare
Allow patients to secure access to digitized health related data such as:

- Medical Conditions
- Lab Results
- Treatments Received
- Prescriptions
- Doctor Visits

Storage Providers
Allow users to secure their digital files and data stored on

- internet based digital library
- network based cloud storage
- web hosting

Payroll Processors, Staffing Agencies
Allow employees, job candidates to secure access to their employment, salary and other employee associated sensitive data like SSN, Driving License stored on

- Payroll websites
- Candidate data store, Job Boards

Sample Configuration

Banking & Finance

John Smith wants to do account maintenance tasks such as link bank accounts, deposit/withdraw money to/from his trading account from/to bank account or withdraw funds using wire transfer from

home area (Main street, Old Bridge, N.J.) only, and do actual trades from home as well as office area (located at times square, New York city) using computing devices like PC or laptop or any other or using wireless devices and mobile payment platforms or any other means.

He wants this access from within say 2 mile radius from office location's centre and 5 miles radius from home location's centre as well as the route that he is using to commute to office. He doesn't want to allow his trading account to be accessed from any other location.

Based on this requirement, when ever John accesses his trading account our system will check his credentials and current geographical location against locations configured in system by John himself. When match found account features are enabled or disabled as per location.

Now even if John Smith's trading account details get stolen anyhow, hacker must have to use it from locations configured by John Smith to be able to use it. So hacker would not be able to access account from any random location and if tried from within 2 miles radius of John's time square location then he would get limited access.

If John Smith receives alert indicating rejection or suspicious activity or become aware that his trading account details are stolen he can immediately change it and or reduce radius and or cut down on locations allowed.

eCommerce

John Smith wants to use his credit card with overall credit limit $10000 for online payments from home area (‘Main street, Old Bridge, N.J.), office area (located at ‘times square, New York city’) using computing devices like PC or laptop or any other or using wireless devices and mobile payment platforms or any other means.

He wants this access from within say 2 mile radius from given location's centre. He doesn't want to allow his credit card to be utilized from any other location for online shopping. Also he wants to further security by limiting amount of invoice during online payment to $1000 maximum if credit card used from ‘times square, NYC’ area. Based on this requirement, when ever John does online payment, our system will check his credit card details and current geographical location against locations configured in system by John

himself. When card details are valid, amount is approvable and location match found, amount within location limit set if any, payment is allowed to succeed. Now even if John Smith's credit card details get stolen anyhow, hacker must have to use it from locations configured by John Smith to be able to use it. So hacker would not be able to use it from any random location and if used from within 2 miles radius of John's time square location then he would get limited access—cannot use for amount more than $1000.

If John Smith receives alert indicating rejection or suspicious activity or become aware that his card/card details are stolen he can immediately reduce spending limit and or reduce radius and or cut down on locations allowed.

Shopping & Payments

John Smith wants to use his credit card with overall credit limit $10000 for offline payments from home area (Main street, Old Bridge, N.J.), office area (located at times square, New York city) using computing devices like PC or laptop or any other or using wireless devices and mobile payment platforms or any other means.

He wants this access from within say 2 mile radius from office location's centre and 50 miles radius from home location's centre. He doesn't want to allow his credit card to be utilized from any other location for offline shopping. Also he wants to further security by limiting amount of invoice during offline payment to $500 maximum if credit card used from times square, NYC area.

Based on this requirement, when ever John does offline payment, our system will help validate current geographical location of recipient/payment accepting merchant terminal (for e.g. POS terminal) to which payment is made against locations configured in system by John himself. Merchant terminal will transmit card details, amount details and its own location details to payment gateway which will handle card details and amount validation with help of card issuer and use our system to validate location. When card details are valid, amount is approvable and location match found, amount within location limit set if any, payment is allowed to succeed.

Now even if John Smith's credit card/credit card details get stolen anyhow, hacker must have to use it from locations configured by

John Smith to be able to use it. So hacker would not be able to use it from any random location and if used from within 2 miles radius of John's time square location then he would get limited access cannot use for amount more than $500.

If John Smith receives alert indicating rejection or suspicious activity or become aware that his card/card details are stolen he can immediately reduce spending limit and or reduce radius and or cut down on locations allowed.

Markets

John Smith wants to do account maintenance tasks such as link bank accounts, deposit/withdraw money to/from his trading account from/to bank account or withdraw funds using wire transfer from home area (Main street, Old Bridge, N.J.) only, and do actual trades from home as well as office area (located at times square, New York city) using computing devices like PC or laptop or any other or using wireless devices and mobile payment platforms or any other means.

He wants this access from within say 2 mile radius from office location's centre and 5 miles radius from home location's centre as well as the route that he is using to commute to office. He doesn't want to allow his trading account to be accessed from any other location. Based on this requirement, when ever John accesses his trading account our system will check his credentials and current geographical location against locations configured in system by John himself. When match found account features are enabled or disabled as per location.

Now even if John Smith's trading account details get stolen anyhow, hacker must have to use it from locations configured by John Smith to be able to use it. So hacker would not be able to access account from any random location and if tried from within 2 miles radius of John's time square location then he would get limited access.

If John Smith receives alert indicating rejection or suspicious activity or become aware that his trading account details are stolen he can immediately change it and or reduce radius and or cut down on locations allowed.

Investment, Asset Management Firms, Mutual Funds

John Smith wants to do account maintenance tasks such as link retirement/investment account with bank accounts, change plans, do internal or external account transfers to/from his retirement/investment account from home area (Main street, Old Bridge, N.J.) only, and review account balances, account history or view pending transactions from home as well as office area (located at times square, New York city) using computing devices like PC or laptop or any other or using wireless devices and mobile payment platforms or any other means of access. He wants this access from within say 2 mile radius from office location's center and 5 miles radius from home location's center as well as the route that he is using to commute to office. He doesn't want to allow his retirement/investment account to be accessed from any other location.

Based on this requirement, whenever John accesses his retirement/investment account our system will check his credentials and current geographical location against locations configured in system by himself. When match found account features are enabled or disabled as per location.

Now even if John Smith's retirement/investment account details get stolen anyhow, hacker must have to use it from locations configured by John Smith to be able to use it. So hacker would not be able to access account from any random location and if tried from within 2 miles radius of John's time square location then he would get limited access. If John Smith receives alert indicating rejection or suspicious activity or become aware that his retirement account details are stolen he can immediately change it and or reduce radius and or cut down on locations allowed.

Communication & Collaboration

John Smith wants to do account maintenance tasks such as set rules/filters, set email archival policy, change out of office greeting, manage folders, delete old emails/messages, manage contacts, add friends, change server account connection details, from home area (Main street, Old Bridge, N.J.) only, and use it to compose, send receive emails, read, send messages, set status messages, from home area as well as office area, (located at times square, New York city) using computing devices like PC or laptop or any other or using wireless devices or any other means of communication.

He wants this access from within say 2 mile radius from office location's centre and 5 miles radius from home location's centre as well as the route that he is using to commute to office. He doesn't want to allow his email/chat/IM/Social Network account to be accessed from any other location.

Based on this requirement, whenever John accesses his account our system will check his credentials and current geographical location against locations configured in system by John himself. When match found account features are enabled or disabled as per location.

Now even if John Smith's communication account details get stolen anyhow, hacker must have to use it from locations configured by John Smith to be able to use it. So hacker would not be able to access account from any random location and if tried from within 2 miles radius of John's time square location then he would get limited access.

If John Smith receives alert indicating rejection or suspicious activity or become aware that his communication account details are stolen he can immediately change it and or reduce radius and or cut down on locations allowed.

Storage Providers

John Smith wants to do maintenance tasks such as purge older data, upload new data, create new data; manage folders, change security settings, connection details, from home area (Main street, Old Bridge, N.J.) only, and have read only access from home area as well as office area, (located at times square, New York city) using computing devices like PC or laptop or any other or using wireless devices or any other means of communication.

He wants this access from within say 2 mile radius from office location's center and 5 miles radius from home location's centre as well as the route that he is using to commute to office. He doesn't want to allow his data files to be accessed from any other location. Based on this requirement, whenever John accesses his medium our system will check his credentials and current geographical location against locations configured in system by John himself. When match found access given would be as per location.

Now even if John Smith's credential details to access his files get

stolen anyhow, hacker must have to use it from locations configured by John Smith to be able to use it. So hacker would not be able to access his flies from any random location and if tried from within 2 miles radius of John's time square location then he would get limited access.

If John Smith receives alert indicating rejection or suspicious activity or become aware that his credential details are stolen he can immediately change it and or reduce radius and or cut down on locations allowed.