

Beveiligingsmaatregelen RoutIT

RoutIT

Datum: 19 december 2016

Versielog RoutIT

Start document	Juli 2015
Nieuwe layout en aanpassing internet linken ivm nieuwe website CBG Connect B.V.	19 december 2016

Inhoudsopgave

1	Voice portal beveiliging met pincode	4
2	Beveiligingsmaatregelen Voice over IP Telefooncentrale	4
3	Richtlijnen beveiligen eindgebruikersapparatuur	10
4	Algemene kaderzetting van deze dienstbeschrijving	10

1 Voice portal beveiliging met pincode

Disclaimer: Op het moment dat een klant een beveiligingsinstelling aanpast binnen het Voice over IP Telefonie platform, kan CBG Connect niet meer instaan voor de (financiële) gevolgen van deze aanpassing.

Standaard stelt RoutIT de beveiligingsparameters binnen het Voice over IP-platform zo in dat het platform maximaal beveiligd is. Als er geen wijzigingen worden aangebracht in deze instellingen, is de kans relatief klein dat er misbruik kan worden gemaakt van het Voice over IP-platform. Onder misbruik verstaan we het ongewenst bellen op kosten van de klant.

De zwakste schakel in beveiliging is de menselijke factor, de klant. Het Voice over IP-platform biedt de mogelijkheid om via de telefoon het voice portal te benaderen. Vanuit het voice portal kan de klant zijn of haar voicemail afluisteren, maar ook call forwarding instellen. Om te voorkomen dat iedereen hierbij kan, is het voice portal beveiligd met een pincode. De klant moet zich realiseren dat deze pincode hetzelfde behandeld moet worden als de pincode die hij gebruikt voor zijn bankpas. Immers, in beide gevallen kan slordig omgaan met de pincode resulteren in een aanzienlijke schade voor de klant.

2 Beveiligingsmaatregelen Voice over IP Telefooncentrale

Disclaimer: RoutIT en CBG Connect aanvaarden geen aansprakelijkheid voor schade door misbruik die ontstaat doordat onbevoegden toegang hebben tot het HIP-platform via gegevens of systemen van gebruikers van het HIP-platform.

Dit document beschrijft een pakket aan beveiligingsmaatregelen die zijn opgesteld voor het RoutIT HIP-platform. De maatregelen zijn gericht op het voorkomen en detecteren van misbruik, en het beperken van de mogelijke financiële schade.

RoutIT biedt de partner in specifieke gevallen de mogelijkheid van deze maatregelen af te wijken. Het advies van RoutIT is alleen van de maatregelen af te wijken op verzoek van de klant en na uitleg en vastlegging van de risico's. Als er wordt afgeweken draagt de klant hiervoor vanzelfsprekend de verantwoordelijkheid.

Maatregelen voor de hosted telefooncentrale

In de onderstaande tabel worden de beveiligingsmaatregelen opgesomd. Tevens wordt aangegeven op welke manier een partner hiervan kan afwijken. In de volgende paragrafen wordt beschreven waar de verschillende instellingen binnen het HIP-platform te vinden zijn om eventuele afwijkingen te kunnen implementeren.

Beveiligingsmaatregel	Afwijken van de maatregel
<p>Pincode policy voor het Voiceportal</p> <ul style="list-style-type: none"> • Initiële instelling van de pincode is onbekend en niet gemakkelijk te raden • Pincode bestaat uit tenminste 6 cijfers • 2 gelijke opeenvolgende getallen is niet toegestaan • Pincode mag niet gelijk zijn aan telefoonnummer of extensie • Pincode mag niet gelijk zijn aan de oude pincode • Pincode mag niet gelijk zijn aan de oude pincode omgekeerd • Pincode verloopt na 30 dagen • Login mogelijkheid wordt uitgeschakeld na 3 mislukte pogingen 	<p>Er kan worden afgeweken van de standaard pincode policy op Enterprise, Group niveau. Neem contact op met CBG Connect voor advies en wijzigingen.</p>
<p>Beperken gelijktijdige gesprekken</p> <ul style="list-style-type: none"> • Het aantal gelijktijdige gesprekken per gebruiker (user) is beperkt tot vijf • Het aantal gelijktijdige doorgeschakelde gesprekken per gebruiker (user) is beperkt tot drie 	<p>Er kan worden afgeweken van het standaard maximaal aantal gelijktijdige (doorgeschakelde) gesprekken per gebruiker (user) op Enterprise, Group en User niveau via 'call processing policies'</p> <p>Neem contact op met CBG Connect voor advies en wijzigingen.</p>
<p>Beperken doorschakelmogelijkheden</p> <ul style="list-style-type: none"> • Het is niet mogelijk door te schakelen naar internationale nummers • Het is niet mogelijk door te schakelen naar 090x nummers 	<p>Er kan worden afgeweken op Group niveau via 'Outgoing Calling Plan'.</p> <p>Neem contact op met CBG Connect voor advies en wijzigingen.</p>
<p>Blokkeringslimiet op verbruik</p> <ul style="list-style-type: none"> • In de VOIP portal wordt een blokkeringslimiet ingesteld bij iedere klant. Bij overschrijding van de limiet wordt het account geblokkeerd voor alle gesprekken, behalve alarmnummers en nationale vaste nummers. 	<p>De standaard limiet waarde wordt automatisch ingesteld bij initiatie van het account. Door CBG Connect kan in overleg met de klant naar eigen inzicht de limiet worden bijgesteld.</p> <p>CBG Connect plaatst altijd een standaard melding bij 80% van gebruik.</p>

Beveiliging devices

Voor wat betreft telefoontoestellen, lokale telefooncentrales en modems waarin VOIP accounts worden geconfigureerd gelden de volgende best-practices met betrekking tot beveiliging:

- Maak zoveel mogelijk gebruik van Autoprovisioning, waarin standaard de best-practices voor beveiliging zijn opgenomen.
- Maak gebruik van een IP-VPN, of zorg ervoor dat telefoontoestellen niet bereikbaar zijn vanaf het (publieke) internet
- Schakel de web interface van het telefoontoestel of modem uit (standaard bij Autoprovisioning)
- Wijzig het standaard (beheer) wachtwoord van het modem of toestel in een veilig wachtwoord (standaard bij Autoprovisioning)
- Stel voor elke klant in de Billingportal nauwgezet de waarschuwings- en blokkeringslimiet in
- Pas de beveiligingsmaatregelen toe voor VOIP die beschreven zijn in de RoutIT Kennisdatabase onder VOIP / VOIP Algemeen / Securityrichtlijnen

3 Beveiligingsmaatregelen Voice over IP gebruiker

Disclaimer: Op het moment dat een klant een beveiligingsinstelling aanpast binnen het Voice over IP platform, kunnen RoutIT en CBG Connect niet meer instaan voor de (financiële) gevolgen van deze aanpassing. Wijzigingen vallen onder de verantwoordelijkheid van de eindklant.

Bij het aanmaken van een nieuwe gebruiker (account) wordt er standaard een random pincode gegenereerd t.b.v. de voice portal. Als de nieuwe gebruiker de voice portal wil gebruiken, dient eerst de pincode in de Broadworks webinterface gereset te worden. Wat betreft de nieuwe pincode zijn er de volgende regels actief:

1. Pincode mag niet bestaan uit herhalende karakters (bijv. 0000).
2. Pincode mag niet de extensie of het telefoonnummer van de gebruiker zijn.
3. Pincode mag niet de omgekeerde extensie of het telefoonnummer van de gebruiker zijn.
4. Bij het verlopen van de pincode (na 30 dagen) mag de nieuwe pincode niet de oude pincode zijn.
5. Bij het verlopen van de pincode (na 30 dagen) mag de nieuwe pincode niet de omgekeerde oude pincode zijn.
6. Pincode moet bestaan uit minimaal vier en maximaal acht cijfers.
7. Pincode wordt geblokkeerd na drie foutieve inlogpogingen. Verder adviseren wij u om geen opvolgende cijfers (1234) te gebruiken voor de pincode.

De pincodepolicy kan op meerdere niveaus worden aangepast. RoutIT heeft bovenstaande policy ingesteld op systeemniveau. Op zowel partnerniveau als klantniveau kan afgeweken worden van deze policy. Als eindklant bent u zelf verantwoordelijk voor de mogelijke gevolgen van het aanpassen van de policy (zie disclaimer).

4 Instellen van pincode Policy

Instellen op Group-niveau via: Group: Utilities > Passcode Rules

Passcode Rules

Configure the passcode rules to be used when creating or updating Portal passcodes.

OK Apply Cancel

Portal users use:
 System Rules
 Service Provider / Enterprise Rules
 Group Rules

Passcode format:
 cannot be the user's own extension or phone number
 cannot be the user's own extension or phone number reversed
 cannot contain 3 or more repeated digits
 cannot contain more than 3 sequentially ascending digits or 3 sequentially descending digits
 cannot be repeating patterns
 cannot be any of the last 1 passcode(s)
 cannot be the reversed old passcode
 must be at least 6 characters, no more than 12 characters

Passcodes expire:
 Never After 30 Days

Disable login:
 Never After 3 failed login attempts
 When login is disabled, send e-mail to:
broadsoft-in@routit.nl

OK Apply Cancel

5 Instellen mogelijke bel en doorschakel bestemmingen

Instellen op Group-niveau via: Group: Calling Plan > Outgoing Calling Plan

Zie [Outgoing Calling Plan](#) voor een beschrijving van de inhoud van de verschillende categorieën.

Toegestane bel-bestemmingen op tabblad: Originating. **Schakel de volgende categorieën UIT: Unknown.**

Outgoing Calling Plan

Customize the Outgoing Calling Plan for the group and/or departments.

OK Apply Cancel

Originating Initiating Call Forwards Being Forwarded/Transferred

Department	Group	Local	Toll Free	Toll	International	Operator Assisted	Chargeable Directory Assistance	Special Services I	Special Services II	Premium Services I	Premium Services II	Casual	URL Dialing	Unknown
Group Default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select from drop-down list to permit call type; Users can be configured with their own custom settings in user-level Calling Plan

Legend

- Allow Y
- Block N
- Authorization code required A
- Transfer to 1st transfer number T1
- Transfer to 2nd transfer number T2
- Transfer to 3rd transfer number T3

OK Apply Cancel

Toegestane doorschakelbestemmingen op tabblad: Initiating Call Forwards. **Schakel de volgende categorieën UIT: International, Special Services I, Special Services II, Premium Services I, Casual en Unknown**

Outgoing Calling Plan

Customize the Outgoing Calling Plan for the group and/or departments.

OK Apply Cancel

Originating Initiating Call Forwards Being Forwarded/Transferred

Department	Group	Local	Toll Free	Toll	International	Operator Assisted	Chargeable Directory Assistance	Special Services I	Special Services II	Premium Services I	Premium Services II	Casual	URL Dialing	Unknown
Group Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Check box to permit call type; Users can be configured with their own custom settings in user-level Calling Plan

OK Apply Cancel

6 Instellen aantal gelijktijdige gesprekken per user

Instellen op Enterprise-niveau via: Profile > Call Processing Policies

Options:

- Profile
- Resources
- Services
- Call Center
- Communication Barring
- Meet-Me Conferencing
- Utilities

Call Processing Policies

View or modify Call Processing Policies for the enterprise.

OK Apply Cancel

Calling Line ID

External Calls: Use user phone number for Calling Line Identity
 Use configurable CLID for Calling Line Identity

Enterprise Calls: Use extension
 Use location code plus extension
 Use External Calls Policy

Group Calls: Use extension
 Use location code plus extension
 Use External Calls Policy

Emergency Calls: Use user phone number for Calling Line Identity
 Use configurable CLID for Calling Line Identity

Allow Alternate Numbers for Redirecting Identity
 Allow Configurable CLID for Redirecting Identity
 Block Calling Name for External Calls

Media

Media Policy: Force Use of Uncompressed Codec
 Use Supported Media:
 None

Call Limits

Enable Maximum Number of Concurrent Calls Calls
 Enable Maximum Number of Concurrent Video Calls Video Calls
 Enable Maximum Duration for Answered Calls Minutes
 Enable Maximum Duration for Unanswered Calls Minutes
 Enable Maximum Number of Concurrent Redirected Calls Calls
 Enable Maximum Number of Concurrent Find Me/Follow Me Invocations Invocations
 Enable Maximum Find Me/Follow Me Depth
Maximum Redirection Depth:

Instellen op Group-niveau via: Group: Profile > Call Processing Policies

Call Limits

Use Group Call Limits Policy Use Service Provider/Enterprise Call Limits Policy

Enable Maximum Number of Concurrent Calls Calls

Enable Maximum Number of Concurrent Video Calls Video Calls

Enable Maximum Duration for Answered Calls Minutes

Enable Maximum Duration for Unanswered Calls Minutes

Enable Maximum Number of Concurrent Redirected Calls Calls

Enable Maximum Number of Concurrent Find Me/Follow Me Invocations Invocations

Enable Maximum Find Me/Follow Me Depth

Maximum Redirection Depth:

Instellen op Group-niveau via: User: Profile > Call Processing Policies

Call Limits

Use User Call Limits Policy Use Group Call Limits Policy

Enable Maximum Number of Concurrent Calls Calls

Enable Maximum Number of Concurrent Video Calls Video Calls

Enable Maximum Duration for Answered Calls Minutes

Enable Maximum Duration for Unanswered Calls Minutes

Enable Maximum Number of Concurrent Redirected Calls Calls

Enable Maximum Number of Concurrent Find Me/Follow Me Invocations Invocations

Enable Maximum Find Me/Follow Me Depth

Maximum Redirection Depth:

7 Richtlijnen voor een veilig wachtwoord

- Zorg dat uw wachtwoord langer is dan 8 tekens.
Hoe langer een wachtwoord is des te moeilijker is het te raden. Een lang 'makkelijk' wachtwoord is zelfs beter dan een kort moeilijk wachtwoord.
- Combineer hoofd- en kleine letters, cijfers en symbolen.
Maar kies geen opeenvolgende reeksen zoals '98765432' of '22222222' of bijvoorbeeld lettercombinaties van toetsen die naast elkaar op het toetsenbord staan zoals 'qwerty' of '!@#\$\$%'.
• Bedenk een makkelijk te onthouden zin met minstens één getal en één leesteken (symbool).
Bijvoorbeeld: 'Ik houd honderd keer meer van Simon dan van Arnold.' Neem van elk woord daarna de eerste letter en verander de getallen en leestekens. Het veilige wachtwoord luidt dan: Ih100kmvSdvA.
- Voor een nog veiliger wachtwoord vervangt u nog enkele tekens door andere tekens die erop lijken.
Vervang in bovenstaand voorbeeld de hoofdletter "I" door een "1", de letter "k" door de hoofdletter "X", de "S" door een dollarteken en de hoofdletter "A" door een "@". Het wachtwoord is dan vrijwel onherkenbaar voor anderen, maar niet voor u en ziet er als volgt uit: 1h100Xmv\$dv@.
- Verander de wachtwoorden regelmatig, bijvoorbeeld elke 60 dagen.
- Hanteer voor verschillende systemen verschillende wachtwoorden.
- Maak in het wachtwoordbeleid onderscheid in de wachtwoorden die bedoeld zijn voor 'vertrouwde' diensten zoals de lokale pc en publieke diensten zoals bijvoorbeeld een website t.b.v. webmail.

8 Algemene kaderzetting van deze dienstbeschrijving

Deze dienstbeschrijving vormt een onlosmakelijk deel van de ondertekende offerte in combinatie met Algemene koop- en leveringsvoorwaarden CBG Connect, de Algemene Voorwaarden Service Provider RoutIT en mogelijke bedrijfsspecifieke voorwaarden en afspraken en productbrochures.

De informatie in deze dienstbeschrijving is gelijk aan de informatie van Service provider RoutIT

CBG Connect behoudt zich het recht voor deze dienstbeschrijving zonder voorafgaande melding te wijzigen.

De dienstbeschrijving is uitsluitend bestemd voor intern gebruik binnen uw organisatie. Het maakt onderdeel uit van het contract tussen u en CBG Connect. Het document is aan u verstrekt om een afgewogen keuze te kunnen maken voor CBG Connect als leverancier van deze dienst.

Alle rechten met betrekking tot dit document zijn voorbehouden aan CBG Connect. Niets uit deze publicatie of delen ervan mag op enigerlei wijze worden gereproduceerd, toegankelijk gemaakt in een database of op andere wijze aan derden beschikbaar worden gesteld, tenzij CBG Connect hier op uitdrukkelijk verzoek van uw bedrijf schriftelijk toestemming voor heeft verleend.

Wijzigingen en typefouten voorbehouden.

CBG Connect B.V., December 2016