Manual do Desenvolvedor

3.0.4

senhasegura

v2.0 2020–2.

Sumário

1 Integração **4**

1.1 Integração via Webservice. 4

1.2 Uso de requisições padrão 5

1.3 Atividades 5

1.4 Métodos 6

1.4.1 Consulta de um único dispositivo 6

1.4.2 Listagem de dispositivos 7

1.4.3 Consulta de Credencial e Chave 9

1.4.4 Cadastro e Alterações de Credenciais 12

1.4.5 Criação e alteração de chaves 13

1.4.6 Inativação de Credencial ou Chave 15

1.4.7 Consulta a Informações Protegidas. 16

1.4.8 Criação e alteração da informação protegida 17

1.4.9 Inativação da informação protegida 18

1.4.10 Encerramento compulsório de sessão proxy 19

1.5 WebService App2App 20

1.5.1 Atividades 20

2 Certificate Management - Integração **27**

2.1 Introdução 27

2.1.1 Como o Certificate Management funciona 27

2.1.2 Definições 27

2.1.3 Atividades 28

2.2 Métodos 28

2.2.1 Criar/Modificar Request 28

2.2.2 Consultar/Listar Request 32

2.2.3 Assinar Request 37

2.2.4 Consultar/Listar Certificados 38

2.3 Funcionalidades 45

2.3.1 Publicar Certificado 45

2.3.2 Consultar/Listar Publicações 47

2.3.3 Criar/Editar Perfil de Publicação Apache 49

2.3.4 Criar/Editar Perfil de Publicação IIS 51

2.3.5 Criar/Editar Perfil de Publicação F5 BigIP 53

2.3.6 Criar/Editar Perfil de Publicação WebSphere WAS 56

3 Termos e condições de uso **59**

3.1 Licenças senhasegura 59

3.2 Outras licenças 60

1 Integração

1.1 Integração via Webservice

A ***API*** de integração do senhasegura® permite outras aplicações a criar, consultar, modificar e inativar credenciais, chaves e outras informações protegidas via webservices. O webservices segue uma arquitetura ***REST*** e utiliza autenticação pelo método ***OAuth v2.0***.

Cada requisição ao serviço é registrada com a data, tempo, IP de origem, e identificação de qual aplicação cliente ***API***. Dados sensíveis como senhas e chaves, serão removidas desta mensagem de log.

Cada acesso proveniente de aplicação cliente é controlada, em adição ao método de autenticação ***OAuth v1.0***, pelo IP do requisitante.

Cada cliente tem acesso apenas as credenciais registradas por ele próprio ou direcionada através de configuração na aplicação.

Senhas podem ser ***Credenciais*** para acesso a ***Dispositivos*** como servidores e roteadores, tanto quanto chaves RSA utilizadas para acesso ***SSH***. Senhas são automaticamente alteradas pela aplicação conforme as políticas configuradas.

Informação protegida é um tipo de informação que não é alterada pelo senhasegura® . Pode ser utilizado para armazenar informações sensíveis como as chaves de certificados ***SSH*** ou chaves de ***API***.

1.2 Uso de requisições padrão

Cada requisição no WebService App2App deve ter o ***OAuth Consumer Key*** e o ***OAuth Token*** do cliente. Desta forma, cada URI de requisição apresenta-se aproximadamente como seguinte exemplo:

`https://senhasegura/iso/`*`MODULO`*`/`*`FUNCAO`*`?oauth_consumer_key=`*`KEY`*`&oauth_token=`*`TOKEN`*

MODULO senhasegura® WebService App2App function module

FUNCAO Module function

KEY Client OAuth key

TOKEN Client OAuth token

Quando utilizado o método `GET`, não esqueça de adicionar `oauth_consumer_key` e `oauth_token` antes dos demais argumentos.
Quando utilizado o método `POST`, ambos parâmetros deve estar preenchidos na URL como se faz nos métodos `GET`.

1.3 Atividades

Nesta seção, as seguintes funcionalidades do senhasegura® serão apresentadas:

- Executar requisições
- Receber respostas
- Consulta de credenciais e chaves
- Criação e alteração de credenciais e chaves
- Inativação de credenciais e chaves
- Consulta de informações protegidas
- Criação e alteração de informações protegidas
- Inativação de informações protegidas

1.4 Métodos

O senhasegura® WebService App2App possui métodos de consulta, criação e alteração de informações armazenadas na aplicação.

1.4.1 Consulta de um único dispositivo

```
GET /iso/coe/dispositivo/[id]?[&parameter=value]
```

Retorna as informações do dispositivo que estão armazenadas na aplicação.

Parâmetros de requisição

Campo	Tipo	Descrição	Requerido
id	Texto	Id do dispositivo	Sim

Resposta

A resposta consiste em um dicionário do dispositivo com os seguintes campos:

Campo	Tipo	Descrição
id	Número	Id do dispositivo
hostname	Texto	Hostname do dispositivo
ip	Texto	Endereço IPv4
site	Texto	Site do dispositivo

```
1 {
```

```
  "response": {
    "status": 200,
    "mensagem": "Dispositivo 1",
    "erro": false
  },
  "dispositivo": {
    "id": "4",
    "hostname": "w12kca2012",
    "ip": "10.0.0.11",
    "site": "Production"
  }
}
```

1.4.2 Listagem de dispositivos

```
GET /iso/coe/dispositivo?[&parameter=value]
```

Retorna uma lista de dispositivos que coincidem com os campos da consulta.

Parâmetros de requisição

Campo	Tipo	Descrição	Requerido
hostname	Texto	Hostname do dispositivo	Não
ip	Texto	Endereço IPv4	Não
tipo	Texto	Nome do tipo de dispositivo	Não
fabricante	Texto	Fabricante do dispositivo	Não
modelo	Texto	Nome do modelo de dispositivo	Não
site	Texto	Site do dispositivo	Não
offset	Número	Paginação da resposta	Não
limit	Número	Quantidade máxima de registros na resposta	Não

Resposta

Uma lista de dispositivos que coincidem com os campos pesquisados:

Campo	Tipo	Descrição
id	Número	Id do dispositivo
hostname	Texto	Hostname do dispositivo
ip	Texto	IPv4 do dispositivo
tipo	Texto	Nome do tipo de dispositivo
fabricante	Texto	Fabricante do dispositivo
modelo	Texto	Modelo do dispositivo
site	Texto	Site do dispositivo


```
{
  "response": {
    "status": 200,
    "mensagem": "2 equipamentos encontrados",
    "erro": false
  },
  "dispostivos": [
    {
      "id": "5",
      "hostname": "Windows 2016",
      "ip": "10.0.0.121",
      "modelo": "Windows Server 2016",
      "tipo": "Server",
      "fabricante": "Microsoft",
      "site": "Default"
    },
    {
      "id": "8",
      "hostname": "sbox-deb9",
      "ip": "10.0.0.171",
      "modelo": "8.0 Jessie",
      "tipo": "Server",
      "fabricante": "Debian",
      "site": "Default"
```

```
    }
  ]
}
```

1.4.3 Consulta de Credencial e Chave

```
GET /iso/coe/senha/[identificador]
```

```
GET /iso/coe/chave/[identificador]
```

Retorna a credencial o chave armazenada na aplicação.

Parâmetros

Campo	Tipo	Descrição	Requerido
Identificador	Número	Id da credencial ou identificador para webservice	Sim

Resposta para credenciais

A resposta consiste em um dicionário composto pelos seguintes campos:

Campo	Tipo	Descrição
id	Número	Id da credencial
tag	Texto	Identificador para webservices da credencial
username	Texto	Username da credencial
senha	Texto	Senha da credencial
conteudo	Texto	Senha da credencial

hostname	Texto	Hostname do dispositivo dono da credencial
senha_pai_cod	Número	Id da credencial pai
senha_pai	Texto	Credencial pai
adicional	Texto	Informações adicionais
ip	Texto	IP do dispositivo da credencial
porta	Número	Porta de acesso padrão do dispositivo
modelo	Texto	Modelo do dispositivo
datahora_expiracao	Data/Hora	Data e hora de expiração da credencial.


```
{
    "response": {
        "status": 200,
        "mensagem": "Senha 1",
        "erro": false
    },
    "senha": {
        "id": "1",
        "tag": null,
        "username": "usrdomadm",
        "senha": "c3Rlcjg4QHF3ZW1h",
        "conteudo": "c3Rlcjg4QHF3ZW1h",
        "hostname": "w2012data",
        "senha_pai_cod": null,
        "senha_pai": null,
        "adicional": null,
        "dominio": "sbox.lab",
        "ip": "10.0.100.50",
        "porta": "3389",
        "modelo": "Windows Server 2012 R2",
        "datahora_expiracao": "2019-03-02T11:59:50"
    }
}
```


Resposta para chaves

A resposta consiste em um dicionário composto pelos seguintes campos:

Campo	Tipo	Info
id	Número	Id da credencial
username	Texto	Username da credencial
hostname	Texto	Hostname do dispositivo dono da credencial
ip	Texto	IP do dispositivo da credencial
chave_privada	Texto	Chave privada, se aplicável
chave_publica	Texto	Chave pública, se aplicável
senha	Texto	Senha da credencial
datahora_expiracao	Data/Hora	Data e hora de expiração da credencial.

```
{
    "response": {
        "status": 200,
        "mensagem": "Chave 37",
        "erro": false
    },
    "chave": {
        "id": "37",
        "username": "usrltdo",
        "hostname": "sbox-demo-rhel",
        "ip": "172.16.35.100",
        "chave_privada": "-----BEGIN OPENSSH PRIVATE KEY-----
        ...
        -----END OPENSSH PRIVATE KEY-----",
        "chave_publica": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQA
        ...
         usrltdo@sbox-demo-rhel",
        "senha": "123456",
        "datahora_expiracao": null
    }
}
```

1.4.4 Cadastro e Alterações de Credenciais

```
POST /iso/coe/senha/[identificador]
```

Cria ou altera uma credencial

Parameters

Campo	Tipo	Descrição	Requerido
identificador	Texto	Id da credencial. Se não for especificado, uma nova credencial será criada e o ID será retornado na resposta	Não
hostname	Texto	Hostname do dispositivo	Sim
ip	Texto	IP de acesso do dispositivo	Sim
conteudo	Texto	Senha ou conteúdo da chave	Sim
tipo_senha	Texto	Nome do tipo de credencial	Não
username	Texto	Usuário da credencial ou chave	Não
site	Texto	Site do dispositivo	Não
modelo	Texto	Modelo do dispositivo	Não
fabricante	Texto	Fabricante do dispositivor	Não
tipo	Texto	Tipo de dispositivo	Não
conectividades	Texto	Conectividades separadas por vírgula. Ex: SSH:22,TELNET:21	Não
dominios_dispositivo	Texto	Domínios do dispositivo separados por vírgula	Não
tags_dispositivo	Texto	Tags do dispositivo	Não
dominio	Texto	Domínio da Credencial	Não
tags	Texto	Tags da credencial	Não
adicional	Texto	Informação adicional da Credencial	Não
senha_pai	Número	Id da Credencial pai	Não

Resposta

A resposta consiste em um dicionário de credenciais ou chaves com seguintes campos:

Campo	Tipo	Descrição
id	Número	Id da credencial
tag	Texto	Identificador da credencial, caso haja um.

```
{
  "response": {
    "status": 201,
    "message": "Password created successfully",
    "error": false
  },
  "password": {
    "id": "5",
    "tag": null
  }
}
```

1.4.5 Criação e alteração de chaves

```
POST /iso/coe/chave/[identificador]
```

Cria ou altera o registro de uma chave.

Parâmetros

Campo	Tipo	Descrição	Requerido

identificador	Texto	ID numérico da chave. Se não for especificado, uma nova chave será criada e seu ID retornado na resposta.	Não
hostname	Texto	Hostname do dispositivo	Sim
ip	Texto	IP de acesso do dispositivo	Sim
chave_privada	Texto	Conteúdo da chave privada	Sim
chave_publica	Texto	Conteúdo da chave pública	Sim
tipo_senha	Texto	O nome do tipo de credencial	Não
username	Texto	Usuário da credencial, se aplicável	Não
senha	Texto	Senha da chave, se aplicável	Não
site	Texto	Site do dispositivo	Não
modelo	Texto	Nome do modelo de dispositivo	Não
fabricante	Texto	Nome do fabriante do dispositivo	Não
tipo	Texto	Nome do tipo de dispositivo	Não
conectividades	Texto	Conectividade separada por vírgula. Ex: SSH:22,TELNET:21	Não
dominios_dispositivo	Texto	Domínio separado por vírgula	Não
tags_dispositivo	Texto	Tags do dispositivo separado por vírgula	Não
tags	Texto	Tags da credencial separado por vírgula	Não

Resposta

A resposta consiste em um dicionário de credenciais contendo os seguintes campos:

Campo	Tipo	Descrição
id	Número	Id da chave
tag	Texto	Identificador da chave, se aplicável

```
{
  "response": {
    "status": 201,
```

```
    "message": "Chave cadastrada com sucesso!",
    "error": false
  },
  "password": {
    "id": "5",
    "tag": null
  }
}
```

1.4.6 Inativação de Credencial ou Chave

```
DELETE /iso/coe/senha/[identificador]
```

```
DELETE /iso/coe/chave/[identificador]
```

Inativa o registro e uso de uma credencial ou chave. Uma vez inativo, a credencial ou chave não pode mais ser retornada ou alterada por métodos WebService App2App . Um usuário com permissão poderá reativar a credencial através da interface web.

Parâmetros

Campo	Tipo	Descrição	Requerido
identificador	id	Id numérico da credencial ou chave	Não

Resposta da Inativação de Credencial

```
{
    "response": {
        "status": 410,
        "mensagem": "Credencial inativa",
        "erro": false
```

```
    }
}
```

Resposta da Inativação de Chave

```
{
    "response": {
        "status": 200,
        "mensagem": "Chave removida",
        "erro": false
    }
}
```

1.4.7 Consulta a Informações Protegidas

```
GET /iso/coe/info/[identificador]
```

Retorna o registro de uma informação protegida.

Parameters

Campo	Tipo	Descrição	Requerido
Identificador	Texto	ID numérico da informação protegida ou identificador registrado na informação protegida.	Sim

Resposta

A resposta consiste em um dicionário da informação protegida contendo os seguintes campos:

Campo	Tipo	Descrição
id	Número	ID da informação protegida
tag	Texto	Identificador da informação protegida
tipo	Texto	Tipo da informação protegida
conteudo	Texto	Conteúda da informação

```
{
    "response": {
        "status": 200,
        "mensagem": "Informacao 3",
        "erro": false
    },
    "info": {
        "id": "3",
        "tag": "myidentifier",
        "tipo": "Access credential",
        "conteudo": "My secret notes"
    }
}
```

1.4.8 Criação e alteração da informação protegida

```
POST /iso/coe/info/[identificador]
```

Parâmetros

Campo	Tipo	Descrição	Requerido
identificador	Texto	ID numérico da informação protegida ou identificador registrado a informação protegida. Zero para criar um novo registro.	Não

nome	Texto	Nome da informação	Sim
conteudo	Texto	Conteúdo da informação	Sim
tipo	Id	Tipo de informação: 1- Certificado Digital 2- Credencial de Acesso	Não

Resposta

A resposta consiste em um dicionário contendo os seguintes campos:

Campo	Tipo	Descrição
id	Número	ID da informação
tags	Texto	Identificador da informação, se aplicável

```
{
    "response": {
        "status": 201,
        "mensagem": "Informacao cadastrada com sucesso!",
        "erro": false
    },
    "info": {
        "id": "4",
        "tag": null
    }
}
```

1.4.9 Inativação da informação protegida

```
DELETE /iso/coe/info/[identificador]
```

Inativa o registro da informação protegida. Uma vez inativa, a informação não retornará nas

consultas via WebService App2App . Um usuário com privilégios poderá reativa-la através da interface web.

Parâmetros

Campo	Tipo	Descrição	Requerido
Identificador	Texto	Id numérico da informação protegida, ou identificador atribuído a informação.	Não

Resposta

```
{
    "response": {
        "status": 200,
        "mensagem": "Informacao removida",
        "erro": false
    }
}
```

1.4.10 Encerramento compulsório de sessão proxy

```
DELETE /iso/remoto/sessao/[identificador]
```

Encerra a sessão proxy indicando o motivo do encerramento. Utilize essa funcionalidade para que sistemas extermos como SIEM possam encerrar sessões baseadas nos alertas emitidos pelo próprio senhasegura® .

Parâmetros

Campo	Tipo	Descrição	Requerido
identificador	Texto	Identificador hash da sessão	Sim
session_id	Texto	Identificador hash da sessão	Sim
err_code	Inteiro	Código do motivo de encerramento	Não
err_msg	Texto	Descrição do motivo de encerramento	Não

Resposta

```
{
  "response": {
    "status": 200,
    "mensagem": "Sessao encerrada",
    "erro": false
  }
}
```

1.5 WebService App2App

O objetivo desta seção é auxiliar os usuários com privilégios administrativos a instalar o agente WebService App2App que provém a interface de comunicação para as tarefas relacionadas a credenciais.

Neste documento utilizaremos a biblioteca Java como exemplo. Todas bibliotecas utilizam do mesmo canal REST para comunicação com o senhasegura, facilitando o desenvolvimento em qualquer linguagem que tenha suporte a webservice REST.

Caso deseje bibliotecas em outras linguagens, entre em contato com nosso suporte.

1.5.1 Atividades

Nesta seção, iremos abordar as seguintes funções do senhasegura® :

- Operação da biblioteca Java

- Compatibilidade de versões da biblioteca Java
- Configurações do WebService App2App
- Exemplos de uso

Configurações do WebService App2App

O agente WebService App2App permite que os desenvolvedores utilizem de forma adequada o senhasegura® em uma variedade de aplicações e atividades através de seu código fonte.

Para consultar as credenciais, a aplicação utiliza de um cache reutilizável otimizando a performance. Sendo possível configurar a periodicidade de renovação deste cache. Se a credencial for alterada e a aplicação cliente não conseguir acessar o destino, a API irá limpar o cache e consultar novamente o senhasegura® pela informação atualizada.

Os pré requisitos para utilizar a API são:

- Registrar o cliente de API no senhasegura® ;
- Habilitar o token para este cliente;
- Copiar as seguintes informações de acesso:

    Consumer Key;

    Consumer Secret;

    Token;

    Token Secret.

Ativando as funcionalidades do senhasegura® ao cliente

Através da configuração você permite o cliente de API a utilizar as funções descritas anteriormente.

Para configurar a aplicação cliente:

1. Acessar o menu **Configurações → Serviços → API → Clientes**
2. Clicar na ação de relatório ***Novo***

3. Preencher os campos requiridos
4. Preencher os seguintes campos:

Campo	Descrição
Nome	Nome da aplicação senhasegura.go
Usuário para auditoria	Usuário que será usado para preencher os campos de auditoria nas chamadas
Status	Indica se o aplicativo cliente está ativo ou não
Usar assinatura OAuth	Indica se é necessário usar a assinatura OAuth para chamadas

5. Clicar no botão ***Salvar*** para finalizar o registro

Registrar um token de aplicação

Siga os seguintes passos para registrar um token de aplicação:

1. Acessar o menu: **Configurações → Serviços → API → Tokens**
2. Clicar na ação de registro ***Token de aplicação***
3. Clicar na ação de relatório ***Novo***

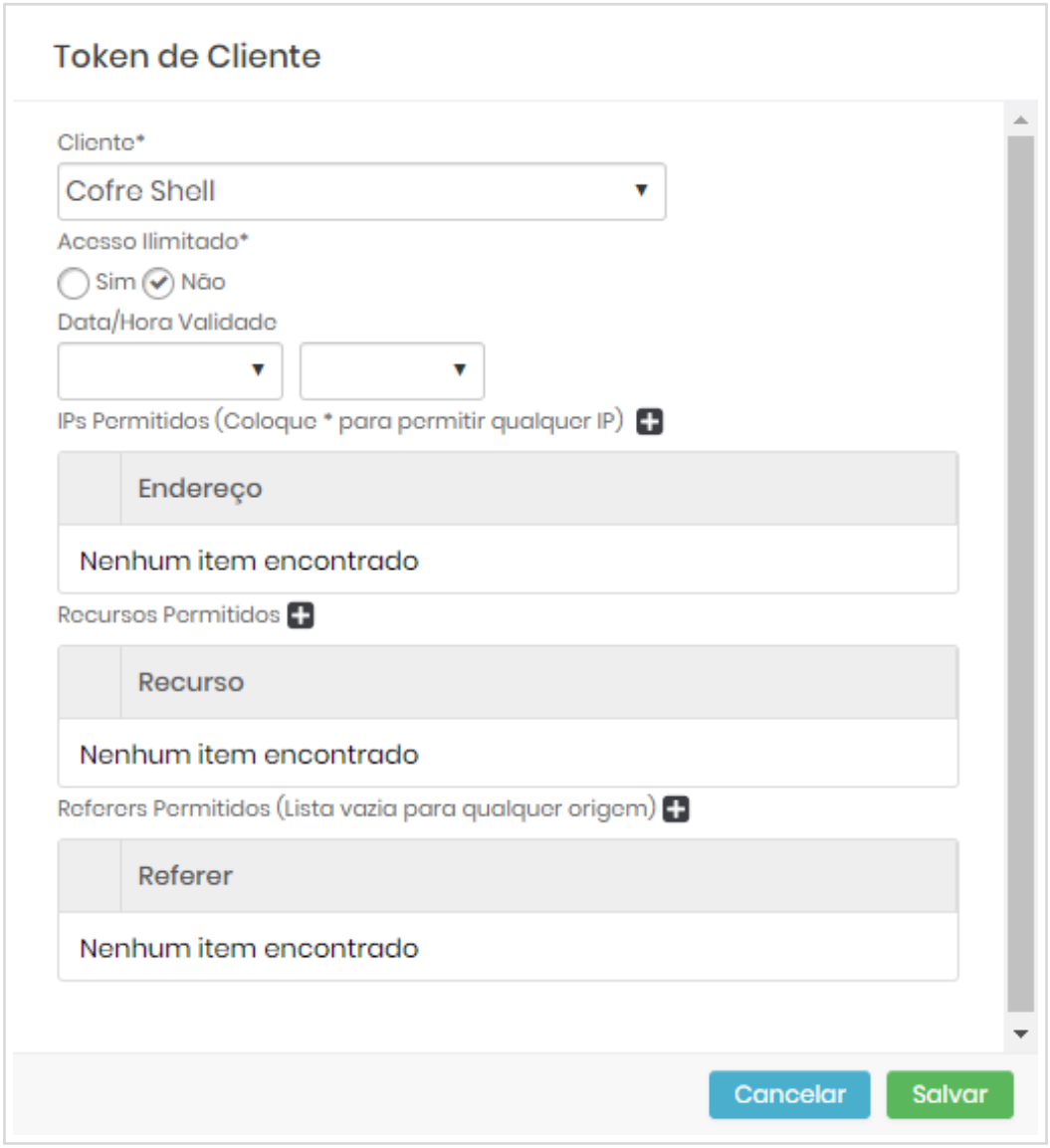

Figura 1.1: Formulário de Token de Aplicação

4. Preencher os seguintes campos:

Campo	Descrição
Clientet	Nome do cliente
Acesso ilimitado	Indica se o acesso será ou não ilimitado. Se a opção Não estiver definida, uma data de validade deve ser definida para este token
Date/Time Expiration	Date and time of token expiration
IP permitidos	IPs permitidos para acessar o token do cliente

Recursos permitidos	O recurso ao qual este token permite acesso.
Referenciador	referenciadores permitidos para este token

5. Clique no botão ***Salvar*** para finalizar o cadastro.

Versões compatíveis do Java

O agente Java v0.1.5 é compatível com o Java 1.5 e superior, permitindo o uso do cache no agente e evitando consultas excessivas no senhasegura® .

O agente na versão v0.1.4 é compatível com versões anteriores ao Java 1.5, mas não provém o uso do cache.

Exemplo de uso

```
1  package br.com.mt4.senhasegura;
2
3  import java.io.IOException;
4  import java.sql.Connection;
5  import java.sql.PreparedStatement;
6  import java.sql.ResultSet;
7
8  //#########################################################
9  // \senhasegura connection class
10 import br.com.mt4.senhasegura.sql.ConnectionFactory;
11 //#########################################################
12
13 import javax.servlet.ServletException;
14 import javax.servlet.http.HttpServlet;
15 import javax.servlet.http.HttpServletRequest;
16 import javax.servlet.http.HttpServletResponse;
17
18 public class QueryServlet extends HttpServlet {
19
20   public void doPost(HttpServletRequest request, HttpServletResponse response) throws
21     try {
22
23       String url = request.getParameter("url");
```

```
24      String consumerKey = request.getParameter("consumerkey");
25      String consumerSecret = request.getParameter("consumersecret");
26      String tokenKey = request.getParameter("tokenkey");
27      String tokenSecret = request.getParameter("tokensecret");
28
29      if (url.endsWith("/") == false) {
30        url = url + "/";
31      }
32
33      // clear cache flag
34      Boolean isClearCache = false;
35      isClearCache = request.getParameter("clearCache").equals("clear");
36
37      // ####################
38      // SENHASEGURA - START
39
40      // Connection factory
41      ConnectionFactory factory = new ConnectionFactory(url, consumerKey, consumerSecre
42      factory.setReferer(request.getRequestURL().toString());
43
44      // Clear the cache if needed
45      if (isClearCache)
46        factory.clearCacheById(Integer.parseInt(request.getParameter("id")));
47
48      // Get database connection with specified password
49      Connection con = factory.getConnection(Integer.parseInt(request.getParameter("id'
50
51      // SENHASEGURA - END
52      // ####################
53
54      // Prepare statement with query
55      PreparedStatement stmt = con.prepareStatement(request.getParameter("query"));
56
57      // Run a query
58      ResultSet rs = stmt.executeQuery();
59
60      // Table
61      response.getWriter().println("<table class='table table-condensed table-bordered'
62
63      // Header
64      response.getWriter().println("<thead><tr>");
65      for (int i = 1; i <= rs.getMetaData().getColumnCount(); i++) {
66        response.getWriter().println("<th>" + rs.getMetaData().getColumnName(i) + "</th
67      }
```

```
68        response.getWriter().println("</tr></thead>");
69
70        // iterate on the ResultSet
71        response.getWriter().println("<tbody>");
72        while (rs.next()) {
73          response.getWriter().println("<tr>");
74          for (int i = 1; i <= rs.getMetaData().getColumnCount(); i++) {
75            response.getWriter().println("<td>" + rs.getString(i) + "</td>");
76          }
77          response.getWriter().println("</tr>");
78        }
79        response.getWriter().println("</tbody>");
80        response.getWriter().println("</table>");
81
82        rs.close();
83        stmt.close();
84        con.close();
85
86      } catch (Exception e) {
87        response.getWriter().println("<div class='alert alert-danger'><b>Erro: </b>" + e.
88        response.getWriter().println("<pre>");
89        e.printStackTrace(response.getWriter());
90        response.getWriter().println("</pre>");
91      }
92    }
93  }
```

2 Certificate Management - Integração

2.1 Introdução

O senhasegura® ***Certificate Management*** fornece gerenciamento centralizado do ciclo de vida do certificado digital dentro da organização, desde o ***Discovery*** através da verificação automática de sites, diretórios e servidores da web, até a renovação automática do ***Certificado*** por meio de Autoridades Certificadoras externa ou interna .

O objetivo desse documento é prover um guia para usuários utilizando o ***Certificate Management*** como administradores, e explicar sobre detalhes de uso, beneficios e procedimentos.

2.1.1 Como o Certificate Management funciona

O senhasegura® Certificate Management gerencia todo o ciclo de vida dos certificados digitais, trabalhando com certificados através de geração por requisições, importação manual de certificados existentes, ou Discovery de certificados em dispositivos, domínios ou containers. Além de monitorar a validade dos certificados e possibilitar a renovação de maneira facilitada, o Certificate Management permite também a visualização de logs e relatórios sobre todas as operações realizadas através da solução.

2.1.2 Definições

O senhasegura® utiliza uma terminologia específica para suas funções e funcionalidades. Assim, alguns termos devem ser compreendidos antes de iniciar o uso da solução:

Usuário O Funcionários próprios, estagiários ou terceiros que utilizam ou possam precisar de acesso aos sistemas da empresa

Certificado Digital Certificados digitais são arquivos que contêm informações, além de chaves, pública e privada, que são usadas para comunicação segura através da Internet, assim como para atestar a autenticidade do remetente

Autoridade Certificadora Autoridade certificadora é uma entidade devidamente registrada nos órgãos responsáveis e que tem função de emitir certificados digitais

2.1.3 Atividades

Nesta seção, serão abordadas as seguintes funções do senhasegura® : realizar requisições, receber respostas e métodos do senhasegura® Certificate Management.

2.2 Métodos

O webservice de integração senhasegura® possui alguns métodos para realizar operações na aplicação.

2.2.1 Criar/Modificar Request

```
POST https://url_do_cofre/iso/certificado/request/[codigo_request]
```

O método ***Criar/Modificar Request*** cria ou modifica um request de certificado no senhasegura® .

Parâmetros

Campo	Tipo	Descrição	Obrig.
codigo_request	Inteiro	Código de um Request já criado. Caso o código não seja incluído no parâmetro, um novo Request será criado.	Não
tipo_certificado	Inteiro	Tipo do certificado. Os possíveis valores são: 1 = DV SSL - Domain SSL; 2 = OV SSL - Organization SSL; 3 = EV SSL - Extended SSL	Sim
tipo_domínio	Texto	Tipo do domínio do certificado. Os possíveis valores são: SING = Single domain MULT = Multiple domains WILD = Wildcard	Sim
organizacao	Inteiro	Código da organização. Deverá ser informado o código de uma organização cadastrada no senhasegura® .	Sim
nome_comum	Texto	Nome comum do certificado.	Sim
san	Array	Subject Alternative Name. Será preenchido com o nome_comum caso o san não seja informado.	Não
tags	Array	Tags de identificação do certificado. Será cadastrada novas tags caso as informadas não existam.	Não
criptografia	Texto	Algoritmo de criptografia. Os possíveis valores são: RSA DSA	Sim
tamanho_chave_criptografia	Inteiro	Tamanho da chave de criptografia. Os possíveis valores são: 4096 2048 1024	Sim

Campo	Tipo	Descrição	Obrig.
algoritmo_certificado	Texto	Algoritmo de assinatura Os possíveis valores são: SHA256 SHA384 SHA512 Se a criptografia escolhida for DSA, será permitido apenas o uso de SHA256.	Sim
validade	Inteiro	Tempo de validade do certificado, em dias.	Sim
senha_chave	Texto	Senha da chave do certificado.	Não
senha_revogacao	Texto	Senha de revogação do certificado.	Não
ambientes	Array	Ambientes do certificado. Serão cadastrados novos ambientes de certificado caso os informados não existam.	Não
sistemas	Array	Sistemas do certificado. Serão cadastrados novos sistemas de certificado caso os informados não existam.	Não
projeto	Texto	Projeto do certificado no request.	Não
ip_externo	Texto	IP externo do certificado no request.	Não
ip_hostname	Texto	IP ou hostname do certificado no request.	Não
justificativa	Texto	Justificativa do request com até 1024 caracteres.	Não
responsavel	Inteiro	Código do responsável pelo request e pelo certificado. Deverá ser um usuário cadastrado no senhasegura® .	Não
descricao	Texto	Descrição do request com até 512 caracteres.	Não

Resposta para certificados

Se o método for executado com sucesso ou com erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	201, para a criação de certificados 200, para a edição de certificados	4xx
messagem	Texto	Created, para a criação de certificados OK, para a edição de certificados	Não foi possível criar o request.
erro	Boolean	false	true
codigo_request	Inteiro	Código do request. Ex.: 123	O código de request informado é inválido
tipo_certificado	Inteiro	Tipo do certificado informado. Ex.: DV SSL - Domain SSL	O tipo de certificado informado é inválido.
tipo_domínio	Texto	Tipo do domínio do certificado informado. Ex.: SING	O tipo do domínio do certificado informado é inválido.
organizacao	Inteiro	Código da organização informado. Ex.: 123	O código da organização informado é inválido
nome_comum	Texto	Nome comum informado. Ex.: senhasegura.com.br	O nome comum do certificado não foi informado.
san	Array	SAN informado(s). Ex.: senhasegura.com.br	N/A
tags	Array	Tags informadas. Ex.: tag1, tag2, tag3	N/A
criptografia	Texto	Algoritmo de criptografia informado. Ex.: RSA	O algoritmo de criptografia informado é inválido.
tamanho_chave_criptografia	Inteiro	Tamanho da chave de criptografia informado. Ex.: 1024	O tamanho da chave de criptografia informado é inválido.
algoritmo_certificado	Texto	Algoritmo de assinatura informado. Ex.: sha256	O algoritmo de assinatura informado é inválido.

Campo	Tipo	Sucesso	Erro
validade	Inteiro	Tempo de validade do certificado informado. Ex.: 365	O tempo de validade do certificado informado é inválido.
senha_chave	Texto	Informação sensível.	A senha da chave do certificado informada é inválida.
senha_revogacao	Texto	Informação sensível.	A senha da chave do certificado informada é inválida.
ambientes	Array	Ambientes informados. Ex.: ambiente 1, ambiente 2	N/A
sistemas	Array	Sistemas informados. Ex.: sistema 1, sistema 2	N/A
projeto	Texto	Projeto informado. Ex.: projeto 1	N/A
ip_externo	Texto	IP informado. Ex.: 192.168.1.1	N/A
ip_hostname	Texto	IP ou hostname informado. Ex.: localhost	N/A
justificativa	Texto	Justificativa informada. Ex.: Novo certificado do cofre.	A justificativa deve ter no máximo 1024 caracteres.
responsavel	Inteiro	Código do responsável informado. Ex.: 123	O código do responsável informado é inválido.
descricao	Texto	Descrição informada. Ex.: Novo certificado do cofre.	A descrição deve ter no máximo 512 caracteres.

2.2.2 Consultar/Listar Request

```
GET https://url_do_cofre/iso/certificado/request/listar/[codigo_request]
```

O método ***Consultar/Listar Request*** consulta uma ou mais requests de certificado no senhasegura®
.

Parâmetros

Campo	Tipo	Descrição	Obrig.
codigo_request	Inteiro	Código de um Request já criado.	Não
status_request	Inteiro	Código de um status de um request.	Não
tipo_certificado	Inteiro	Tipo do certificado. As opções serão: 1 = DV SSL - Domain SSL 2 = OV SSL - Organization SSL 3 = EV SSL - Extended SSL	Não
tipo_domínio	Texto	Tipo do domínio do certificado. As opções serão: SING = Single domain MULT = Multiple domains WILD = Wildcard	Não
organizacao	Inteiro	Código da organização cadastrada no senhasegura® .	Não
nome_comum	Texto	Nome comum do certificado.	Não
san	Texto	Subject Alternative Names, separados por vírgula	Não
tags	Texto	Tags de identificação do certificado, separados por vírgula	Não
criptografia	Texto	Algoritmo de criptografia. As opções serão: RSA DSA	Não
tamanho_chave_criptografia	Inteiro	Tamanho da chave de criptografia. As opções serão: 4096 2048 1024	Não
algoritmo_certificado	Texto	Algoritmo de assinatura As opções serão: SHA256 SHA384 SHA512	Não
validade	Inteiro	Tempo de validade do certificado em dias.	Não
senha_chave	Texto	Senha da chave do certificado.	Não
senha_revogacao	Texto	Senha de revogação do certificado.	Não
ambientes	Texto	Ambientes do certificado, separados por vírgula	Não

Campo	Tipo	Descrição	Obrig.
sistemas	Texto	Sistemas do certificado, separados por vírgula	Não
projeto	Texto	Projeto do certificado no request.	Não
ip_externo	Texto	IP externo do certificado no request.	Não
ip_hostname	Texto	IP ou hostname do certificado no request.	Não
responsavel	Inteiro	Código do responsável pelo request e pelo certificado.	Não
offset	Inteiro	Número base da contagem de registros pela paginação.	Não
limit	Inteiro	Número de registros na paginação.	Não

Resposta para certificados

Se o método for executado com sucesso ou erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	200	4xx
messagem	Texto	OK	Não foi possível encontrar requests com as informações fornecidas
erro	Boolean	false	true
codigo_request	Inteiro	Código do request. Ex.: 123	Não existe um request com o código informado.O código de request informado é inválido.
status_request	Inteiro	Código e nome do status do request. Ex.: 3 - Aguardando aprovação	Não existem requests com o status informado.O código de status informado é inválido
tipo_certificado	Inteiro	Tipo do certificado informado. Ex.: DV SSL - Domain SSL	Não existem requests com o tipo do certificado informado.O tipo de certificado informado é inválido.

Campo	Tipo	Sucesso	Erro
tipo_domínio	Texto	Tipo do domínio do certificado informado. Ex.: SING	Não existem requests com o tipo do domínio informado.O tipo do domínio do certificado informado é inválido.
organizacao	Inteiro	Código da organização informado. Ex.: 123	Não existem requests com o código da organização informado.O código da organização informado é inválido.
nome_comum	Texto	Nome comum informado. Ex.: senhasegura.com.br	Não existem requests com o nome comum informado.
san	Array	SAN informado(s). Ex.: senhasegura.com.br	Não existem requests com o(s) SAN(s) informado(s).
tags	Array	Tags informadas. Ex.: tag1, tag2, tag3	Não existem requests com a(s) Tag(s) informada(s).
criptografia	Texto	Algoritmo de criptografia informado. Ex.: RSA	Não existem requests com o algoritmo de criptografia informado.O algoritmo de criptografia informado é inválido.
tamanho_chave_criptografia	Inteiro	Tamanho da chave de criptografia informado. Ex.: 1024	Não existem requests com o tamanho da chave de criptografia informado. O tamanho da chave de criptografia informado é inválido.
algoritmo_certificado	Texto	Algoritmo de assinatura informado. Ex.: sha256	Não existem requests com o algoritmo de assinatura informado. O algoritmo de assinatura informado é inválido.

Campo	Tipo	Sucesso	Erro
validade	Inteiro	Tempo de validade do certificado informado. Ex.: 365	Não existem requests com o tempo de validade informado. O tempo de validade do certificado informado é inválido.
senha_chave	Texto	Informação sensível.	Não existem requests com a senha da chave informada. A senha da chave do certificado informada é inválida.
senha_revogacao	Texto	Informação sensível.	Não existem requests com a senha de revogação informada. A senha de revogação do certificado informada é inválida.
ambientes	Array	Ambientes informados. Ex.: ambiente 1, ambiente 2	Não existem requests com os ambientes informados.
sistemas	Array	Sistemas informados. Ex.: sistema 1, sistema 2	Não existem requests com os sistemas informados.
projeto	Texto	Projeto informado. Ex.: projeto 1	Não existem requests com o projeto informado.
ip_externo	Texto	IP informado. Ex.: 192.168.1.1	Não existem requests com o IP externo informado.
ip_hostname	Texto	IP ou hostname informado. Ex.: localhost	Não existem requests com o IP ou hostname informado.
justificativa	Texto	Justificativa informada. Ex.: Novo certificado do cofre.	
responsavel	Inteiro	Código e nome do responsável informado. Ex.: 123- Nome responsável	Não existem requests com o código de responsável informado. O código do responsável informado é inválido.
descricao	Texto	Descrição informada. Ex.: Novo certificado do cofre.	

2.2.3 Assinar Request

```
GET https://url_do_cofre/iso/certificado/request/assinar/[codigo_request]
```

O método ***Assinar Request*** assina um request existente no senhasegura® .

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_request	Inteiro	Código do request a ser assinado..	Sim
auto_assinado	Inteiro	Indica se é auto-assinado. As opções serão: 1 = true 0 = false	Sim
ca	Inteiro	Código da CA responsável pela assinatura request. Obrigatório, caso auto_assinado seja false.	Condicional
justificativa	Texto	Texto de até 1024 caracteres para justificativa.	Não
motivo	Inteiro	Código do motivo da assinatura. Deverá informar um código de um motivo cadastrado no senhasegura®	Sim
gmud	Texto	30 caracteres para determinar o código do ITSM. Obrigatório caso no grupo de acesso do certificado o parâmetro "Código de governança obrigatório ao justificar" esteja habilitado. Realizar as validações no ITSM da mesma forma que é feito na interface web.	Condicional

Resposta para certificados

Se o método for executado com sucesso, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	200	4xx
messagem	Texto	OK	Não foi possível assinar o request.
erro	Boolean	false	true
codigo_request	Inteiro	Código da request. Ex.: 123	Informe um código de request. O código da request informado é inválido.
auto_assinado	Inteiro	Valor informado. Ex.: false	Não existem requests para este valor de auto-assinado informado. O valor para auto-assinado informado é inválido.
ca	Inteiro	Código e nome da CA informado. Ex.: 123 - Minha CA	Não existem requests com o código da CA informado. O código da CA informado é inválido
justificativa	Texto	Justificativa informada. Ex.: Novo certificado do cofre.	A justificativa deve ter no máximo 1024 caracteres.
motivo	Inteiro	Código e nome do motivo informado. Ex.: 3 - Certificado para email	O código do motivo informado é inválido.
gmud	Texto	Código da GMUD informado. Ex.: abc123	Informe o código da GMUD.

2.2.4 Consultar/Listar Certificados

```
GET https://url_do_cofre/iso/certificado/listar/[codigo_certificado]
```

O método ***Consultar/Listar Certificados*** consulta uma ou mais certificados no senhasegura.

Parameters

Campo	Tipo	Descrição	Obrig.
codigo_certificado	Inteiro	Código de um certificado já criado no senhasegura.	Não
status_certificado	Inteiro	Código de um status de um certificado. As opções serão: 1 = Válido 2 = Revogado 3 = Renovação pendente 4 = Expirado	Não
ativo	Inteiro	Estado do certificado no senhasegura. As opções serão: 1 = Ativo 0 = Inativo	Não
inicio_validade	Texto	Data de início da validade. Ex.: 2019-05-25T04:08:15	Não
fim_validade	Texto	Data de fim da validade. Ex.: 2020-05-25T04:08:15	Não
origem_certificado	Inteiro	Origem do certificado no senhasegurao. As opções serão: SCAN = Scan e Discovery REQU = Request IMPO = Importado manualmente	Não
tipo_certificado	Inteiro	Tipo do certificado. As opções serão: 1 = DV SSL - Domain SSL 2 = OV SSL - Organization SSL 3 = EV SSL - Extended SSL	Não
tipo_domínio	Texto	Tipo do domínio do certificado. As opções serão: SING = Single domain MULT = Multiple domains WILD = Wildcard	Não
organizacao	Inteiro	Código da organização.	Não
nome_comum	Texto	Nome comum do certificado.	Não

Campo	Tipo	Descrição	Obrig.
san	Texto	Subject Alternative Name. Poderá informar mais de 1 separados por vírgula.	Não
tags	Texto	Tags de identificação do certificado. Poderá informar mais de 1 separados por vírgula.	Não
criptografia	Texto	Algoritmo de criptografia. As opções serão: RSA DSA	Não
tamanho_chave_criptografia	Inteiro	Tamanho da chave de criptografia. As opções serão: 4096 2048 1024	Não
algoritmo_certificado	Texto	Algoritmo de assinatura As opções serão: sha256 sha384 sha512	Não
validade	Inteiro	Tempo de validade do certificado em quantidade de dias.	Não
senha_chave	Texto	Senha da chave do certificado.	Não
senha_revogacao	Texto	Senha de revogação do certificado.	Não
ambientes	Texto	Ambientes do certificado. Poderá informar mais de 1 separados por vírgula.	Não
sistemas	Texto	Sistemas do certificado. Poderá informar mais de 1 separados por vírgula.	Não
projeto	Texto	Projeto do certificado no request.	Não
ip_externo	Texto	IP externo do certificado no request.	Não
ip_hostname	Texto	IP ou hostname do certificado no request.	Não
auto_assinado	Inteiro	Indica se é auto-assinado. As opções serão: 1 = true 0 = false	Não

Campo	Tipo	Descrição	Obrig.
ca	Inteiro	Código da CA responsável pela assinatura request.	Não
responsavel	Inteiro	Código do responsável pelo request e pelo certificado.	Não
offset	Inteiro	Número base da contagem de registros pela paginação.	Não
limit	Inteiro	Número de registros na paginação.	Não

Resposta para certificados

Se o método for executado com sucesso ou erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	200	4xx
messagem	Texto	OK	Não foi possível encontrar certificados com as informações fornecidas.
erro	Boolean	false	true
codigo_certificado	Inteiro	Código da request. Ex.: 123	Não existe um certificado com o código informado. O código do certificado informado é inválido.
status_certificado	Inteiro	Código e nome do status do certificado. Ex.: 4 - Expirado	Não existem certificados com o status informado. O código de status informado é inválido.
ativo	Inteiro	Código e nome do estado do certificado no senhasegura. Ex.: 1 - Ativo	Não existe nenhum certificado com o estado informado. O código do estado informado é inválido.
inicio_validade	Texto	Data de início da validade. Ex.: 2019-05-25T04:08:15	Não existem certificados com a data de início da validade informada. A data de início da validade informada é inválida.

Campo	Tipo	Sucesso	Erro
fim_validade	Texto	Data de fim da validade. Ex.: 2020-05-25T04:08:15	Não existem certificados com a data de fim da validade informada. A data de fim da validade informada é inválida.
origem_certificado	Inteiro	Origem do certificado no senhasegura. Ex.: SCAN - Scan e Discovery	Não existem certificados com a origem informada. A origem informada é inválida.
tipo_certificado	Inteiro	Tipo do certificado. Ex.: DV SSL - Domain SSL	Não existem certificados com o tipo informado. O tipo de certificado informado é inválido.
tipo_domínio	Texto	Tipo do domínio do certificado. Ex.: SING	Não existem certificados com o tipo do domínio informado. O tipo do domínio do certificado informado é inválido.
organizacao	Inteiro	Código e nome da organização informado. Ex.: 123 - Nome organização	Não existem certificados com o código da organização informado. O código da organização informado é inválido.
nome_comum	Texto	Nome comum do certificado. Ex.: senhasegura.com.br	Não existem certificados com o nome comum informado.
san	Texto	SAN do certificado. Ex.: senhasegura.com.br, mt4.com.br	Não existem certificados com o(s) SAN(s) informado(s).
tags	Texto	Tags do certificado. Ex.: tag1, tag2, tag3	Não existem certificados com a(s) Tag(s) informada(s).
criptografia	Texto	Algoritmo de criptografia do certificado. Ex.: RSA	Não existem certificados com o algoritmo de criptografia informado.O algoritmo de criptografia informado é inválido.

Campo	Tipo	Sucesso	Erro
tamanho_chave_criptografia	Inteiro	Tamanho da chave de criptografia do certificado. Ex.: 1024	Não existem certificados com o tamanho da chave de criptografia informado. O tamanho da chave de criptografia informado é inválido.
algoritmo_certificado	Texto	Algoritmo de assinatura do certificado. Ex.: sha256	Não existem certificados com o algoritmo de assinatura informado. O algoritmo de assinatura informado é inválido.
validade	Inteiro	Tempo de validade do certificado. Ex.: 365	Não existem certificados com o tempo de validade informado. O tempo de validade do certificado informado é inválido.
senha_chave	Texto	Senha da chave do certificado.	Não existem certificados com a senha da chave informada. A senha da chave do certificado informada é inválida.
senha_revogacao	Texto	Senha de revogação do certificado.	Não existem certificados com a senha de revogação informada. A senha de revogação do certificado informada é inválida.
ambientes	Texto	Ambientes do certificado. Ex.: ambiente 1, ambiente 2	Não existem certificados com o(s) ambiente(s) informado(s).
sistemas	Texto	Sistemas do certificado. Ex.: sistema 1, sistema 2	Não existem certificados com o(s) sistema(s) informado(s).
projeto	Texto	Projeto do certificado. Ex.: projeto 1	Não existem certificados com o projeto informado.
ip_externo	Texto	IP externo do certificado. Ex.: 192.168.1.1	Não existem certificados com o IP externo informado.
ip_hostname	Texto	IP ou hostname do certificado. Ex.: localhost	Não existem certificados com o IP ou hostname informado.

Campo	Tipo	Sucesso	Erro
auto_assinado	Inteiro	Informação se o certificado é auto-assinado. Ex.: false	Não existem certificados para este valor de auto-assinado informado. O valor para auto-assinado informado é inválido.
ca	Inteiro	Código e nome da CA informado. Ex.: 123 - Minha CA	Não existem certificados com o código da CA informado.O código da CA informado é inválido.
responsavel	Inteiro	Código e nome do responsável informado. Ex.: 123 - Nome responsável	Não existem certificados com o código de responsável informado.O código do responsável informado é inválido.
descricao	Texto	Descrição do certificado. Ex.: Novo certificado do cofre.	

informacoes_publicacao	Array	Informações adicionais para publicação.Ex.:
		{
		“nome_servico” = “IIS”,
		“ip_acesso” = “192.138.10.10”,
		“etc...”
		}	

dispositivos	Array	Código dos dispositivos atrelados ao certificado.Ex.:
		{
		123,
		321
		}	

2.3 Funcionalidades

O webservice de integração senhasegura® possui algumas funcionalidades para realizar operações na aplicação.

2.3.1 Publicar Certificado

```
POST https://url_do_cofre/iso/cert/publicar/
```

A funcionalidade ***Publicar Certificado*** solicita a publicação de um certificado em um ou mais dispositivos

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_certificado	Inteiro	Código do certificado a ser publicado.	Sim
codigo_perfil_publicacao	Inteiro	Código do perfil de publicação. Será utilizado um perfil de publicação previamente cadastrado no senhasegura® .	Sim
justificativa	Texto	Justificativa da publicação com até 1024 caracteres.	Não
motivo	Inteiro	Código do motivo da publicação. Deverá informar um código de um motivo cadastrado no senhasegura® .	Sim
gmud	Texto	30 caracteres para determinar o código do ITSM. Obrigatório caso no grupo de acesso do certificado o parâmetro "Código de governança obrigatório ao justificar" esteja habilitado. Realizar as validações no ITSM da mesma forma que é feito na interface web.	Condicional

Campo	Tipo	Descrição	Obrigatório
dispositivos	Array	Array com os códigos dos dispositivos onde o certificado deverá ser publicado. Ex.: [123, 321] Os dispositivos devem existir no senhasegura® .	Sim

Resposta para certificados

Se a funcionalidade for executado com sucesso ou erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	200	4xx
messagem	Texto	Created	Código de certificado inválido.
erro	Boolean	false	true
codigo_publicação	Inteiro	Código do agendamento da publicação. Ex.: 123	
motivo	Inteiro	Código e nome do motivo da publicação. Ex.: 3 - Certificado para email	O código do motivo informado é inválido.
gmud	Texto	Código da GMUD informado. Ex.: abc123	Informe o código da GMUD.Código de GMUD não existe no sistema de ITSM integrado ao senhasegura® . O código deve ter no máximo 30 caracteres.
dispositivos	Array	Códigos de dispositivos para publicação. Ex.: 123, 321, 456, 654	

2.3.2 Consultar/Listar Publicações

```
GET https://url_do_cofre/iso/cert/publicar/listar/[codigo_publicacao]
```

A funcionalidade ***Consultar/Listar Publicações*** consulta uma ou mais publicações no senhasegura®
.

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_publicacao	Inteiro	Código da publicação.	Não
codigo_certificado	Inteiro	Código do certificado a ser Publicado.	Não
codigo_perfil_publicacao	Inteiro	Código do perfil de publicação.	Não
data_criacao	Texto	Data de cadastro da publicação. Ex.: 2019-05-25T04:08:15	Não
processado	Inteiro	Status do processamento da publicação. As opções serão: 1 = Sim 0 = Não	Não
erro	Inteiro	Status de erro da publicação. As opções serão: 1 = Sim 0 = Não	Não
motivo	Inteiro	Código do motivo da publicação.	Não
gmud	Texto	Texto da GMUD informada.	Não
dispositivo	Inteiro	Código do dispositivo da publicação.	Não
offset	Inteiro	Número base da contagem de registros pela paginação.	Não
limit	Inteiro	Número de registros na paginação.	Não

Resposta para certificados

Se a funcionalidade for executado com sucesso ou erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	200	4xx
messagem	Texto	OK	Não foi possível encontrar publicações com as informações fornecidas.
erro	Boolean	false	true
codigo_publicação	Inteiro	Código do agendamento da publicação. Ex.: 123	Não existe uma publicação com o código informado. O código da publicação informado é inválido.
processado	Inteiro	Status do processamento da publicação. Ex.: 1	
erro	Inteiro	Status de erro da publicação. Ex.: 0	
motivo	Inteiro	Código e nome do motivo da publicação. Ex.: 3 - Certificado para email	O código do motivo informado é inválido.
gmud	Texto	Código da GMUD informado. Ex.: abc123	Informe o código da GMUD. Código de GMUD não existe no sistema de ITSM integrado ao senhasegura® . O código deve ter no máximo 30 caracteres.
codigo_credencial	Inteiro	Código da credencial para publicação. Ex.: 123	O código da credencial informado é inválido.
username	Texto	Username para busca de credenciais. Ex.: admin	

Campo	Tipo	Sucesso	Erro
qtd_dispostivos	Inteiro	Quantidade de dispositivos da publicação. Ex.: 10	

dispositivos	Array	Códigos de dispositivos da publicação.
		Ex.:
		{
		123: [
		“status”:”Efetuada com sucesso”,
		“resultado”:”Operação executada com sucesso”
		],
		...
		}	

2.3.3 Criar/Editar Perfil de Publicação Apache

```
POST https://url_do_cofre/iso/cert/perfil/apache/
```

A funcionalidade ***Criar/Editar Perfil de Publicação Apache*** cria ou edita um perfil de publicação do plugin Apache.

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_perfil	Inteiro	Código de um perfil já criado. Caso o código não seja passado, o sistema interpretará como a criação de um perfil.	Não
nome_perfil	Texto	Nome do perfil a ser criado.	Sim

Campo	Tipo	Descrição	Obrigatório
site	Texto	Site onde o certificado deverá ser instalado. Se não for informado, o certificado será instalado no site padrão do Apache.	Não
config_path	Texto	Endereço da configuração. Padrão: /etc/apache2/sites-available/default.com.conf	Não
porta	Inteiro	Porta. Padrão: 443	Não
codigo_credencial	Inteiro	Código da credencial a ser utilizada na publicação. Será utilizada uma credencial previamente cadastrada o cofre. Esta informação será obrigatória caso não seja informado um username.	Condicional
username	Texto	Username que será utilizado para localizar credenciais para a publicação. Esta informação será obrigatória caso não seja informado um codigo_credencial	Condicional
dispositivos	Array	Array com os códigos dos dispositivos onde o certificado deverá ser publicado. Ex.: [123, 321] Os dispositivos devem existir no senhasegura® .	Sim

Resposta para certificados

Se a funcionalidade for executada com sucesso ou erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	201 - Criar 200 - Editar	4xx
messagem	Texto	Created OK	Não foi possível criar o perfil.
erro	Boolean	false	true

Campo	Tipo	Sucesso	Erro
codigo_perfil	Inteiro	Código do perfil de publicação. Ex.: 123	O código do perfil informado é inválido.
nome_perfil	Texto	Nome do perfil. Ex.: Perfil Apache	
site	Texto	Site informado. Ex.: senhasegura® .com.br	
config_path	Texto	Endereço da configuração. Ex.: /etc/apache2/sites-available/sites.conf	
porta	Inteiro	Porta. Ex.: 443	
codigo_credencial	Inteiro	Código da credencial para publicação. Ex.: 123	O código da credencial informado é inválido.
username	Texto	Username para busca de credenciais. Ex.: admin	
dispositivos	Array	Códigos de dispositivos para publicação. Ex.: 123, 321, 456, 654	

2.3.4 Criar/Editar Perfil de Publicação IIS

```
POST https://url_do_cofre/iso/cert/perfil/iis/
```

A funcionalidade ***Criar/Editar Perfil de Publicação IIS*** cria ou edita um perfil de publicação do plugin IIS.

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_perfil	Inteiro	Código de um perfil já criado. Caso o código não seja passado, o sistema interpretará como a criação de um perfil.	Não
nome_perfil	Texto	Nome do perfil a ser criado.	Sim
site	Texto	Site onde o certificado deverá ser instalado. Se não for informado, o certificado será instalado no site padrão do IIS.	Não
cert_store	Texto	Repositório de gerenciamento de certificados do IIS. Padrão: MY	Não
porta	Inteiro	Porta. Padrão: 443	Não
codigo_credencial	Inteiro	Código da credencial a ser utilizada na publicação. Será utilizada uma credencial previamente cadastrada o cofre. Esta informação será obrigatória caso não seja informado um username.	Condicional
username	Texto	Username que será utilizado para localizar credenciais para a publicação. Esta informação será obrigatória caso não seja informado um codigo_credencial.	Condicional
dispositivos	Array	Array com os códigos dos dispositivos onde o certificado deverá ser publicado. Ex.: [123, 321] Os dispositivos devem existir no senhasegura® .	Sim

Resposta para certificados

Se a funcionalidade for executada com sucesso, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	201 - Criar 200 - Editar	4xx
messagem	Texto	Created OK	Não foi possível criar o perfil.
erro	Boolean	false	true
codigo_perfil	Inteiro	Código do perfil de publicação. Ex.: 123	O código do perfil informado é inválido.
nome_perfil	Texto	Nome do perfil. Ex.: Perfil IIS	
site	Texto	Site informado. Ex.: senhasegura.com.br	
cert_store	Texto	Repositório de gerenciamento de certificados do IIS. Ex.: MY	
porta	Inteiro	Porta. Ex.: 443	
codigo_credencial	Inteiro	Código da credencial para publicação. Ex.: 123	O código da credencial informado é inválido.
username	Texto	Username para busca de credenciais. Ex.: admin	
dispositivos	Array	Códigos de dispositivos para publicação. Ex.: {123, 321, 456, 654}	

2.3.5 Criar/Editar Perfil de Publicação F5 BigIP

```
POST https://url_do_cofre/iso/cert/perfil/bigip/
```

A funcionalidade ***Criar/Editar Perfil de Publicação F5 BigIP*** cria ou edita um perfil de publicação do

plugin F5 BigIP.

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_perfil	Inteiro	Código de um perfil já criado. Caso o código não seja passado, o sistema interpretará como a criação de um perfil.	Não
nome_perfil	Texto	Nome do perfil a ser criado.	Sim
nome_particao	Texto	Nome da partição.	Não
nome_certificado	Texto	Nome do certificado. Se já existir um certificado com o mesmo nome configurado, na publicação ele será substituído.	Não
perfis_client_vips	Array	Array de Perfis SSL Client e seus VIPs Ex: ["MEU_CLIENT_1"=>"VIP_1", "MEU_CLIENT_2"=>"VIP_2"]	No
perfis_server_vips	Array	Array de Perfis SSL Server e seus VIPs. Ex: ["MEU_SERVER_1"=>"VIP_1", "MEU_SERVER_2"=>"VIP_2"]	Não
codigo_credencial	Inteiro	Código da credencial a ser utilizada na publicação. Será utilizada uma credencial previamente cadastrada o cofre. Esta informação será obrigatória caso não seja informado um username.	Condicional
username	Texto	Username que será utilizado para localizar credenciais para a publicação. Esta informação será obrigatória caso não seja informado um codigo_credencial.	Condicional
dispositivos	Array	Array com os códigos dos dispositivos onde o certificado deverá ser publicado. Ex.: [123, 321] Os dispositivos devem existir no senhasegura® .	Sim

Resposta para certificados

Se a funcionalidade for executada com sucesso, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Error
status	Inteiro	201 - Criar 200 - Editar	4xx
messagem	Texto	Created OK	Não foi possível criar o perfil.
erro	Boolean	false	true
codigo_perfil	Inteiro	Código do perfil de publicação. Ex.: 123	O código do perfil informado é inválido.
nome_perfil	Texto	Nome do perfil. Ex.: Perfil BigIP	
nome_particao	Texto	Nome da partição. Ex.: common	
nome_certificado	Texto	Nome do certificado que será exibido na aplicação web. Ex.: senhasegura®	

perfis_client	Array	Nome completo do perfil. Ex:
		{
		"MEU_CLIENTE_1"=>"VIP_1",
		"MEU_CLIENTE_2"=>"VIP_2"
		}	

perfis_server	Array	Nome completo do perfil. Ex:
		{
		"MEU_SERVER_1"=>"VIP_1",
		"MEU_SERVER_2"=>"VIP_2"
		}	

codigo_credencial	Inteiro	Código da credencial para publicação. Ex.: 123	O código da credencial informado é inválido.

Campo	Tipo	Sucesso	Error
username	Texto	Username para busca de credenciais. Ex.: admin	
dispositivos	Array	Códigos de dispositivos para publicação. Ex.: {123, 321, 456, 654}	

2.3.6 Criar/Editar Perfil de Publicação WebSphere WAS

```
POST https://url_do_cofre/iso/cert/perfil/was/
```

A funcionalidade ***Criar/Editar Perfil de Publicação WebSphere Was*** cria ou edita um perfil de publicação do plugin WebSphere WAS.

Parâmetros

Campo	Tipo	Descrição	Obrigatório
codigo_perfil	Inteiro	Código de um perfil já criado. Caso o código não seja passado, o sistema interpretará como a criação de um perfil.	Não
nome_perfil	Texto	Nome do perfil a ser criado.	Sim
key_db_path	Texto	Endereço e nome da Key Database.	Sim
key_db_password	Texto	Senha do servidor.	Sim
label	Texto	Label do servidor.	Sim
codigo_credencial	Inteiro	Código da credencial a ser utilizada na publicação. Será utilizada uma credencial previamente cadastrada o cofre. Esta informação será obrigatória caso não seja informado um username.	Condicional

Campo	Tipo	Descrição	Obrigatório
username	Texto	Username que será utilizado para localizar credenciais para a publicação. Esta informação será obrigatória caso não seja informado um codigo_credencial.	Condicional
dispositivos	Array	Array com os códigos dos dispositivos onde o certificado deverá ser publicado. Ex.: [123, 321] Os dispositivos devem existir no senhasegura® .	Sim

Resposta para certificados

Se a funcionalidade for executada com sucesso ou erro, a resposta consiste em um bloco certificado com os campos:

Campo	Tipo	Sucesso	Erro
status	Inteiro	201 - Criar 200 - Editar	4xx
messagem	Texto	Created OK	Não foi possível criar o perfil.
erro	Boolean	false	true
codigo_perfil	Inteiro	Código do perfil de publicação. Ex.: 123	O código do perfil informado é inválido.
nome_perfil	Texto	Nome do perfil. Ex.: Perfil WebSphere WAS	
key_db_path	Texto	Endereço e nome da Key Database. Ex.: /path/serverkey.kdb	
key_db_password	Texto	Senha do servidor. Ex.: asdf123	
label	Texto	Label do servidor. Ex.: webadmin	

Campo	Tipo	Sucesso	Erro
codigo_credencial	Inteiro	Código da credencial para publicação. Ex.: 123	O código da credencial informado é inválido.
username	Texto	Username para busca de credenciais. Ex.: admin	
dispositivos	Array	Códigos de dispositivos para publicação. Ex.: 123, 321, 456, 654	

3 Termos e condições de uso

Estes termos e condições definem o uso de qualquer informação desta documentação do senhasegura. Ao usar a documentação ou fazer o download de materiais, você concorda que conhece e entende esses termos e condições e os aceitou. Caso contrário, não use este documento. A MT4 se reserva o direito de alterar este documento e estes termos e condições a qualquer momento.

As informações neste documento são protegidas por leis e tratados internacionais de direitos autorais e outras leis e tratados de propriedade intelectual. Você pode fazer o download, reproduzir, exibir e distribuir os materiais do manual apenas para uso informativo, não comercial ou pessoal, desde que não o modifique e mantenha todos os avisos de direitos autorais e de propriedade, conforme são mostrados nesses materiais.

A MT4 não se responsabiliza por quaisquer danos, incluindo, entre outros, danos indiretos, especiais, incidentais ou consequentes, como resultado de ações contratuais, negligentes ou outras ações defeituosas resultantes do uso deste material, mesmo que a MT4 tenha ou não alertado sobre a chance de tal dano.

Se você tiver dúvidas em relação a estes Termos, ou se desejar entrar em contato com a MT4 senhasegura, envie um e-mail para ***atendimento@senhasegura.com.br*** ou ***suporte@senhasegura.co***

3.1 Licenças senhasegura

Os termos e condições de uso das licenças de software do senhasegura são estabelecidos nos contratos de venda.

3.2 Outras licenças

O desenvolvimento do software senhasegura na MT4 usa outros softwares. As condições de uso de licenças destes softwares são respeitadas em todo o aplicativo. Os softwares usados parcial ou totalmente em um ou mais módulos senhasegura estão listados abaixo:

Bootstrap https://getbootstrap.com/docs/4.0/about/license/

DataTables https://datatables.net/license

Debian https://www.debian.org/legal/licenses/

Dojo https://dojotoolkit.org/license.html

Fontawesome https://fontawesome.com/license/free

Goutte https://github.com/FriendsOfPHP/Goutte/blob/master/LICENSE

Guacamole https://github.com/apache/guacamole-server/blob/master/LICENSE

Highcharts https://www.highcharts.com/blog/products/highcharts/

iCheck https://github.com/fronteed/iCheck/

inputmask https://github.com/RobinHerbots/jquery.inputmask

Jquery https://jquery.org/license/

jQuery Tags Input https://github.com/xoxco/jQuery-Tags-Input

MariaDB https://mariadb.com/kb/en/library/licensing-faq/

Mozilla Firefox https://www.mozilla.org/en-US/MPL/

NGINX https://nginx.org/en/

NProgress http://ricostacruz.com/nprogress

Oracle Java 8 https://www.oracle.com/technetwork/java/javase/overview

Paramiko https://github.com/paramiko/paramiko/blob/master/LICENSE

PhantomJS https://phantomjs.org/

PHP https://www.php.net/license/index.php

Python https://docs.python.org/3/license.html

SmartWizard https://github.com/mstratman/jQuery-Smart-Wizard

Switchery https://www.javascripting.com/view/switchery

Tomcat http://tomcat.apache.org/legal.html

WInRM https://github.com/WinRb/WinRM

XRDP https://github.com/deskor/xrdp/blob/master/LICENSE

CaitSith https://caitsith.osdn.jp/