

SAFECENTRAL IS *CITRIX READY*[®]

Citrix[®] certifies SafeCentral as compatible with *XenApp*[™] and *XenDesktop*[®]



SafeCentral Enterprise Server

Administrator Guide 1.8

2015
Wontok Inc.

Table of Contents

SafeCentral Enterprise Configuration	3
Creating Administrators	3
Enterprise Settings	4
Subscription Settings	5
License Administration	5
Creating Groups	6
Configuring Computers in Groups	7
Configuring Policies	8
Reports	10
Enterprise Client Configuration	10
Client Requirements	10
SafeCentral Enterprise Client Installation	10
Send Invitation Email	10
Enterprise Client Installation	11
Web Based Installation	12
Silent Installation Method	13
Enterprise Client Startup	13
SafeCentral Enterprise Client Installation (Silent - Optional)	13
Touring the Enterprise Client	13

SafeCentral Enterprise Configuration

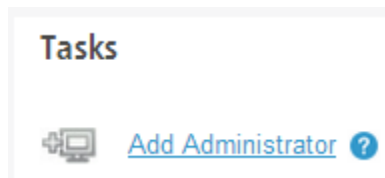
The SafeCentral Enterprise Configuration section will guide an Administrator on how to setup their instance via the Enterprise Server console. The Enterprise Server is available in English, Simplified Chinese, Korean and Thai languages presently.

Creating Administrators

After requesting an instance to be provisioned from Wontok, an Administrator will be created for you based on your implementation and distribution requirements. If you want to create additional Administrators you can do so.

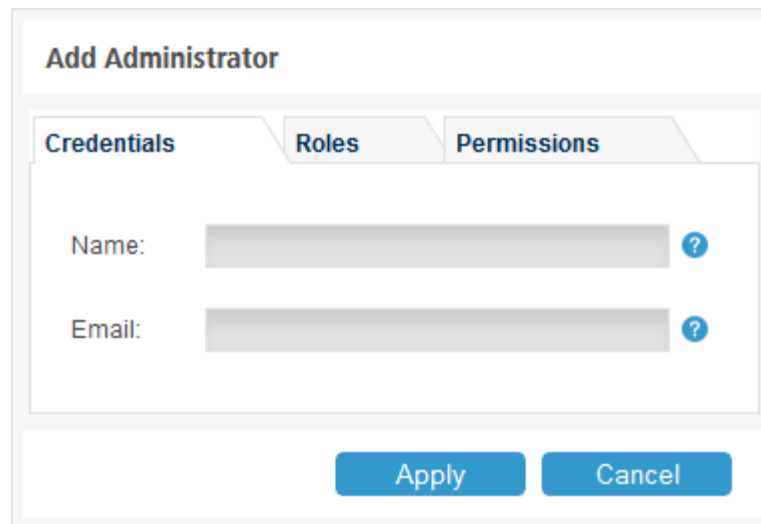
To create additional Administrators:

1. **Log into** Enterprise Server with your Enterprise Administrator email and password. The URL and credentials will be provided to you by email.
2. Select the **Admins** tab.
3. Select **Add Administrator** under the Tasks section.



ES1 Tasks Tab

4. **Enter** the name and email for the administrator.



ES1 Add Administrator Tab

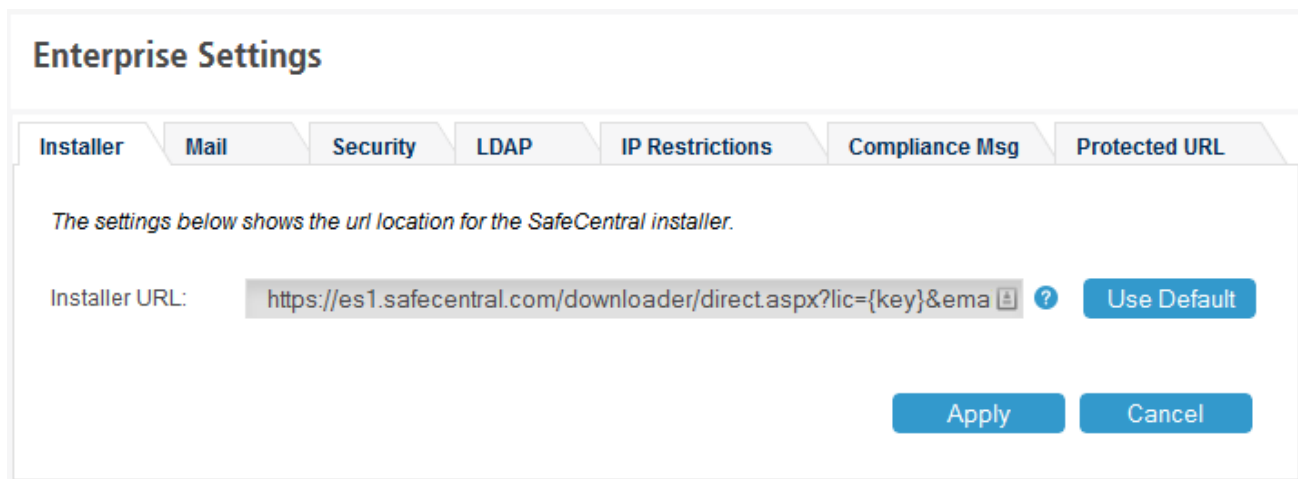
5. Select the **Roles** tab.
6. **Select** the level of administration desired. There are three types of administrators:
 - a. Enterprise Administrator - the highest level of access has access to all of the system functions and features.
 - b. Subscription Administrator - the second highest level has access to most system functions and manages individual subscriptions, or multiple subscriptions.

- c. Group Administrator - the lowest level, with access to manage individual groups within a subscription.
7. On the Permissions tab you can elect optional reporting access.

The new Administrator will receive a Welcome to ES1 email with steps to create a password.

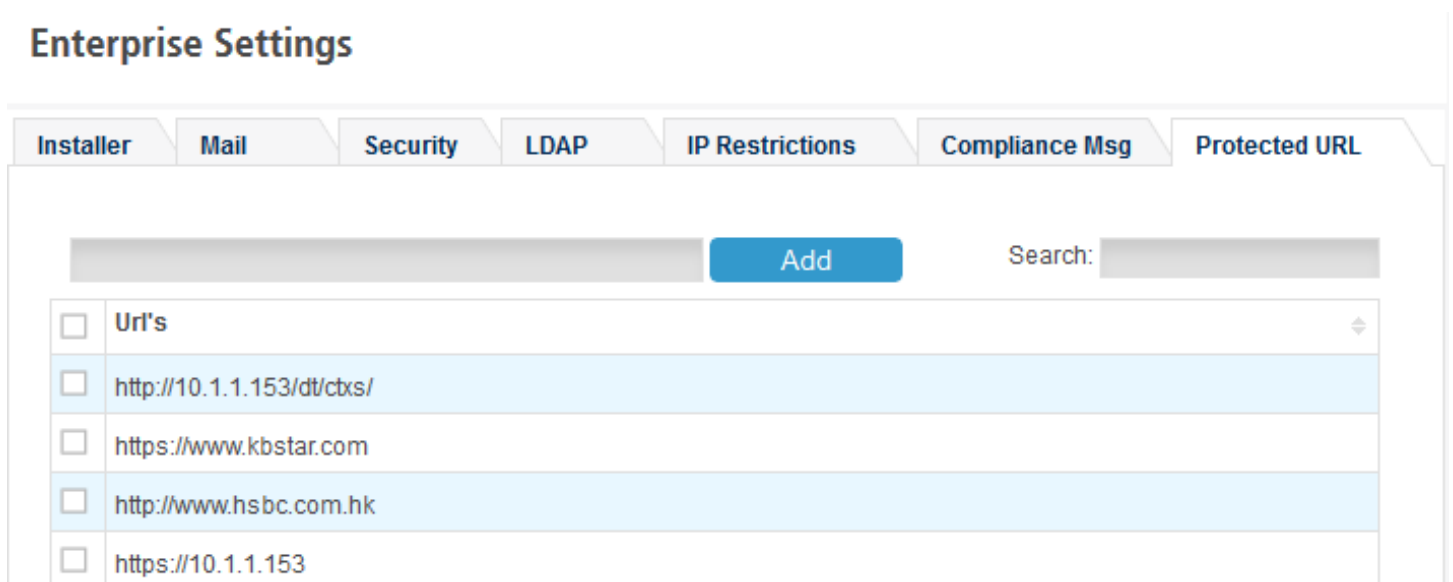
Enterprise Settings

The Enterprise is the highest level defined in the ES1 portal. Distributors or MSPs (managed service providers) would be setup at this level. Each Enterprise could then house a number of subscriptions. These settings include Installer download locations, SMTP mail settings, Security, LDAP, IP white/blacklisting, Compliance Messages, and Enterprise Protected URLs.



ES1 Enterprise Settings

Enterprise Protected URLs give the administrator the ability to add specific URLs that will be forced into SafeCentral's secure session. ProtectedURLs can be added manually, or can be imported via a csv file if processing a large number of URLs at the same time. The add field does not support wildcards or subdomains. Each specific URL, both http and https protocols need to be entered exactly.



ES1 Protected URLs

Subscription Settings

Subscription settings can be defined and unique within an Enterprise so Subscription A settings can be different than Subscription B, if required. If such settings exist for a subscription then endpoints in the group that belong to the subscription will get those settings, else it would inherit from the Enterprise settings. Only a Subscription and Enterprise administrator can view or administer the Subscription settings.

Subscriptions

Select subscription(s) to perform task on. Search:

<input type="checkbox"/>	Subscription Name	Subscription Key	Seats	Used	Expires
<input type="checkbox"/>	First Wontok Demo Subscription	2URR-2UU3-2QTV-LW2X-TD9V	401	262	12/31/2999 12:00:00 AM
<input type="checkbox"/>	Second Wontok Demo Subscription	5WRC-7Q9G-XCJX-TM88-XC86	20	0	12/31/2999 12:00:00 AM

Tasks

Add/Edit Subscription setting ?

Delegate control to provider ?

Delete Subscription setting ?

Delete LDAP Setting ?

ES1 Subscription Settings

License Administration

The License Administration section will give you the ability to query license details based on an email address or endpoint license key entered. License details will provide the expiration date, activation date, last update time, Computer Name, seat keys and whether the license is active. Once you have the license available you can perform such tasks as blocking, expiring or moving the license to a different group within your Enterprise. Querying an Enterprise or Subscription key will not yield any results.

Email Address/License Key: Search

License Details

<p>License Key: 3GAR-GVQ2-X44X-J5AV-6Z8C</p> <p>Expiration Date: 12/31/9999 12:00:00 AM</p> <p>Last Updated: 12/18/2013 8:42:45 AM</p> <p>Last Reported Policy: Capucine test - version 5.0</p> <p>Group Policy: Capucine test - version 5.0</p>	<p>Email Address: test110721334243774productionXP@safecentral.com</p> <p>Activation Date: 11/7/2013 12:13:15 PM</p> <p>Group: Capucine</p> <p>SC Admin Contact: bchris.gardner@gmail.com, noc@safecentral.com, wangshui@mochasoft.com.cn, 775n@sina.com, freem2n@lotte.net, gujian@elitus.cn</p> <p>Subscription: First Wontok Demo Subscription</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Computer Details

<p>Computer Name: bps2test-xp</p> <p>OS: Windows_XP</p>	<p>Description: bps2test-xp</p> <p>CPU: x86</p>
-----------------------------------------------------------------------	---------------------------------------------------------------

Seat Key	Product	Version	State
QECW-XJJA-X2G6-8QHX-K2ER-4C7N	Enterprise Browser		Active
E5UP-PBJC-WA4H-X7VF-KVXP-MJUT	Enterprise SecureDesktop		Active
4N55-EB46-STDV-MNCT-WYSR-7HBP	Enterprise Updater		Active

Tasks

- [Block License ?](#)
- [Unblock License ?](#)
- [Expire License ?](#)
- [Unexpire License ?](#)
- [Clean License for re-installation ?](#)
- [Move computer to a different group ?](#)

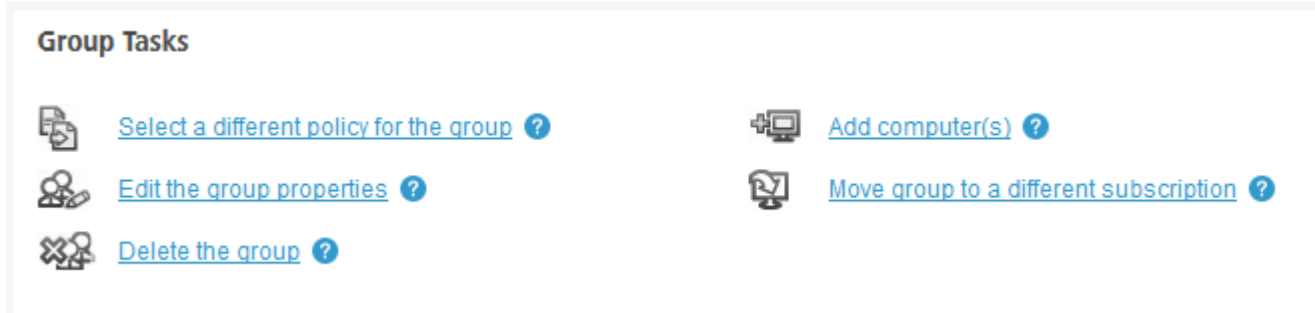
Creating Groups

An Administrator will likely want to setup different groups to manage based on location, executive users, low bandwidth users, contractors, remote users, domains, etc. This is configurable within the Enterprise Server console.

1. Log into Enterprise Server with your Enterprise Administrator email and password. The URL and credentials will be provided to you by email.
2. Click the **Groups** tab. The **Add Group** menu item will be selected by default.
3. To add a new Group, **enter** a Group name.
4. **Enter** a Description for the group such as Operations
5. **Select** a Policy. This policy can be changed at a later time.
6. **Select** how you want to apply updates (defaulted to automatically).
7. Your group is now created and listed under the Groups tab in the left pane on the console.

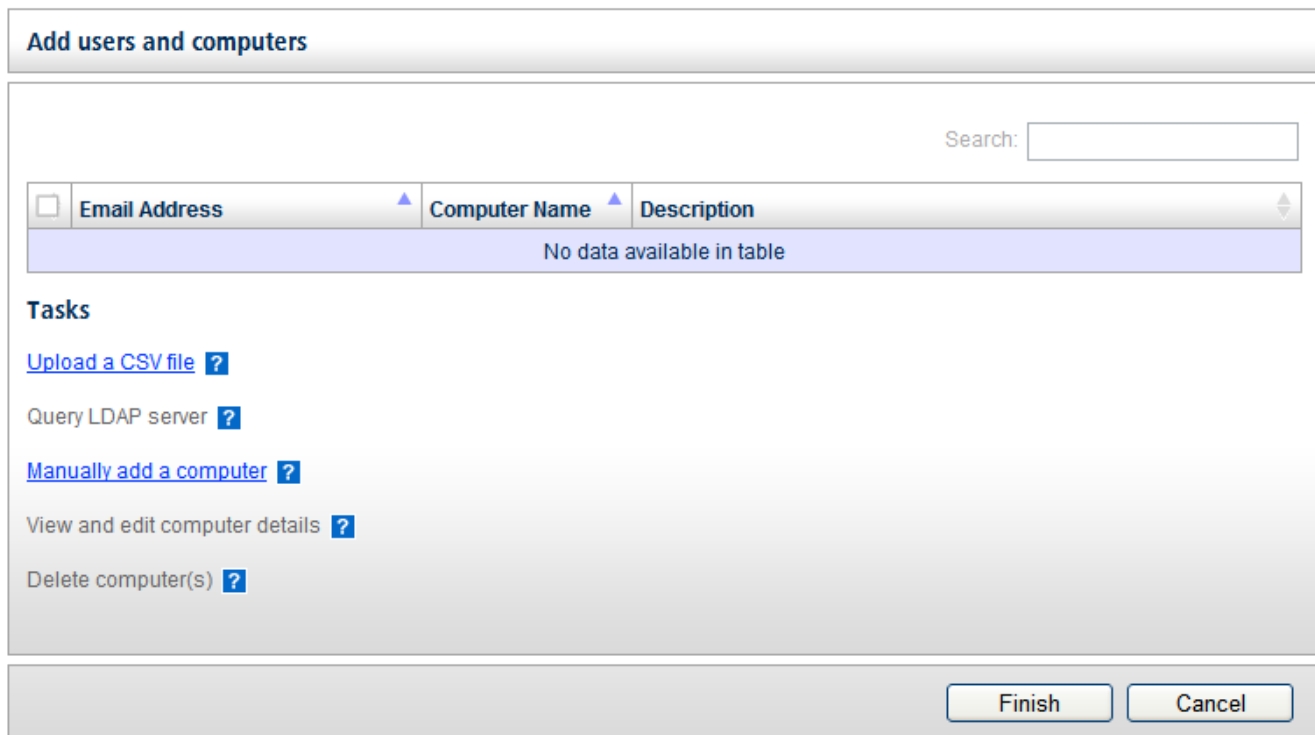
Configuring Computers in Groups

1. Click the **Groups** tab. Select the group you want to manage.
2. Click the **Add computer(s)** link under the Group Tasks section of the console.



ES1 Group Tasks Tab

3. If adding computers with the upload CSV feature, make sure CSV file has appropriate fields: Customer email address, Computer Name, and Description.



ES1 Add users and computers Tab

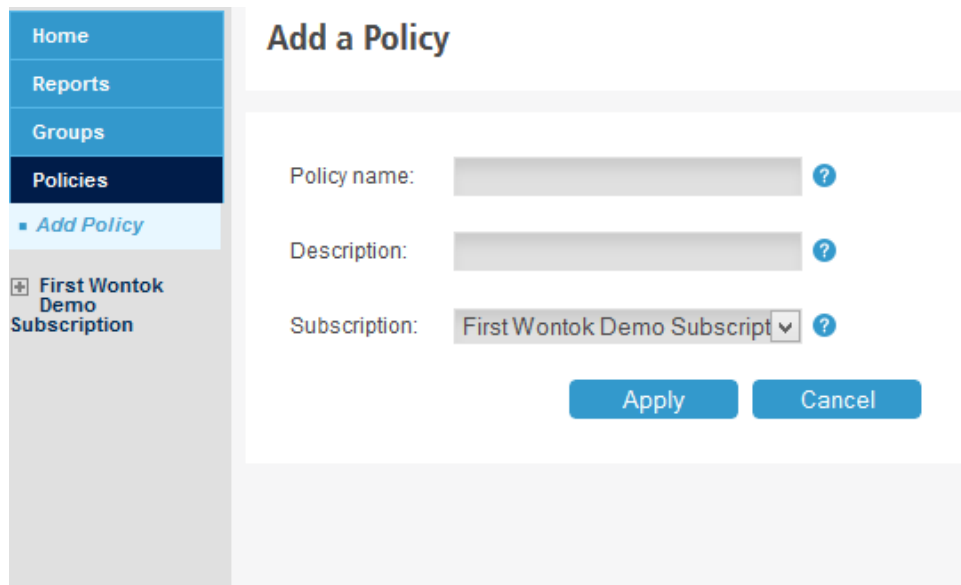
4. If adding computers with the manual feature, enter either a valid email address or computer name and description. The Computer Name field can be left blank if it is not known.
5. Click the **Apply** button.
6. Your computer(s) are now listed under the Groups associated in the left pane on the console.

Configuring Policies

Policies enable an Administrator to setup global settings for specific groups to be managed collectively.

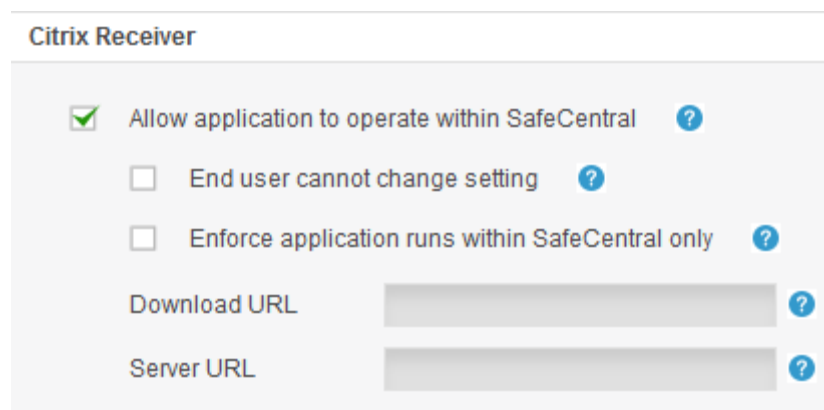
To setup policies for plug-ins:

1. Click the **Policies** tab. The **Add Policy** menu item will be selected by default.
2. **Enter** a policy name.
3. **Enter** a description
4. Click the **Apply** button.



ES1 Add a Policy Tab

5. Your policy is now created and listed under the Policies tab in the left pane on the console.
6. **Select** the Policy you created from the Policies section.
7. **Expand** the plug-in you wish to configure. In our example you see Citrix Receiver. From here you can manage the settings of the SafeCentral Enterprise client being deployed on the endpoint and enter specific download and server URL to download the plugin on the endpoint if it is not installed.



ES1 Plugin Settings

[Allow application to operate within SafeCentral](#) – On the client settings screen determines if the user can see this setting.

[End user cannot change setting](#) – determines if user can change setting

[Enforce application runs within SafeCentral only](#) – forces application to run in SecureDesktop

[Download URL](#) – URL where users will download and install the application

Server URL – URL of landing page associated with the application i.e. location of the VPN server.

8. If a proxy is required you are able to configure this in the Advanced Settings tab.
9. If desired you can also adjust the minutes between update checks for the selected policy by selecting the Updater Settings tab. It is recommended to leave it at the default setting of 360 minutes.

Policy: Citrix Policy for Demo

Groups using this policy: | [+ First Wontok Demo Subscription](#)

Plugins | **Advanced Settings** | **Updater Settings**

SafeBrowser

Show In Default Browser Addon available? [?](#)

Home Page [?](#)

BankID

Cisco AnyConnect VPN Client

Citrix Receiver

Juniper Citrix

Microsoft Remote Desktop

OpenVPN

Palo Alto Global Protect

VMware View

ES1 Plugins Tab

To setup policies for Advanced Settings:

1. Select the policy's Advanced Settings tab
2. To allow copy and paste between the normal and SecureDesktop enable the setting.
3. To allow end users to change these settings locally on the endpoint enable the setting.

Plugins | **Advanced Settings** | **Updater Settings**

Copy & Paste

Copy & Paste feature allowed? [?](#)

End User can change these settings

ES1 Advanced Settings Tab

Reports

After client installation the Administrator can monitor endpoints using the reports provided in the Enterprise console.

Filters - Limits the data shown in the reports to a specific subscription or group.

Current Status - Three pie charts are shown to illustrate activity within your enterprise. The percentage of the total number of endpoints has been activated, the percentage that is active (has checked in for updates in the last seven days) and the percentage that reported the most recently released product versions policy versions and is thus considered up to date.

Last 30 Days - One line chart and one bar chart are shown. The line chart shows the number of installations of SafeCentral Enterprise clients and the number of clients checking for updates in the last 30 days. The bar chart shows the number of clients reporting a specific version of a SafeCentral Enterprise component in the last 30 days.

Enterprise Client Configuration

The SafeCentral Enterprise Client Configuration section will guide an Administrator on the user experience once the client is installed on the local endpoint.

Client Requirements

In order to install the SafeCentral Enterprise client the local computer must meet the following system requirements.

Windows XP (32 bit)

256MB of RAM minimum, 384MB or more recommended.
CPU: P3 class 700MHz or better

Windows Vista and Windows 7 (32 and 64-bit)

1 GB of RAM minimum
CPU: P4 class or better

Windows 8 (32 and 64-bit)

1 GB of RAM minimum; 2GB for 64-bit
CPU: 1Ghz

SafeCentral Enterprise Client Installation

SafeCentral Enterprise client installations are conducted through an invitation email sent via the Enterprise Server.

Send Invitation Email

1. Click the **Groups** tab.
2. **Select** the Group you wish to send an invitation email to. In our example we selected unassigned.

Groups

- » Add Group
- » Applabs Testing
- » Default
- » Internal Testing
- » Unassigned

Installed Pending Inactive Search:

<input checked="" type="checkbox"/>	Computer Name ▲	Email Address ▲	Status ▲	Activation Date (EST) ▲	Last Update Check (EST) ▲	Policy Version ▲
<input checked="" type="checkbox"/>	dtapp1047	Manoj_9-Mar-11_1@safecentral.com	Uninstalled	3/9/2011	3/9/2011	
<input checked="" type="checkbox"/>	mmarcus-xptest	mmarcus1test@safecentral.com	Uninstalled	2/7/2011	2/7/2011	
<input checked="" type="checkbox"/>	win7-x64-mm	mmtest123@safecentral.com	Uninstalled	4/28/2011	4/28/2011	1.0

Computer Tasks

- View and edit computer details ?
- Send invitation email ?
- Move computer(s) to a different group ?
- Delete computer(s) ?

Policies

Updates

ES1 Groups Tab

3. **Select** the computers you wish to send an invitation email to.
4. Click the **Send invitation email** link.
5. The invitation email script will open showing what will be sent to users. You are able to configure the email.
6. Once reviewed/edited click the **Send email** link.

Invitation email for selected customers

```
[p]Please use [a href="https://es1.safecentral.com/downloader/direct.aspx?lic={key}&email={email}"]this link[/a] to install SafeCentral Enterprise.[/p]
[p]If clicking the link above doesn't work, please copy and paste the URL in a new browser window instead.[/p]
[p]Thank you for using SafeCentral Enterprise.[/p]
[p]For questions or concerns about your account, please contact your SafeCentral Enterprise Global Administrator.[/p]
[p]This is a post-only mailing. Replies to this message are not monitored or answered.[/p]
```

Tasks

- Send email ?

ES1 Email Invite

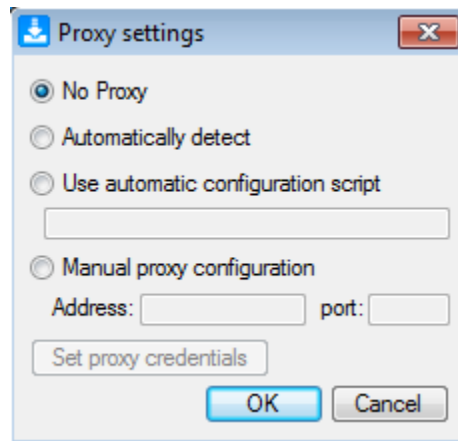
Enterprise Client Installation

When the SafeCentral Enterprise Administrator sends the email invitation to users they will receive an email titled **SafeCentral Enterprise Installation**. The installer will run and load the Enterprise client on the local computer. SafeCentral can be activated on more than one computer per email address if needed.

To install the Enterprise client:

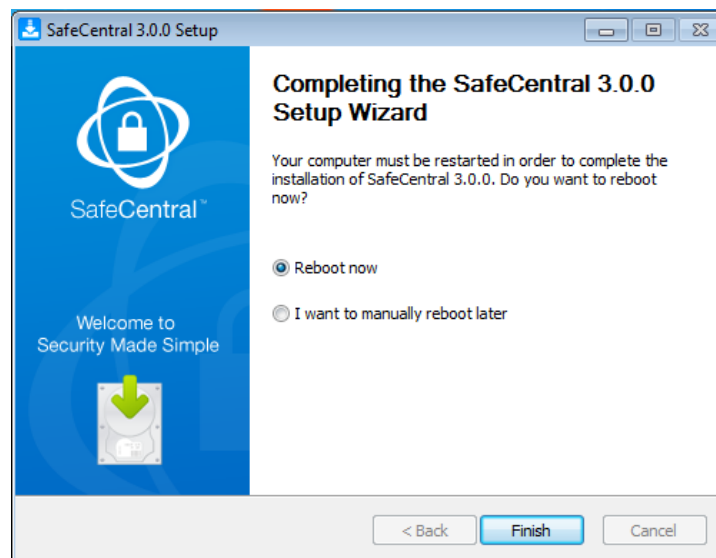
1. **Launch** the invitation email.

2. **Select** the link to download or copy and paste the URL into a new browser window.
3. It is recommended to close other running applications. Click **Next** at the welcome setup screen.
4. Select **I Agree** at the License Agreement screen.
5. Your SafeCentral key should auto populate your key at the Create an Account screen.
6. If applicable verify your proxy settings and credentials.



Proxy Settings Screen

7. The installer will install files to the local computer.
8. Once completed the installer will prompt you to reboot. It is recommended to reboot. Click **Finish**.



SafeCentral Setup

Web Based Installation

Administrators can also direct end users to install directly from the web utilizing the following format (substituting the GUID with your Enterprise key and end user email address):

[https://es1.safecentral.com/downloader/direct.aspx?lic=**GUID**&email=**email@domain.com**](https://es1.safecentral.com/downloader/direct.aspx?lic=GUID&email=email@domain.com)

These values will be populated automatically into the SafeCentral installer.

Silent Installation Method

Administrators who wish to install SafeCentral silently on their network without end user interaction can do so using one of the following two commands.

```
SafeCentral.exe /S /USERNAME=username /PWD=password
```

```
SafeCentral.exe /S /LICKY=EnterpriseKey
```

Enterprise Client Startup

By default after installation SafeCentral will add the black deskband to your Windows toolbar. This deskband will launch automatically every time you start the end point. Clicking the deskband will manually launch the SecureDesktop.



If system tray icons and notifications are enabled within Windows the SafeCentral updater icon will also display in the Windows system tray at every startup. The SafeCentral updater will communicate with the server to check for policy changes, updates, and license status at every reboot, depending on the policy set for updates, or when the user manually updates.

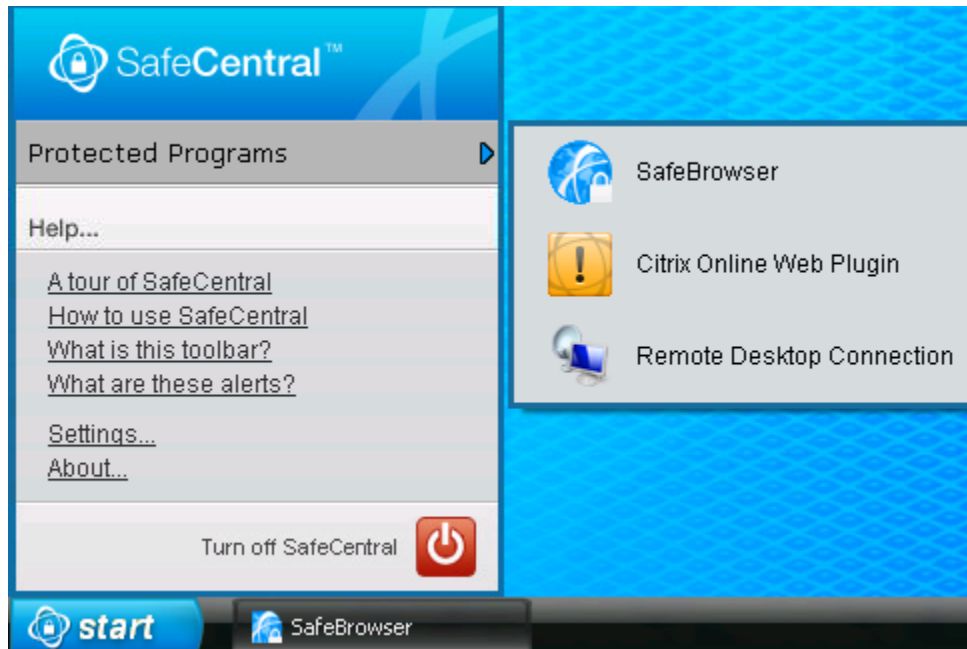


SafeCentral Enterprise Client Installation (Silent - Optional)

For Administrators wishing to bypass user interaction with the installer SafeCentral can be installed silently where no setup user interface is shown during installation.

Touring the Enterprise Client

The SafeCentral SecureDesktop can be launched either by the desktop shortcut, start menu shortcut, or by manually launching the black deskband. Depending on your configuration Protected Programs will vary in the start menu. In our example the Citrix Online Web plug-in client was installed prior to installing SafeCentral and was configured by the Administrator to be a protected program that is able to run in SecureDesktop. Other configurations may include the SafeCentral SafeBrowser, Microsoft RDP, etc.



SecureDesktop Start Menu

If protected programs are not properly configured or installed prior to installing SafeCentral Enterprise you will not see the proper icon in the SecureDesktop or start menu.

Technical Support

For technical support please contact us [here](#) to raise a support issue.