راهنمای نرم افزار مدیریت توکن امنیتی در سبلان

شرکت فنی مهندسی ایپا

(ایده پژوهان اسپادانا)

(سهامی خاص)

www.eepaco.ir

فهرست

مقدمه 3

روش نصب نرم افزار 4

اجزا نرم افزار 10

1-1- صفحه ورود به نرم افزار 10

1-2- Host to Net 10

1-2-1- صفحه تنظیمات سرور 10

1-2-2- تنظیمات HA 12

1-2-3- تعریف مدیر 14

1-2-4- Zabbix server 16

1-2-5- پیکربندی توکن 16

1-3- سوییچ توزیع شده 18

1-3-1- ارتباط سوییچ شبکه 18

1-3-2- تنظیمات سوییچ 18

1-3-1-Zabbix Server 20

1-4- GClient 21

مقدمه

این مستند به معرفی نرم افزاری از سامانه سبلان می‌پردازد که توسط آن مدیران، قادر خواهند بود توکن های سامانه سبلان را برنامه‌ریزی کنند. نام این نرم افزار e_token_manager می‌باشد. در ادامه به شرح قسمت های مختلف این برنامه پرداخته خواهد شد.

روش نصب نرم افزار

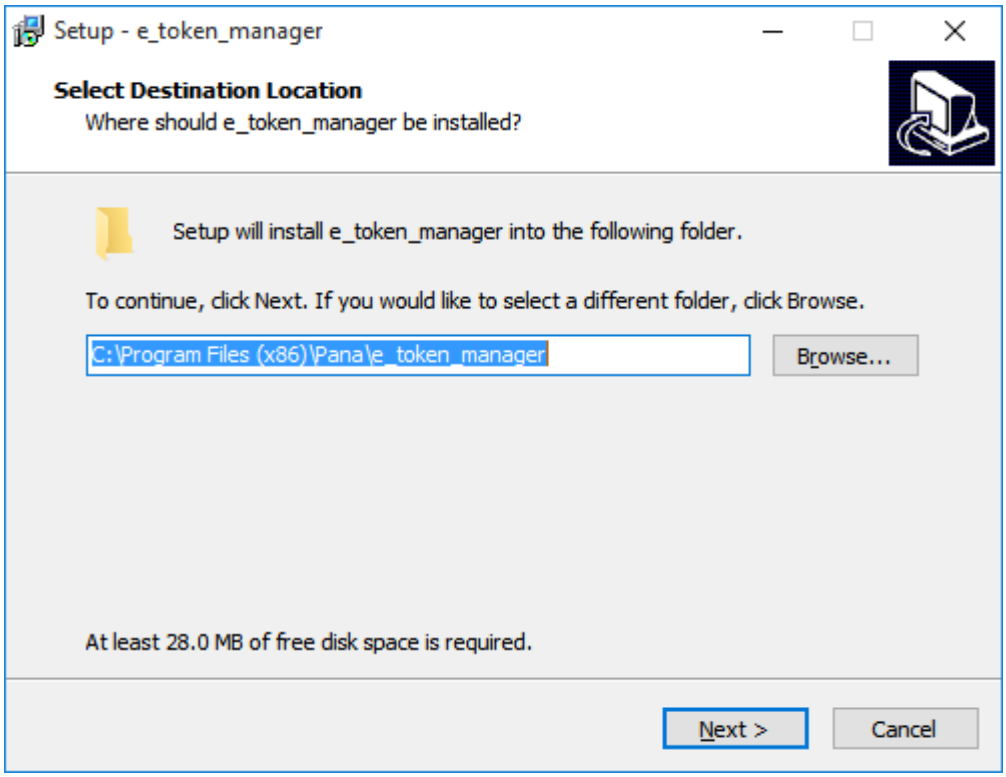
برای نصب این نرم افزار کافی است که فایل نصبی e_token_manager_setup اجرا شود. توجه شود که اگر این نرم افزار از قبل بر روی سیستم کاربر نصب شده است، برای نصب مجدد ابتدا آن را از قسمت Control Panel\Programs\Programs and Features از نصب خارج و سپس برنامه مجددا نصب گردد. بعد از نصب آیکون زیر بر روی دسکتاپ ظاهر می‌شود. برای استفاده از برنامه کافی است بر روی آن دابل کلیک شود.

شکل 1: میانبر مدیریت توکن

در ادامه مراحل نصب این نرم افزار را توضیح داده می‌شود.

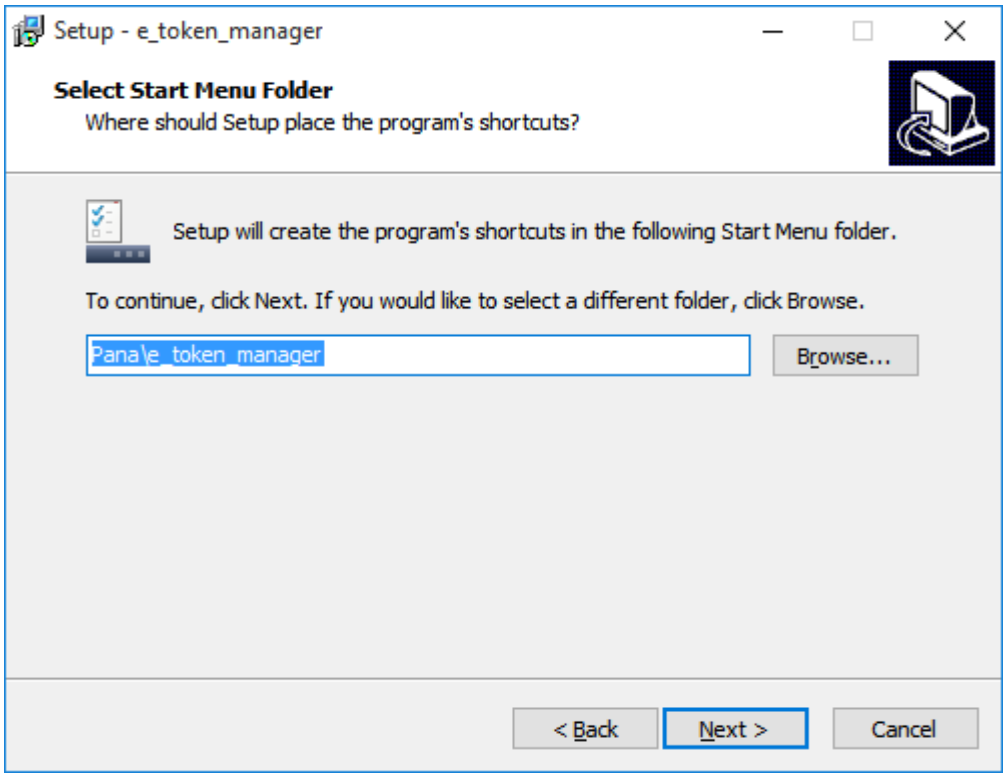
برای نصب ابتدا فایل نصبی e_token_manager_setup با دسترسی مدیر اجرا شود.

1- در مرحله اول نصب نام پوشه محل نصب را سوال می‌کند که این فیلد با پارامتر مشخصی مقدار دهی اولیه شده است و در صورتی که کاربر مایل باشد در محل پیش فرض نصب می‌شود.



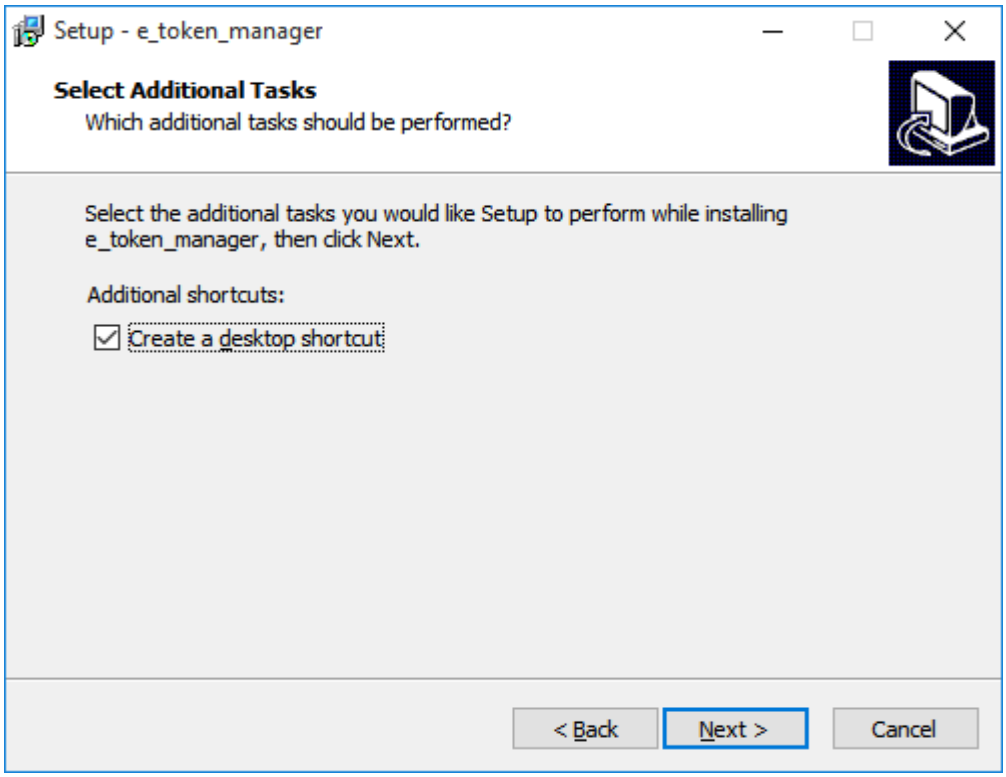
شکل 2: مرحله اول نصب

2- مرحله دوم نام و محل میانبر برنامه را سوال می‌کند که این پارامتر هم با مقدار پیش فرض و مناسب به صورت اتوماتیک پر شده است. در صورت نیاز می‌توان این مقدار را به مقدار دلخواه خود تغییر داد.



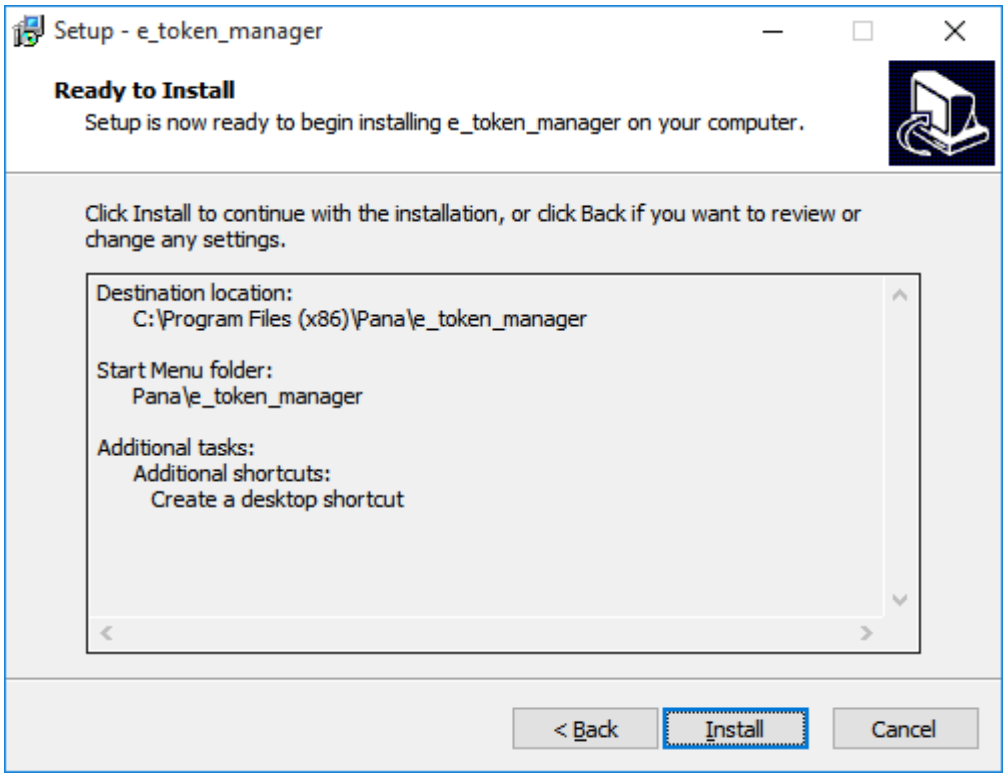
شکل **3**: مرحله دوم نصب

3- در مرحله سه سوال می‌کند که آیا کاربر مایل به قرار دادن میانبر برنامه بر روی دسکتاپ خود هست؟ می‌توان با تیک زدن چک به این منظور دست پیدا کرد. به صورت پیش فرض میانبر انتخاب شده است.



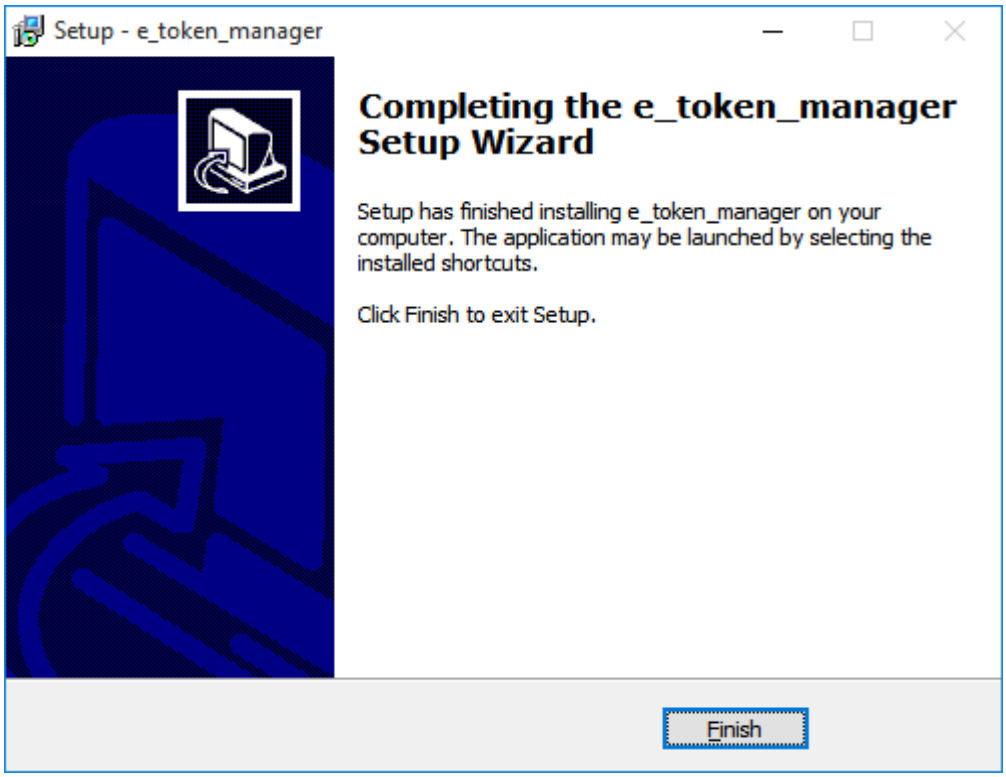
شکل 4: مرحله سوم نصب

4- در مرحله چهارم تمام سوالات قبل از نصب از کاربر سوال شده است و اکنون سوال می‌کند که برنامه برای نصب آماده است آیا مایل به نصب آن هستید. با انتخاب دکمه install برنامه نصب می شود. این مرحله ممکن است چندین دقیقه به طول انجامد.



شکل 5: مرحله چهارم نصب

5- این مرحله آخرین کافی است بر روی کلید finish کلیک شود تا نصب به پایان برسد.



شکل 6: مرحله پنجم نصب

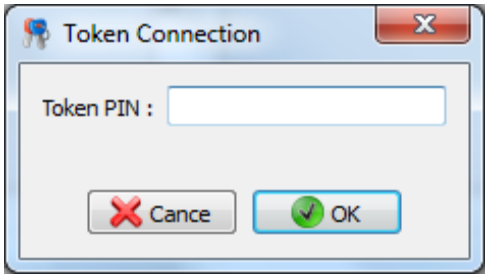
در این مرحله نصب به اتمام رسیده و برنامه آماده استفاده است. در بخش بعد استفاده از این برنامه را توضیح داده می شود.

اجزا نرم افزار

1-1- صفحه ورود به نرم افزار

برای استفاده از سامانه مدیریت توکن ایتدا باید توکن امنیتی را ورودی USB ماشین متصل و سپس کلید Connect to Token انتخاب شود تا صفحه ورود نمایش داده شود.

در این صفحه برای ورود به سیستم باید رمز توکن را وارد شود. رمز توکن به صورت پیشفرض 1234 است که با ورود به برنامه می‌تواند این رمز را تغییر داد. در ادامه نحوه انجام این کار توضیح داده می‌شود.

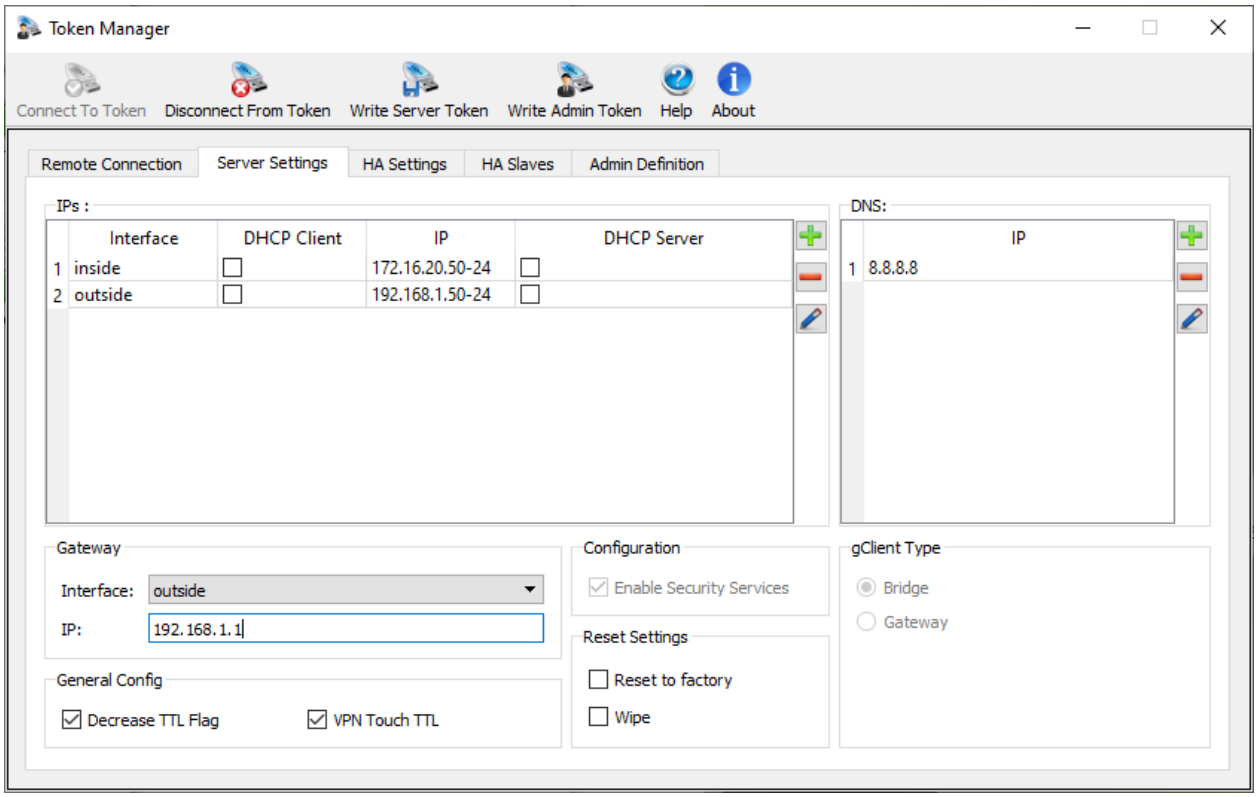


شکل 7:صفحه ورود به مدیر توکن

Host to Net -2-1

1-2-1- صفحه تنظیمات سرور

با ورود به نرم افزار قسمت تنظیمات سرور نمایش داده می‌شود. همانطور که در شکل زیر مشاهده می‌شود، تنظیمات سرور شامل قسمت های مختلفی است که در زیر توضیح هر کدام آورده شده است.



شکل 8:تنظیمات سرور مدیر توکن

:Ips

در این قسمت آی پی هایی که باید روی سرور تنظیم شود را بر حسب نام اینترفیس اضافه می‌شود.

:DNS

در این قسمت آی پی های DNS سرورهایی را که باید برای سرور تنظیم شود را اضافه می‌شوند.

:Gateway

برای سیستم باید یک Gateway تنظیم شود. ابتدا باید نام اینترفیسی که متصل به gateway انتخاب و سپس آدرس Gateway مورد نظر را درج گردد.

1-2-2- تنظیمات HA

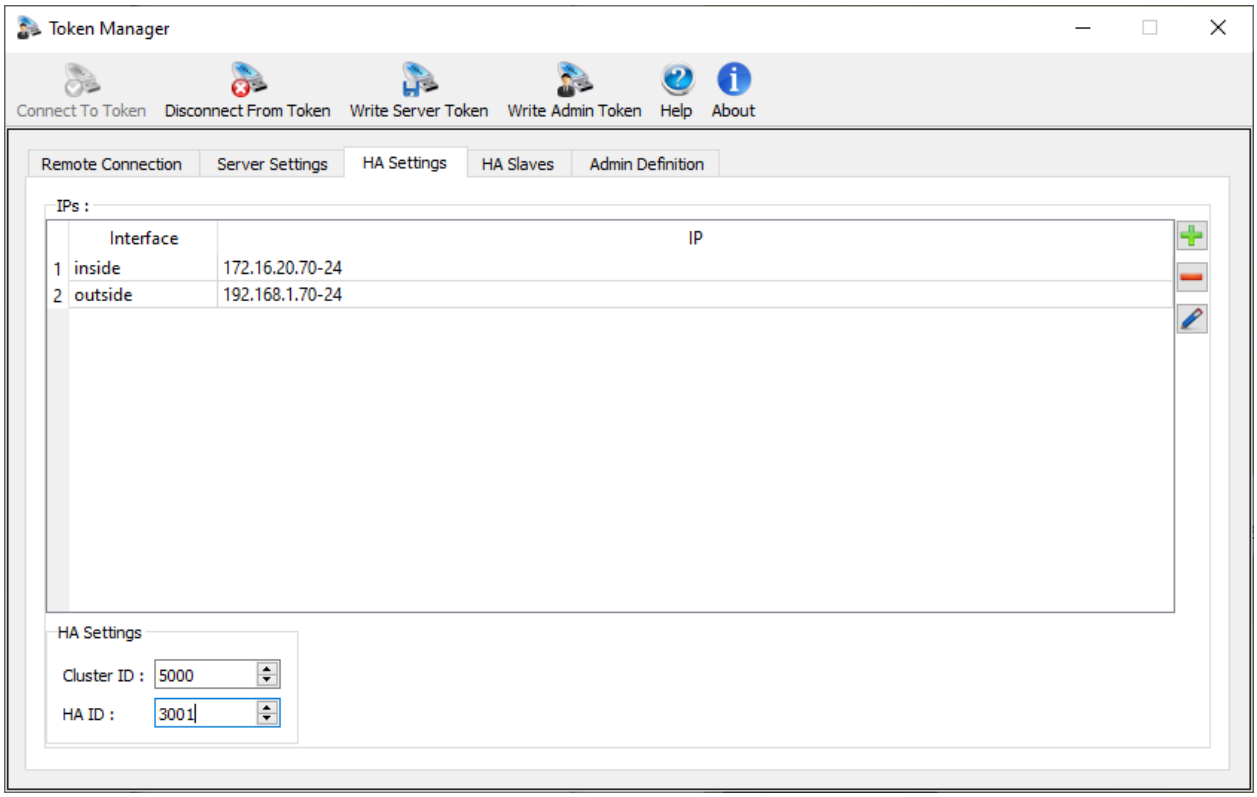
تذکر: قابلیت دسترسی بالا مربوط به رمز کننده سبلان است و در حال حاضر در سوییچ توزیع شده فعال نمی باشد.

این قسمت مربوط به تنظیمات High Availability می‌باشد. برای مثال، اگر قرار است دو عدد سرور راه اندازی شود تا این دو سرور در نقش HA با همدیگر فعالیت داشته باشند، باید cluster id را برای این دو ماشین یکسان، مثلا هر دو ماشین را روی 5000، تنظیم شود. همچنین، ha id را برای هر کدام منحصر به فرد ، مثلا ماشین اول 3001 و ماشین دوم 3002، تنظیم شود.

هر ماشین در نقش ha دو مجموعه آدرس ip دارد: یکی برای حالتی که master است و دومی برای حالتی که master نیست. همچنین، هر ماشین باید آدرس ip دیگر ماشینهای حاضر در کلاستر خود را نیز بداند. اگر ماشین در حالت master قرار گیرد، باید آدرسهایی را که در قسمت server setting ذکر شده‌اند، داشته باشد. در غیر این صورت، آدرس ip ماشین مقادیری است که در قسمت ha setting تنظیم می‌شوند.

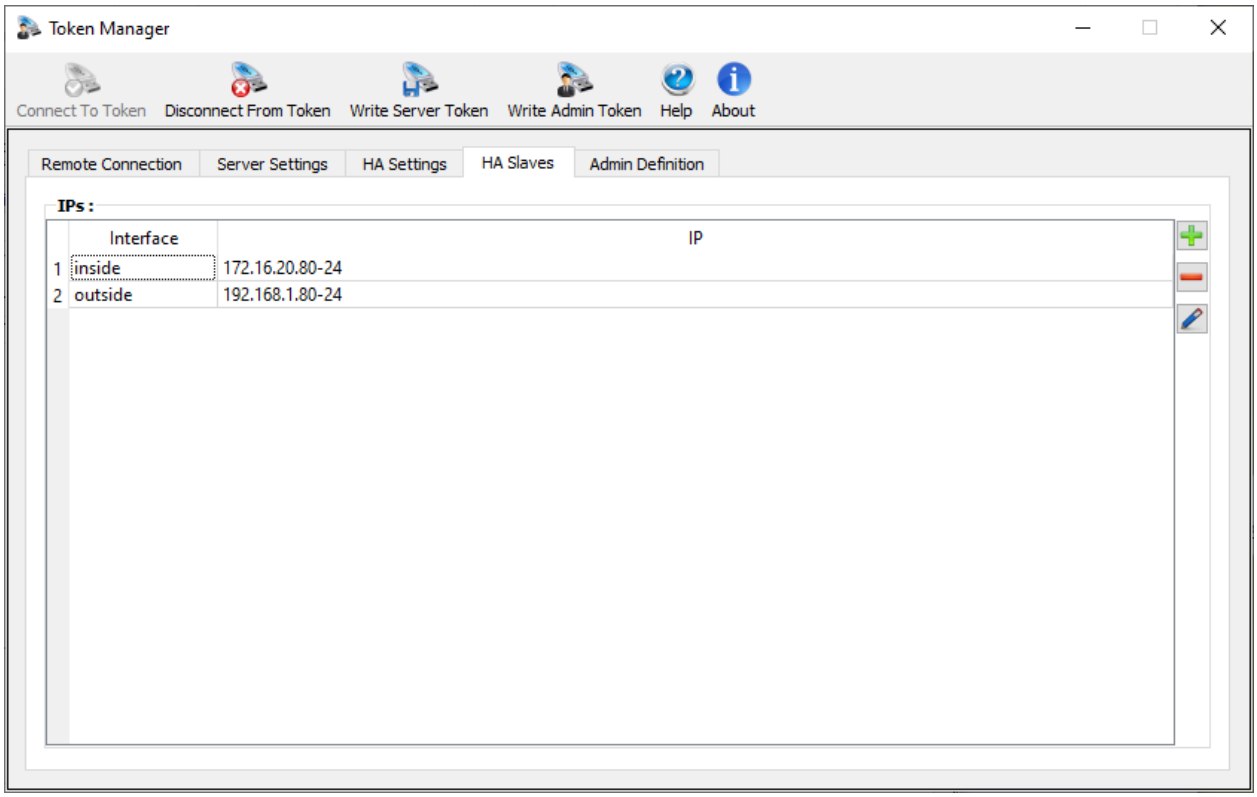
آی پی های HA (High Availability):

در قسمت HA settings همانطور که در شکل زیر مشخص است، باید آی پی های را وارد شوند که اگر این ماشین در ha در حالت master، یعنی سرور اصلی نیست، باید این آی پی ها بر روی آن تنظیم شود.



شکل 9:آی پی های سرور

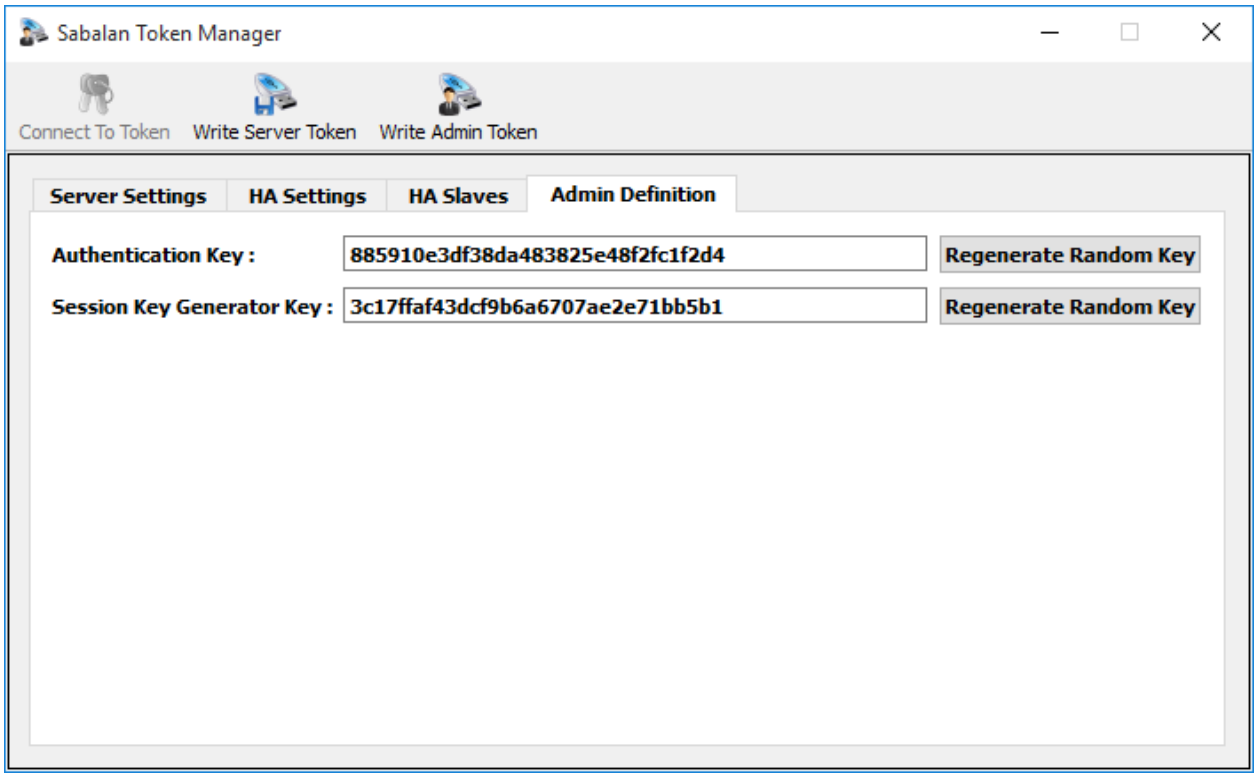
همچنین در قسمت slave ips آی پی های ماشین یا ماشینهایی اضافه می‌شوند که در نقش پشتیبان ماشین اصلی هستند. همانند شکل زیر



شکل 10:آی پی های slave

3-2-1- تعریف مدیر

در قسمت تعریف مدیر نام مدیر و کلمه عبور مدیر را مشخص می‌شود. این اطلاعات با وصل کردن توکن مدیر به کامپیوتر و زدن دکمه ی write admin token، بر روی توکن مدیر نوشته می‌شود. این فرم را در شکل زیر نشان داده شده است.



شکل 11:تعریف مدیر

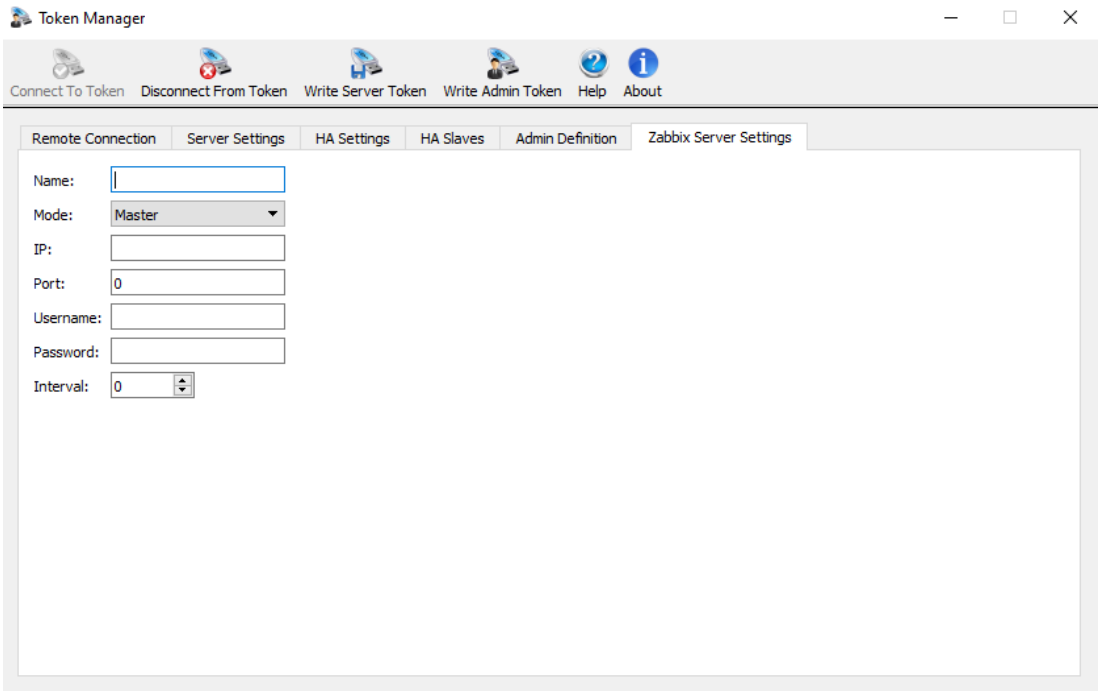
تذکر مهم

بعد از اینکه تمام تنظیمات مورد نظر را انجام گرفت برای ثبت این اطلاعات بر روی توکن امنیتی باید حتما دکمه write server token انتخاب گردد. در غیر این صورت، هیچ اطلاعاتی بر روی توکن ذخیره نمی‌شود و سرور به درستی اجرا نمی‌گردد.

همچنین، برای تعریف مدیر باید حتما دکمه write admin token را زمانی که توکن مدیر همزمان با توکن سرور در کامپیوترتان می‌باشد، فشار داده شود تا اطلاعات مورد نظر بر روی آن ثبت شود و مدیر بتواند با سرور ارتباط بر قرار کند.

Zabbix server -1-2-4

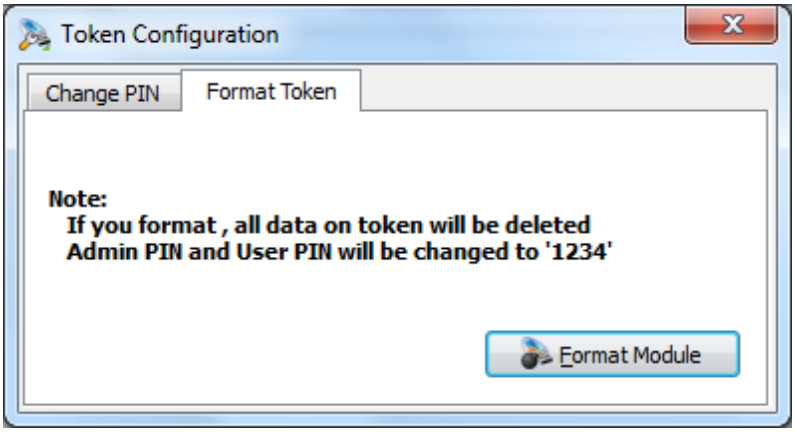
برای لاگ گیری از سرور در سناریو Host to net، می توان در سربرگ Zabbix server setting اطلاعات سرور Zabbix را قرار داد و سپس با استفاده از این اطلاعات روی توکن، سروری که به عنوان master انتخاب شده است می تواند سرور Zabbix را بشناسد و با آن ارتباط بگیرد.



شکل 12 معرفی Zabbix server به سرور سبلان

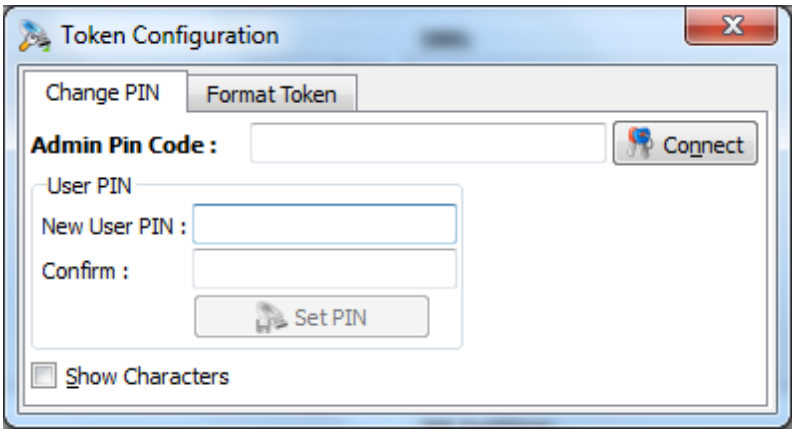
1-2-5- پیکربندی توکن

در قسمت پیکربندی توکن می‌توان توکن مورد نظر را به کلی فرمت کرد تا تمام اطلاعات روی آن از بین برود و توکن را به حالت اولیه کارخانه درآید. در شکل زیر فرم مربوط به این گزینه را نشان می‌دهد.



شکل **13** :فرمت کردن توکن

همچنین، می‌توان کلمه عبور توکن را تغییر داد. این کار با استفاده از فرم زیر صورت می‌گیرد.



شکل **14** :تغییر کلمه عبور

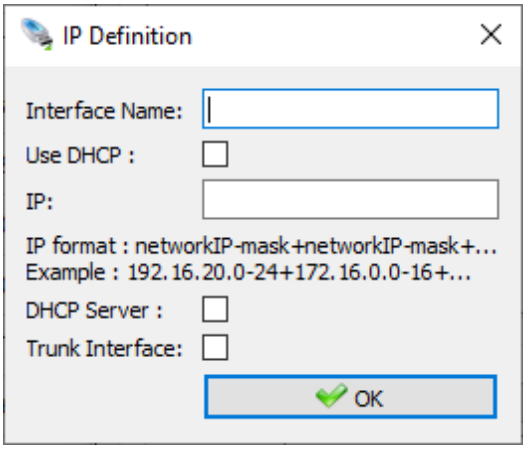
1-3- سوییچ توزیع شده

با استفاده از قابلیت سوییچ توزیع شده چند شبکه که سرور رمز کننده در لبه آنها قرار دارد می‌توانند با یکدیگر مرتبط شوند. شمای یک شبکه سوییچ را نشان می‌دهد.

هر سرور با یک نام(node_name) به شبکه سوییچ معرفی می‌شود. نام سرورها باید یکتا باشد. هنگام تنظیم سوییچ باید لیستی از نودهای حاضر در شبکه را به سوییچ معرفی نمود که در واقع سایر نودهای شبکه هستند.

1-3-1- ارتباط سوییچ شبکه

هنگام تعریف اینترفیس باید تعیین کرد کدام اینترفیس دستگاه سوییچ ارتبط آن را با شبکه سوییچ برقرار می کند. به عبات دیگر، باید برای اینترفیسی که نود سوییچ را به دیگر نودهای سوییچ متصل می کند تعیین نمود. برای این منظور گزینه Enable switch برای اینترفیس مورد نظر انتخاب می‌شود.

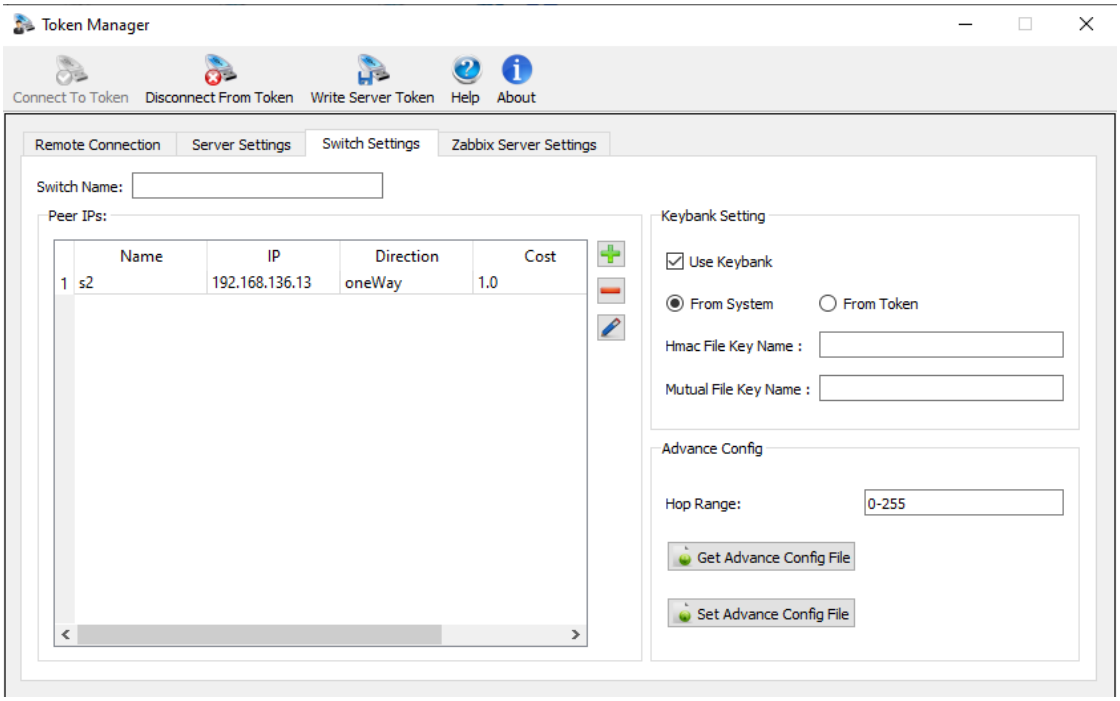


شکل 15 معرفی IP اینترفیس سوییچ جهت ارتباط با شبکه سوییچ

تذکر: آدرس IP درج شده برای اینترفیس کاربردی ندارد و می‌تواند خارج از رنج آدرس شبکه داخلی باشد.

1-3-2- تنظیمات سوییچ

در تب switch setting، باید شناسه شبکه سوییچ و یک نام برای نود انتخاب شود. شناسه برای همه نودهای یک شبکه یکسان است و نام باید متفاوت باشد.



شکل 16 تنظیمات سوییچ

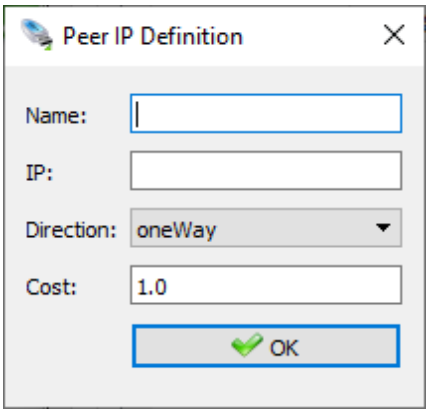
در صورتی که ادمین بخواهد می تواند از مدیریت کلید در سامانه جهت افزایش امنیت استفاده نماید. برای این منظور ادمین باید گزینه use_key_bank را انتخاب نموده و نام فایل کلید مربوطه را درج نماید. در صورتی که فایل کلید روی توکن انتخاب شود باید با استفاده از برنامه مدیریت بانک کلید کلید مربوطه در توکن سرور درج شود.

علاوه بر این با توجه به قابلیتهای مختلف دستگاه رمز کننده، امکان اعمال قوانین دیگر روی سرور نیز فراهم شده است. مدیر می‌تواند با آگاهی از دستورات ec فایل کانفیگی آماده کند و روی توکن ذخیره نماید. ذخیره فایل حاوی قوانین با گزینه set صورت می‌گیرد. همچنین مدیر می‌تواند این قوانین را با استفاده از کلید get دریافت و بررسی نماید.

همچنین، برای هر نود محدوده تعداد گام تعیین می‌شود. با توجه به اینکه در سناریوهای مختلف سوییچ توزیع شده امکان قرارگیری نودها در مسیر ارتباطی بین دو نود وجود دارد، توپولوژیهای ارتباطی گوناگونی مانند خطی، ستاره ای، مش و غیره قابل پیاده سازی است. در صورتی که ادمین شبکه بخواهد می تواند با تعیین تعداد گام عدم ارتباط محلی بین زیرشبکه‌های مختلف یک نود (حذف تعداد گام صفر با تعیین محدوده 1–255)یا

محدود سازی ارتباط به حالت نقطه به نقطه (حذف بیش از یک گام در انتقال با تعیین محدوده 0–1 یا 1–1) را فراهم سازد.

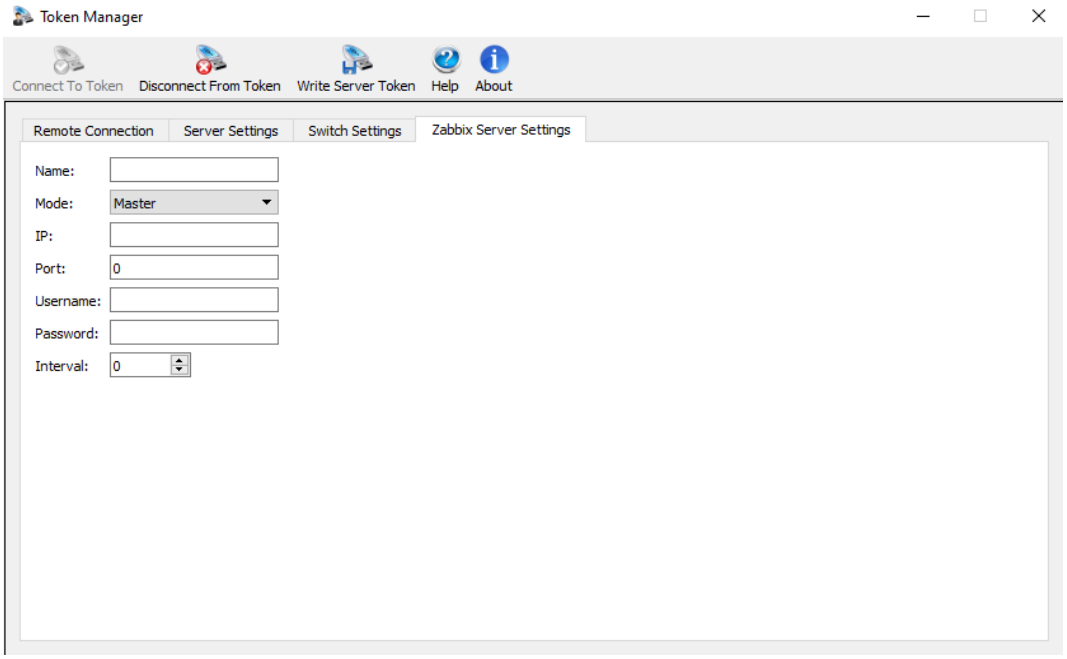
در بخش peer Ips باید سایر نودهای همجوار را برای این نود تعریف نمود. نام نود همان نامی است که برای نود انتخاب شده، آدرس IP نود که از طریق شبکه زیرساخت قابل دستیابی است، جهت ارتباطی که میتواند یک یا دو طرفه باشد و همچنین هزینه مسیر. جهت ارتباط میتواند یکطرفه باشد یعنی تنها خود نود بتواند با نود دیگر ارتباط برقرار نماید و نود مقابل تنها می‌تواند پاسخ دهنده باشد. اگر جهت ارتباط دوطرفه باشد، نود این مساله را به اطلاع نود مجاور می‌رساند و نود مجاور به صورت خودکار بدون تغییر در تنظیمات ارتباط دوسویه با این نود را می‌پذیرد. تعیین جهت ارتباط در کاربردهای تحمل پذیری خرابی و توزیع بار برای ساخت چند مسیر بین دو نقطه اهمیت دارد. همچنین، هزینه مسیر ارتباطی بین دو گره نیز در تصمیم گیری برای انتخاب مسیر با هزینه کمتر مورد استفاده قرار می‌گیرد. تعیین هزینه اختیاری است و به صورت پیش فرض هزینه هر دو نود مجاور 1 در نظر گرفته می‌شود.



شکل 17 تعریف نودهای مجاور به نود موردنظر

Zabbix Server -1-3-1

برای لاگ گیری از سرور در سناریو سوییچی، می توان در سربرگ Zabbix server setting اطلاعات سرور Zabbix را قرار داد و سپس با استفاده از این اطلاعات روی توکن سوییچی که به عنوان master انتخاب شده است می تواند سرور Zabbix را بشناسد و با آن ارتباط بگیرد.

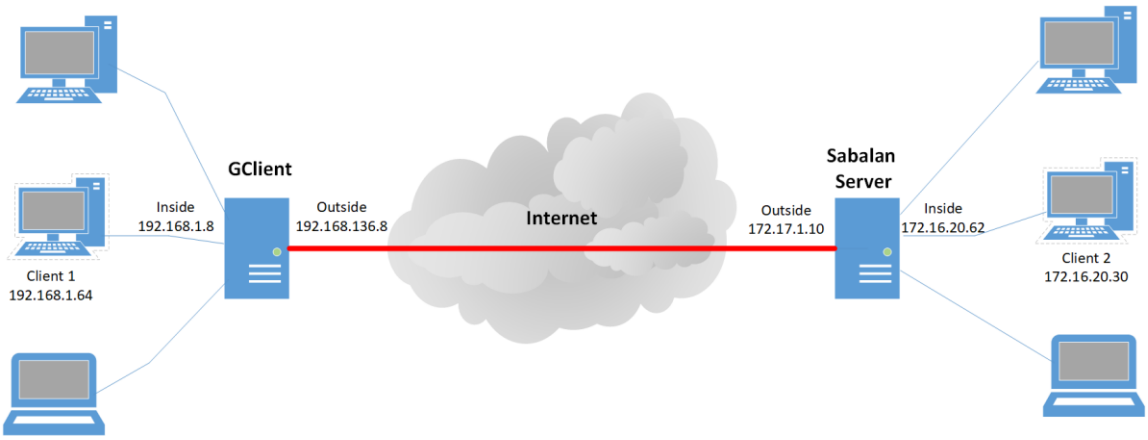


شکل 18: معرفی Zabbix server به سوییچ

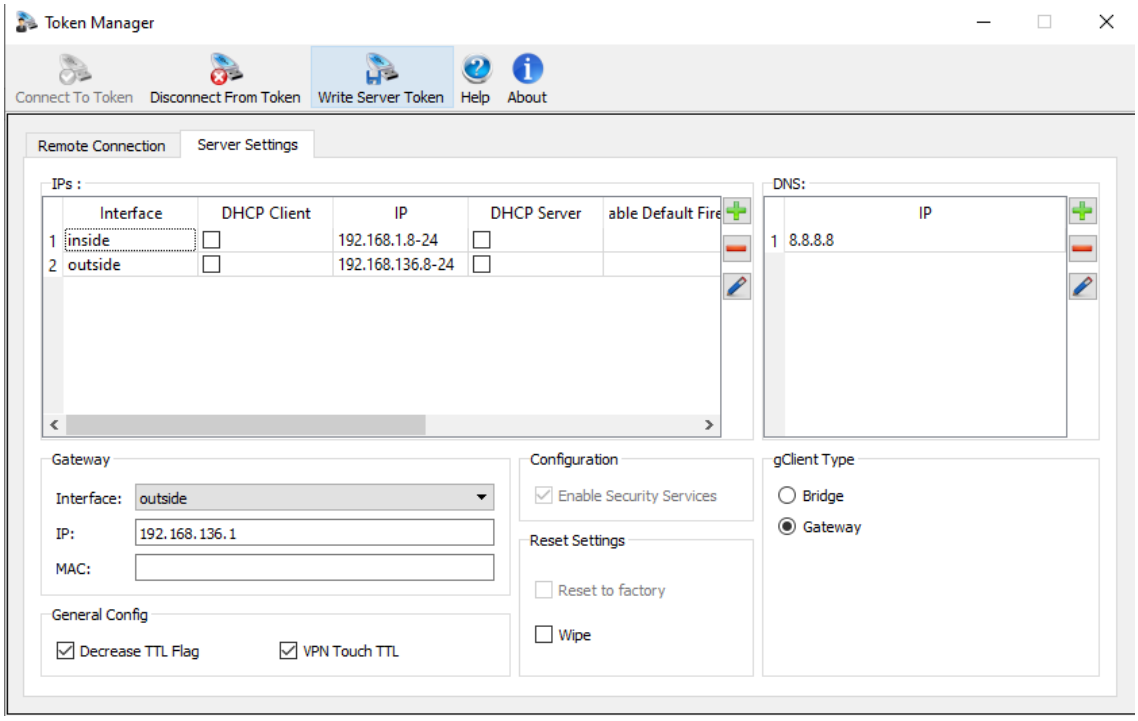
gClient -1-4

برای ارتباط امن از دفاتر با سازمان نیاز به یک سرور به اسم gClient است. این سرور تونلی امن به سرور اصلی که در سازمان قرار دارد، برقرار می کند و کاربران درون دفاتر از طریق این تونل به صورت امن به اطلاعات و دیتابیس سازمان خود دسترسی خواهند داشت. برای کانفیگ این سرور باید یک کاربر که از نوع اتصال با توکن gClient است را به سرور درون سازمان اضافه کنیم (برای جزییات بیشتر به e_sabalan_manager مراجعه کنید.) و سپس آن کاربر را روی توکنی که تنظیمات gClient مطابق با سناریو موردنظر روی آن است، write می کنیم. در این مستند به تنظیمات موردنیاز روی توکن می پردازیم.

مطابق با سناریویی که شبکه سازمان مطابق آن بسته شده است اطلاعات را روی توکن قرار می دهیم. برای مثال اگر شبکه سازمان و دفتر مطابق شکل 19 باشد، در آن صورت اطلاعات توکن به شکل زیرخواهد بود.



شکل **19**: سناریو شبکه سازمان و دفتر



شکل **20**: اطلاعات توکن **GClient**

اگر یک gateway از قبل برای سیستم های سازمان تعیین شده است gClient type توکن را روی حالت bridge قرار می دهیم تا لازم نباشد گیت‌وی شبکه را عوض کنیم اما بتوانیم از طریق gClient به سرور تونل

بزنیم. اما اگر امکان عوض کردن گیت‌وی شبکه به ip دست inside از gClient باشد در تنظیمات توکن gClient Type آن را روی gateway می گذاریم.

مورد دیگری که قابل تنظیم است استفاده از DHCP server است. یعنی اگر بخواهیم دست gClient از دست DHCP server درون شبکه IP بگیرد باید در توکن برای آن دست تیک use dhcp را بزنیم. اگر می خواهیم gClient خودش به عنوان DHCP server نیز عمل کند و به سیستم های متصل به خود IP در رنج IP فعلی خود بدهد باید در تنظیمات توکن برای آن دست gClient تیک گزینه DHCP server را بزنیم.

در نهایت، با زدن گزینه Write server token اطلاعات را روی توکن ذخیره می کنیم و آن را به سرور gClient متصل می کنیم. با اینکار سرور gClient به صورت خودکار تونل را با سرور برقرار می کند.