Internet Explorer

Requirements

Internet Explorer requires the user to be logged into the computer with a domain account. IE will only send Kerberos tickets to sites which are in the **Local Intranet** Security Zone.

Edge and Google Chrome will also allow Kerberos to sites in the **Local Intranet Zone.**

Manual configuration and inspection

For testing purposes, you might be able to configure Zone settings locally in Internet Explorer.

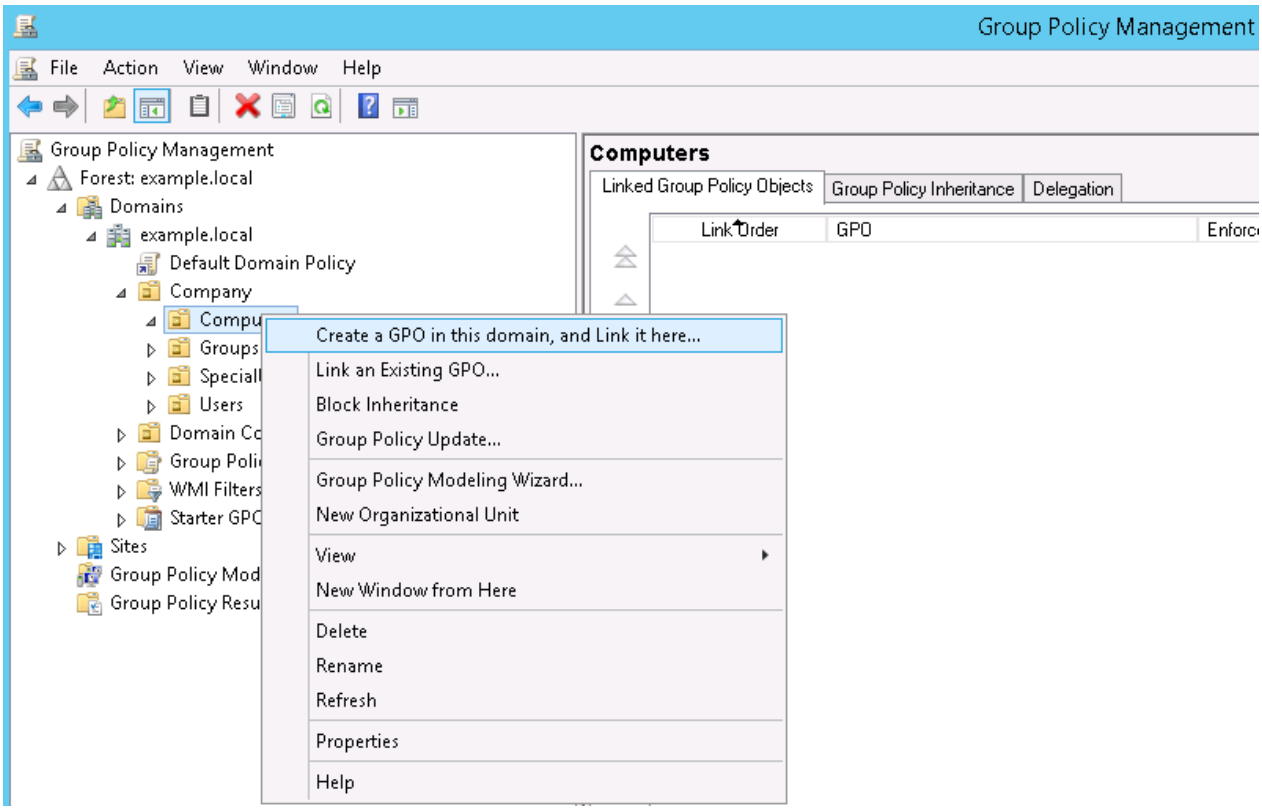
Go to Tools / Internet Options / Security / Local Intranet / Sites / Advanced

However, in most organizations, the zone assignment is done centrally through the use of Group Policy Objects.

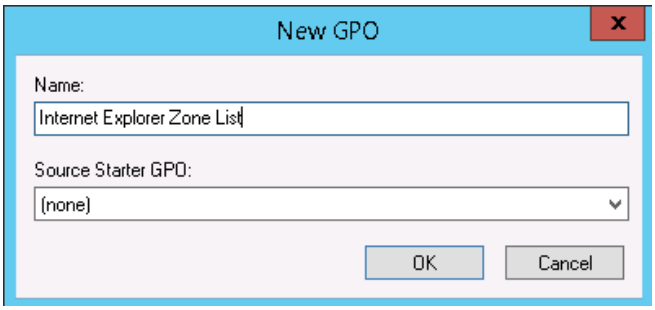
> Ensure "Display company intranet sites in compatibility view" is disabled for IE. Jira/Confluence will not work properly in compatibility mode. See the following for further details.

Group Policy configuration

In this example we create a new policy to hold the settings.

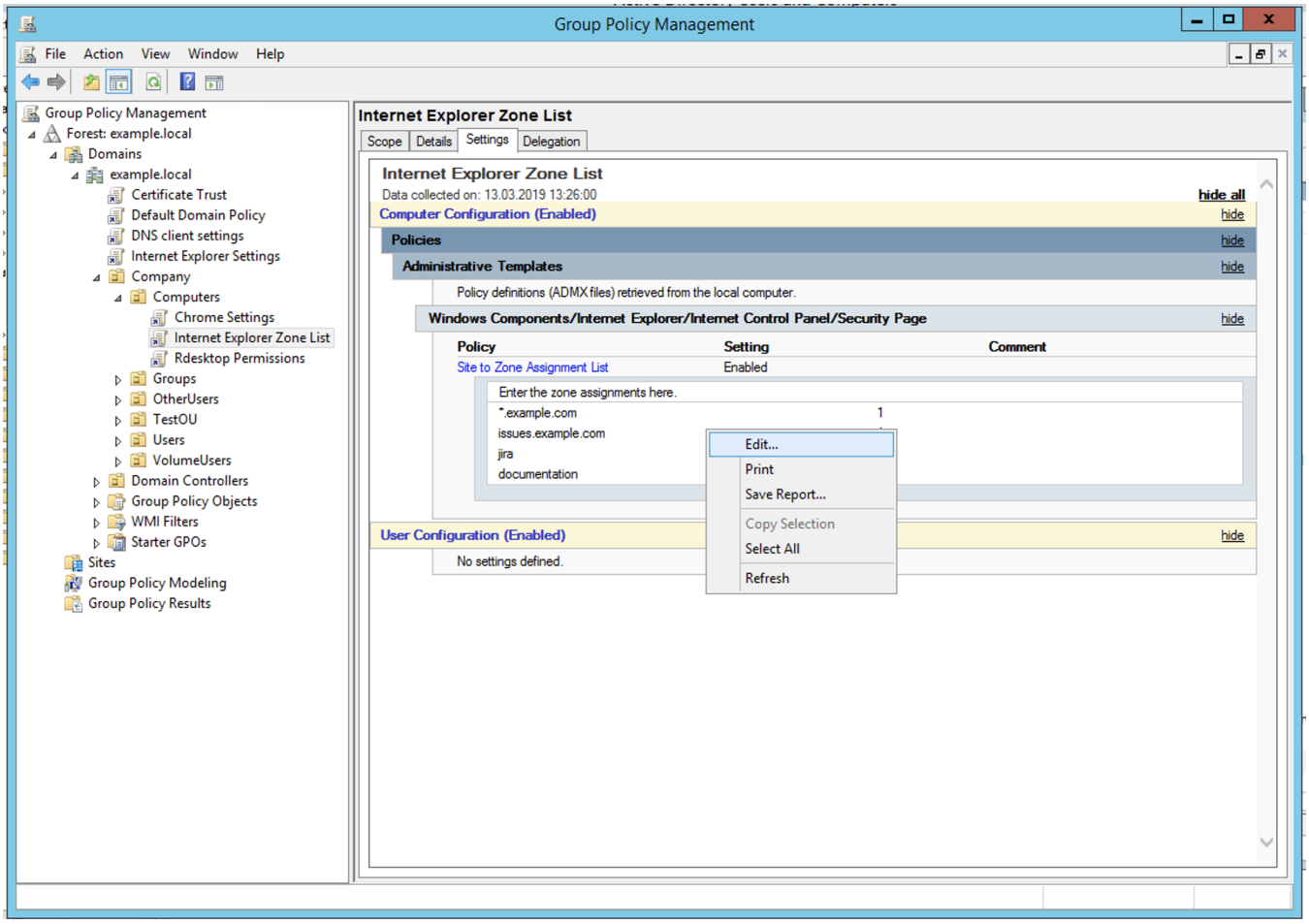


Create the new Group Policy and edit it after creation



Setting appropriate values

Right clicking and select Edit your Policy (see screenshot below):



In Group Policy Management Editor that comes up, navigate to:

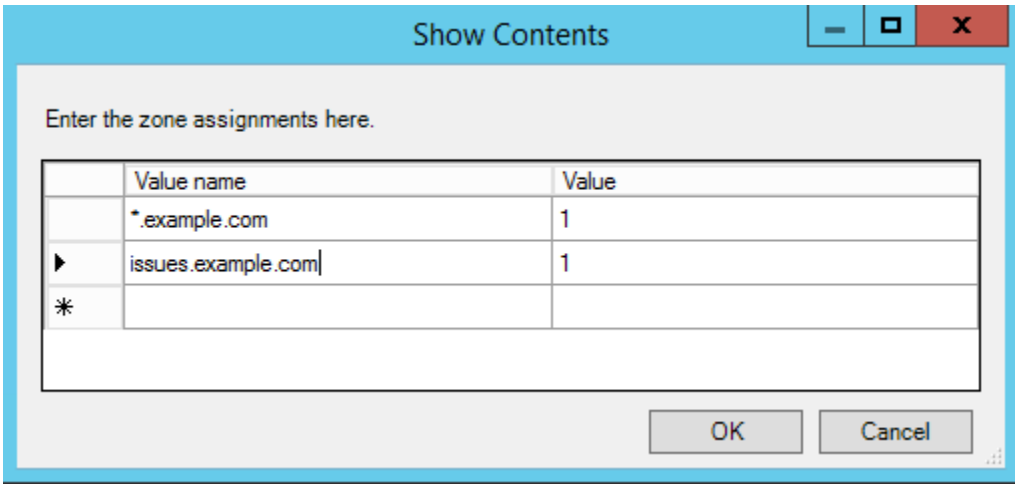
Computer Configuration / Policies / Administrative Templates / Windows Components / Internet Explorer / Internet Control Panel / Security Page / Site to Zone Assignment List.

And press "Show" button on the left to edit list.

Place the site host from the URL (e.g. issues.example.com) in zone 1, Intranet Zone.

The address can be specified with a wildcard (*.example.com), or with a FQDN (issues.example.com)

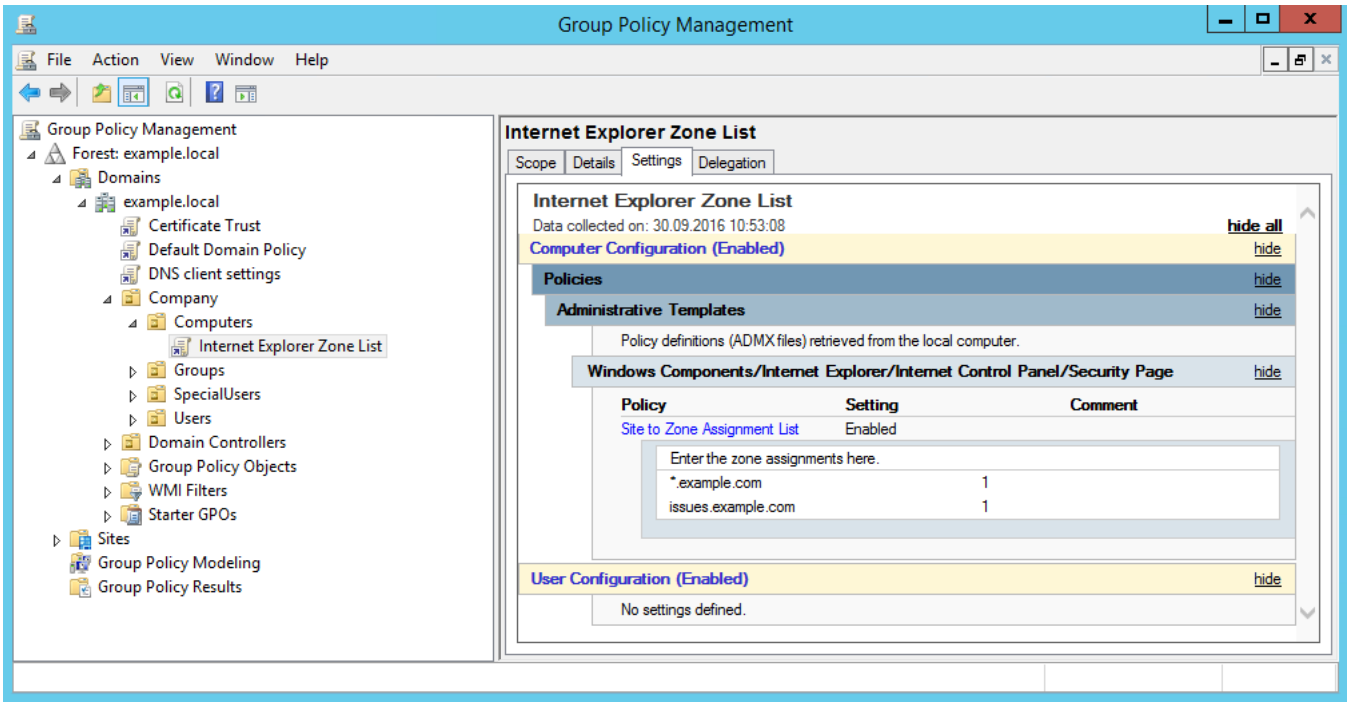
Chrome has been known to interpret wildcard and FQDN differently in some cases. If Kerberos does not work with Chrome, try adding FQDN of the server URL to zone 1



Verifying the settings in Group Policy Management

Choose the newly created policy and Settings to the right. Verify that the Site to Zone Assignment List is correct.

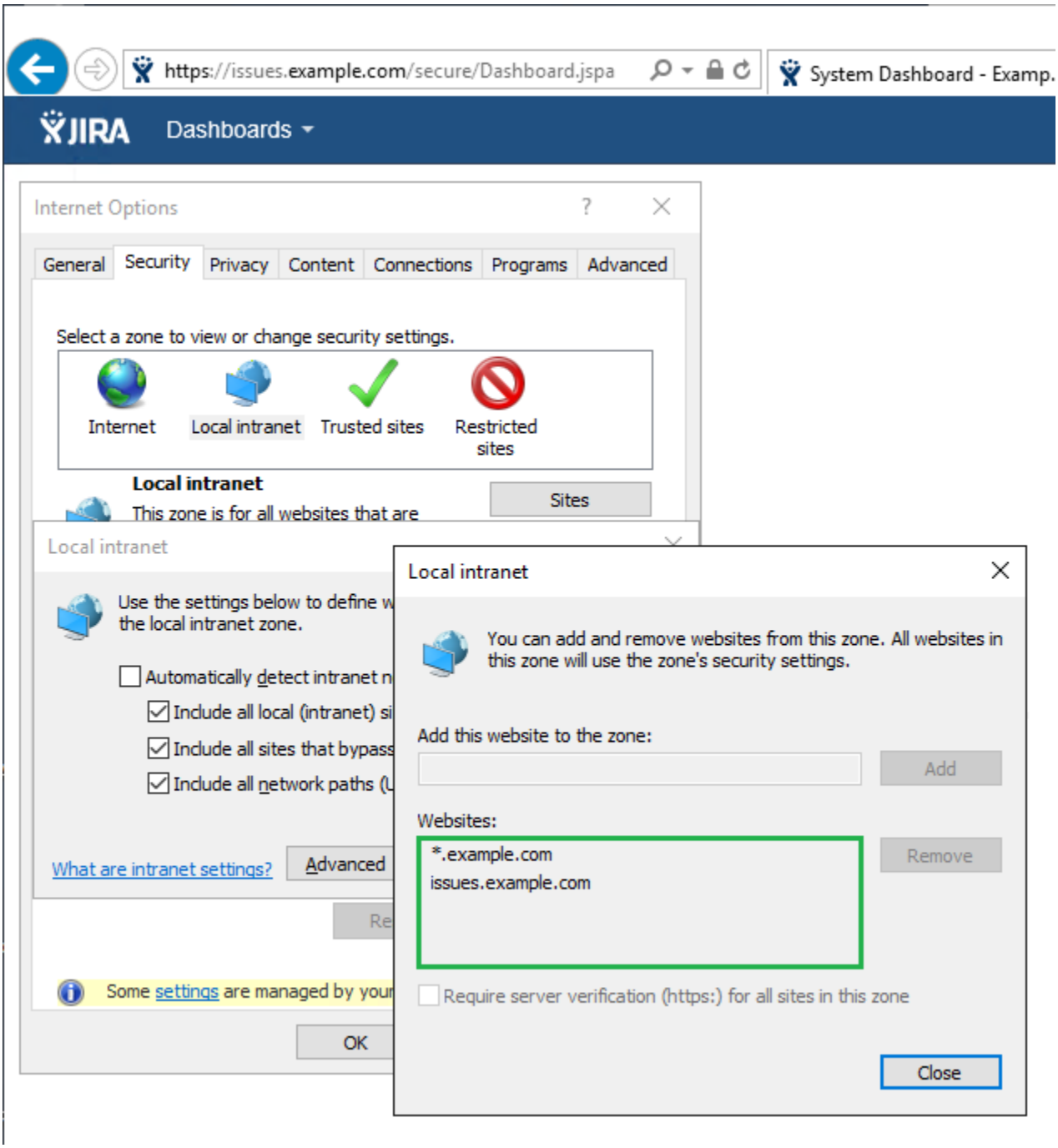
> If the settings is applied to **Computer Configuration**, the policy must be placed on an OU with **computers** or placed so that the policy is inherited.
>
> If the settings is applied to **User Configuration**, the policy must be placed on an OU with **users** or placed so that the policy is inherited.



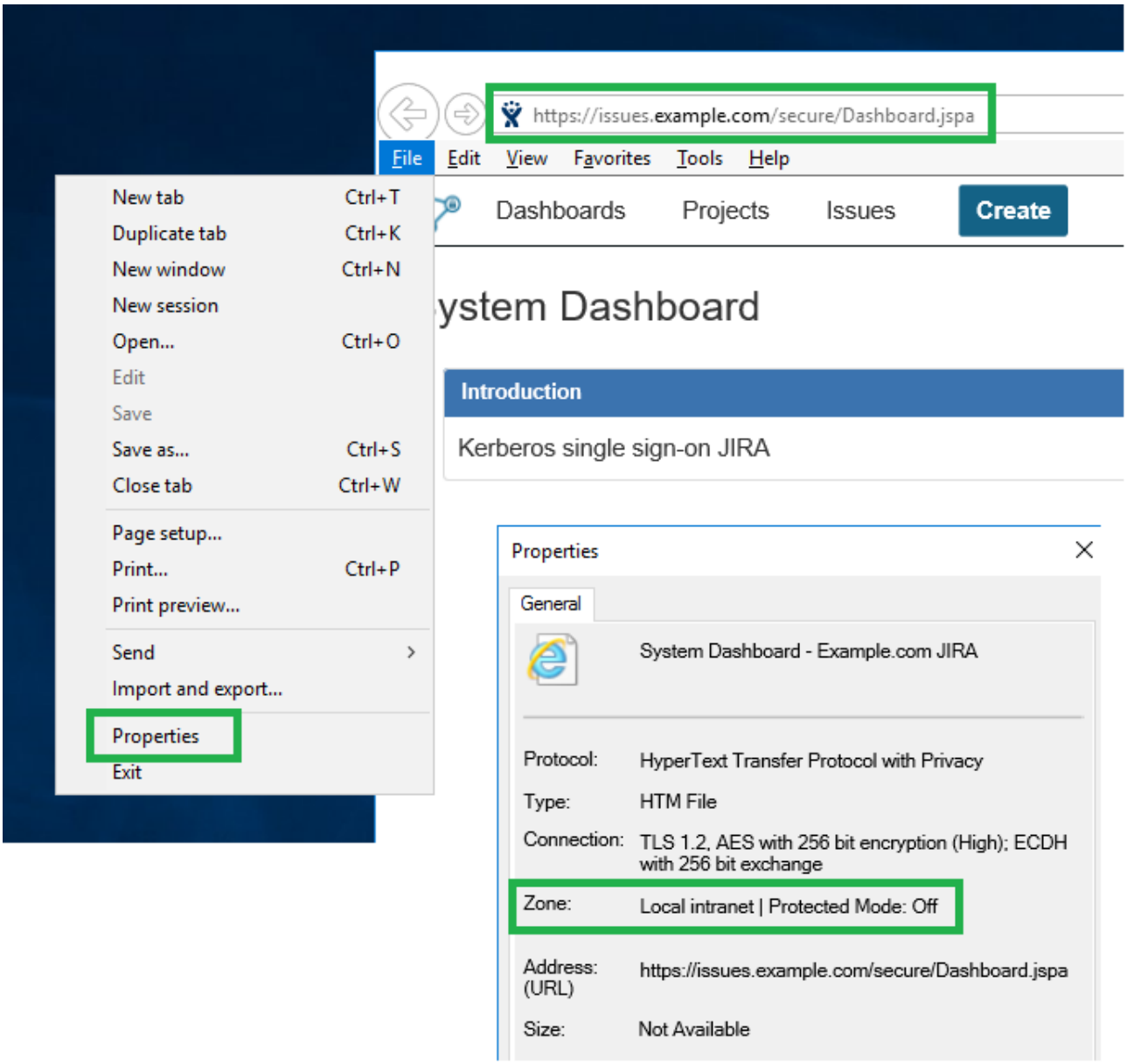
Verifying the settings on the client

Navigate to Internet Options - Security - Local Intranet - Sites - Advanced

Verify that the settings from Group Policy are applied. "*Automatically detect intranet network*" should be left unchecked as we have seen unstable conditions for Kerberos if this is checked.



Verifying wheter the site has been added to Local Intranet Zone can also be checked by access ing https://issues.example.com and checking the Zone value.


https://issues.example.com/secure/Dashboard.jspa
File Edit View Favorites Tools Help
Dashboards Projects Issues Create
ystem Dashboard
Introduction
Kerberos single sign-on JIRA
New tab Ctrl+T
Duplicate tab Ctrl+K
New window Ctrl+N
New session
Open... Ctrl+O
Edit
Save
Save as... Ctrl+S
Close tab Ctrl+W
Page setup...
Print... Ctrl+P
Print preview...
Send
Import and export...
Properties
Exit
Properties
General
System Dashboard - Example.com JIRA
Protocol: HyperText Transfer Protocol with Privacy
Type: HTM File
Connection: TLS 1.2, AES with 256 bit encryption (High); ECDH with 256 bit exchange
Zone: Local intranet | Protected Mode: Off
Address: (URL) https://issues.example.com/secure/Dashboard.jspa
Size: Not Available