Microsoft Forefront UAG - Creating a portal with Forefront UAG

Abstract

In this article I will show you the basic concepts behind a Forefront UAG trunk to create a portal for web access to access different internal applications like Microsoft Sharepoint, Exchange Server and more.

Let's begin

One of the biggest enhancements in Microsoft Forefront UAG comparing with Forefront TMG is the UAG capability to provide a web portal for users on the Internet which needs access to internal applications.

Forefront UAG uses a terminology called a portal trunk. A Trunk is a combination of a IP address, HTTP/HTTP port and a certificate when a HTTPS trunk should be created. The portal trunk is the entry point for all published applications into this portal. It is possible to authenticate against this portal again different directory services like Active Directory, Novell, Netscape and more. A portal trunk also allows the Administrator to apply Forefront UAG Endpoint access policies. An Endpoint access policy is able to check the client for compliance state. For example the client must have the Windows Firewall enabled, all Windows updates must be installed on the machine and the machine must be joined to the internal Active Directory domain. I will give you more insight into UAG endpoint access policies in another article published here at www.isaserver.org.

The client can access the UAG portal after some Forefront UAG Endpoint components have been installed on the client.

To create a new trunk we must open the Forefront UAG Management console (MMC). There are two types of trunks which can be created: A HTTP and a HTTPS trunk.

For the example in this article we will create a HTTPS portal trunk. This portal trunk can be used to publish different applications. I will give you more information about how to publish internal applications through a Forefront UAG portal in some additional articles published in the near future at www.isaserver.org.

🗟 Microsoft Forefront Unifie	d Access Gatew	/ay Management	_ <u>8 ×</u>
File View Admin Messages	Help		
🔚 🔇 🗾			
Forefront UAG Forefront UAG HTTP Connections HTTPS Connections DirectAccess		ont Access Gateway 2010	HTTPS Connections
	A Forefron connectio	nt UAG trunk is a channel via which you publish corporate resources. Remote client devices connect to the trunk on to access the published internal applications.	over an HTTPS
	Click here	e to create an HTTPS trunk, or right-click the HTTPS Connections node.	
	Other	helpful links	
	Read	more about <u>planning</u> and <u>deploying</u> Forefront UAG publishing.	
Message Time	Message Type	Message	

Figure 1: Empty Forefront UAG portal

Before we create a new portal we should first create a Authentication and Authorization repository. For the example in this article we will use Active Directory as a the authentication provider. Start the Forefront UAG MMC and navigate to Admin – Authentication and Authorization Servers.

Specify the Domain controllers used for authentication, the entry point (Distinguished Name (DN)) and a service account which must have read access to the Active Directory configuration. For SSO (Single Sign On) it is possible to enter the internal Active Directory Domain name.

Edit Authenticat	tion Server		>
Server type:	🚊 Active	Directory	Ţ
Server name:	DOMAIN.L	OCAL	
Connection sett	tings		
Define dom	nain controllers		Define
C Use local A	ctive Directory f	orest authentica	tion
Search settings			
Specify the se	arch root and so	ope.	
Base DN:	DC=doma	ain,DC=local	
Include sub	bfolders		
Level of neste	d groups: 0		
Server access			
Specify creden retrieving user	tials used to acc information and	ess Active Direct changing passw	tory for ords.
User (domain\	user): DOMAIN	Administrator	
Password:	•••••	••	
⊂ Default domain	name		
Provide a defa required if you authenticating sign-on (SSO).	ult domain when want to use this users to publish	users log on. Th repository when ed applications w	is setting is n vith single
Domain:	DOMAIN.LOCAL		
Help		OK	Cancel
nep		UK I	Cancer

Figure 2: Configure authorization servers

After the Authorization/Authentication repository has been configured, we are able to create a new trunk. Right click the HTTPS connection and start the Welcome to the Create trunk Wizard. We would like to create a Portal Trunk as shown in the following screenshot.

Create Trunk Wizard	×
Step 1 - Select Trunk Type	
Select the trunk type through which to publish your applications.	
Portal trunk Create a portal, and publish applications that can be accessed via the portal.	
Publish Exchange applications via the portal	
C Active Directory Federation Services (AD FS) 1.x trunk Use this option to publish an AD FS 1.x server for session authentication.	
Note: To authenticate using an AD FS 2.0 server, create a por trunk and define the AD FS 2.0 server as an authentication ser	tal rver.
C HTTP to HTTPS redirection	
P Help	
< Back Next >	Cancel

Figure 3: Create a Forefront UAG portal trunk

We must specify a portal trunk name and a public hostname which clients use to access the portal. The public Host name must match the certificate name you use for the HTTPS connection. Enter the public IP address and the port number used for the trunk and click Next.

Create Trunk Wizard		×
Step 2 - Setting the Ti	runk	
Enter the details for your Trunk name: P Public host name: P External Web Site IP address: HTTP port: HTTPS port:	trunk. ortal ortal.isaserver.org	
	< Back Next >	Cancel

Figure 4: UAG trunk settings

In Step 3 we use the Authorization repository created earlier.

Create Trunk Wizard			X
Step 3 - Authentication			
Select authentication servers u accessing the trunk. Session authentication servers:	sed to validate	credentials for u	sers
DOMAIN.LOCAL		Add Remove]
Specify how users log on to the servers are configured. These authentication servers.	e trunk when mu settings are not	ltiple authentica applicable for A	tion D FS 2.0
 User selects from a server li Show server names 	ist		
User provides credentials for Use the same user name	or each selected	server	
	< Back	Next >	Cancel

Figure 5: Specify authentication servers

The next step is to select the certificate which should be used to establish the SSL connection between the external clients and the Forefront UAG Server. The certificate can be issued from an internal Certification Authority (CA) or a commercial CA. In most cases it makes sense to use a certificate issued by a commercial CA because this certificate is trusted by the most used Web browsers today. The certificate must be stored with the private key (.PFX) into the local computer certificate store on the Forefront UAG Server.

Create Trunk Wizard			×
Step 4 - Certificate			
Select a server certificate used t server to client endpoints.	to authenticate t	the Forefront UA	G
Server certificate:	🔄 portal.isase	rver.org	.
Launch Certificate Manager			
Help			
	< Back	Next >	Cancel

Figure 6: Specify authentication servers

You can use Forefront UAG Endpoint access policies or you can use NAP (Network Access Protection) to check clients before they can use the portal. You are able to use local NAP policies from the local installed NPS (Network Policy Server) or Forefront UAG own endpoint access policies. In most cases I recommend using Forefront UAG policies because they are more powerful.

		×
l by evaluating e olicies.	ndpoint setting:	s against
olicies		
on (NAP) policie	s	
< Back	Next >	Cancel
	l by evaluating e olicies on (NAP) policies < Back	l by evaluating endpoint setting: olicies on (NAP) policies < Back Next >

Figure 7: Endpoint Security

If you decided to use Forefront UAG policies you can now select which Endpoint policies you want to use. Forefront UAG comes with a lot of builtin Endpoint policies and Administrators are able to create its own Endpoint policies.

Create Trunk Wizard			X
Step 6 - Endpoint Policies			
Choose a session access policy f	or privileged and	d nonprivileged e	endpoints.
Nonprivileged access policy:			
Pefault Session Access			•
Privileged access policy:			
🔒 Default Privileged Endpoint			•
€ Help		Edit Endpoint P	Policies
	< Back	Next >	Cancel

Figure 8: Endpoint access policies

After the wizard has been finished you will now see the created Forefront UAG portal trunk as shown in the following screenshot.

S Microsoft Forefront Unifie	d Access Gateway Management		_ 8 ×
File View Admin Messages	Help		
🔚 🔅 🔜			
	Portal		<u>^</u>
		A self-self-se	
	External Site Name	Applications	
	Specify the name that dients type in the browser to access the site.	Application Name Application Type	<u>• </u>
	Public host name: portal.isaserver.org Port: 443	Portai Portai	
	External Site Address		
	HTTPS Port: 443		
	IP address: 212 . 212 . 20 . 222 💌		
		Add Edit,	Remove
		Limit applications to the following subnets:	
		Subnet Address Subnet Mask	
	Initial Internal Application		
	Portal home page: Portal	Add Edit	Remove
	usplay nome page within portal frame		
	Trunk Configuration		
	Configure trunk settings: Configure		
Message Time	Message Type Message		

Figure 9: UAG portal overview

We must now save the configuration to store the changes to the UAG configuration. Click the floppy symbol to save the configuration. After that we can activate the configuration so that all changes will be effective after a short amount of time. To activate the configuration click the button right from the floppy symbol.

Configure trunk settings

After the trunk has been created we are now able to customize the trunk settings. I will give you a high level overview about the different configuration options. On the General tab we are able to specify the maximum number of users which should be able to currently access the portal trunk and we can also check the certificate used in the HTTPS portal trunk.

🪂 Portal	🛛 🖇 🖇 🖇	L Inspection	🔎 Global URL Settings	📄 URL Set
🤡 General	🚨 Authentication	Session 🛞	🐓 Endpoint Access Settings	Application Customizatio
laximum concurrent	connections: 100000			
External Web Site -		Web	Site Logging	
IP address:	212 . 212 . 20 .	222 💌	Log trunk traffic in IIS	
HTTP port:			Include user name in log	
HTTPS port:		443 Deb	ugging	
Site name:	portal		Disable all security features for the trunk (use with Customer Support Services only)	
Server Certificate —				
Server certificate:	🛱 portal.isaserver.	org 💌		
Certificate hash:	E0 C9 8E FF A0 06 9	D 2D B3 19 4D BC 9B 53	E5 D4 72 37 75 DA	

Figure 10: General portal settings

On the Authentication tab it is possible to specify the Authentication Server, if users should be able to change their passwords through the trunk and if you are familiar with Forefront UAG you are able to customize the Logon and Logoff scheme used by Forefront UAG.

Market Section Section	Global URL Settings	URL Set
🍪 General 🧏 Authentication 🥵 Session	😴 Endpoint Access Settings	Application Customization
General Authentication Session Require users to authenticate at session logon Select authentication servers: DOMAIN.LOCAL Add Remove Domain.Local Add Remove Some settings are not applicable when using AD FS 2.0 authentication. Wultiple authentication server settings: Output: Desire choose an authentication server Provide a server list at user logon Users authenticate to each server Authenticate to each server Add credentials on the fly Change passwords Notify user Preferation Service Forefront UAG relying party settings: Realm: Federation Metadata:	Endpoint Access Settings Logon Scheme User logon page: On the fly user logon page: Maximum logon attempts: Block period after failed logon (minutes): Image: Apply an Outlook Web Access look and logoff schemes Image: Logoff URL: Logoff message: Image: Wait 30 seconds and then end if Image: Send the logoff request to the application server resp.	Application Customization

Figure 11: Authentication servers

The Session tab let you customize all relevant session access settings like connection timeouts, maxium session times for the Default and Privileged session access. Forefront UAG is able to distinguish between default (unmanaged) clients and more trusted (managed) clients. This configuration tab also allows Administrators to handle with some Endpoint access settings for clients connecting to the UAG portal.

Portal	URL Inspection	Global URL Settings	URL Set
Portal Portal Portal General Authe Session Configuration Maximum concurrent sessions: Session threshold before issuing eve Maximum unauthenticated concurrer Unauthenticated session threshold b Session timeout notification (seconds Error message URL: //Internal Disable component installation ar Disable scripting for portal applica Use certified endpoints Verify user name with endpoi Delete application-specific files w Use DNS suffix :	VRL Inspection Intication Session It sessions: 100000 It sessions: It sessions: 100000 It sessions: It sessions: 0 It session: It certificate It certificate it hendpoint Session Cleanup	✓ Global URL Settings ✓ Endpoint Access Settings Default Session Settings Inactive session timeout (seconds): ✓ Trigger automatic logoff after ✓ Delete cookies at logoff Request no browser caching ✓ Activate Endpoint Session Cleanup of ✓ Prompt user to disconnect if the porta ✓ Reopen the portal if the user doe Privileged Session Settings Inactive session timeout (seconds): ✓ Trigger automatic logoff scheme after ✓ Delete cookies at logoff Request no browser caching ✓ Activate Endpoint Session Cleanup of ✓ Activate Session Settings	Application Customization Application Customization 300 60 minutes omponent I closes without logging off s not disconnect 1800 r 1440 minutes component
	session	Prompt user to disconnect if the porta Reopen the portal if the user doe	al is closed without logging off is not disconnect

Figure 12: Portal session settings

The Endpoint Access Settings tab allows Administrator to decide to use NAP (Network Access Protection) or Forefront UAG Endpoint access policies to control which clients should be able to access the portal trunk.

🪂 Portal	🔰 🖇 🖇 🖇	RL Inspection	🔎 Global URL S	ettings	🗎 🔡 URL Set
🥸 General 🛛	S Authentication	Session	📝 Endpoint Access	Settings	Application Customizatio
nfigure Forefront UAC	G access policies, and Netw	vork Access Protection (NA	P) policies. NAP policies are	downloaded from a	a Network Policy Server (NPS)
Use NAP policies					
C Deny acces	s to the logon page from en	dpoints that do not have N/	AP installed and running		
🖲 Use Forefrom	nt UAG endpoint policies wi	nen endpoints do not have l	NAP installed and running		
Select NPS serve	rs:				
			id		
1		Her	nove		
Session Access Pol	icy	Privileged Endpoint P	olicy	C Socket Forward	ing Component Installation Pol
Access method:		Access method:	-	Access method	:
📟 Endpoint policy	v only	Endpoint policy of	nlv 👻	📼 Endpoint d	olicy only
Endpoint policy:		Endpoint policy:		Endpoint policy	· · ·
Default Sessio	n Access 💌	Default Privilege	d Endpoint 💌	Always	•
,			·		
				I Uninstall the	Socket Forwarding componer
					Edit Endersist Delision
Do not block this	site in the Internet Explorer	pop-up blocker			
Prompt user befor	re retrieving information from	n endpoint			

Figure 13: UAG Endpoint access settings

The Application Customization tab allows you to specify the file extensions for which Forefront UAG should be able to compress the content. It is also possible to enable GZip compression support

	IU 🖓	RL Inspection	🎾 Global URL Settings	📔 URL Set
🥸 General 🛛	パ Authentication	😣 Session	😴 Endpoint Access Settings	Application Customizatio
 Enable applicatio 	n customization		Compression Handling in Response	s
Select customized ter	mplate:			
Automatic				
Other (manual con	nfiguration)		aspx	Remove
			php	
Search and Replace	Using Content-Type		html	
text/.*		Add	htc	
application/x-javas	cript.*			
application/xhtml+x	ml	E GIT	js	
		Remove	🔒 xsl	
			s xml	
				_

Figure 14: Application customization

The URL Inspection tab let Administrators specify the allowed HTTP access methods which should be allowed when users access the portal. Forefront UAG also uses deep HTTP inspection to filter the HTTP/HTTPS traffic for allowed and illegal characters as shown in the following screenshot.

🍪 General 💦		Authentication	an Session	ו ו 📝 🗗	ndpoint Access Se	ettings	🛛 🖂 Applica	ation Customization
🤮 Portal		🜮 URL Inspec	ction	J	Global URL Set	tings		🖹 URL Set
/alid URL Access M	ethods							
	Predefine	d and custom methods		Default group me	thods			
Add Remove	GET POST PUT		Add >> Remove		T tř U	his list can be us ne default group (JRL Set tab.	ed as on the	
Remove All	DELETE TRACE HEAD	R	lemove All	j				
Data and Headers	/PUT size	.[-1	_					
Data and Headers Maximum POST, Block Negotiate Global URL Charact	/PUT size authoriza er Rules	:[-1 tion headers						
Data and Headers Maximum POST, Block Negotiate Global URL Charact Type	/PUT size authoriza er Rules Le	:[-1 iion headers gal Characters	Fo	orbid Encoding of:	Include NULL	Enable %u Enc	coding	
Data and Headers Maximum POST, Block Negotiate Global URL Charact Type Portal	/PUT size authoriza er Rules Le ab	:[-1 iion headers gal Characters vcdefghijklmnopqrstuvwxyzA	ABCD /	orbid Encoding of: \\.*?'''<> .%	Include NULL Yes	Enable %u Enc	coding	
Data and Headers Maximum POST, Block Negotiate Global URL Charact Type Portal Internal Site	/PUT size authoriza er Rules b b b b c c c c c c c c c c c c c c c	: [-1 tion headers gal Characters cdefghijklmnopqrstuvwxyzA cdefghijklmnopqrstuvwxyzA	ABCD /	orbid Encoding of: **?""<\% \\.**?""<\%	Include NULL Yes Yes	Enable %u Enc No No	coding	
Data and Headers Maximum POST, Block Negotiate Global URL Charact Type Portal Internal Site	/PUT size authoriza er Rules Le ab	:[-1 tion headers gal Characters scdefghijklmnopqrstuvwxyzA scdefghijklmnopqrstuvwxyzA	ABCD /^	arbid Encoding of: \\:*?""<> .%	Include NULL Yes Yes	Enable %u Enc No No	coding	
Data and Headers Maximum POST, Block Negotiate Global URL Charact Type Portal Internal Site	/PUT size authoriza er Rules b b b b b b b b b b b b b b b b b b b	:[-1 tion headers gal Characters vcdefghijklmnopqrstuvwxyzA vcdefghijklmnopqrstuvwxyzA	ABCD /^	orbid Encoding of: \\.*?'''<> .% \\.*?'''<> .%	Include NULL Yes Yes	Enable %u Enc No No		

Figure 15: URL inspection

On the URL set tab Forefront UAG automatically creates global URL sets depending on the portal configuration and the applications published through the portal to control the allowed / illegal characters and the allowed / forbidden HTTP access methods. These created URL sets will be used by the underlying installed Forefront TMG Server as Firewall policy rules to controll access to the Forefront UAG Server.

🥑 General 🛆 🍓 Portal	Authentication	Session Inspection	Endpoi	int Access Settings obal URL Settings	Αρ	plication Customizatio
L list			1			
me	Action	URL	Parameters	Note	Methods	_
Portal_Rule1	Accept 💌	/(secure)?[^	Ignore 💌		POST, GET	
Portal_Rule2	Accept	/(secure)?[^	Ignore		GET	
Portal_Rule3	Accept	/(secure)?[^	Ignore		POST, GET	
Portal_Rule4	Accept	/(secure)?[^	Ignore		POST, GET	
Portal_Rule5	Accept	/(secure)?[^	Ignore		POST, GET	
Portal_Rule6	Accept	/(secure)?[^	Reject		GET	
Portal_Rule/	Accept	/(secure)?[^	Reject		GET	
Portal_Rule8	Accept	/(secure)?[^	Reject		GET	
Portal_Rule9	Accept	/(secure)?[^	Reject		GET	
Portal_Rule10	Accept	/(secure)?[^	Reject		GET	
unceer nsu						
Name N	lame Type	Value	Value Type	Length		Existence
Name N	lame Type	Value	Value Type	Length		Existence
Name N	lame Type	Value	Value Type	Length		Existence
Name N	lame Type	Value	Value Type	Length		Existence
Name N	lame Type	Value	Value Type	Length		Existence
Vame N	lame Type	Value	Value Type	Length		Existence
Name N	lame Type	Value	Value Type	Length		Existence
Name N	lame Type	Value	Value Type	Paste	Add	Existence
r Name N	lame Type	Value	Value Type	Paste	Add	Existence Remove
Name N Reject unlisted parameters	lame Type	Value	Value Type	Paste	Add	Existence
Name N Reject unlisted parameters Accept unlisted parameters Imaximum name leng	s	Value	Value Type	Paste	Add Allow multiple occ	Existence Remove

Figure 16: URL sets

This was a high level overview about the basic Forefront UAG portal trunk configuration. You should invest some time to get familiar with the powerful configuration options in Forefront UAG.

Conclusion

In this article I tried to explain the basic concepts behind Forefront UAG trunks to create a web portal for user which must access internal applications through the portal, created by Forefront UAG.

Related links

Microsoft Forefront UAG – Overview of Microsoft Forefront UAG <u>http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html</u> Forefront UAG technical overview <u>http://technet.microsoft.com/en-us/library/ee690443.aspx</u>