1 Introduction

This document outlines the procedure for installing and configuring Websense Authentication Service and the procedure to follow to configure the corresponding Websense Web filtering product (either Websense® TRITON™ Cloud Web Security or Websense Web Security Gateway Anywhere). Authentication Service is the interface between the Websense proxy server and the Microsoft Active Directory or LDAP services used on-premises at your location.

What is Authentication Service?

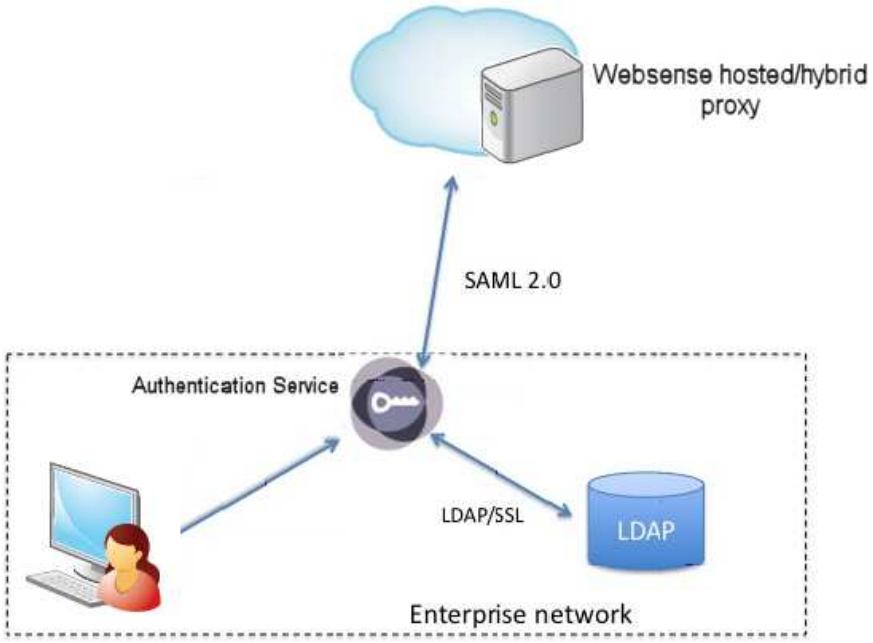
Authentication Service facilitates username/password validation using your on-premises Active Directory/LDAP server. Authentication Service is installed as a virtual appliance and communicates with your local directory using LDAP over SSL. It can operate in the DMZ or inside the local area network (LAN), or both, based on the mode(s) of operation:

- **Desktop single sign-on (SSO)**. This option applies to end users using cloud or hybrid filtering to access the Internet from within your network. In this case, the user's desktop credentials are validated by Authentication Service using Kerberos tickets distributed by your Key Distribution Center (KDC) machine. Authentication Service is installed inside the LAN and acts as a federation server within your network, creating an in-network federation authority that communicates with the Websense proxy using SAML 2.0 assertions.

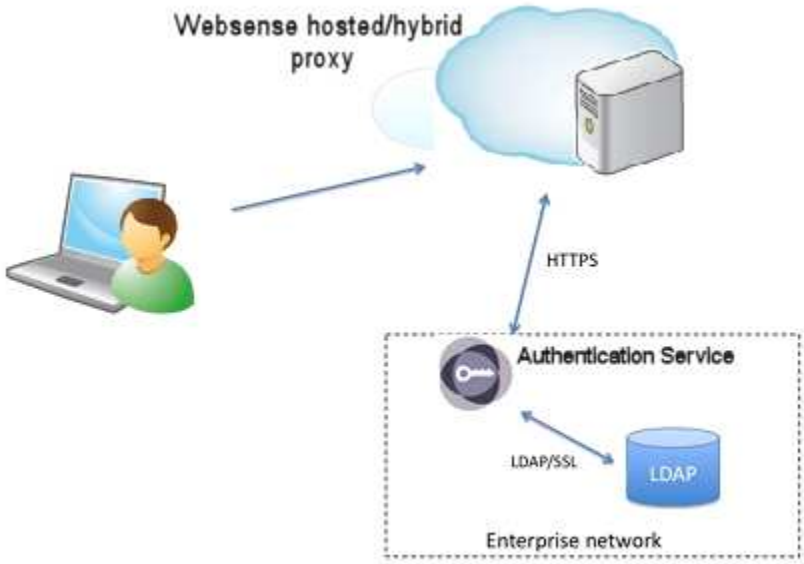
  The user authenticates with the Active Directory/LDAP server within the network (leveraging existing network security). When a user from within the corporate network accesses an external URL, they are redirected to Authentication Service, which authenticates the user with the LDAP directory and generates a SAML assertion to the Websense proxy. The user credentials never leave the corporate network.

  Note that using this configuration, all user authentications happen in-network; the Websense proxy does not enforce multiple authentication factors, but simply

accepts the SAML assertion from Authentication Service. Users can also use this mode from outside the network via a VPN connection.



- **Username/Password verification.** This option applies to off-site users. In this case, the users can access the Websense proxy from outside their LAN and Authentication Service needs to run in your DMZ. The user's Active Directory/ LDAP credentials are collected by the Websense proxy and passed to Authentication Service to be validated against your Active Directory/LDAP server. Once authenticated, the user has full access to Web sites according to their policy settings.



- **Hybrid (both)**. Here both internal desktop SSO and external username/password validation are required. Users can connect to Authentication Service internally or from outside the LAN.

Getting started

This section outlines the main steps required to install and configure Authentication Service.

Before you start

- Establish a host name and IP address for your Authentication Service. This information must be added to your DNS before you start the installation (see *Add Authentication Service host name to DNS*, page 6).

Installation

1. Download the Authentication Service virtual machine (VM) (see *Download Authentication Service*, page 6).
2. Convert the installation file, if required, to a format recognized by your hypervisor; then install Authentication Service (see *Install and start the VM*, page 7).
3. Set the correct IP address on the Appliance Console menu (see *Configure network interface*, page 8).
4. Set the correct host name on the Appliance Console menu (see *Configure network interface*, page 8).

Configuration

1. Log on to the Administration Console (see *Using the Administration Console*, page 11).
2. Configure the connection to your directory service (see *Set up Active Directory/ LDAP connection*, page 12).
3. If you are using Active Directory, then set up Kerberos for seamless authentication (see *Set up Kerberos connectivity*, page 15).
4. Add Websense metadata to your configuration, to enable Authentication Service to talk to the Websense proxy (see *Upload Websense metadata*, page 26).
5. Copy the metadata URL provided by Authentication Service into your Websense product configuration (see *Configure Authentication Service metadata in your Websense product*, page 26).

2 Installing Authentication Service

Websense Authentication Service is supplied as a Virtual Machine (VM). To install the VM, you need the following:

- The Authentication Service VM, provided as an Open Virtual Appliance (.ova) file.
- A compatible hypervisor/server, such as VMware ESX.
- A VM client that provides access to the VM's VGA console. This console is used only for early configuration and is not protected.
- A converter tool, if your hypervisor does not open OVA files directly. VMware offers a free tool for Windows and Linux at http://www.vmware.com/appliances/getting-started/learn/ovf.html.

Note the following important security considerations:

- The Authentication Service management interfaces are not encrypted and should not be exposed to public networks.
- The text-based Appliance Console Menu is accessible to anyone with access to the hypervisor (VM server) where the Authentication Service VM is hosted. Protection here relies on firewalling and authentication to the hypervisor.
- The browser-based Application Platform Administration Console listens on HTTP port 8080. Access is granted via HTTP basic authentication. Access should be limited to the local network or VPN.

Minimum hardware requirements

The minimum RAM requirement for the virtual machine is 512MB (1GB is recommended). The recommended minimum processing power is the equivalent CPU capacity of a 1.0-1.2 GHz 2007 Opteron or 2007 Xeon processor.

The minimum hardware requirements for the hypervisor to run the Authentication Service VM are:

- **Processor:** One Intel Xeon Dual Core, 3.0 Gigahertz (GHz), 4 Megabyte (MB) Cache
- **Memory:** 4 Gigabyte (GB) DDR2 667 MHz, ECC registered
- **On-board LAN:** Two 10/100 /1000Base-TX ports

- **HDD Interface:** Intel RAID Smart Battery
- **HDD Drives:** 750 GB (3x250 GB 7.2K RPM in RAID 5) SATA Hard Drive
- **Power supply:** Dual 750W, 90-264 VAC, 50-60Hz
- **Disk space:** 1.5 GB free

Installation procedure

Follow the steps in this section to download and install Authentication Service.

1. *Add Authentication Service host name to DNS*, page 6
2. *Download Authentication Service*, page 6
3. *Install and start the VM*, page 7
4. *Configure network interface*, page 8

Add Authentication Service host name to DNS

Choose a host name and IP address for Authentication Service, and add a record in your Domain Name Service (DNS). We recommend that you do this several days before you start the installation, as the new DNS record may take time to propagate and Authentication Service must be recognized on the network for the subsequent steps.

For further information on creating DNS records, contact your DNS provider.

Download Authentication Service

This section explains how to download Authentication Service from your Websense Web filtering product.

Downloading from Cloud Web Security

1. Log on to the Cloud Web Security portal.
2. Go to **Setup > Web > Authentication Service**.
3. Under Authentication Service Installer, click on a file name to download that version of Authentication Service. You can also view a PDF of the release notes for each version by clicking a release notes link.

Downloading from Web Security Gateway Anywhere

1. Log on to the TRITON Unified Security Center as a Global Security Administrator or a TRITON - Web Security administrator.
2. Go to **Settings > Hybrid Configuration > Hybrid User Identification**.
3. Mark **Enable Authentication Service**.

4. Click **Authentication Service Files** to view the available Authentication Service downloads. Click on a file name to download that version. You can also view a PDF of the release notes for each version by clicking a release notes link.
5. Click **Close** when done.

Install and start the VM

The Authentication Service image is in OVA format, which may need to be converted to VMX format, depending on the VM host you are using to run the VM. For example, VMWare Workstation requires VMX format.

For VMWare, you can use the OVF tool, a free command-line utility available for Windows and Linux. Download the OVF tool from http://www.vmware.com/appliances/getting-started/learn/ovf.html. Follow the installer instructions to install the tool.

> **Note**
> You may be asked to register with VMWare as part of this process.

To convert an OVA file to VMX:

1. Create a directory in your hypervisor's data store (where VMs reside). Name the directory appropriately.
2. Move to that directory. The OVF tool places output files in the current directory.

Start the converter tool. The tool copies the OVA to a new set of files in VMX format and leaves the OVA file unchanged.

Command: `path-to-ovftool -tt=vmx ova-file-name vmx-file-name`

Example: `/usr/bin/ovftool -tt=vmx fb72-641-32bit-ec-vm.ova central-ec`

The operation may take a few minutes. Sample output is shown below.

```
Opening OVA source: ../fb72-641-32bit-ec-vm.ova
Opening VMX target: central-ec
Target: central-ec.vmx
Disk progress: 36%
□
Disk Transfer Completed
Completed successfully
```

The output is a .vmdk file (disk image) and .vmx file (VM configuration) in your current directory. For example:

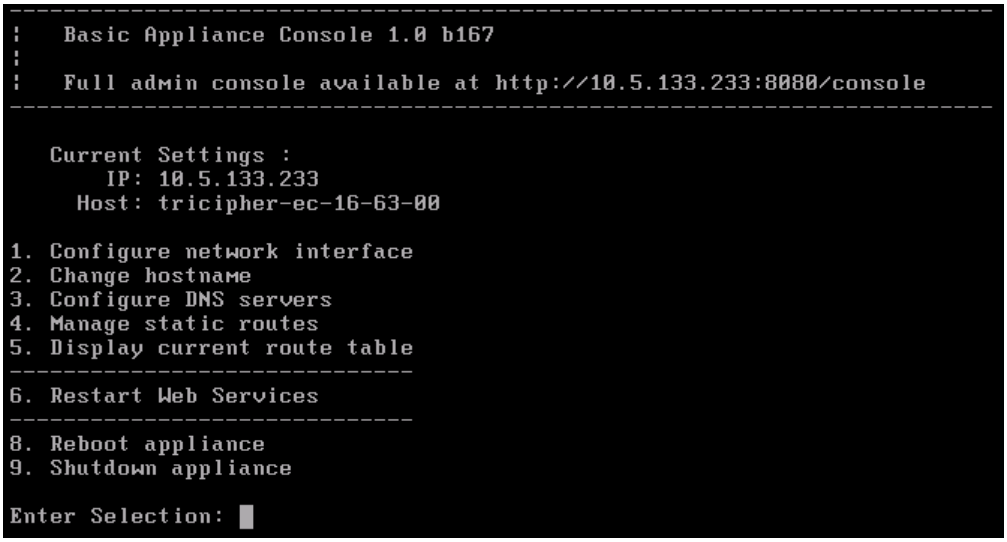
```
-rw------- 1 root root 1.6G 2010-08-09 14:46 central-ec-disk1.vmdk
-rw-r--r-- 1 root root 1.1K 2010-08-09 14:46 central-ec.vmx
```

Once you have converted the file, if required, do the following:

1. Add the Authentication Service VM to your hypervisor inventory. Refer to your hypervisor documentation for more details.
2. In your hypervisor, start the VM. This will boot the VM's operating system, start the Authentication Service processes, and connect to a DHCP server (if present) to acquire an IP address.

Configure network interface

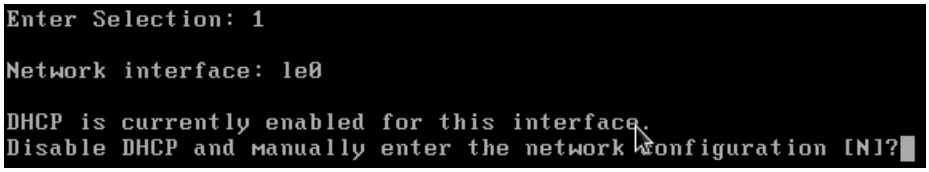
During startup, the VM outputs boot messages to the VGA console. You do not usually need to watch these. When boot up is complete, the Appliance Console Menu appears.



Authentication Service has acquired an IP address for its single network interface (if a DHCP server is present) and generated a temporary host name. You will probably want to change both.

To change the IP address and host name using the Appliance Console Menu:

1. Press **1** to start configuring the interface.



   In this menu, the default response (i.e. if you press **Enter** without typing anything else) is shown in brackets; in the example above, pressing **Enter** would return you to the main menu.
2. To disable DHCP, type **Y** and press **Enter**.
3. Enter the interface's IP address, subnet mask, and gateway.

If defaults are shown for any of the fields, these are the current settings obtained from the DHCP server. You can use dotted quad format for each field, although a default may show hexadecimal format.

In this example, the IP address is set to 10.5.133.111, the subnet mask is set to the default 255.255.255.0 (/24), and the gateway is left as the default 10.5.133.254:

```
Network interface: le0

DHCP is currently enabled for this interface.
Disable DHCP and manually enter the network configuration [N]?y
Enter IP address for  [10.5.133.246]: 10.5.133.111
Enter subnet for 10.5.133.111 [255.255.255.0]:
Enter default gateway [10.5.133.254]:
```

4. After you enter this information, Authentication Service redisplays its menu. Press **2** to change the host name.
5. Enter the new host name and press **Enter**.
6. Once the host name is updated, you must regenerate the self-signed certificate for Authentication Service. Regenerate the SSL certificate for the new host name by pressing **Y**.

```
Enter Selection: 2
New hostname [tricipher-ec-16-63-00]?tricipher-test.odd.blackspider.com
Hostname updated.
Changing the hostname usually requires changing the SSL cert.
If you are using the default SSL cert, you can regenerate it now.
Regenerate SSL cert now [Y]?y
```

7. Authentication Service redisplays its menu. To start using the new settings, select **8** (Reboot appliance) from the menu.

```
Reboot is required for host name changes to take effect.

--------------------------------------------------------------------------------
¦   Basic Appliance Console 1.0 b167
¦
¦   Full admin console available at http://10.5.133.111:8080/console
--------------------------------------------------------------------------------

   Current Settings ( changes pending reboot ):
       IP: 10.5.133.111
     Host: tricipher-test.odd.blackspider.com

1. Configure network interface
2. Change hostname
3. Configure DNS servers
4. Manage static routes
5. Display current route table
-----------------------------
6. Restart Web Services
-----------------------------
8. Reboot appliance
9. Shutdown appliance

Enter Selection: 8
Are you sure you want to reboot [N]: y
```

Once Authentication Service has restarted, it will display the new settings.

3 Using the Administration Console

Once you have installed Authentication Service, set up the correct IP address and host name, and successfully rebooted, you can access the browser-based Horizon Connector administration console.

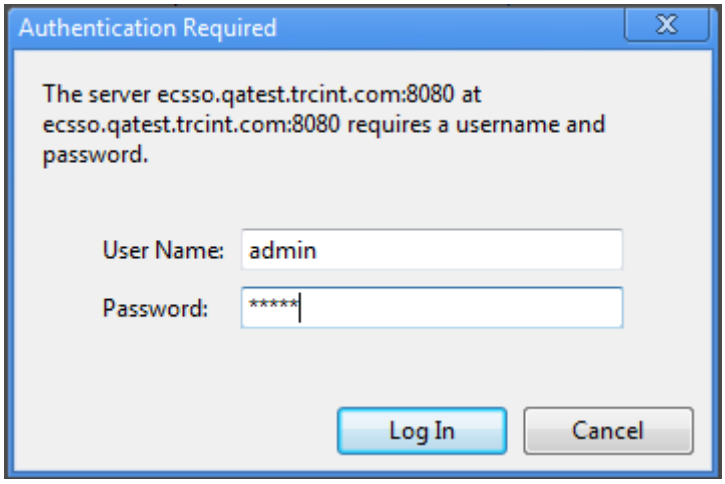
All Authentication Service configuration (including network configuration and host name) can be done using the browser-based interface. You will not need to use the Appliance Console Menu again unless a network change or other event makes Authentication Service inaccessible to your browser.

To log on to the administration console, open a browser on the Authentication Service machine and enter the following:

```
http://<DNS name>:8080/console/go.do
```

Substitute the DNS name of the Authentication Service.

At the logon page, enter your **User Name** and **Password**, then click **Log In**. The defaults are “admin” and “admin”.

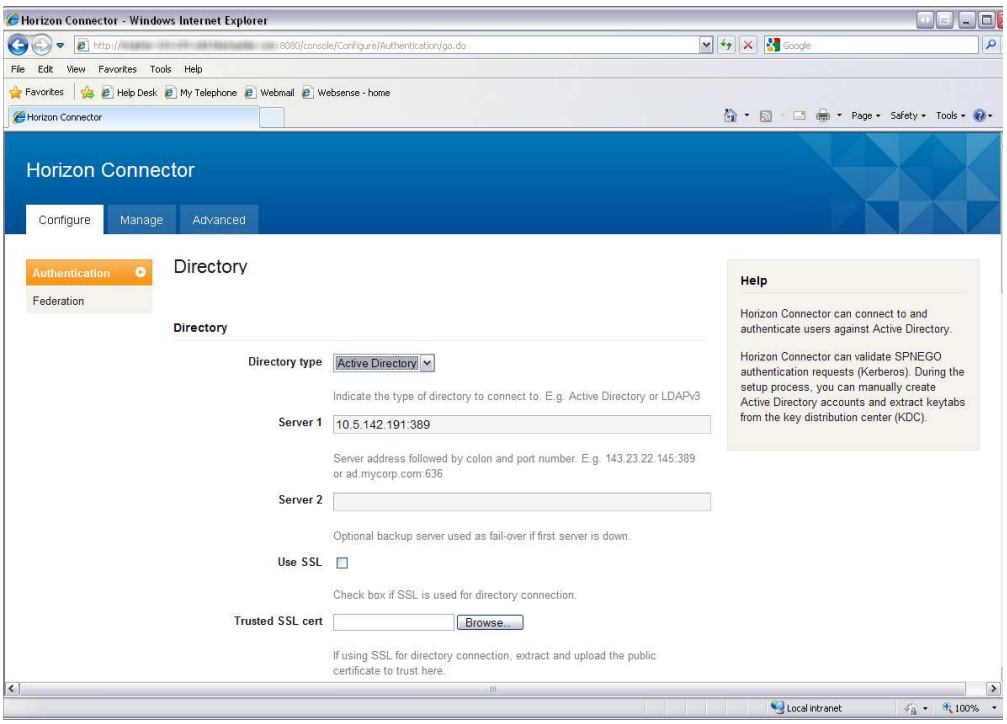


Set up Active Directory/LDAP connection

You must set up a connection to your Active Directory or other LDAP service in order to support off-site user authentication.

> **Note**
> If you have Active Directory, local user authentication is routed through Kerberos, but if you are using a different LDAP service, local user authentication will also use the LDAP directory rather than Kerberos.

1. In Horizon Connector, go to **Configure > Authentication**.



2. Select your **Directory type**, either Active Directory or LDAP as appropriate.
3. In the **Server 1** field, enter the IP address and port of your directory server.

> **Note**
> Do not edit the **Search attribute** field. This must always be set to the default of sAMAccountName.

4. In the **Base DN** field, enter the DN at which to start account searches. For example, to search in Users in the domain accounts.example.com, you would enter:

   `cn=Users, dc=accounts, dc=example, dc=com`

5. In the **Bind DN** field, enter the account that has the permissions to search for users. For example, for an account belonging to your IT administrator, you might enter:

   `cn=ITAdmin,cn=Users,dc=accounts,dc=example,dc=com`

   Note

   If one of the fields in your Bind DN contains a comma, it must be escaped with 2 backslashes for the Administration Console to accept it. For example:

   `cn=Smith\\,Joe,cn=Users,dc=accounts,dc=example,dc=com`

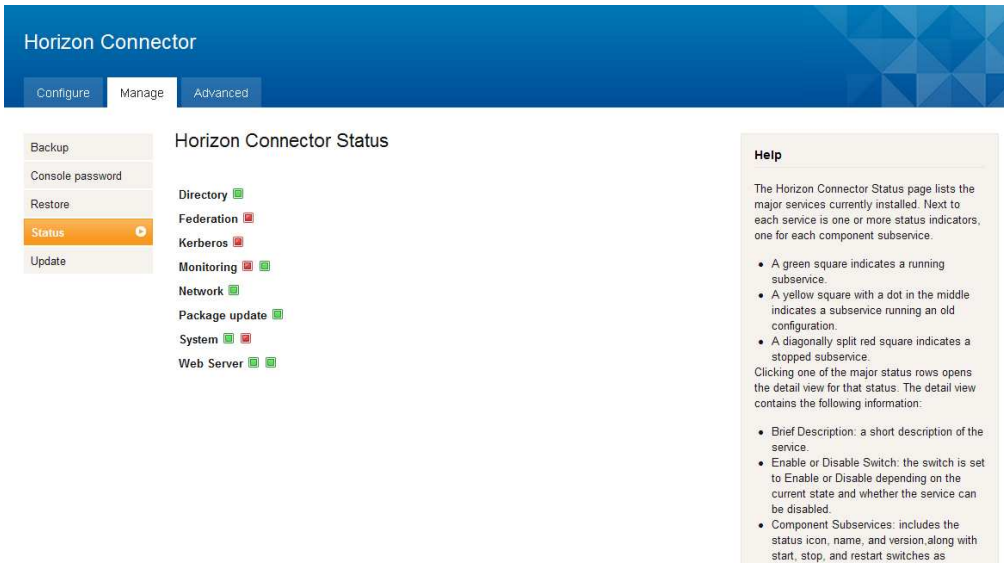
6. In the **Bind password** field, enter the password for the Bind DN account.
7. Optionally, in the **Session timeout URL** field, enter http://proxy-login.blackspider.com/sessiontimeout. This page is displayed to an end user if they leave their browser open and idle and their authentication session times out, and they then try to browse again. The page tells the user to retry their original request, which prompts the re-authentication.

   If you do not enter this URL in the field, by default Authentication Service displays a page containing a link. The link takes the end user to a page showing their user credentials.
8. Click **Save and Restart**.

Test the directory connection

Once Horizon Connector has restarted, it should be able to connect to your directory service and perform searches. To check the directory connection is correctly configured, in the Administration Console, go to **Manage > Status**. The status takes

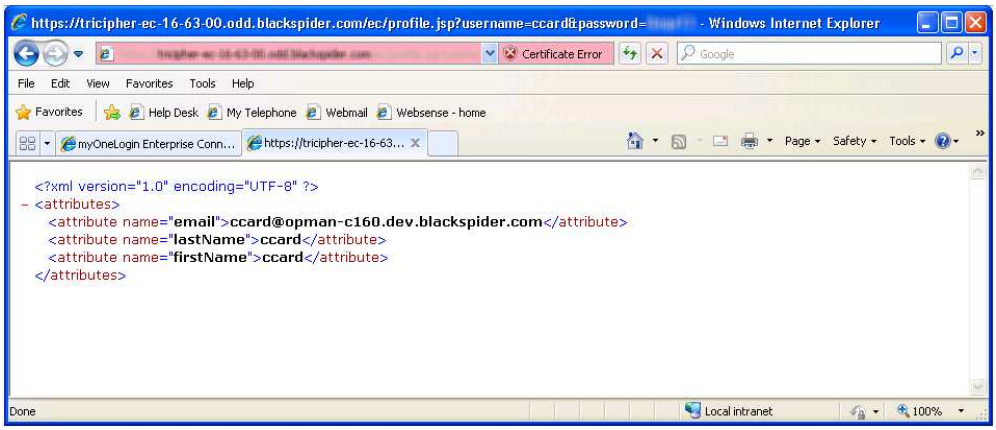
1-2 minutes to refresh, and when it does it should have a green status indicator next to **Directory**.



You can test the connection by entering this URL:

https://<*DNS name*>/ec/profile.jsp?username=*usr*&password=*pwd*

where *usr* and *pwd* are the credentials of a user in the directory. If this succeeds, the user's LDAP attributes should be displayed:

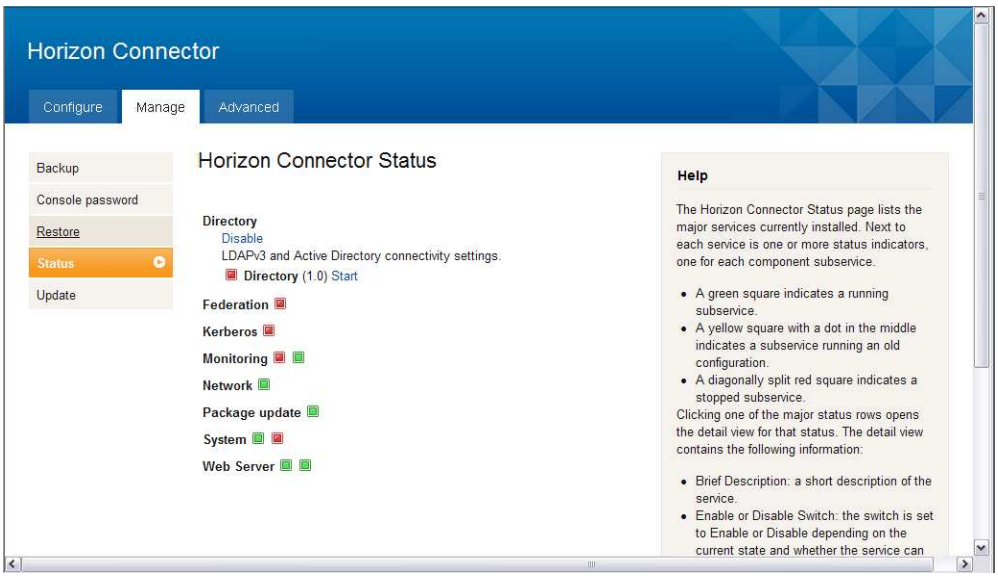


Confirm that the correct attributes are shown.

If the directory connection is not working (i.e. the status indicator is not green, or the test URL does not return the user's attributes) then:

- check that a directory service is running on the configured IP address and port
- check that Authentication Service has network connectivity to the directory service

- check the Bind DN and password are correct using an independent LDAP browsing tool
- check that the credentials passed to the test URL are correct
- if the status indicator on the **Manage > Status** page is red (stopped) for the directory service, try starting the directory service manually by clicking on the Directory row and then clicking **Start**:



If these troubleshooting options do not solve the issue, try rebooting Authentication Service to see if the error clears.

If the failure persists, try using a tool such as Wireshark to check the messages (if any) that are being sent between Authentication Service and the directory service, in order to diagnose the problem.

Set up Kerberos connectivity

If you are using Active Directory, then Authentication Service supports Kerberos for seamless authentication.

The main steps for setting up Kerberos are:

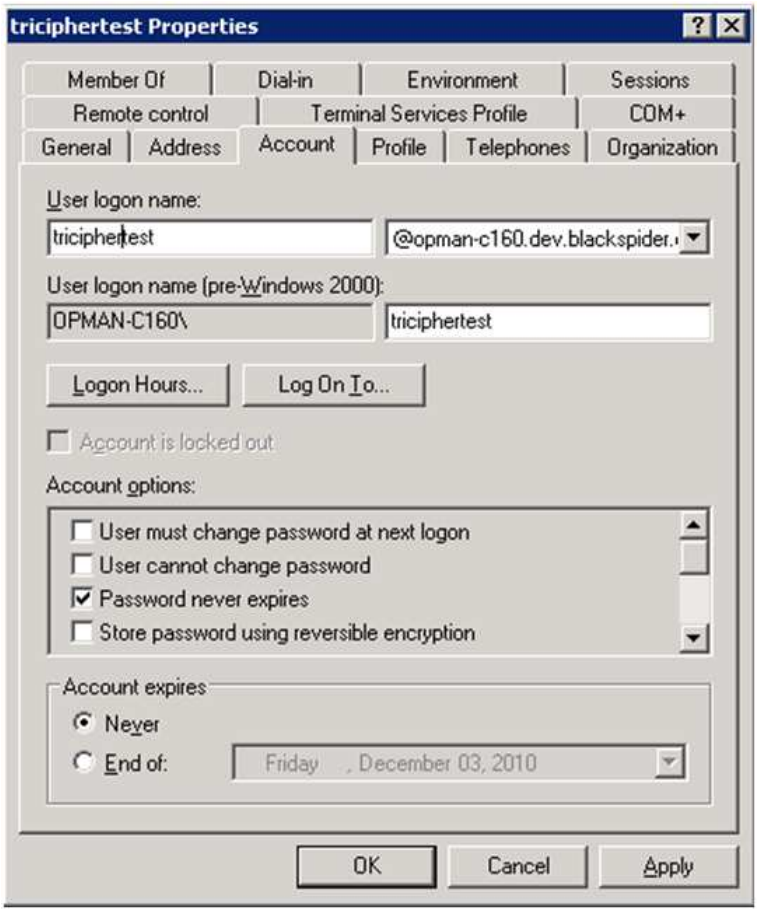
- *Add a user account to Active Directory*, page 16
- *Generate a Kerberos keytab*, page 16
- *Configure Kerberos in the administration console*, page 18

- *Test the Kerberos connection*, page 19

> **Note**
> Before starting this step, ensure your Windows network is fully operational, and your DNS is set up to resolve all machines involved.

Add a user account to Active Directory

On your Active Directory Domain Controller and Key Distribution Center (KDC) machine, create a user account for Authentication Service. This account will connect with the KDC and authenticate users.



The **User logon name** is the legacy user name of the account. Ensure the user belongs to the domain users group and set the password to never expire.

Generate a Kerberos keytab

To complete the KDC setup, generate a keytab that will be used for authentication.

To generate a keytab file, you will need to use the support tools from the Windows CD on your domain controller. Start by installing them if they are not already installed.

For more information about Windows Server Support Tools, see http://technet.microsoft.com/en-us/library/cc758202%28WS.10%29.aspx.

These support tools include the ktpass utility. Use this utility to create a keytab for the EC account, as follows:

ktpass /pass <*User Password of the Authentication Service AD account*> /mapuser <*Legacy User Name of the AD account*> /out <ec.keytab> /princ HTTP/<*FQDN*>@<*DOMAIN NAME*> /ptype KRB5_NT_PRINCIPAL /crypto RC4-HMAC-NT /Target <*DOMAIN NAME*>

The utility generates the file <ec.keytab> in your working directory. You will upload this keytab file to Authentication Service later.

Note the following when using ktpass:

- The <DOMAIN NAME> must be all in uppercase.
- The legacy user name used as the /mapuser argument should match the sAMAccountName in Active Directory. This is also the **User logon name** you set up in *Add a user account to Active Directory*, page 16.
- the /princ argument contains the fully-qualified Authentication Service host name.

> **Note**
> The legacy user name is used when mapping the user account to avoid issues of long Win2003 usernames that are not supported by ktpass.

The output in ktpass will look similar to this:

```
Using legacy password setting method
Successfully mapped HTTP/ec001.mydomain.com to authuser.
Key created.
Output keytab to ec.keytab:
Keytab version: 0x502
keysize 105 HTTP/ec001.mydomain.com@DEV.MYDOMAIN.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x4968e35c0c5586d1f63a9454e242d1c4)
```

Troubleshooting

If the ktpass command fails, try the following troubleshooting options:

- If you get output similar to:

```
Using legacy password setting method
WARNING: search term "(&(objectClass=person)
(samaccountname=authuser))" produced no results.
```

```
Failed to locate user "(&(objectClass=person)
(samaccountname=authuser))".
Could not locate user.
```

check that the /mapuser and /pass arguments correspond to the user created in Active Directory for Authentication Service

- If the user is found but ktpass fails to create the keytab, there may be problems with the domain controller setup. Run the `netdiag` command (also part of the Windows Server 2003 Support Tools), and check that the DNS and Kerberos tests pass.

  If the DNS test fails, it is probable that some of the DNS entries required by the domain controller are not registered. In this case, try running `ipconfig /registerdns` to see if this fixes the problem.

Configure Kerberos in the administration console

To add the KDC information, including the keytab file, to Authentication Service:

1. In Horizon Connector, go to **Configure > Authentication**.
2. Fill in the fields on this page as follows:

Field	Description	Example
KDC	Enter the host name or IP address of your KDC machine.	kdc.mycompany.com
Keytab	Browse to and select the location of the keytab file.	C:\temp\ec.keytab

> **Note**
> The **Domain** and **Principal** fields are read-only at this stage. These fields will be populated with your Windows domain and the principal (/princ argument) used by the ktpass utility after you have uploaded the keytab file and rebooted the Authentication Service VM.

3. Click **Save and Restart**.
4. Reboot the Authentication Service VM.

> **Note**
> Selecting only **Save and Restart** is not sufficient at this stage: you must reboot the whole VM for Kerberos to be started.

After reboot, note that it takes several minutes to start up all services. Once the post-reboot configuration is complete, the Kerberos service on the **Manage > Status** page

of the administration console should have a green status indicator. If the status indicator is not green, click on the Kerberos service, then click **Start.**

At this stage it is also recommended that you reconfirm the connection to your directory service by entering the test URL as described in *Test the directory connection*, page 13. If required, you can restart the directory service on the **Manage > Status** page.

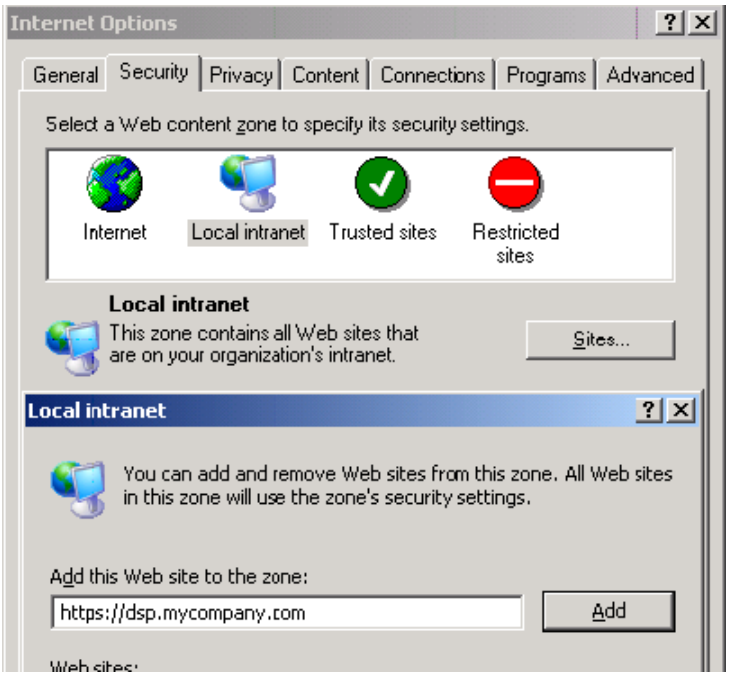
Test the Kerberos connection

This section provides instructions for testing the Kerberos authentication in the following browsers:

- *Internet Explorer 7*
- *Mozilla Firefox*
- *Internet Explorer 8*

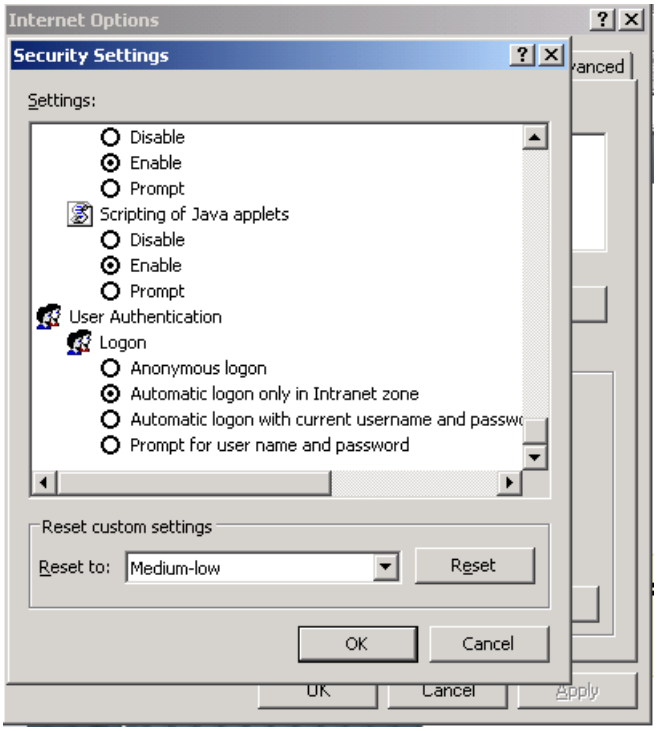
Internet Explorer 7

1. Make sure you are logged on to Windows as a user in the domain.
2. In Internet Explorer, go to **Tools > Internet Options** and select the **Security** tab.
3. Select **Local intranet**, and click **Sites**.
4. Click **Advanced**, and add the Authentication Service URL to your local intranet.



5. Under Security level, click **Custom level** and scroll down to User Authentication.

6. Ensure automatic logon is enabled only for your Intranet zone.



7. Click **OK** twice to exit.
8. Log on to Kerberos by going to the following URL:

   https://<*full Authentication Service DNS name*>/ec/UI/Login

   You should see a user profile page.

Mozilla Firefox

1. Open Firefox, and browse to **about:config**.
2. Click through the warning message, if displayed, to access the Advanced Settings page.

   Warning

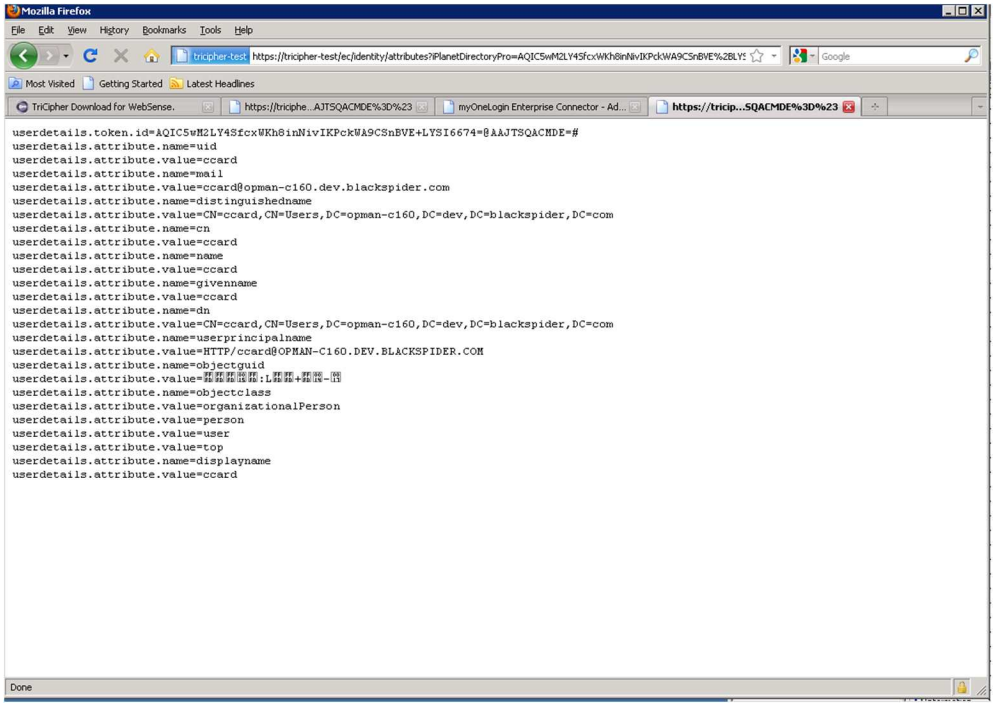
   Take care when making changes to this page. Any changes you make are at your own risk.

3. Double-click the following options, and add your Authentication Service domain URL to each:
   - network.negotiate-auth.trusted-uris
   - network.negotiate-auth.delegation-uris

   Note that you should include the port as part of the URL, for example https://authserv.mycompany.com:8080.
4. Log on to Kerberos by going to the following URL:

https://<*full Authentication Service DNS name*>/ec/UI/Login

You should see a user profile page:

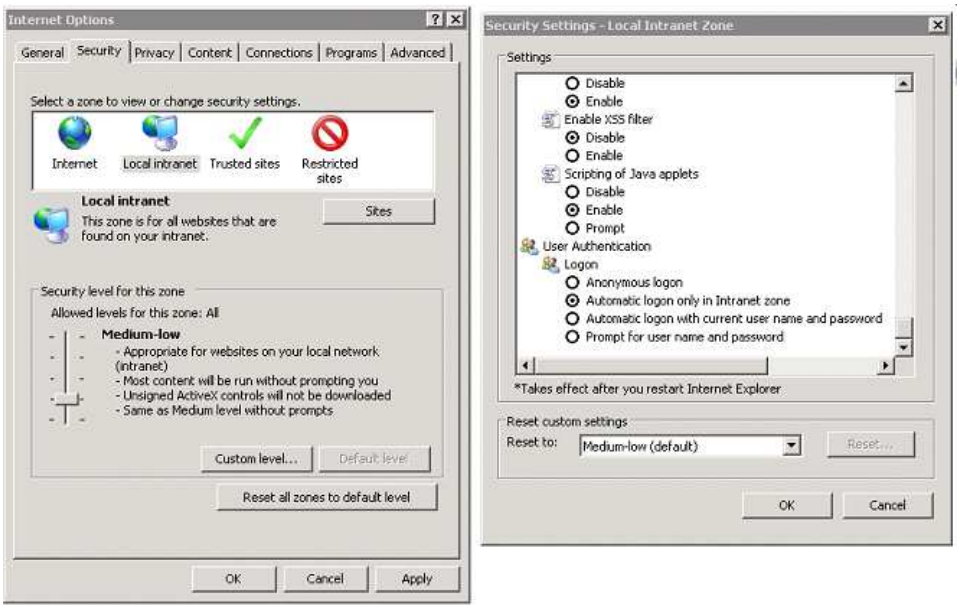



```
userdetails.token.id=AQIC5wM2LY4SfcxWKh8inNivIKPckWA9CSnBVE+LYSI6674=@AAJTSQACMDE=#
userdetails.attribute.name=uid
userdetails.attribute.value=ccard
userdetails.attribute.name=mail
userdetails.attribute.value=ccard@opman-c160.dev.blackspider.com
userdetails.attribute.name=distinguishedname
userdetails.attribute.value=CN=ccard,CN=Users,DC=opman-c160,DC=dev,DC=blackspider,DC=com
userdetails.attribute.name=cn
userdetails.attribute.value=ccard
userdetails.attribute.name=name
userdetails.attribute.value=ccard
userdetails.attribute.name=givenname
userdetails.attribute.value=ccard
userdetails.attribute.name=dn
userdetails.attribute.value=CN=ccard,CN=Users,DC=opman-c160,DC=dev,DC=blackspider,DC=com
userdetails.attribute.name=userprincipalname
userdetails.attribute.value=HTTP/ccard@OPMAN-C160.DEV.BLACKSPIDER.COM
userdetails.attribute.name=objectguid
userdetails.attribute.value=▯▯▯▯▯▯▯:L▯▯▯+▯▯▯-▯▯
userdetails.attribute.name=objectclass
userdetails.attribute.value=organizationalPerson
userdetails.attribute.value=person
userdetails.attribute.value=user
userdetails.attribute.value=top
userdetails.attribute.name=displayname
userdetails.attribute.value=ccard
```

Internet Explorer 8

1. Log on to a Windows account that belongs to the trusted domain.
2. To validate your Internet Explorer settings, go to **Tools > Internet Options** and select the **Security** tab.
3. Select **Local intranet**.
4. Under Security level, click **Custom level** and scroll down to User Authentication.

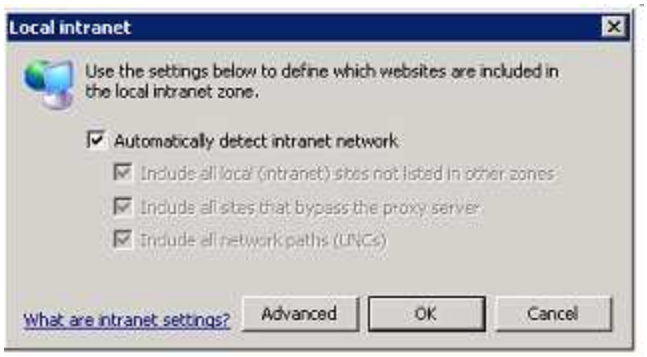
5. Ensure automatic logon is enabled only for your Intranet zone. This is the default setting for the Medium-low security level.



6. To validate that Authentication Service is in the intranet zone, browse to the logon URL for the administration console and check the zone in the bottom right corner of the window.

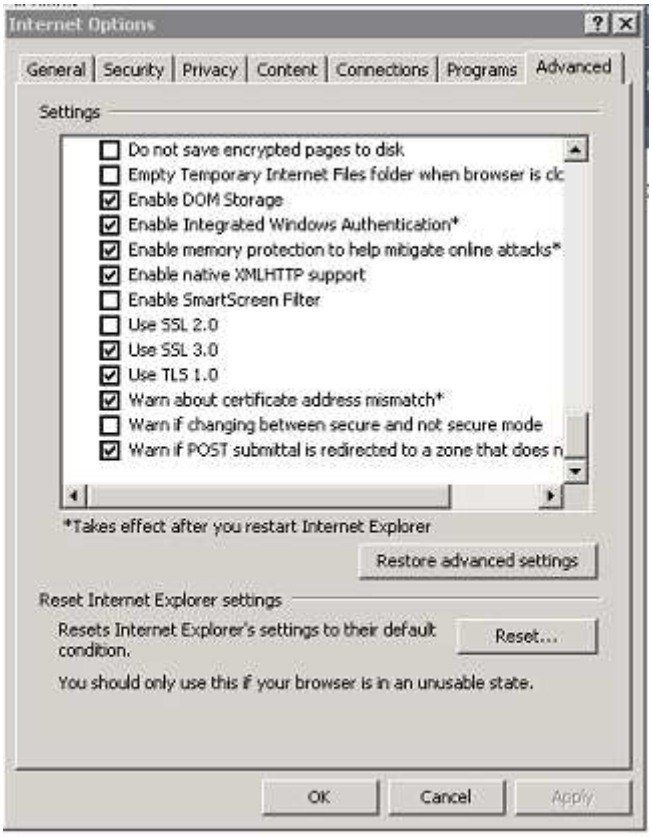
If the zone is not 'Local intranet', there are 2 methods you can use to add Authentication Service to the intranet zone:

- Go to **Tools > Internet Options** and select the **Security** tab. Select **Local intranet**, and click **Sites**. Check that **Automatically detect intranet network** is selected in the dialog below.



If this option is already selected, click **Advanced** and add Authentication Service to the list of intranet sites. Make sure that the protocol is correct, i.e. HTTPS or HTTP.

Next, go to the Internet Options **Advanced** tab and confirm that Internet Explorer is allowed to pass the Windows authentication to the trusted site by validating that Enable Integrated Windows Authentication is selected.

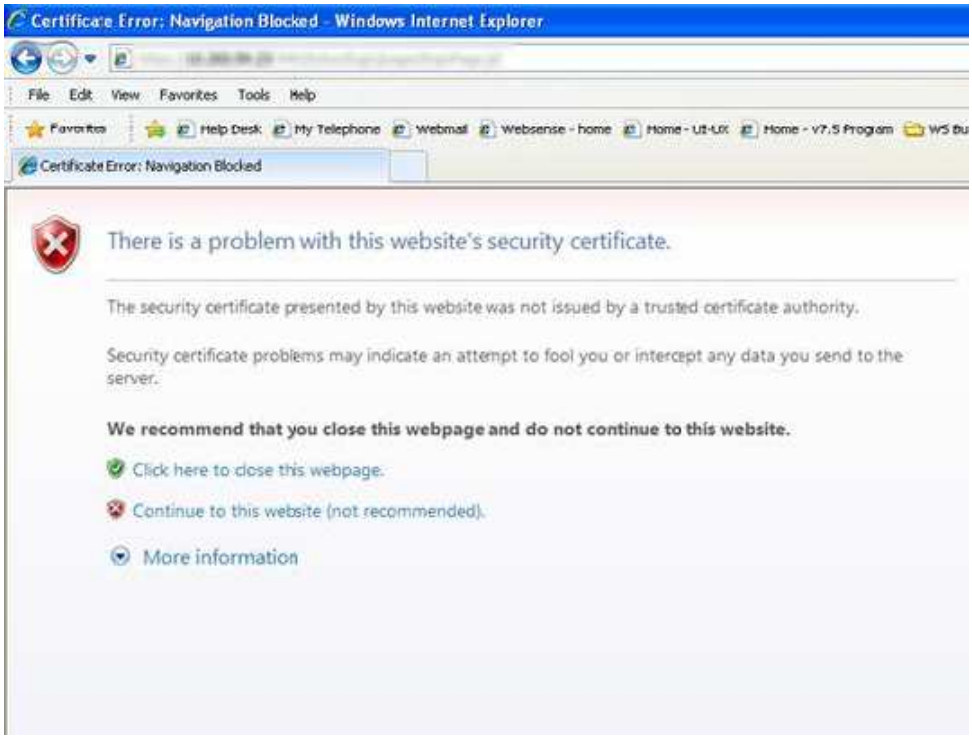


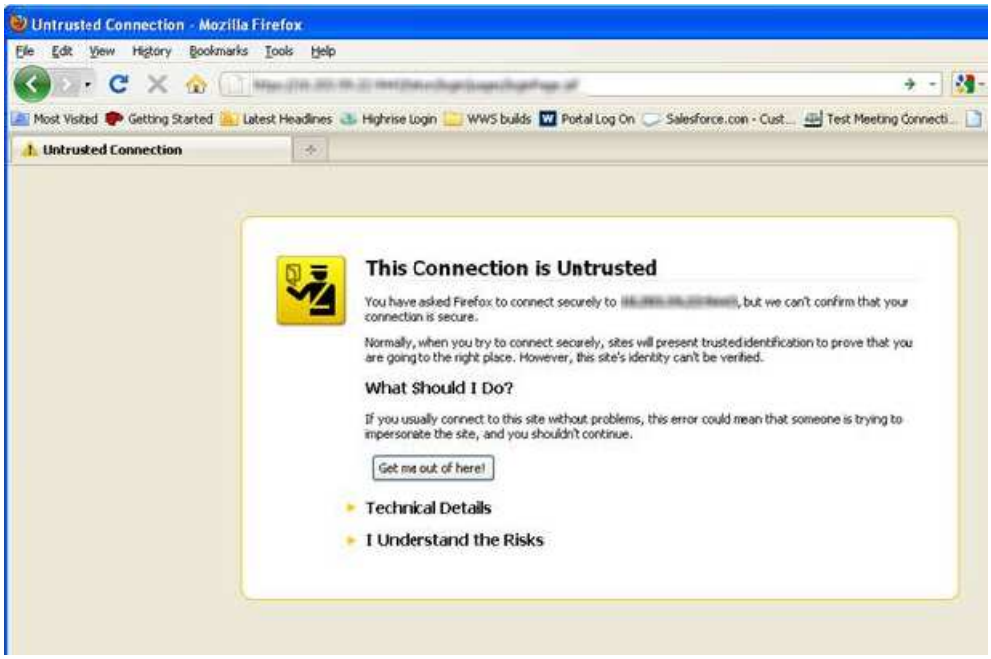
7. Log on to Kerberos by going to the following URL:
   https://<*full Authentication Service DNS name*>/ec/UI/Login
   You should see a user profile page.

Deploy SSL certificate

When your end users authenticate, their browsers will be redirected to the Authentication Service HTTPS URL. To ensure this happens seamlessly, it is recommended that you install an Authentication Service SSL certificate on all client machines.

If you do not install a certificate, users will see a page similar to the following every time they try to browse via Authentication Service, unless they manually add an exception:

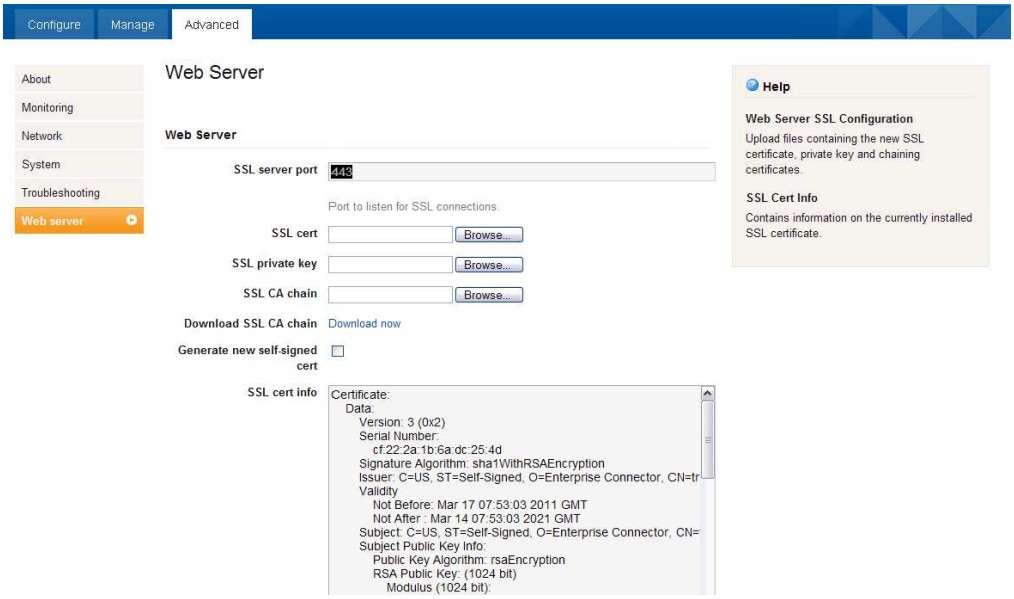




Authentication Service provides a default SSL certificate in the administration console that you can deploy to client machines. Alternatively, you can provide your own certificate.

To use the default Authentication Service certificate:

1. In Horizon Connector, go to **Advanced > Web Server**.



2. Copy the contents of the **SSL cert info** field and save as a .CRT file in the location of your choice.
3. Deploy the certificate to the client machines that will authenticate using Authentication Service using your preferred distribution method, for example Microsoft Group Policy Object.

To use your own SSL certificate:

1. If you wish to purchase a new certificate for use with Authentication Service, create a Certificate Signing Request and private key on the Authentication Service VM. Use these to create your SSL certificate.
2. Once you have purchased your certificate, go to **Advanced > Web Server** in the administration console.
3. In the **SSL cert** field, browse to the location of your SSL certificate and select the certificate file to upload.
4. In the **SSL private key** field, browse to the location of your private key and select the key file to upload.
5. In the **SSL CA chain** field, browse to the location of the certificate chain that goes back to the root Certificate Authority (also known as the certification path), and select the relevant file.
6. Click **Save and Restart**.

   Once the administration console has restarted, the **SSL cert info** field contains details of your new certificate.
7. Deploy the certificate to the client machines that will authenticate using Authentication Service using your preferred distribution method, for example Microsoft Group Policy Object.

Upload Websense metadata

In order for the Websense proxy to play the role of a SAML service provider and talk to Authentication Service, you must upload Websense SAML metadata to your administration console. The metadata is an XML file that contains the public key certificates needed to validate signed SAML AuthnRequests sent to Authentication Service, and defines the URL that receives SAML Responses from Authentication Service.

The XML metadata file is available at http://www.mailcontrol.com/crl/sp_metadata.xml.

To upload the file to your Authentication Service:

1. Copy the Websense metadata file to a location that is accessible from the browser session being used for the Administration Console.
2. In the administration console, go to **Configure > Federation**.
3. In the **Upload SP metadata** field, enter the path to the XML file.
4. Click **Save and Restart**.
5. After the restart, define the SAML attributes to use by checking all of the boxes.
6. Click **Save and Restart**.

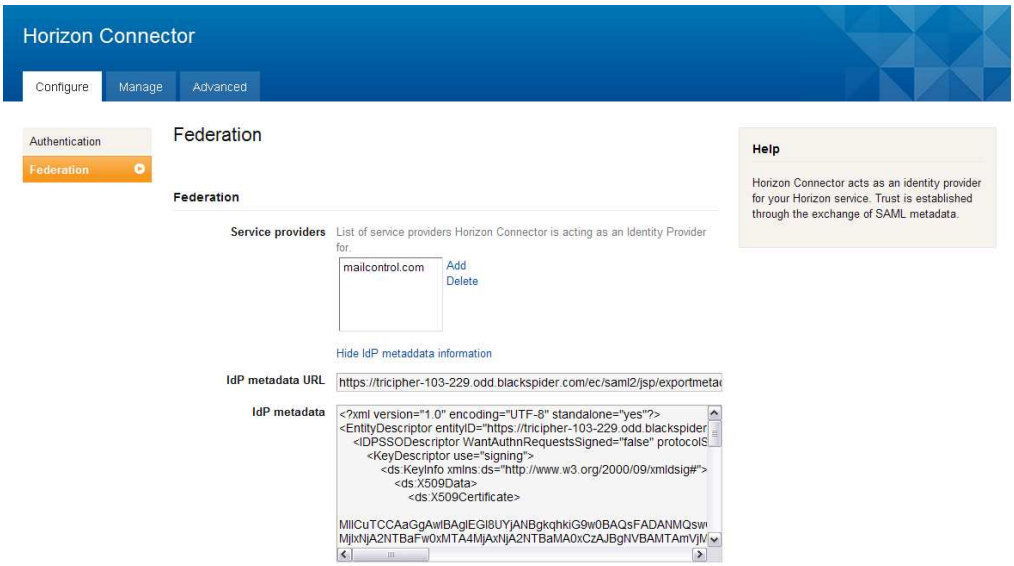
Configure Authentication Service metadata in your Websense product

To enable Authentication Service to work with Websense Web filtering, you must enter a metadata URL from the administration console in your Cloud Web Security or Web Security Gateway Anywhere interface. This manages the inclusion of the metadata XML in your Web filtering policy or policies.

To locate the metadata URL:

1. In the administration console, go to **Configure > Federation**.

2. Click **Show IdP metadata information**:



3. Copy the IdP metadata URL.
4. Paste the URL into a browser and save the resulting metadata to an XML file.

Cloud Web Security

> **Note**
> Authentication Service is supported on Internet Explorer 7 or later, Firefox version 3.5 or later, and Google Chrome 10.x or later.

1. Log on to the Cloud Web Security portal.
2. Go to **Web Security > Settings > Authentication Service**.
3. Enter the IdP metadata URL in the **Identity Provider Metadata URL** field.
4. Click **Get metadata**.
5. Click **Submit**.
6. For each Web policy that will use Authentication Service to authenticate end users:
   - Click the policy name.
   - Select the **Access Control** tab.
   - Under Authentication settings, mark **Authentication Service provided by VMware Horizon**.
   - Under Session Timeout, define how long user credentials are valid for use with Authentication Service. Credentials must be revalidated periodically for security reasons: this happens transparently once the selected period has elapsed.

- Click **Submit**.

To complete your configuration of Cloud Web Security with Authentication Service, you may also want to define the following:

- Authentication Service relies on SSL decryption to redirect SSL sites for authentication. If you want Authentication Service to seamlessly authenticate end users browsing to HTTPS sites, you should download the Websense root certificate from the **Web Security > Settings > Authentication Service** page, and install it on all client machines that will use Authentication Service.
- If there are some sites where you don't want SSL decryption performed (for example, sites that include personal identification information that should not be decrypted), you can maintain a list of host names on the **SSL Decryption** tab of each policy for which decryption is bypassed.
- If you wish to enforce the use of Authentication Service for certain end users, overriding the authentication settings in the policy, you can deploy a PAC file URL to those users that ends in the a=t parameter:

  ht t p: / / webdef ence. gl obal . bl ackspi der . com 8082/ pr oxy. pac?a=t

See the Cloud Web Security Help and the Cloud Web Security Getting Started Guide for more information.

Web Security Gateway Anywhere

> **Note**
> Authentication Service is supported on Internet Explorer 7 or later, Firefox version 3.5 or later, and Google Chrome 10.x or later.

1. Log on to TRITON Unified Security Center.
2. In TRITON - Web Security, go to **Settings > Hybrid Configuration > Hybrid User Identification**.
3. Under Authentication Service, enter the IdP metadata URL in the **Metadata URL** field.
4. Under Session Timeout, define how long user credentials are valid for use with Authentication Service. Credentials must be revalidated periodically for security reasons: this happens transparently once the selected period has elapsed.
5. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

To complete your configuration of Web Security Gateway Anywhere with Authentication Service, you may also want to define the following:

- If you want Authentication Service to seamlessly authenticate hybrid users browsing to HTTPS sites, you should download the hybrid SSL certificate and install it on all client machines that will use Authentication Service. Go to **Settings > Hybrid Configuration > User Access**, and under HTTPS Notification

Pages, click **View Hybrid SSL Certificate**. Save the certificate file to a location on your network. You can then deploy the certificate manually, using your preferred distribution method such as Group Policy Object (GPO).

4 Troubleshooting

Use this section to find solutions to common issues before contacting Technical Support.

Console shows IP as 127.0.0.1

This probably means that one of the network settings (IP address, subnet mask, or gateway) is invalid. Select **1** from the console menu to configure the interface and correct the error.

I want to re-enable DHCP

Select **1** to restart the network configuration. Authentication Service will ask you if you want to re-enable DHCP.

Cannot contact the browser-based interface

Narrow down the problem by testing the following:

- **Ping**. Authentication Service does respond to pings, so running ping from your client can tell you whether it is reachable.
- **Network settings**. Use the Appliance Console Menu (see *Configure network interface*, page 8) to verify these are correct.
- **DNS (if applicable)**. Look up the Authentication Service DNS name with nslookup or dig.
- **Routing**. Use tracert.exe or traceroute to check the routing.
- **Firewall**. Ports 443 and 8080 should be allowed between your client and Authentication Service.

If you have just changed the Authentication Service host name or have re-generated the Web server SSL certificate, the Web server may stop responding to requests until Authentication Service is restarted.

End user sees internal server error

If a local end user sees an error page similar to “HTTP Status 500 - The SAML request is invalid” in their browser, the Websense metadata may not have been uploaded successfully. Repeat the process described in *Upload Websense metadata*, page 26.

Kerberos troubleshooting

If you are having trouble with SSO using your Windows logon, the first thing to check is that all clocks involved are set. Authentication Service, the KDC, and your local desktop all have to be synchronized. Use an NTP server to make sure they are all within a minute of each other. Open up a command window and run:

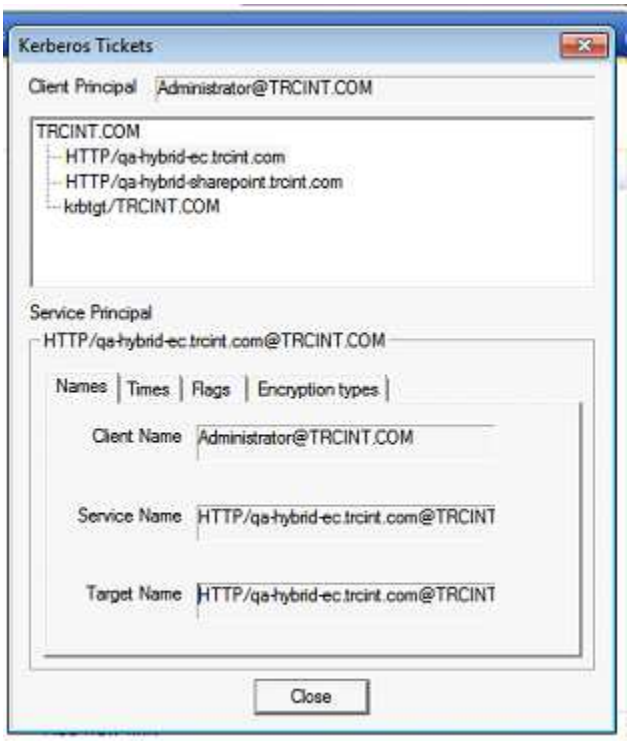
```
net time /set
```

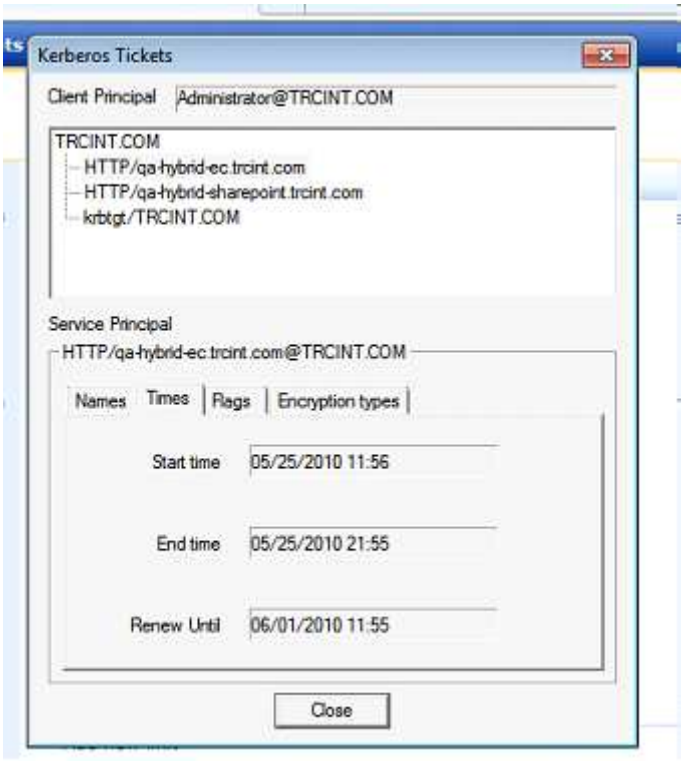
If clocks are not the issue, you may have a problem with:

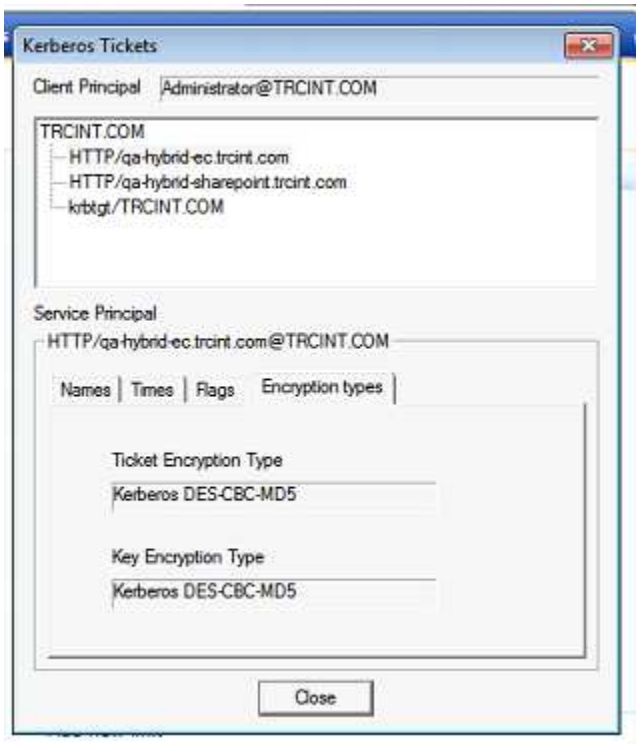
- the setup of the KDC
- Active Directory
- your local desktop setup.

You can use Kerbtray from Microsoft to validate that you are receiving a valid Kerberos ticket from your KDC:

http://www.microsoft.com/downloads/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88&displaylang=en


Kerberos Tickets
Client Principal
Administrator@TRCINT.COM
TRCINT.COM
HTTP/qa-hybrid-ec.trcint.com
HTTP/qa-hybrid-sharepoint.trcint.com
krbtgt/TRCINT.COM
Service Principal
HTTP/qa-hybrid-ec.trcint.com@TRCINT.COM
Names
Times
Flags
Encryption types
Client Name
Administrator@TRCINT.COM
Service Name
HTTP/qa-hybrid-ec.trcint.com@TRCINT
Target Name
HTTP/qa-hybrid-ec.trcint.com@TRCINT
Close


Kerberos Tickets
Client Principal
Administrator@TRCINT.COM
TRCINT.COM
HTTP/qa-hybrid-ec.trcint.com
HTTP/qa-hybrid-sharepoint.trcint.com
krbtgt/TRCINT.COM
Service Principal
HTTP/qa-hybrid-ec.trcint.com@TRCINT.COM
Names
Times
Flags
Encryption types
Start time
05/25/2010 11:56
End time
05/25/2010 21:55
Renew Until
06/01/2010 11:55
Close



After attempting to log on to Authentication Service, you should have a Kerberos ticket in the list that matches the Authentication Service URL. If you don't, it could be because:

- the KDC didn't distribute a ticket. Check you logged on to the correct domain, rather than just locally to your desktop.
- your system rejected the ticket. The most common reason for this is incompatibility with encryption types.

This screen can also be used for further diagnostics. You could double-check the following:

- Verify all names and targets on the Names tab match the WindowsDesktopSSO configuration in Authentication Service.
- Make sure the time stamps for the Kerberos ticket that matches your Authentication Service is current. Invalid times could indicate mis-configuration of your KDC.
- If using the older DES encryption, you will need to make sure all systems allow for it, as some service packs and operating systems from Microsoft have removed support for DES.