Machine Authentication Using Certificates

# Table of Contents

- Introduction .................................................. 3
- Scope .......................................................... 3
- Design Considerations ........................................ 3
  - Microsoft Windows CA Configuration .................. 4
  - Infranet Controller Configuration ....................... 8
  - Request and Install Workstation Authentication Certificate ............. 11
  - Odyssey Access Client Configuration .................. 13
  - Confirm Proper Operation .................................. 18
  - Simultaneous Machine Authentication and User Authentication .......... 19
- Summary ........................................................ 21
- About Juniper Networks ..................................... 21
Introduction

What happens in an 802.1X environment when there is no user around to sign into a PC and authenticate it onto the network? What happens if routine system maintenance such as automated backups, software updates and patches need to be performed at night when everyone has gone home and logged out of their machines? The answer is “absolutely nothing.” With 802.1X, unless proper authentication can be performed, the machine won’t be able to get onto the network. This is where machine authentication comes in. It permits an unattended machine to authenticate onto the network through the normal 802.1X authentication mechanisms. There are a couple of different forms of machine authentication, one involving machine credentials similar to a username and password, and another using machine certificates. This application note focuses specifically on machine certificates: how to generate them, how to configure the Juniper Networks Infranet Controller to accept them, and how to configure Juniper Networks Odyssey Access Client to use them.

Scope

This application note will describe how to configure the Windows Certification Authority, Infranet Controller and the Odyssey Access Client to provide machine authentication using digital certificates.

Design Considerations

Hardware Requirements

- Infranet Controller models IC4000 or IC6000
- Windows (2000/XP/Vista) PC
- Network switch configured for 802.1X authentication

Software Requirements

- Infranet Controller version 2.1R1 or greater
- Odyssey Access Client v4.7 or greater
- Windows 2003 Enterprise Certification Authority

Description and Deployment Scenario

In order to use machine certificates to perform machine authentication, you need to complete several configuration steps, starting with the generation of the proper machine certificate on the Microsoft Windows 2003 Enterprise Certification Authority (CA). After this step is completed, you need to configure the Infranet Controller (IC) for layer 2 access control and certificate authentication. In a final step, you will configure the Odyssey Access Client Enterprise Edition (OAC-EE) for machine authentication using certificates.
Machine Authentication Using Certificates

**Microsoft Windows CA Configuration**

In order to have the Windows CA issue proper machine certificates, you will first have to make a modification to the Workstation Authentication template or, alternatively, you can use a workaround in the Infranet Controller configuration. This template change or the IC workaround is necessitated by the fact that the default Workstation Authentication certificate template used on the Windows CA does not contain a Subject field. This missing Subject field causes authentication to fail on the IC without some changes. The following procedure describes how to modify the default Workstation Authentication certificate template on the Windows CA. The workaround on the IC configuration is described later in this note.

On the Windows CA, sign in as a Domain Administrator and launch the Microsoft Management Console by clicking **Start > Run…**, enter **mmc** in the Run box and click **OK**.

![Start > Run… Dialog](image)

*Figure 1: Start > Run… Dialog*

Within the MMC, select **Add/Remove Snap-in…** from the **File** menu.

![Launch Add/Remove Snap-in](image)

*Figure 2: Launch Add/Remove Snap-in*
Click the **Add**… button. Select the **Certificates Templates** snap-in and click **Add**. Then select the **Certification Authority** snap-in and click **Add**. After adding both snap-ins, click **Close** to close the Add Standalone Snap-in window and then click **OK** to finish.

![Figure 3: Add Snap-ins](image)

In the **Certificate Templates** snap-in, right-click on the **Workstation Authentication** template and select **Duplicate Template** from the contextual menu.

![Figure 4: Create Duplicate Certificate Template](image)
When the **Properties of New Template** dialog appears, enter a new name for the **Template Display Name** on the **General Tab**.

![Figure 5: Modify Template Name](image)

On the **Subject Name** tab, select either **Common Name** or **Fully distinguished name** from the **Subject name format** pull-down menu. Click **OK** when done.

![Figure 6: Define Subject Name Format](image)
The new certificate template should now appear in the list of templates.

Figure 7: New Certificate Templates List

In order to make this new template available to users, you must issue the template within the certificate authority. Click on the plus sign next to the Certification Authority snap-in, then on the plus sign next to your certificate authority. Finally, right-click on the Certificate Templates folder and select New > Certificate Template to Issue from the contextual menu.

Figure 8: Issue New Certificate Template
Select the Workstation Authentication template that you just created and click OK.

![Figure 9: Select Certificate Template to Issue](image)

That completes the modifications to the Windows CA. Your workstations can now request a machine certificate that includes a Subject Name and will function properly with the Infranet Controller.

![Figure 10: Available Certificate Templates](image)

**Infranet Controller Configuration**

The first step on the IC configuration is to create a Certificate Authentication server. Go to **Authentication > Auth Servers**, select **Certificate Server** from the pull-down menu and click **New Server**... Supply a **Name** for the server instance. If you have made the modifications to the Windows CA as described above, leave the **User Name Template** at its default value. If you chose not to make those modifications, you will need to modify the **User Name Template** in the auth server configuration. Instead of `<certDN.CN>` use `<certAttr.altName.DNS>`. The **User Name Template** is used by the IC to extract from the certificate the data that will be used to form the username.

Using the default **User Name Template** in conjunction with the default **Certificate Template** on the Windows CA will result in a non-existent username (since the Subject field in the certificate is blank).
Create a new role for the authenticated machine. Go to Users > User Roles and click on New Role... You can, of course, use any existing role including those used for users. For this role you should require the Agent, but don’t permit Agentless. You also shouldn’t require any Host Checking for this role.

Create a new realm to handle machine certificate authentication. Go to Users > User Realms and click on New Realm... Select the server you created above for the Authentication Server and create a role mapping rule that maps all users to the role you just created.

When editing, start on the Role Mapping page.

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.
Go to Authentication > Signing In > Sign-in Policies and click New URL... to define a new sign-in policy. Alternatively you can use the default sign-in policy */. In the example below, the sign-in policy is */machinecert/. Assign the realm created above to the sign-in policy.

![Image: Machine Authentication Sign-in Policy](image)

**Figure 14: Machine Authentication Sign-in Policy**

Create a Location Group (or use an existing one) and assign the Sign-in Policy you just created to the Location Group.

![Image: Location Group Using Machine Authentication Sign-in Policy](image)

**Figure 15: Location Group Using Machine Authentication Sign-in Policy**

Define a RADIUS Client and assign the Location Group that you created above. The configuration is in UAC > Network Access > RADIUS Client.

![Image: RADIUS Client Configuration](image)

**Figure 16: RADIUS Client Configuration**
This completes the chain of configuration within the IC from switch or access point to role assignment. For example: (1) a RADIUS request is received from a RADIUS Client; (2) the RADIUS Client determines the Location Group; (3) the Location Group determines the Sign-in Policy (URL); (4) the Sign-in Policy determines the Realm, (5) the Realm determines the Authentication Server and, if authenticated, the Roles.

As an option, you can define a RADIUS Attributes policy to perform VLAN assignment for those machines that successfully authenticate. For instance, machines that authenticate could be placed into a System Update VLAN so that software upgrades and patches could be pushed to the machine even when no user is logged in. Go to UAC > Network Access > RADIUS Attributes.

**Request and Install Workstation Authentication Certificate**

In order to make any of this work, you need a machine certificate of the proper type installed on the PC that needs access. In order to get the certificate, you need to open the Certificates MMC snap-in on the PC (not on the Windows CA like you did earlier). Go to Start > Run… and enter mmc in the Run dialog box. Within the MMC, select Add/Remove Snap-in... from the File menu. Click the Add… button. Select the Certificates snap-in and click Add.

![Add Certificates Snap-in](Image 17)

Select Computer Account for the certificate type to manage and then click Next >. Choose Local Computer for the computer you want to manage and click Finish. After adding the snap-in, click Close to close the Add Standalone Snap-in window and then click OK to finish.

![Complete Adding Certificate Snap-in](Image 18)
You now need to request the machine certificate. In the Certificates MMC, go to Personal > Certificates, right-click and select All Tasks > Request New Certificate.

Figure 19: Request New Certificate

NOTE: Should you receive the following error, it typically means that you are not logged into the Windows domain where the CA lives. In order to get the machine certificate, you must have logged onto the Windows domain and been authenticated by a domain controller. You cannot have used cached credentials to log into Windows. This usually means that the PC must be able to reach the domain controller on the network when you log into Windows. You cannot do this operation remotely or in an 802.1X environment without some special provisions.

Figure 20: Certificate Request Error

Complete the Certificate Request Wizard. Click Next >, enter a Friendly Name for your certificate and click Next >, then click Finish. When the certificate request process completes, click OK in the final dialog box.

Figure 21: Completing the Certificate Request
After completion of the wizard, you should have a new machine certificate shown in the Certificates MMC. You can tell this is a machine certificate in a couple of different ways. First, it’s in your personal certificate store for the Local Computer, not the Current User (which is where user certificates would be stored). Second, it’s Issued To your machine name, not your username. Finally, its Intended Purpose is only Client Authentication (user certificates will have other purposes such as Secure Email).

Figure 22: Installed Machine Certificate

Odyssey Access Client Configuration

Now it’s time to turn to the configuration of Odyssey Access Client. Before you begin, make sure that your version of Odyssey has been licensed as an Enterprise Edition. In the Odyssey Access Client Manager, go to Help > About and look for the words Enterprise Edition. If instead you see the words UAC Edition, you will need to obtain an Enterprise Edition license key.

Figure 23: Verify OAC Version
Open the Odyssey Access Client Administrator by selecting **Odyssey Access Client Administrator** from the **Tools** menu.

**Figure 24: Opening OAC Administrator**

Within the Odyssey Access Client Administrator, double-click on the **Connection Settings** icon.

**Figure 25: Connection Settings**

Go to the **Machine Account** tab and **check the box** to enable connections using machine account. Click **OK**.

**Figure 26: Enable Machine Account**
Next you need to configure the machine account settings. Double-click on the **Machine Account** icon.

![Figure 27: Machine Account Settings](image)

Open the **Configuration** section and click **Profiles**. Click **Add...** to create a new machine account profile.

![Figure 28: Add Machine Account Profile](image)

First, supply a **Profile Name**. Next check the **Use machine credentials** box and uncheck the **Permit login using password** box.

![Figure 29: User Info/Password Tab](image)
On the **Certificate** tab, check the **Use machine credentials** box. Check the **Permit login using my certificate** checkbox and select the Use the following certificate radio button. Click the **Browse**… button and select the machine certificate that you added in the previous section.

**Figure 30: User Info/Certificate Tab**

On the **Authentication** tab, make sure that EAP-TTLS is the only Authentication Protocol. You can uncheck the **Validate server certificate** if you’re using a private CA and this is a testing environment, however in a production environment you should leave the **Validate server certificate** box checked. In that case, you must add the CA root certificate into one of the Local Computer’s Trusted CA stores, and add the CA to the list of Trusted Servers within the Odyssey Access Client.

**Figure 31: Authentication Tab**
On the **T TLS** tab, remove EAP-MS-CHAP-V2 from the Inner Protocol list. Click the **Use my certificate and perform inner authentication** radio button under **Personal certificate usage**. This last setting is easy to miss and will render all of your other work useless if you forget it. Click **OK** when you’re finished.

![Figure 32: TTLS Tab](image)

You now need to add an adapter to the configuration. This adapter will be used by the machine to connect to the network. Under **Configuration > Adapters** click **Add…** and then select either a **Wireless** or, more typically, a **Wired** adapter that will be used for 802.1X authentication.

![Figure 33: Add Adapter](image)
Finally, in the **Adapters > [ADAPTER]** section, select the **Profile** that you created earlier and check the **Connect to the network** checkbox. You can now close the **Machine Account** window and the **Odyssey Access Client Administrator** window. This will save your client configuration.

![Machine Account (Odyssey Access Client)](image)

**Figure 34: Completing the OAC Configuration**

**Confirm Proper Operation**

Reboot your PC and wait for the Windows logon dialog box to appear. At this point your PC should have been authenticated onto the network using the machine certificate. On the Infranet Controller, go to **System > Status > Active Users** and observe the list of users. You should see an entry for your PC in the list (note the entry for RFILER-LAP2 below).

![Active Users](image)

**Figure 35: Active Users**
You can also take a look at the user access log. On the IC go to System > Log/Monitoring > User Access > Log. You should see log entries similar to those shown in the following figure.

<table>
<thead>
<tr>
<th>Severity</th>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>EAM21459</td>
<td>2007-10-29 20:22:56 - ic - [0.0.0.0] RFILER-LAP2(MachineCert)[Machine] - User attempt to connect to MachineCert.</td>
</tr>
<tr>
<td>info</td>
<td>AUT24141</td>
<td>2007-10-29 20:22:55 - ic - [0.0.0.0] RFILER-LAP2(MachineCert)[Machine] - Agent login on LAP2/MachineCert from 00-03-47-19-12-e2.</td>
</tr>
</tbody>
</table>

Figure 36: User Log

**Simultaneous Machine Authentication and User Authentication**

The entire configuration up to this point has been geared to permit an unattended machine to authenticate into an 802.1X network. If you want to also permit a user to authenticate from the same machine, there are a couple of simple configuration changes that must be made, both to the Infranet Controller and the Odyssey Access Client.

On the IC, it’s assumed that you have a working user authentication setup. The details of setting that up are not included here. To permit a user to authenticate as well as the machine, add the **User Authentication Realm** to the existing **Sign-in policy** you used for machine authentication. In the example below, the realm **Agent** is used for **User Authentication**. Simply add it to the list of realms used for authentication for the given **Sign-in Policy**.

**Signing In**

In addition to the change to the IC, you need to make two changes to the Odyssey Access Client configuration. The first change is to the machine authentication profile. Open the **Odyssey Access Client Manager** and select **Odyssey Access Client Administrator** from the Tools menu. Double-click on **Machine Account**, then go to **Configuration > Profiles**. Select the machine account profile you created earlier and click **Properties**... Go to the **JUAC** tab and enter the **Realm name** that you used on the IC for machine authentication. In this example, the realm name is **MachineCert**. Click **OK**, then close both the **OAC Administrator** windows.

![Profile Properties](image)
In addition to modifying the machine authentication profile, you need to modify the user authentication profile as well. On the JUAC tab, enter the Realm name that is used for user authentication. This should be the same Realm name that you added to the Sign-in Policy above.

Following these changes, you should be able to use both machine authentication and user authentication with the same Odyssey Access Client on the same 802.1X port, authenticating with the same Infranet Controller. Using the configuration described in this application note, when the PC boots it will attempt to authenticate with the IC using a machine certificate. Once the user presses CTRL-ALT-DEL and logs into Windows, the machine connection is dropped and the user authentication is attempted. Your active user list should no longer show the machine as authenticated but should now show the user as authenticated.

**Active Users**

Following these changes, you should be able to use both machine authentication and user authentication with the same Odyssey Access Client on the same 802.1X port, authenticating with the same Infranet Controller. Using the configuration described in this application note, when the PC boots it will attempt to authenticate with the IC using a machine certificate. Once the user presses CTRL-ALT-DEL and logs into Windows, the machine connection is dropped and the user authentication is attempted. Your active user list should no longer show the machine as authenticated but should now show the user as authenticated.

**Active Users**

<table>
<thead>
<tr>
<th>User</th>
<th>Realm</th>
<th>Roles</th>
<th>Signed In</th>
<th>Signed In ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Admin Users</td>
<td>Administrators</td>
<td>2002/10/29 20:00:19</td>
<td>1.0.0.100</td>
</tr>
<tr>
<td>rlier</td>
<td>Agent</td>
<td>Employee w/o Odyssey, Employee, Remediation</td>
<td>2007/10/31 13:03:55</td>
<td>1.0.0.110</td>
</tr>
</tbody>
</table>
Summary

Using the Infranet Controller in conjunction with Odyssey Access Client Enterprise Edition enables the use of machine certificates for machine authentication in an 802.1X environment. This permits unattended machine access to an 802.1X-secured network.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.
Machine Authentication Using Certificates