SSH Communications
Tectia SSH

Secured by RSA Implementation Guide for 3rd Party PKI Applications

Last Modified: December 8, 2014

Partner Information

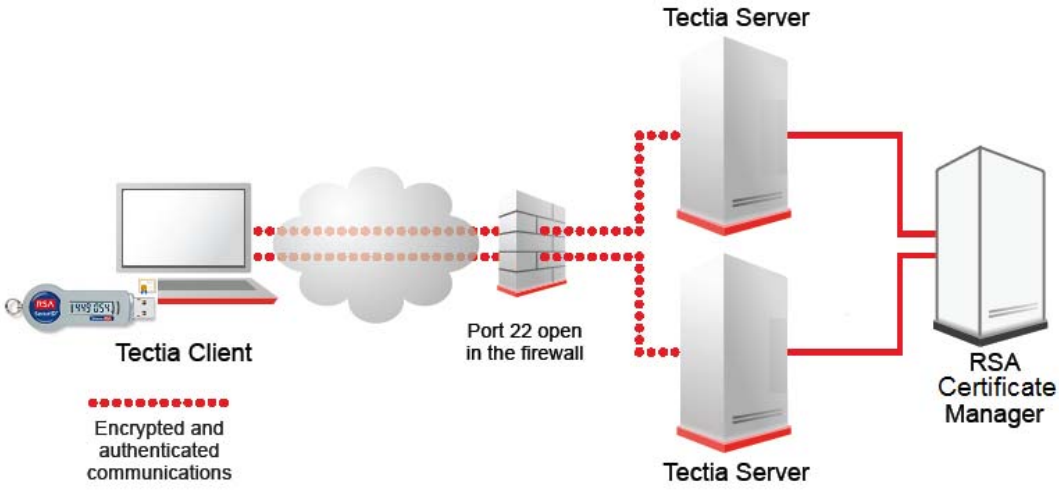
Product Information	
Partner Name	SSH Communications
Web Site	www.ssh.com
Product Name	Tectia SSH Server and Tectia SSH Client
Version & Platform	6.4.X Windows
Product Description	Tectia SSH is the leading end-to-end communications security solution for the enterprise. The Tectia SSH solution is based on the SSH Secure Shell and SSH's other industry leading technologies used by millions worldwide. Tectia SSH enables secure system administration, secure file transfer and secure application connectivity with centralized management throughout the internal and external network. Tectia SSH provides transparent strong encryption and authentication and easily integrates into heterogeneous, multi-platform environments.

ssh® Securing the path to your information assets

Solution Summary

Tectia SSH Client and Server form an enterprise-class Secure Shell solution for securing system administration, file transfer, and application connectivity in heterogeneous enterprise networks. Tectia SSH Client and Server are based on the IETF standard Secure Shell (version 2) protocol.

Tectia SSH Client supports using the RSA SID 800 Hybrid Authenticator for PKI certificate based authentication. Tectia SSH Client unlocks the RSA SID 800 Hybrid Authenticator with a pre-defined user PIN allowing the certificate to be used for certificate based authentication.



Product Requirements

Partner Product Requirements: Tectia SSH Client	
CPU	No special requirements
Memory	No special requirements
Storage	100 MB free disk space
Firmware Version	N/A
Operating System	
Platform	**Required Patches**
Various OSes	Reference the Tectia Client User Manual for specific OSes.

Partner Product Requirements: Tectia SSH Server	
CPU	No special requirements
Memory	1 GB RAM for hundreds of simultaneous tunnels.
Storage	100 MB free disk space
Firmware Version	Reference the TectiaServer_adminManual for specific OSes.
Operating System	
Platform	**Required Patches**
Various OSes	Reference the TectiaServer_adminManual for specific OSes.

Product Configuration for Interoperability

Interoperability between the RSA Authenticators and Tectia SSH requires the installation of the RSA Authentication Client, Tectia SSH Server, Tectia SSH Client(s). A PKI smartcard user certificate provisioned from an RSA Certificate Manager is stored on an RSA SID800 Hybrid Authenticator.

Before You Begin

This section provides instructions for integrating the RSA SID800 Hybrid Authenticator with Tectia SSH. The document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

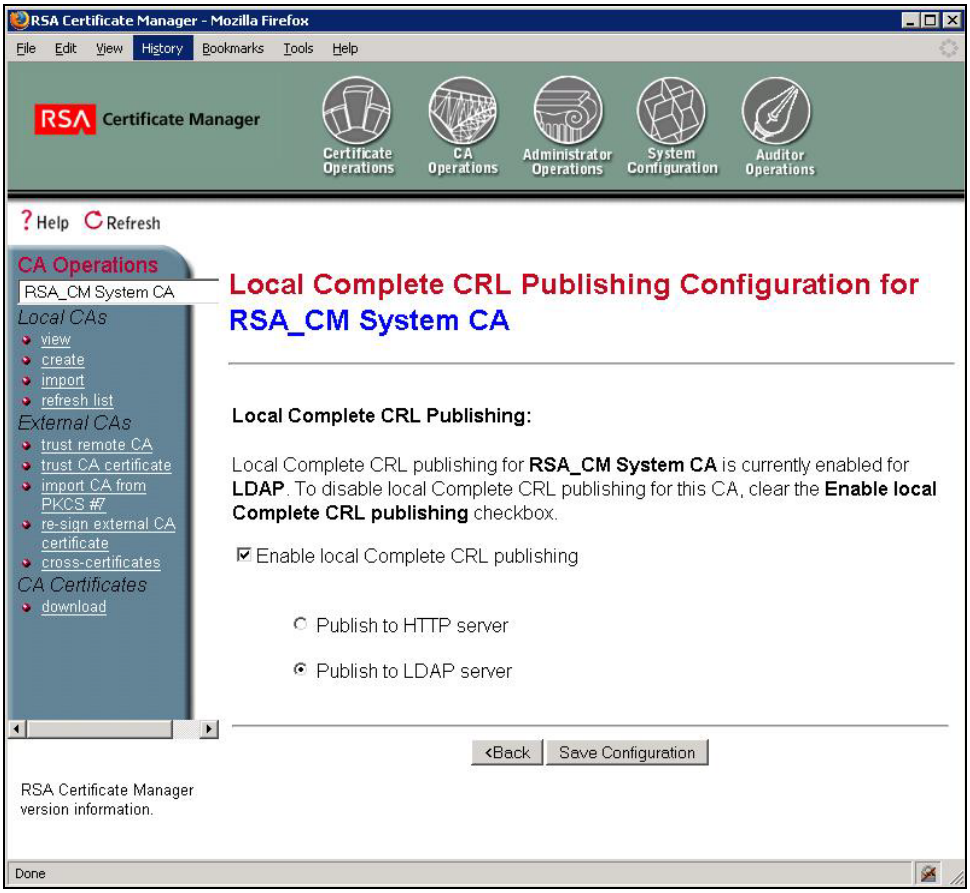
RSA Certificate Manager installable elements

RSA Certificate Manager 6.9

RSA Certificate Manager configurable elements

Configuration of CRL Publishing

1. Browse to the RSA Certificate Manager Administration.
2. Select CA Operations.
3. Select the appropriate CA and click **Local Complete CRL Publishing** in the CA Configuration section.
4. Select **Enable local Complete CRL publishing** and **Publish to LDAP server.**
5. Click **Save Configuration** and then OK to change the configuration of the chosen CA.



Partner Product Configuration

Partner product's installable elements

Tectia SSH Client/Server version 6.0 or later.

Partner product's configurable elements

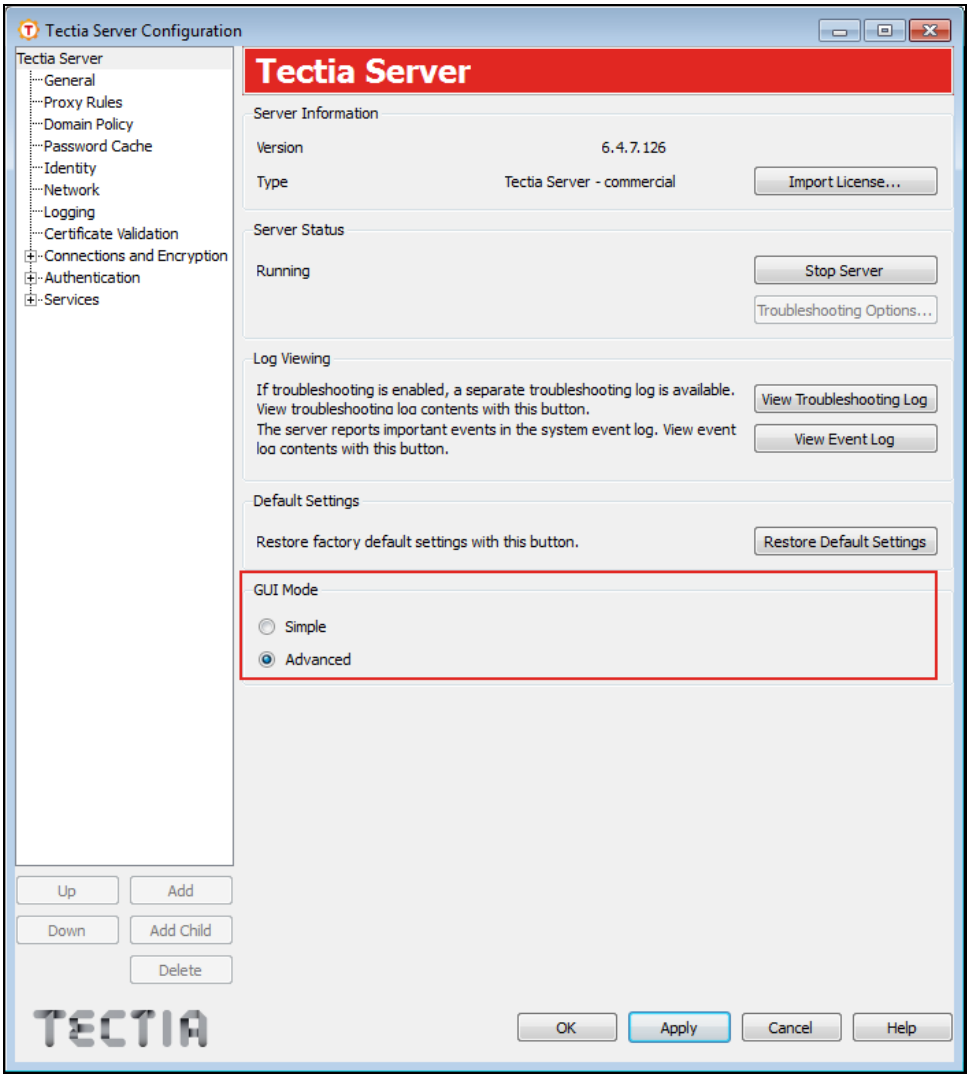
Refer to the RSA Certificate Manager Administrator documentation to ensure the necessary setup for certificate compatibility with Tectia SSH Client/Server/ConnectSecure. This includes CRL distribution points, client certificate extensions (e.g. RFC822 email extension) as the server will need to map a certificate attribute to a user account.

Configuring User Authentication with Certificates on Windows

To configure Tectia Server to allow user authentication with X.509 certificates, perform the following tasks using Tectia Server Configuration GUI:

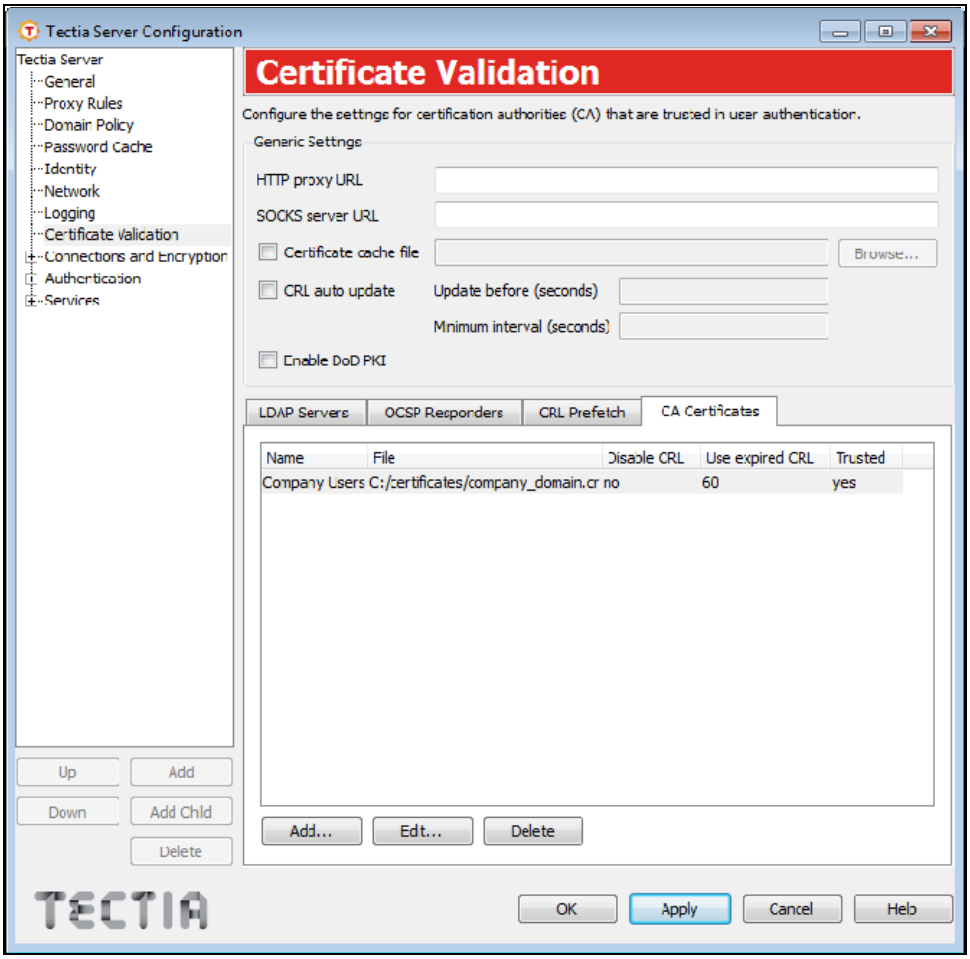
1. Launch Tectia Server Configuration GUI and select **Start** > **All Programs** > **Tectia Server** > **Tectia Server Configuration**.

2. Under **GUI Mode**, select **Advanced** to view all available options and groups.



3. Go to the **Certificate Validation** page and select the **CA Certificates** tab.
4. Add the trust anchors and intermediate CA certificates that are needed for the certificate validation. Root CA certificates or intermediate CA certificates can be added as trust anchors. Normally you need to add only the CA certificate that can issue certificates for the users into Tectia Server configuration. That is, you need not create the whole trust path in the configuration.

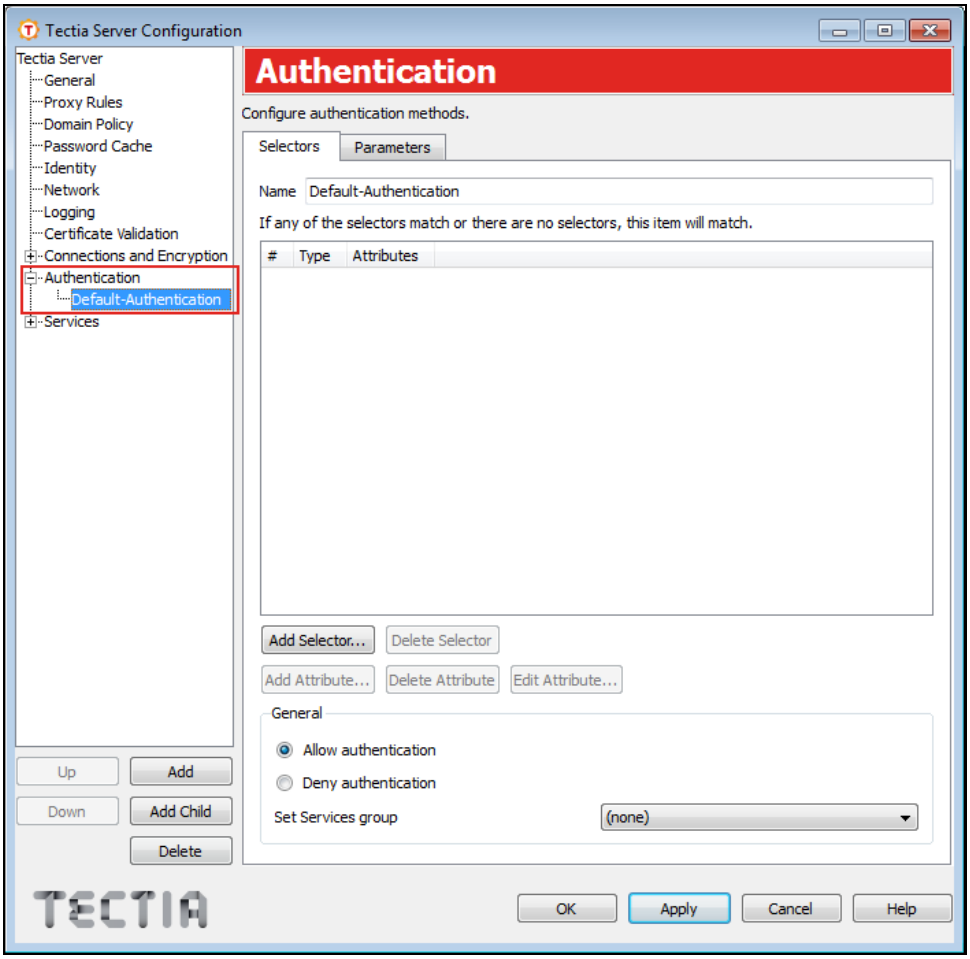
> **Note: CA certificates are by default added to the CA Certificates list as trust anchors, meaning that revocation checks are not performed on them. When adding a new intermediate CA certificate, clear the Trusted CA check box to enable revocation checks.**



Note: In case you have an LDAP server in use, you only need to add the root CA certificate into the server configuration. Tectia Server can retrieve the intermediate CA certificates that are issued by the root CA certificate automatically from the LDAP server. For example, if Company Users is added as a trust anchor and the intermediate CA certificates are stored in the LDAP, end entities certified by the root or intermediate CA certificates will be trusted.

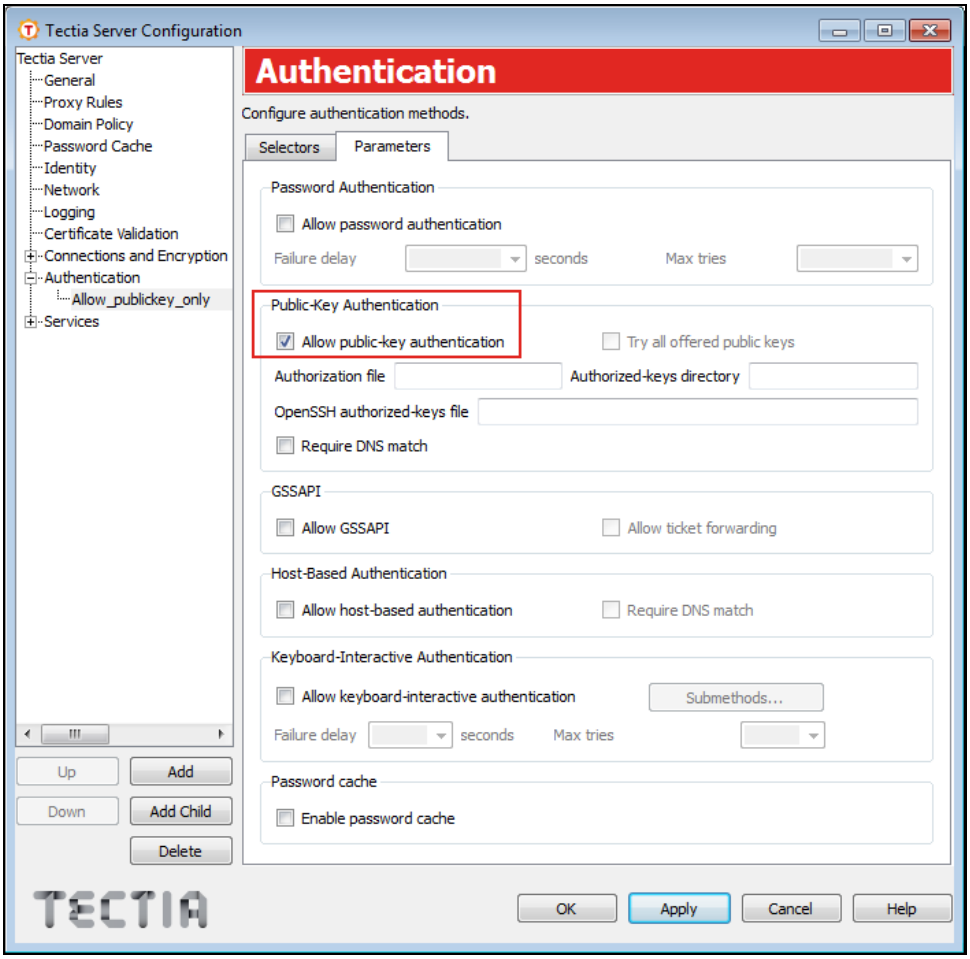
5. Go to **Authentication** and select **Default Authentication** to configure selectors and parameters for the group.

Note: This authentication group is available in the default configuration of Tectia Server.

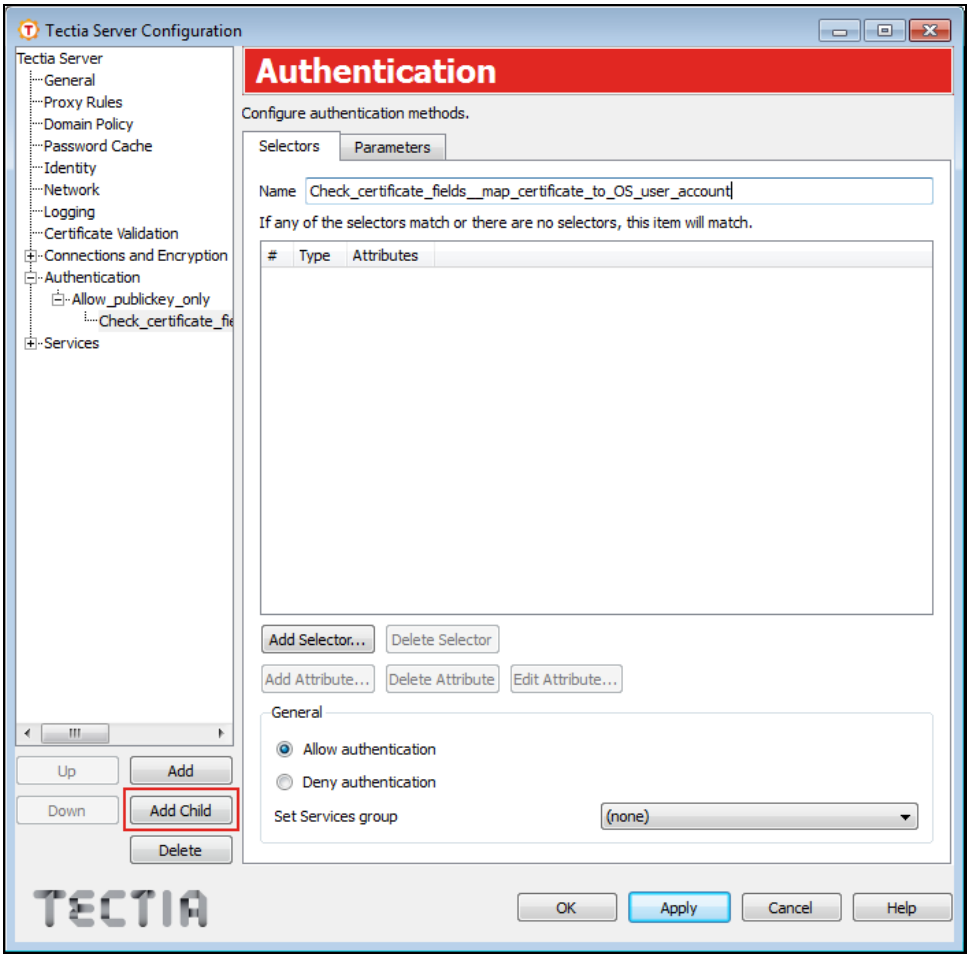


6. On the **Selectors** tab, enter a name for the authentication group.
7. Leave the selectors list empty, all incoming users are selected into this authentication group and to the authentication method chain. This is the first authentication group that you need to create for the authentication method chain. There will be two authentication groups in the chain.

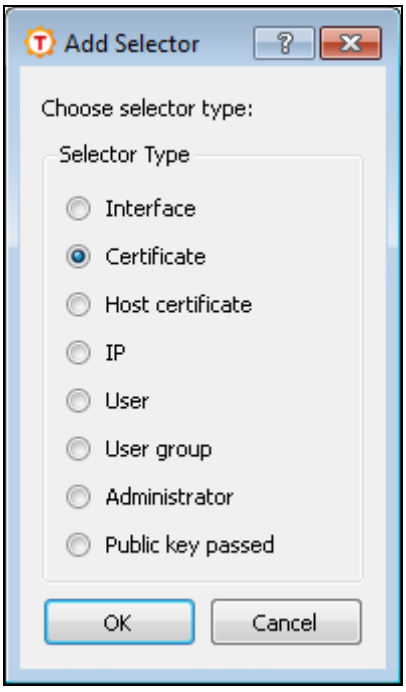
8. On the **Parameters** tab, make sure that the **Allow public-key authentication** option is selected.



9. Create a child authentication group which will be used to check certain fields from the end user's certificate. That is, you are configuring your selector for the certificates. Click the **Add Child** button and enter a name for the child authentication group.



10. On the **Selectors** tab of the child authentication group, click the **Add Selector** button. From the list, select **Certificate** and click **OK**.

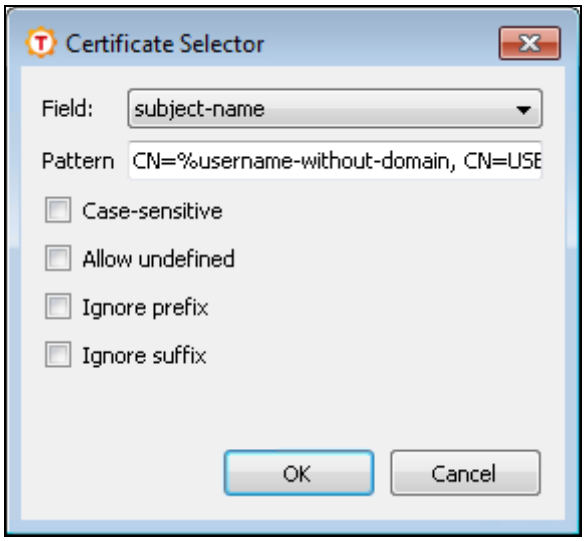


11. In the **Certificate Selector** dialog box, select which field on the certificate you wish to authenticate against.

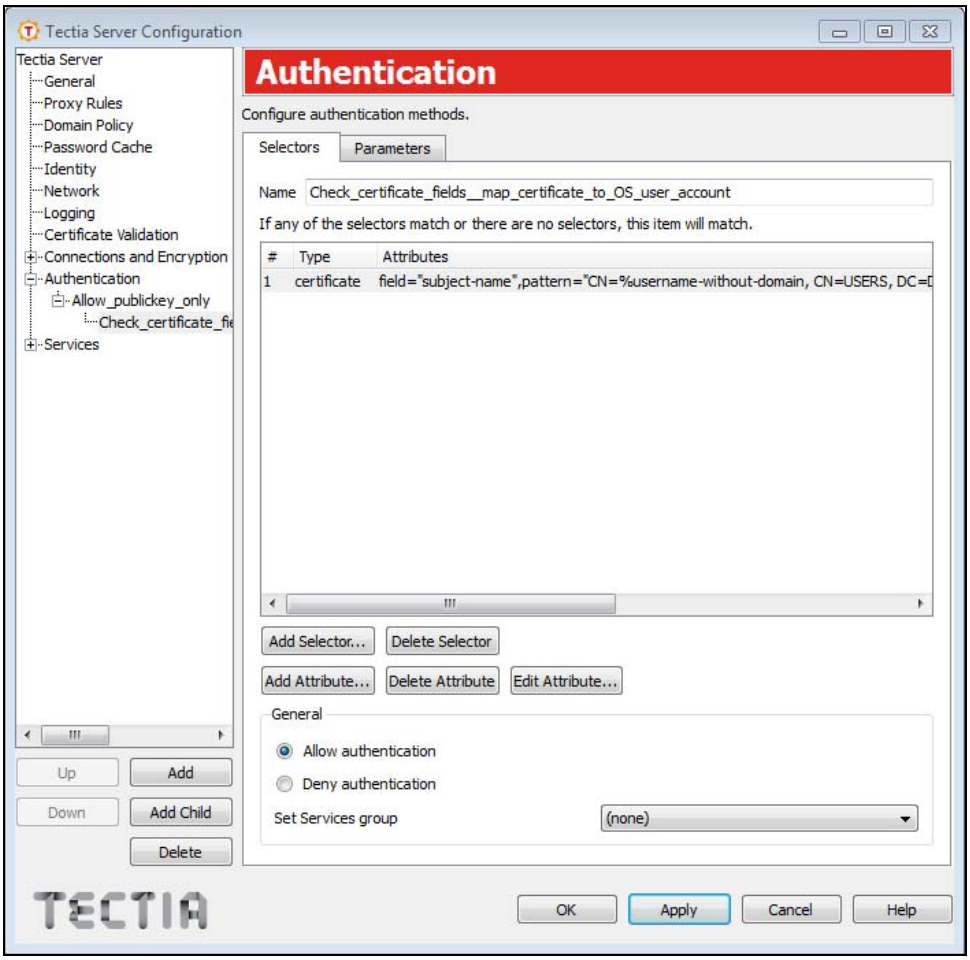
12. Enter the pattern in the field.

```
CN=%username-without-domain%, CN=USERS, DC=DEMO, DC=SSH, DC=COM
```

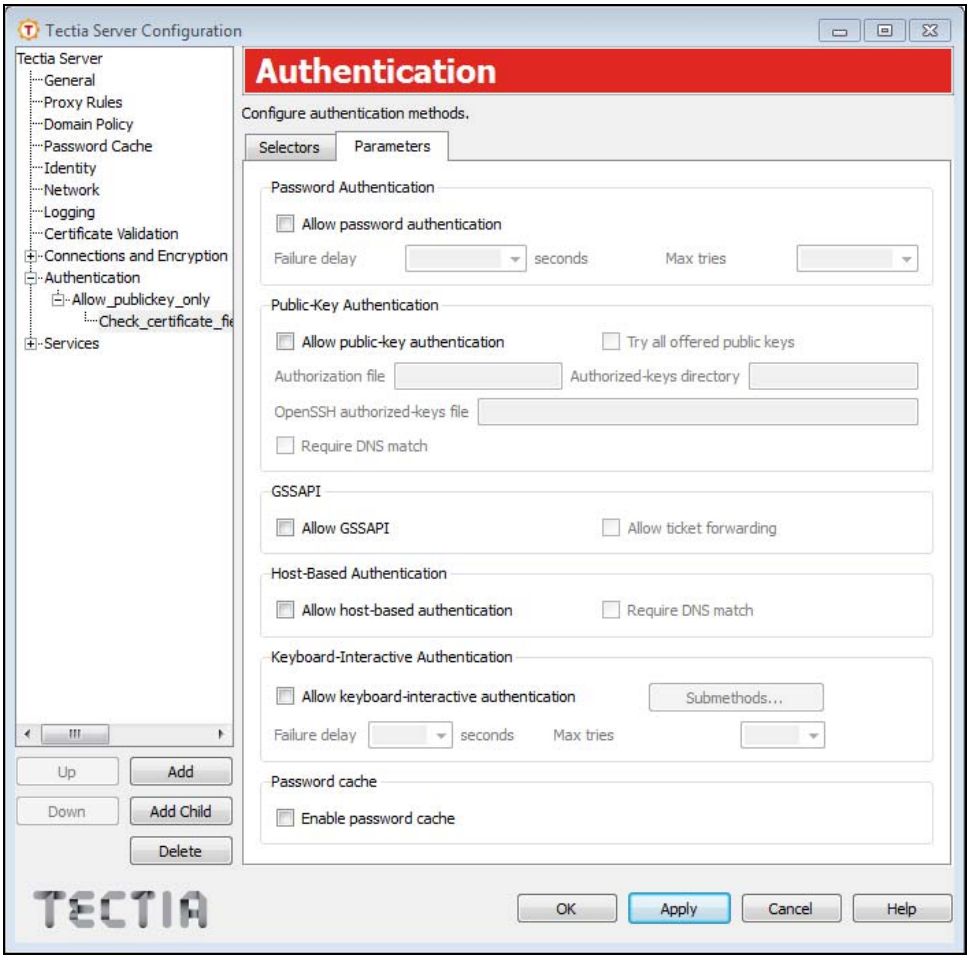
Note:It is extremely important to create a mapping between real OS user accounts and the end users' certificates so that a single end user can only access a single specific OS user account with their personal certificate and not all OS user accounts. For example, if you use subject-name, the pattern could be:



13. Once you have made your changes, click **OK**.



14. On the **Parameters** tab, unselect all authentication methods because the parent authentication group checks whether the public key authentication is successful.



15. Click **Apply** to save your changes.

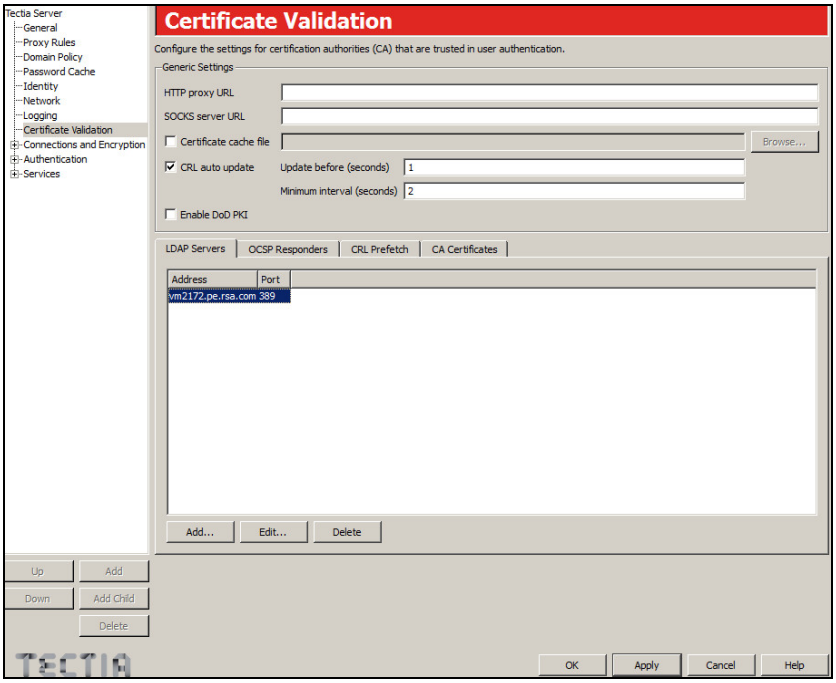
CRL Checking Mechanism

If Tectia SSH Server authenticates using certificates and the certificate does not contain the LDAP url as CRL DistributionPoints extension, the location of the LDAP server must be defined on the client side. If the Tectia SSH Server user wants to authenticate using certificates, the location of the LDAP server must be defined on the server side.

Ensure that you have the Tectia SSH Client software installed correctly on the system prior to moving to the configuration steps.

1. Open and select **Certificate Validation** and then **LDAP Servers**.

2. Click **Add** and enter LDAP server address.



Note: Certificates can only be valid if the issuer is trusted. The issuer can be trusted directly or through path verification. Add Trusted CA certificates into Tectia SSH by first exporting them from a web browser and then importing them into Tectia SSH Client and/or Server.

Tectia SSH client's installable elements

The RSA Authentication Client is required on each client to insure proper communication between the Tectia SSH Client and the RSA SID800 Hybrid Authenticator.

Tectia SSH client's configurable elements

Server-side Certificate Mapping

Certificate authentication is a part of the public-key authentication method. It is recommended that you use the Tectia SSH Product Guides for setting up the Tectia SSH Server and Client.

Tectia SSH client's CA configuration

Exporting the CA Certificate with Microsoft Internet Explorer:

1. Choose **Tools** -> **Internet Options**.
2. Click the **Content tab**.
3. Click **Certificates**
4. Choose the desired CA certificate(s) under Intermediate Certification Authorities or Trusted Root Certification Authorities.
5. Click the **Export button** and then **Next**.
6. Choose the export format to be either DER encoded binary X.509 (.CER) or Cryptographic Message Syntax Standard – PKCS #7 (.P7B) and click **Next**.
7. Specify the name of the file you want to export and then click **Next**, and **Finish**.
8. Alternatively the CA certificates can be downloaded from the RSA Certificate Manager Certificate Authority Enrollment Server.
9. Browse to the enrollment page, and choose **CA options**.
10. From the Save a CA Certificate or a CRL Signer Certificate to a File section select the **certificate authority** from the drop down menu.
11. Select the format of the certificate to be either **PKCS #7** or **DER-encoded** certificate.
12. Click **Save CA Cert…**

Importing CA certificates to Tectia SSH Client is described in detail below:

Tectia SSH Client/ConnectSecure for Windows

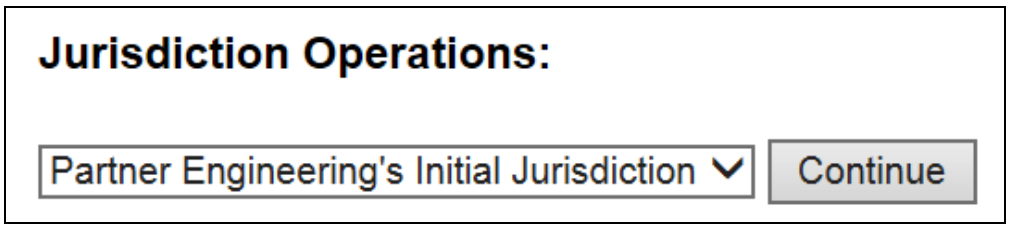
1. Open the Tectia Connections Configuration GUI.
2. Select CA Certificates under Server Authentication.
3. Click **Add** to import required CA certificate(s).

> **Note: If the certificate was exported in the Cryptographic Message Syntax Standard – PKCS #7 (.P7B) format, the certificates must be extracted from the package before adding them.**
>
> **This can be done with the ssh-keygen-g3 -7 option:**
>
> **> ssh-keygen-g3 -7 *certfile.p7b***

Tectia SSH User Certificate

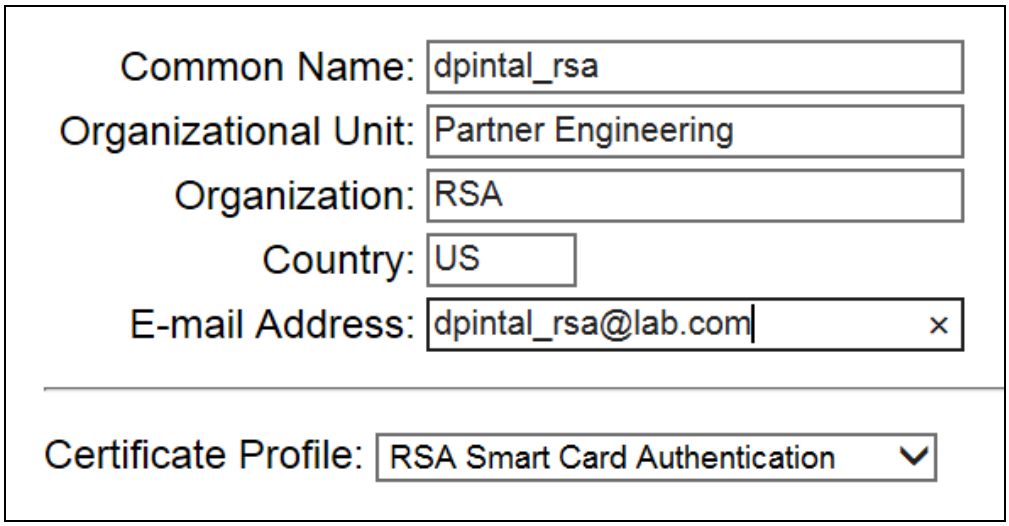
User Certificate Enrollment

1. Browse to an RSA Certificate Manager enrollment page select the jurisdiction and **Continue** button.



2. Select **Make an End-Entity certificate request**.

3. Complete the certificate request form, selecting a Certificate Profile for PKI use, click the S**ubmit** button.



Note: The RSA Certificate Manager Administrator must create a new Certificate Profile to be used for certificate authentication (RSA Smart Card Authentication). Refer to the RSA Certificate Manager document and the SSH product guide for more details on creating the Certificate Profile and the key requirements for the Tectia SSH User Authentication certificate.

4. Click **OK** to start the creation of the certificate.
5. Provide your password/PIN for the browser security database, and then click **OK**.
6. If the request is successful a confirmation page will be displayed. The RSA Certificate Manager will generate a private key and provides steps to download.

Export/Import the PKI User Certificate

The certificate import is done by first exporting the certificate from the browser and then importing onto the RSA SID 800 Hybrid Authenticator.

Use Microsoft Internet Explorer to export the user certificate:

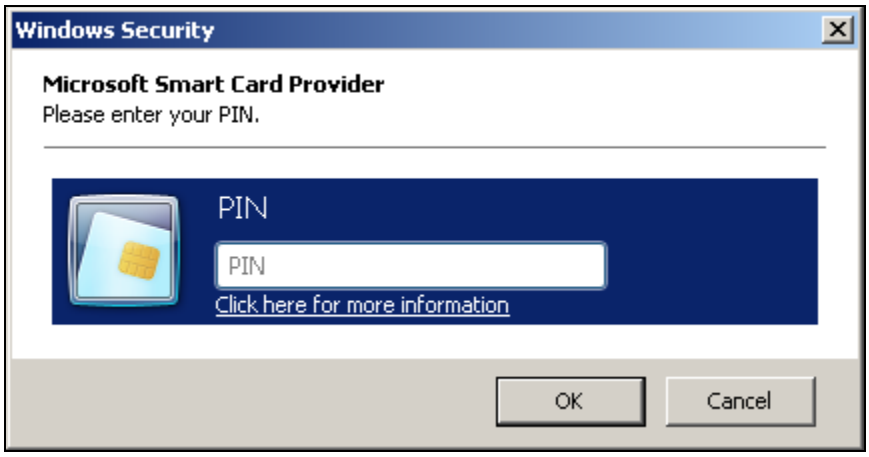
1. Choose **Tools** -> **Internet Options**.
2. Click the **Content tab**.
3. Click **Certificates**.
4. Choose the desired certificate under Personal.
5. Click **Export** and then **Next**.
6. Choose, **export the private key** and click **Next**.
7. The certificate can only be imported in PKCS #12 format. Select **first and/or third check boxes** also if desired and click **Next**.
8. Type and confirm the password and click **Next**.
9. Specify the file name, click **Next** and **Finish**.

Use the RSA Authentication Client to import the certificate onto the RSA SID 800 Hybrid Authenticator:

1. Open the RSA Authentication Client Control Center.
2. Select **Import**.
3. **Browse** to the location of the downloaded PKCS#12 certificate file.
4. Select the **.PFX** file containing the private key and certificate you just exported.
5. Give the password needed for PFX integrity check and click **Next**.
6. Select **Finish** to import the users smart card certificate.
7. Enter the **Smart card PIN** as requested to complete the import.

SSH Client Logon and Authentication

1. Initiating an Tectia SSH Client session will require the user to input the RSA SID 800 Hybrid Authenticator PIN which will unlock the device and allow the Tectia SSH application to use protected user certificate for authentication.



Certification Checklist for 3rd Party Applications

Date Tested: December 8, 2014

Product	Tested Version	Operating System
Tectia SSH Server	6.4.5	Windows 2008 R2
Tectia SSH Client	6.4.6	Windows 7 SP1
RSA Authentication Client	3.6	Windows 7 SP1
RSA SecurID 800	D4	NA

Test Case			Results
Certificate Enrollment			
P10 Certificate Request			N/A
P7 Response installed correctly			N/A
CMP Certificate Request			N/A
CMP Response installed correctly			N/A
SCEP Certificate Request			N/A
SCEP Response installed correctly			N/A
Import Certificate			
Import PKCS#12 envelope			N/A
Import via cut & paste			N/A
Install Root Certificate via cut/paste			✓
Install SubCA Certificate via cut/paste			N/A
Install Root Certificate via SCEP			N/A
Install SubCA Certificate via SCEP			N/A
Verify Certificate chain is installed			N/A
Certificate Usage	**Sign**	**Encrypt**	**SSL**
S/MIME	N/A	N/A	N/A
Document and Files	N/A	N/A	N/A
SSL Client Authentication	N/A	N/A	N/A
SD800 Client Authentication	N/A	✓	✓
LDAP Support			**Results**
Name lookup			✓
Certificate retrieval			N/A
Status Check of Certificate	**OCSP**	**CRL**	**Other**
Success with a valid certificate	✓	✓	N/A
Fails with a revoked certificate	✓	✓	N/A
Fails with a suspended certificate	✓	✓	N/A
Pass with a re-instated certificate	✓	✓	N/A
RSA Remote Authentication Client			**RAC**
Access certificates via MS CAPI (Internet Explorer)		✓	✓

DRP / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function